ENABLING TRUST IN THE DIGITAL WORLD

EXPLORING THE MARKET FOR AUTHENTICATION TECHNOLOGIES IN INTERNATIONAL DIGITAL TRANSACTIONS

IKED
INTERNATIONAL ORGANISATION
FOR KNOWLEDGE ECONOMY
AND ENTERPRISE DEVELOPMENT

GTC
GLOBAL TRUST CENTER

This publication is distributed by the International Organisation for Knowledge Economy and Enterprise Development (IKED) on behalf of the Global Trust Center (GTC). The work has been undertaken under the aegis of the international steering committee for GTC.

GTC is an international network that is in the process of establishing formal national entities, nodes and contact points in various countries around the world. The report explores the rationale and viability, as well as possible organisational modes, of GTC.

IKED is an independent, non-profit association and international organisation focusing on the emerging issues of the knowledge-based economy.

IKED – International Organisation for Knowledge Economy and Enterprise Development

PO Box 298
SE-210 22 Malmö
Sweden

Tel: +46 (0) 40 – 17 65 00
Fax: +46 (0) 40 – 17 65 01

info@iked.org
www.iked.org

ISBN-10 91-85281-08-5
ISBN-13 978-91-85281-08-4

Title: ENABLING TRUST IN THE DIGITAL WORLD
Exploring the Market for Authentication Technologies in International Digital Transactions
Authors: Thomas Andersson, Andreas Jacobsson, Andreas Mossberg, Jens Sörvik
Published: Malmö, September 2006
Publisher: IKED
Layout: Boyan Kostadinov

FOREWORD

Information and communications technology (ICT) offers organisations around the world unprecedented opportunities to process information and to perform commercial transactions in virtually any location. The market for international electronic transactions is expanding at great speed, but beneficial results are not a given. For the potential use of ICT to be fulfilled, a number of enabling conditions need to be in place. These include effective development and deployment of security-enhancing techniques, in ways that are able to meet the requirements of specific users, organisations and governments on a global basis. Without the assurance of security in digital transactions, the use of ICT will be thwarted and result in costly side-effects.

Fundamental complications arise, however, because of a combination of information problems, transaction costs, institutional failure and strategic interplay between the various actors involved in designing and deploying ICT. Together these factors hamper diffusion of comprehensive solutions to the issues that arise with respect to digital trust and security. So far, this playing field has been strongly fragmented.

Against this background, the present report examines what could be done to enhance trust in the digital world. The focus is particularly on mechanisms to support effective authentication. Reflecting on ways to improve outcomes, and what can be judged feasible given the evolving trends and the present state of institutions and markets around the world, the study in part takes the shape of a feasibility study in regard to options of developing the "*Global Trust Center*" (GTC).

Financial sponsorship of the publication from the Australian Department of Communication, Information Technology and the Arts, is gratefully recognised. Andreas Jacobsson, Andreas Mossberg and Jens Sörvik of IKED are thanked for their substantive work on the report. Professor Jean-Pierre Briffaut, Institut National des Télécommunications, Paris, and Anna Öhrwall Rönnbäck, Linköping University, produced important background reports. Experts from other parts of the world also provided valuable substantive input. Professor Hamid Jahankhani, University of East London, provided useful comments. Boyan Kostadinov, graphic design, and Karin Hélène, both of IKED, are thanked for their invaluable assistance. The work was undertaken under the aegis of an international steering committee, featuring representatives from industry and the public sector, mainly in Europe and Australia.

September 2006

Thomas Andersson
Chairman, International Steering Committee, GTC

ABSTRACT

With the advance of information and communication technologies (ICT), the costs of diffusing and using information are fast decreasing. Organisations around the world encounter unprecedented opportunities to engage in multiple types of transactions over the Internet, including via electronic commerce. The market for electronic transactions has tremendous potential to generate a range of benefits, through increased transparency, intensified innovation, the introduction of new products, stronger competition, more effective entry by newcomers, and so on. Such outcomes are not a given, however.

Major threats and hurdles emanate from the increasing misuse of ICT, ranging from spam to fraud, hate crime, extremism, child pornography, terrorism and other forms of cybercrime. There is a risk of serious consequences, not only for the digital world itself, but also for the international economy more broadly. The means to address the problem are available, but their application and implementation are impeded by a combination of information problems, transaction costs, institutional failure and strategic interplay. These impediments are giving rise to a highly fragmented playing field.

Following a process of consultations and debate at a series of international conferences, this report examines the issues at hand. We further advance, and evaluate, the rationale and validity of a proposed new tool to improve the playing field for ICT security, and notably for authentication, namely the "*Global Trust Center*" (GTC). In effect, the report takes the shape of a feasibility study in this regard. Particular focus is placed on the need to strengthen conditions for the provision of authentication services.

This report is based on material gathered through literary reviews and interviews with leading actors involved in digital authentication processes. It reviews the situation across a number of players and sectors, drawing notably on experience from Australia, the European Union (and individual member states Austria, Belgium, Denmark, Estonia, Finland and Sweden), Hong Kong and the United States. The analytical framework examines four principal aspects: organisational, legal, economic and technological. Based on these complementary factors, the study incorporates the findings of empirical surveys. The government, finance, e-health and university sectors were investigated in some detail.

The overall findings suggest that improved coordination and diffusion of viable authentication services are urgently needed. Serious differences prevail between countries in the governance of transaction services. A severe lack of interoperability between existing systems is, in fact, hampering the potential use of e-services. At the same time, the alliances formed so far to address the outstanding challenges have had limited success.

It is not possible to undertake any precise monetary estimation of the net benefits that could be generated through the GTC. However, the report concludes that a frontline international research and policy body is needed that can work with multiple stakeholders as well as analyse, assess and communicate the importance of various instruments to address digital security and trust. Through the combination of analytical and policy work on a global basis, the GTC would be anticipated to help bridge interests in various geographical regions

as well as in sectors. While there is no sign at present that similar bodies or mechanisms would be initiated as a consequence of prevailing market forces or of mainstream international policy cooperation, the GTC, if established and organised appropriately, could generate substantial benefits.

This report recommends that a serious effort is made by relevant stakeholders to establish and engage in the GTC, organised as a combination of an international network and organisation, drawing on a form of public-private partnership. The GTC would cover legal, economic and organisational aspects of e-security in general and e-integrity and authentication in particular, on a global level. A viable setup should include a structure for incorporating practically useful pilots, aiming to advance specific opportunities in the technological or economic spheres, and be tailored to meet the needs of specific geographical regions and/or market sectors. Recommended potential key roles and implications of the GTC include a brokerage function as well as features of a global clearing house.

TABLE OF CONTENTS

FIGURES

BOXES

TABLES

EXECUTIVE SUMMARY

Establishing trust between parties that enter a continuous relationship, whether backed by formal or informal contractual conditions, represents one of the oldest prerequisites for successful human activities. Over the years, a fabric of social norms, business practices and legal frameworks has evolved to help support the establishment of trust. In the digital world, however, the playing field is different. Parties "meet" and experience vast opportunities for mutual exchange and benefit while, possibly, having less clear-cut means of establishing each others' relevant features.

This report examines what can be done to enhance trust in the digital world. Electronic transactions are currently taking place in an environment constituted within a technical superstructure where time and space are in a state of flux, and where anonymity and antagonistic activities may go together. Reflecting on which paths can be taken to improve outcomes, and that appear possible, given the nature of the issues, the evolving trends, and the present state of institutions and markets around the world, the document takes the shape of a feasibility study in regard to the option of establishing the Global Trust Center (GTC).[1]

The report aims to assess ways to improve security and enable trust in the information society. The most basic issue is the need to strengthen the market for the provision of authentication services. Based on the findings of empirical surveys, methods are structured for how to put in place more effective cross-recognition and cross-certification of services, spanning the gaps between national jurisdictions as well as institutional and sector frameworks. A fundamental observation concerns the presence of a public good component, which is presently unheeded but which needs to be addressed in any strategy hoping to succeed in enhancing trust and security in digital transactions.

The report provides a map and sets out to analyse a range of national and international activities of relevance to the implementation of authentication services – including their legal and regulatory frameworks, security perceptions of dependent parties and individual countries. It describes various implementation strategies employed at national level. Different aspects influencing transactions are gathered under the heading of a Global Authentication Framework. This framework may be viewed as a model to advance various processes, issues, institutions and actors that affect the outcome of authentication services in international digital transactions. Market and government failures, technological choice, interoperability aspects,[2] legal systems and governments that provide identification services all play a role.

The report is based on material gathered through literary reviews and from a range of Internet sources, as well as interviews with leading actors involved in authentication processes in digital transactions. It examines a limited number of actors and sectors,

[1] See further Appendix A.

[2] Interoperability refers to the ability of systems to provide services to, and accept services from, other systems, and to use the services exchanged so as to enable them to operate effectively together.

drawing notably on experience from Australia, the European Union, (and the individual member states Austria, Belgium, Denmark, Estonia, Finland and Sweden), Hong Kong and the United States.

In short, the study presents:

i) Analysis of varying authentication services, resulting in:

- A description of selected services in individual countries
- An analysis of fragmentation of these services
- Recommendations on possible ways to overcome such fragmentation

ii) Analysis of similarities and dissimilarities between legal frameworks in a range of countries, resulting in recommendations on steps to advance common terminology.

iii) Reflections on the feasibility and viability of present and evolving practices for achieving orderly conditions for authentication services, followed by recommendations on how to facilitate the use of ICT (information and communication technologies) and electronic commerce globally, by:

- Defining the regulatory strategies employed by countries in the implementation of authentication services.
- Analysing perceptions of electronic transactions by relying parties and countries.
- Detailing country requirements regarding interoperability with respect to online transactions and digital certificates.
- Describing markets and sector requirements for interoperability.
- Exploring how a clearing house structure can be established for the purpose of facilitating dialogue and the application of coordinated solutions on a continuous basis, including analysis and conclusions on how the GTC could support this kind of function.

The scope of the study is based on four principal perspectives:

i) Organisational aspects – business models, systems, risk management, etc.

ii) Legal aspects – legal frameworks and regulatory bodies.

iii) Economic aspects – incentives that form relevant driving forces and impediments.

iv) Technological aspects – technologies, their features and ramifications, including opportunities and challenges.

The study further takes stock of empirical surveys, including private and public sector authentication services. Four sectors were investigated in particular:

i) the government sector;
ii) the financial sector;
iii) the e-health sector; and
iv) the university sector.

Meanwhile, with regard to authentication, attention was paid to:

i) Theoretical as well as empirical aspects of authentication processes, including experience from actual transactions between government, business and individual users.
ii) Authentication concepts, methods and techniques (including legally valid signatures, but also taking on board solutions that do not use "signatures" in a narrow sense, such as PIN-based solutions).

General observations

Despite the divergent nature of the information received, a number of common themes have emerged from the responses and from the analysis. The issues associated with authentication have proven greatly relevant and important. The resulting information has also generated insights on how the GTC may establish priorities for the various steps ahead.

Based on the theoretical review of concepts and models related to authentication of digital transactions, we conclude that authentication processes are partly context-specific. The products offered critically influence what level of an authentication mechanism is most appropriate, as well as how it can be implemented. At the same time, while the problems and the issues are local and highly specific, the needs and the required answers are, in fact, genuinely global.

We further conclude that the implementation of authentication methods needs to be based on risk analysis. This means that prior to implementation of a security-enhancing technology in support of authentication, the need for the implementation should be reviewed, charted and based on a context-specific underlying security need which in turn determines what technology/level of security should be applied. For this purpose, public organisations and standards organisations in some countries have provided national guidelines on how to undertake or pursue a risk evaluation process or exercise and which techniques to choose in order to meet the required level of authentication security.

Most respondents agreed on the need for international coordination, although individual countries must devise their frameworks so as to be consistent with national conditions. There is a need for an agreement on terminology at national as well as international level for technologies and protocols. Also, proper risk evaluation methods need to be developed on an international level. Some responsibilities must be carried by established standardisation bodies. However, there is a need for means that can enable more effective coordination than is presently the case. These should have a tangible influence on such work and the

extent to which it is able to achieve an appropriate coordination of different national standards.

The overall judgement among respondents was that national and international markets are fragmented and that a lack of interoperability gives rise to challenges that are not easily resolved. Problems with enabling system-to-system communication also decrease user trust in digital transactions. Meanwhile, there is no simple way to achieve optimal coordination, neither for market forces nor for government institutions. Innovative ways forward are needed to bridge the gap between the many actors involved and help coordinate common platforms. The establishment of an appropriate GTC may serve as one option to help overcome the interoperability obstacles, as the report will explain later on. A majority of respondents reacted positively to the idea of a GTC that promotes standards and protocols for interoperability and that gathers and organises the available market actors. The opinion was that such an organisation could potentially enhance authentication in international transactions and thereby help enable secure digital transactions. In conclusion, there seems to be strong support for an effective GTC, although visions and opinions diverge on what actions it would undertake.

Reflections

The information collected by the project points to several outstanding issues that require further work and which could be usefully considered by the GTC. At the same time, the analysis identifies an unequivocal need for establishing mechanisms that can allow for more effective coordination in the development and deployment of authentication services across countries, sectors and markets. The GTC may meet such needs by being designed as a clearing house for developing, examining and diffusing proprietary authentication systems and enabling organisations and people to access appropriate instruments for authorisation (tokens, smart cards, and digital certificates) more effectively. In particular, the GTC might facilitate more interoperable digital transactions between users (persons, organisations, government institutions, etc.) in diverse proprietary systems, at less cost. It is possible that the GTC could serve as a catalyst and clearing house for the development of new solutions.

While a number of relevant standards which may be well placed to support the security and authenticity of electronic transactions already are present in the marketplace, no overarching interoperability protocol exists at present. The GTC could promote the development of a high-level protocol for interoperability to help support a healthy development of the market. If the GTC is to be seriously engaged in developing such a protocol, it has important implications for the structure and nature of the organisation. The associated requirements should then preferably be explored in the early phases, or in separate pilot projects, suggesting several structural entities. These would include a policy and research organisation as well as a set of market-based operations that would be more directly engaged in work on technical initiatives, notably related to interoperability.

The decision-making process for advancing security-enhancing mechanisms, systems and software, is inherently complex. Security managers would benefit from generic methods to

explore the actual demands of a certain system or technique, for the purpose of minimising cost and maximising utility throughout their organisations. In this context, risk analysis represents an opportunity, as it can serve as a key means to define an appropriate level of security (and authentication) structure that suits a specific enterprise or government organisation. However, risk analysis in itself is not sufficient for determining which security-enhancing system should be chosen; it merely represents a tool for establishing the state of security. On this theme, one possibility is for the GTC to provide recommendations or guidelines on how to select an appropriate risk analysis tool, what criteria should be applied, and how it may be utilised. Since this process often is the most time-consuming aspect of a risk analysis, corporations have an incentive to save time and money. Another time-consuming and equally important task in conducting (quantitative) risk analyses is finding usable statistics on which to base probabilistic prognoses. Altogether, this might be an opportunity for the GTC to explore.

From a demand-driven, bottom-up perspective, the GTC could engage and involve actors that provide authentication mechanisms which promote interoperability among systems and operators. The GTC could develop methods (for example, guidelines, best practices, protocols and templates for developing agreements) to facilitate interoperability, including through the acceptance of "foreign" solutions. The organisation could thus help to coordinate and facilitate inter-sectoral and inter-governmental contacts and contracts.

Other areas where linkages could potentially be explored include assessing the extent to which authentication can play a dominant role in combating identity theft, the extent to which the use of certain authentication methods can alter the financial incentives for individuals to steal authentication credentials (e.g. through phishing schemes), and the promotion of authentication as an essential element of the Internet's security culture.[3]

It has been suggested in the literature, and in the survey, that the GTC should take advantage of existing national systems and standards, as opposed to developing entirely new (technical and/or organisational) solutions. Obviously, the coordinating function needs to be interoperable with existing systems. At the same time the GTC must be responsive to new needs and therefore not dominated by vested interests in ways that make it prone to promote existing, and possibly obsolete, solutions, at the expense of new opportunities.

Various observations indicate that today's market for secure digital transactions is fuelled by other forces than demand considerations. Respondents emphasised that the market so far has been characterised by a supply-driven agenda. This situation is likely to be marked by misdirected investment and R&D. Problems to identify future standard technology and, hence, reduce possibilities for SMEs to compete, risk leading to technological lock-in and overheating of services and may also fuel offerings that destroy or partly distort fundamental market mechanisms in regard to competition and pricing behaviour.

[3] Phishing is a process through which a perpetrator by deceptive means tries to acquire sensitive personal information, such as passwords, user names, credit card numbers, etc. The malevolent actor tries to acquire this information by masquerading as someone trustworthy with a real need for such information and send the requests in an official-looking message.

A potentially important role for the GTC is therefore to help articulate the demand for authentication mechanisms, and help co-ordinate needs among multiple actors for the promotion of multi-layered security solutions and risk-driven security-enhancing systems.

Enabling trust is a complex task, the success of which will require time, patience and coordination. All in all, the points made underpin the potential merits of a global brokerage organisation that can convey contacts and counselling among the available market actors so as to enhance secure authentication in international transactions. This provides a rationale for the GTC, given that it will be appropriately organised and in a position to improve the status quo.

A feasible path forward

The overarching objective of the feasibility study was to examine roads ahead that could enhance secure digital transactions by improving the global authentication mechanisms. The study proposes that the GTC is organised and developed to address the outstanding challenges facing existing authentication solutions. The analysis departed from four categories of challenges and opportunities (see below).[4] For each of these, the GTC could, in principle, take action in a number of ways so as to potentially aid sound institutional and market responses. Thus, the GTC could:

i) With regard to legal aspects

- Undertake analysis and provide recommendations on existing gaps, malfunctioning elements, or coordination and development needs, to regulators, service and technology providers and to potential new endeavours.

ii) With regard to technological aspects

- Either through partners, joint ventures or by itself develop and improve standards, protocols and technical solutions that help improve the functioning of the market. One such solution could be to develop a risk-driven protocol for interoperation between authentication systems.
- Analyse and advise on technological solutions. The GTC could function as a centre of excellence providing trustworthy and independent information on techniques, best practices, standards and solutions.

iii) With regard to economic aspects

[4] Naturally the issues could be divided differently. In digital jargon, one may speak of issues pertaining to information security (identity and access management systems, strategic approaches to security and security policies and procedures) and digital forensics investigation issues (crime scene/search and seizure processes, criminal data mining, criminal network analysis, cybercrime detection and analysis). Such aspects take priority among overall challenges faced by the e-community today.

- Help facilitate the coordination of supply and demand to address market inconsistencies that currently hinder the development of new and improved services and effective uptake by users of digital solutions. By acting as a broker between existing solutions, it would provide bridging between systems and serve as a catalyst for the development of new services and solutions. The GTC could also facilitate the emergence of a web of trust or a federated identity management structure.
- Analyse direct and indirect effects on national and international markets, and assess incentives and the rationales for action by key stakeholders.

iv) With regard to organisational aspects

- Strengthen market signals by providing and coordinating risk management tools.
- Assist private and public entities in behavioural policies for organisations and recommendations for legislation.
- Organise actors and solutions to facilitate coordination of existing and new efforts towards enhanced interoperability.
- Assemble, package and disseminate information and recommendations on available and successful business models, technologies and standards.

Conclusions

The tentative conclusions of the feasibility study underline the seriousness of the security issue in the digital world. Internet users reportedly abstain from taking up technology or undertaking actions online due to fear of negative consequences. Were this situation to continue or worsen it could be expected to spill over into the wider economy. A clear gap exists between the need for mechanisms and institutions in support of digital trust, and what current and future driving forces (from the policy and market side alike) exist to generate such solutions.

The demand for mechanisms supporting trust in digital transactions is dissipated, meets with fragmented market conditions, and is unable to articulate coherent incentives for putting effective solutions in place. The authentication solutions available today are primarily supply-driven. There appears to be an over-supply of (predominantly technical) solutions. As these are further advanced and put to practical use along diverse time trajectories they will have to comply with and address specific structures, incentives and risks. This may result in technological lock-in, with heavy investments made in obsolete technologies.

Among the responses that now abound, a few international initiatives can be noted. These include networks such as the Liberty Alliance, intergovernmental organisations such as the ITU, IDABC and APEC Tel Group, and partnerships between market leaders such as Verisign, Microsoft, RSA and IBM. Yet all these encounter problems, apparently relating to limitations in respect of resources, capacity to adjust to changing conditions, ability to meet

with user and market demand, political factors, competition, co-ordination problems, and so on. Due to the lingering presence of information and co-ordination problems, the gap between needs and responses may not be closed spontaneously – either by public institutions or by market forces.

A GTC focused on enhancing security for international electronic transactions and introducing means to develop interoperability could make a major beneficial contribution to link the defence of public goods with improved conditions for new professional services that respond to real demand. It is concluded that the notion of putting in place a global trust centre appears to be based on a sound rationale. A range of alternative models for such a body are conceivable. Different forms display their specific pros and cons. Four alternative organisational structures for the GTC are outlined in the study:

i) International organisation
ii) Public-private partnership (PPP)
iii) Corporation
iv) Loose network

Recommendations

As a point of departure, a feasible action plan for the near future includes the following steps:

1. Decide on strategy	*2. Establish network*	*3. Test phase*	*4. Full launch*
Steering committee meeting	Hold conference	Initiate pilots	Provide full-scale web of trust service or back-up for federated identity management
Decide organisational form	Create association	Provide knowledge	
Secure financing	Start development of protocol	Develop marketing strategy and tools	
	Develop risk-management tools	Engage key stakeholders	

The key criteria on which to base recommendations are viewed as *relevance of the purpose of the organisation*, *feasibility* and *funding*. The relevance of the organisation is reflected in the value added it can generate through its activities, including to what extent it can deliver on providing the public good of interoperability and succeed in helping to improve the match between outstanding needs and actually available or potential solutions. The relevance will furthermore depend on the potential ability of the organisation to generate buy-in from key stakeholders and henceforth become a trustworthy actor.

As for the organisational format, this report concludes that there are four alternatives. First, an international organisation, which the report sees as the best structure for dealing with the legal, economic and organisational aspects on a global level. Crucial to the process is that the GTC achieves appropriate support and sufficient decision-making powers. Naturally,

there will be challenges, given the state of the e-political arena, the market, and the speed of the ongoing technological development. However, it is of utmost importance to retain focus on the global tasks the GTC is envisioned to undertake.

Second, an effective public-private partnership for the technological aspects involved would promote a quicker start-up. This kind of structure ought to be better placed to incorporate key market actors and other relevant stakeholders. This alternative may therefore actually be better positioned to deliver the public good of interoperability and be better able to remain constantly up-to-date on the latest innovative technical solutions. Evidently, such a strategy would require launch funding from both the private and public sectors.

The third option – a corporate organisational form – might be somewhat faster and "easier" to establish. It would, however, risk being considered as lacking in credibility in exercising influence, not fully transparent and trustworthy in its objectives, devoid of value, and not able properly to support the public good component. On the other hand, there might be some possibility of basing it on incentives to deepen commitments as opportunities develop. The viability of this option must be thought through carefully due to the likely intrinsic difficulties of creating the trust factor that is a prerequisite for the success of the GTC's core function.

If options one and two are preferred, but current interests lack the initial clout to muster the resources necessary to carry them out, a fourth option would be to launch the GTC initially as a network, which could subsequently be expanded into an association of key stakeholders based on the build-up of several country nodes coordinated under a central function. The respective national actors could bring together their respective interests and experiences while carving out a suitable path towards overall coordination in line with the jointly preferred strategy of the GTC. A full rollout would follow once a critical mass of support, commitment and funding had been achieved. The board and the associate body would require a sufficiently broad geographical and sectoral representation, while avoiding overly diverse interests within the network. The intended members should be invited to working group seminars and conferences so as to advance a common approach to the GTC concept and ensure collaboration in making it concrete.

The development of a protocol for risk management tools and the experience of initiated pilot projects represent important building blocks for further progress. Pilots should be used not primarily to derive final solutions or to strengthen the GTC's financial base, but rather to accumulate practical experience and to demonstrate the organisation's mission. Nevertheless, launching such efforts requires definite and sufficient resources, including contributions from institutions to support and host certain functions. An appropriate division of labour between the participating parties would have to be worked out. The members would provide the various kinds of experience required for the GTC and would help to generate the perceived trust which will be a key to the organisation's success.

In promoting an increase in the use of authentication mechanisms, the GTC will need to remain mindful of the fact that users' needs for ways to manage their digital identities will increase globally. If the GTC is established and organised to address this need, its work

would presumably include an assessment of the degree to which federated identity solutions can meet marketplace demands in this regard, as well as assessments of potential policy issues that these solutions would require. Furthermore, exchanges, seminars and conferences on authentication and digital transaction theme may be needed to boost not only interest in Internet security matters and an enhanced awareness of Internet-related risks and threats, but also to help advance the community of interested parties towards sufficiently common perceptions and perspectives, in other words establishing more shared concepts. Although numerous such meeting places already exist, there is a need to widen the circle of those engaged and to bridge the interaction between public sector, industry and academia on this matter. There is also the need to involve consumer groups as the demand side is often left out in this context. Some observed arguments in support for this vision of cross-sectoral exchanges on authentication is provided below:

i) Trust-enabling methods such as authentication are an agreed topic of importance to the Internet's security culture.
ii) There are a limited number of conferences devoted to cross-sectoral interested parties[5].
iii) Boosting trust by technology as a process (and not a product), which meets the need for a meeting place such as the suggested conference.
iv) Cross-sectoral representation at the conference creates the opportunity to enhance a market driven by demand.

This report recommends that a frontline international research and policy body – a proper Global Trust Center – is founded and organised effectively. The GTC should preferably be structured as a combined international organisation and public-private partnership, covering legal, economic and organisational aspects of e-security and authentication and e-integrity on a global level. It should include a structure for incorporating practically useful pilot projects that aim to solve targeted technological aspects and are tailored to meet the needs of specific market sectors and/or regions. A development in this direction has already been initiated by the Australian group within the steering committee. It has taken the lead in the development of a financial pilot. At present, demands for new digital trust solutions are predominant in the governmental and financial sectors. Coordination in these arenas may help greatly in enabling joint authentication protocols to be strengthened. Experiences learned from this pilot may serve as inspiration for the development of a future protocol and may show the way towards future pilots. The provision of good examples and a track record in promoting efforts which can help create trust will be greatly important in underpinning the formation of an effective GTC.

Important initiatives will have to be taken to examine and advance solutions that can enhance interoperability and support the implementation of cross-cutting solutions. Various initiatives may be needed to advance and explore approaches and methods that can support effective third-party engagement in authentication schemes. Work on the development of

[5] One example may be the World eID conference, see http://www.strategiestm.com/conferences/we-id/05/

an expanded protocol would have to be matched with additional work on risk management tools to start concurrent planning of marketing strategies and engage private and public actors in tandem.

1. INTRODUCTION

This report focuses on what can be done to enhance trust in the digital world. Electronic transactions currently take place within a technical superstructure where time and space are in a state of flux and where anonymity and antagonistic activities may be connected. The report reflects on the strategies that can be adopted to improve outcomes and that are feasible in terms of the issues themselves, the evolving trends and the current state of institutions and markets around the world. The document takes the form of a feasibility study vis-à-vis the Global Trust Center (GTC).

A series of international conferences has proposed and debated the GTC as an instrument to address issues related to security and trust in the digital world. The concept was first introduced at the ASEM conference Globalisation and ICT – "The Role of Government, Private Sector and Civil Society in an Information Society for All", held in Malmö and Helsingborg in March 2003. It was presented and debated at the Third Virtual Opportunity Congress in Sydney in December that year. Next it was proposed by the international business community and endorsed by ministers in the official declaration of the Second OECD Conference for Ministers responsible for SMEs, "Promoting Entrepreneurship and Innovative SMEs in a Global Economy", held in Istanbul in June 2004. The concept has since been addressed primarily in the meetings of the International Steering Group advancing the project, in preparation of the launch of the current feasibility study.

While receiving noteworthy attention, implementing the GTC clearly faces challenges. Primary among these in the near future are the GTC's organisational structure, funding, successful pilots and partnerships, as well as its positioning in respect of initial prioritised activity areas.

BACKGROUND

The advance of information and communications technologies (ICT) has led to rapid reductions in the costs of diffusing, accessing and using information. Not only are information flows expanding at amazing speed, with digital packaging being en route towards integrating multiple functions in new combinations and transactions, but the scope and quality of digital services is becoming a vital building block for success across a widening spectrum of business activities. Use of e-business, e-government and e-learning services is growing every day, and will continue to expand in the future. The level of expectations is indicated by the magnitude of business-to-business (B2B) commerce related to ICT-infrastructure, estimated at some US$2 trillion annually (Mehlman, 2003) and claimed by Gartner Research Group to have hit US$8.5 trillion in 2005.[6]

Clients, partners and competitors are increasingly demanding that business operations adapt to different ICT solutions so that business information can be made available. Although small and medium-sized enterprises (SMEs) have been behind in this development, they are

[6] www.gartner.com

rapidly catching up in important respects. At least in the most advanced information societies, SMEs are as wired as large corporations.

Most organisations recognise the critical role that ICT plays in supporting their business objectives and in fuelling profitability and growth. Due to the increasing amount of valuable information that is being made openly available, the risks of unsolicited, unintended or malicious use have grown. Moreover, the increasingly connected ICT infrastructures exist in an environment which is increasingly hostile: attacks are being mounted with growing frequency and are demanding ever shorter reaction times. As the value of a network increases exponentially as user numbers increase, so society's vulnerability increases too. For example, a computer virus in 1996 would have caused a relatively minor disruption, whereas a virus in 2006 might have cost billions. This indicates rising temptations for malefactors to put their new capabilities to destructive use, and the consequences of such actions reach far and well beyond the digital domain. In their biannual report on information security breaches in the UK, PriceWaterhouseCoopers and the UK DTI (2006) present survey statistics indicating that the average cost of a serious security incident was estimated at £8,000 to 17,000, and for large businesses ranging from £65,000 to 130,000. Some 52 per cent of the companies surveyed had experienced at least one malicious security incident during the previous year. For the overall population of firms, the report estimated costs to have increased by some 50 per cent since 2004. For large firms, costs were estimated to have increased by 20 per cent, suggesting that costs now tend to fall more heavily on smaller firms.

The range of threats towards ICT infrastructures is broad and practically all organisations, small and large, need to consider internal threats (from insiders) as well as external ones (hackers, attackers, competitors, and so forth). Information security is an increasingly important aspect of computerised systems and networks. In this respect, security is about preventing adverse consequences from the intentional and unwarranted actions of others. Although information security is by no means strictly a technical problem, its technical aspects (firewalls, authentication mechanisms, encryption techniques, and so on) are important. Information security is an increasingly high-profile problem since hackers, malicious actors and rivals take advantage of the fact that organisations are opening up parts of their systems to employees, customers and other businesses via the Internet. Much privacy-invasive and malicious software is already available for downloading, execution and distribution. Malware – malicious code planted on computers – gives attackers a truly alarming degree of control over systems, networks and data. Malware can be distributed and planted without the knowledge or control of users, system administrators, companies and organisations. The implication is that malicious actors can take control of vast parts of the Internet community.

Misuse of the new technologies presents fundamental issues for privacy, security and trust.[7] These aspects, and how they are anticipated to develop in the future, are crucially important for the scope and usefulness of digital transactions. In a setting in which organisations are

[7] For further reading on privacy and security see section 2.1 and 2.2, and on trust see section 2.6.

increasingly adjusting to meet the opportunities and requirements of ICT, it is difficult to keep overall ICT-related risks under control. Organisations are often unable to react to new security threats before their business is impacted, let alone recover from incidents and attacks. Managing security of ICT infrastructures, and the business value that those infrastructures deliver, has become a primary concern for most ICT managers.

New legislation that stems from privacy concerns, financial obligations and corporate governance is forcing organisations to manage their ICT infrastructures more closely and effectively than ever before. Many government agencies and organisations that do business with them are required by law to maintain a minimum level of security oversight. Failure to manage security proactively may put managers as well as entire organisations at risk, with downsides materialising not least in the form of legal repercussions due to breaches in legal responsibilities.

While much has been done, and sizable investments have been made to counter or pre-empt various security-related risks, there is an apparent lack of concerted action to establish an orderly framework for addressing these issues. At the heart of the matter lies a fundamental difference in perceptions among countries of what is needed. Some see governments primarily as a source of costly and inefficient interference that hampers the dynamics of market forces. Others see governments as carrying a profound responsibility for ensuring coordinated regulatory conditions required for an orderly playing field. Under the present conditions, countries, sectors and other constellations of actors that are moving forward in the digital domain are in the process of developing parallel means to handle the security and trust issues that confront them. In effect, we appear to be witnessing the configuration of a fragmented playing field, with the emergence of risks that are yet hard to gauge. Renewed efforts are warranted to strengthen the basis for exchange of information and digital transactions in ways that are secure while meeting basic user and cost requirements.

In principle, technologies for secure solutions exist today, but efficient standards and models that address the economic, legal and organisational aspects are not available to the same extent. This knowledge gap puts many companies, particularly SMEs, at risk: securing business administration and operations takes more than implementing technological solutions. Most companies need easily accessible solutions that do not require in-depth knowledge, heavy investments, thorough judicial understanding and security built into existing systems (which is excessively problematic). In addition, sound security investments must be based upon risk analysis, which represents the managerial link between control or no control of information assets and systems. In a risk analysis process, threats, vulnerabilities and possible negative consequences can be outlined, making it possible to determine if the organisation suffers from excessive or uncontrolled risk, or if it has the proper security solutions in place. Conducting risk analysis is not a simple task, however. In a complex and diverse environment, such as the Internet, the uncertainties that affect the perception of risk are numerous and exceedingly challenging to grasp. Nevertheless, risk analysis is the key to selecting and implementing security in transactions, systems and networks so that trust can be enabled.

Issues still arise with respect to what is being applied and how different applications relate to each other in shaping future options. Since "September 11", security is indeed widely viewed as a major issue, which receives massive global attention. That agenda, fuelled by deep concerns for security, has spilled into the digital world. Some issues are characterised by mechanisms similar to those being used in the "real world". In other respects, the digital and the real world are quite different and some of the ordinary solutions, for instance for the important example of building trust, may not yet have been transferred to the digital world. Trust has been described and defined in many ways; a suitable description in this context could be an individual's willingness to be vulnerable to another with the explanation that the other will perform a particular action (Jahankhani, 2006). Simply knowing a person's identity does not provide the adequate trust to engage in business relations or provide confidential information concerning a firm, health, etc. The establishment of trust between actors that do not meet physically and thus have little chance to "feel each other out" requires other mechanisms. The balance between individuals' freedom, reflected in the protection of their right to privacy, and the needs of society or the state to maintain law and order will have to be met but may give rise to different kinds of compromises in the digital world compared to traditional society. There is evidence of a trend towards greater acceptance of security impinging on privacy and a tilting balance towards greater implementation of security measures (Centeno 2003*a*).

Electronic transactions have great potential, but their future success will not be automatic. In order to raise trust among users it will be necessary to design and implement effective methods for identification and authentication (or confirmation). Authentication is an important part of security provision and a well designed authentication mechanism will improve Internet security. However, the general security solutions protecting other areas of an information system also affect the outcome of the authentication process. At the same time, transaction security and trust are context-dependent when it comes to providing appropriate authentication services. This report discusses possible ways forward to make more effective use of authentication mechanisms, such as digital certificates or encryption standards. Successful, appropriate authentication solutions may help reduce transaction costs by strengthening trust, and a range of models and approaches are available and have been applied by public authorities, regulatory bodies, banks, and other public or private actors. Electronic identity cards and smart cards with functions similar to how a passport or driver's licence is used internationally for identification are being developed. Methods are, however, currently lacking for personal identification over the Internet. It may be possible to find a way to incorporate multiple different national schemes for identification into one, single protocol. Such a scheme is bound to run into complications, however, since the areas in which these processes take shape are affected by diverse, simultaneous processes including technologies, organisational aspects, legal regulations and business incentives. There may thus be a need to nurture new methods, for instance, for exploiting third-party relations for digital authentication.

In summary, the report explores critical aspects of trust in digital transactions. It devotes particular attention to issues that arise in regard to authentication to underpin exchange and transactions on the Internet. The study sets out to explain and structure authentication

processes in global and digital transactions. Various aspects influencing the transactions are gathered under a *Global Authentication Framework*, which may be viewed as a model to advance various processes, issues, institutions and actors that affect the outcome of authentication services in digital transactions. Market and government failures, technological choice, interoperability aspects, legal systems and governments that provide identification services all play a role. The report suggests how to move forward in structuring critical strategies and addresses what is required to establish effective mechanisms for digital trust. It recommends that a serious effort is made to create a proper Global Trust Center (GTC), examining the validity and feasibility of this concept and presenting alternative possible models and specific recommendations in this regard.

1.1 STARTING POINTS AND RESEARCH DRIVERS

The rationale for the GTC is based on a number of observations regarding the likely future course of interests and processes among the actors that drive and enable digital transactions. All this emanates from a framework that represents an abstraction of today's digital world, which may be described as an information ecosystem of public and private actors and hybrids that meet with different and partly competing objectives. The aggregate outcome of their decisions will ultimately determine the effectiveness of the overall system. A single government or company is likely to encounter considerable challenges in addressing the outstanding issues alone. Malicious actors, for instance in rogue states, may refuse to follow international agreements. Many simply neglect to comply with lines of action recommended for reducing security risks, which will impact negatively on the overall ecosystem. An information ecosystem is only as strong as its weakest link.

The system can be characterised as a form of distributed governance that lacks central and powerful institutions. Critical activities, however, need coordination, for instance among governments, companies, within civil society, and so on. In the absence of mechanisms that promote coordination, a sound, efficient and secure outcome is unlikely to emerge on its own, making it unlikely that processes for rectifying problems as they arise will be initiated spontaneously. A framework for enabling security in the digital world must be able to balance cost with risk through the appropriate use of technology and policy. Again, managing that task will require a good deal of coordination. Agreeing on what is appropriate for different actors in such a dynamic and distributed environment – and implementing a solution that represents a fair compromise to those actors – is a formidable challenge.

Figure 1: Framework for authentication in global and digital transactions

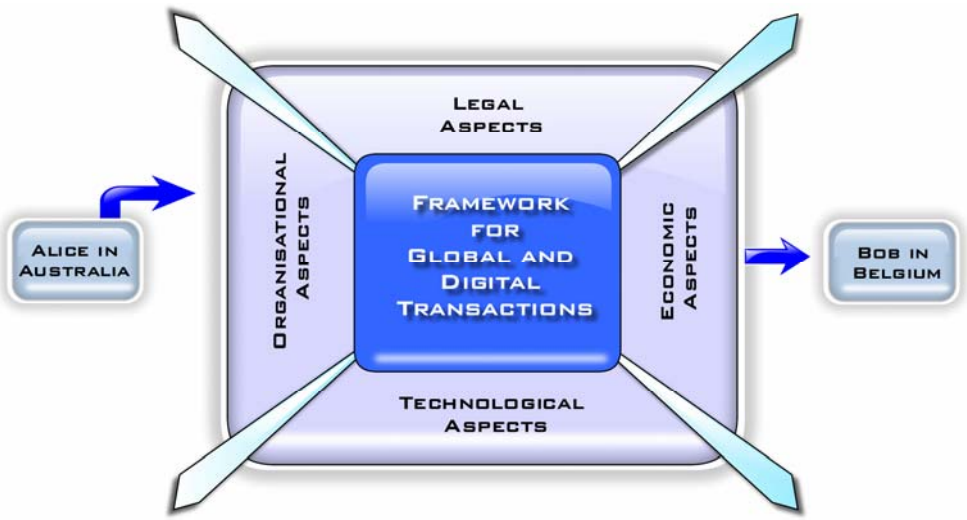


Diagram: IKED 2006

In order to understand the dynamics and inter-relationships of this information ecosystem, it may be helpful to divide the main characteristics into sub-areas. It is useful to draw a distinction between the *organisational*, *technological*, *economic* and *legal* aspects of the authentication component in digital transactions. The *organisational aspects* include whether, for example, an authentication system is centralised or decentralised, how trust can be achieved, what business models for transactions are in place, how security is handled in real life, and so on. The *technological aspects* show what kind of level of security can be achieved if the systems are flexible, scalable, interoperable, open-source based, and so on. The *economic aspects* concern the behaviour and interaction between service providers, regulatory agencies and technology providers, international and national cooperation, entry barriers, the public good component, dependability, fragmentation, and so on. *Legal aspects* characterise how privacy is handled, legal support for signatures, enforcement mechanisms, sanctions, evidence in the case of conflict, degree of regulation, the setting of standards, and so forth.

Governance of the Internet and of authentication can be organised along two extreme lines. On the one hand, there is the perception that things should be left to be settled by the market place (in the spirit of the traditional Internet approach). On the other hand, there is the view that governments and international communities should implement regulations to govern the Internet (in conformity with traditional telecom market regulations). In overcoming current and future risks vis-à-vis authentication it is vital to understand that risks relate not directly to specific market transactions but to the underlying societal and information infrastructure. With current methodologies, it is a challenging task to assess what risks and costs may prevail under varying circumstances. The current arrangement of loosely regulated decentralised governance structures has its strengths and weaknesses but is

a fact and must inevitably form the point of departure for any realistic discussion on how to structure governance of the framework for electronic transactions.

Market approach

The structure underpinning the provision of authentication services for international transactions does not work properly. A range of problems exists. Some are attributed to market failures, some emanate from government failures and others spring from imbalances in the overall systemic setup of interwoven public and private interests and interactions. In a sense, there is an issue with regard to a set of failures that is more generally known as the *tragedy of the commons.*[8] Assuring security is not solely the responsibility of a single business but is an issue that is relevant for the wider community. Though the problems show up locally, the issue of attaining trust in today's digital market place is a genuinely global one. The authentication framework can be seen as an ecosystem consisting of actors and institutions that are interlinked on a world-wide basis.

Since computer networks are interdependent, the issues for authentication frameworks and the linkages between separate systems are similar to those for information security in general. For instance, once a hacker or virus intrudes on a network computer, the remaining computers are more easily contaminated. This threat reduces the incentive for the single actor to protect against malicious activities, especially as even rigorous security may not be sufficient if a hacker has already entered the system. A common feature of these problems is that an organisation can never achieve perfect security. For authentication, specific challenges exist concerning the interaction between people, organisations and systems, where multiple levels of security are demanded. Key considerations here include how to protect the system in online and offline mode, and how to implement a cost-efficient and dependable system.

Another question concerns the interaction between systems originating in separate countries. For instance what happens when a government, with which there was cooperation and exchange of vital information, changes its policy and becomes *"country non grata"*?

A third weak link is the end-users that do not protect their home PCs sufficiently by leaving systems unprotected and open, thereby providing entry points for hackers to exploit for distribution of additional malware. All these issues may result in service providers being reluctant to provide online services online that might otherwise have benefited people, companies and societies worldwide.

The provision of authentication services is currently fragmented at national and international level. Multiple public and private actors provide numerous solutions. Challenges are emerging with respect to compatibility of solutions, risk of technological

[8] The tragedy of the commons describes an event where the costs caused by the actions of a selfish individual are shared by all participants, while the selfish actor reaps all benefits from these actions. In such competitive surroundings there is an obvious risk that the majority of individuals will become worse off.

lock-in and inefficiency due to the limited critical mass of services available that can offset the cost-benefit ratio. Instead of creating proprietary solutions, manufacturers and service providers can overcome issues of critical mass by interoperability.[9] Other sectors such as consumer electronics and software languages indicate why this is desirable. Many actors are of the opinion that standardisation of the general ICT environment is necessary to reduce market fragmentation.[10] Whilst of course there are very many "standards", there is no single system that has won global acceptance, so interoperability becomes a significant issue. CEN/ISSS has pointed to the need for common frameworks, with trusted, secure environments, data alignment (semantics, dictionaries, and so on) and classification and cataloguing.

However, there seem to be coordination problems and associated externalities as many individual companies are reluctant to cooperate with others despite potential gains. There seems to be a fear of competitors gaining insight into a firm's competitive knowledge or of them grabbing the entire cooperation surplus, hence making cooperation unreliable in the first place. The seriousness of this problem is reduced in repeated gains, where reputation effects become more powerful in punishing players that deviate from the common good (Axelrod, 1984). Furthermore, all the advantages of cooperation may not be appropriated by the cooperating companies, but may possibly benefit other actors due to the presence of spill-over or because the risks are completely outside of the transaction. This results in *underinvestment* in capacity-building for cooperation, including capabilities to network and to build joint platforms for interlinkages with external actors.

Information failure presents another case in point, especially for SMEs, which can be short-sighted in approach. Lack of resources reduces the ability to correctly assess risks and value measures for security and the potential benefits of cooperation. Factors such as *adverse selection* may also affect the behaviour of individual actors within SMEs and large companies, thereby affecting the outcome of security measures and the demands on authentication systems. Entrepreneurs who choose to work in SMEs may be more risk prone and care less about security measures, whereas a person choosing the career as security manager within a large cooperation is more likely to be risk averse and demand higher security standards (Anderson, 2001*b*).

The appropriate level of security varies between firms for additional reasons. A larger company will have the upper hand in a relation with the SME due to *asymmetric information and skewed bargaining power* between the two. Entering a long-term relationship implies the sharing of common practices, and SMEs are often required to adapt to larger companies' practices and systems, for instance having to adapt to a business system. This asymmetry will create problems of *lock-in* and *entry barriers* to newcomers if the systems are proprietary and costly to use and implement because SMEs with limited resources will not be able to

[9]Interoperability can have important economic consequences, such as network externalities. If competitors' products are not interoperable, the result may well be monopoly or market failure. For this reason, it may be prudent for governments to take steps to encourage interoperability in various situations.
[10] PriceWaterhouseCoopers report for Presidency. http://www.ictstrategy-eu2004.nl/

adapt to all available systems and will hence be more closely tied to the companies with which they choose to work.

The fragmented framework for authentication by systems that are not interoperable creates a situation where weaker actors risk to lose because their future opportunities to enter market and business networks may be impaired. Market leaders could gain greater control and become ever more difficult to challenge, cocooning transactions with customers and suppliers in specific defensive networks. The actors and opportunities in question may not even have been conceived today and SMEs are therefore unable to voice their concerns and needs for an orderly playing field. The consumers who will have to pay the higher prices, which result from deficiencies in market dynamics, will carry a large share of the cost.

A combination of institutional rigidities and transaction costs explains the inability of the many would-be losers to generate effective pressure for optimal solutions, as laid out by Olson (1965). Optimal solutions would come at the expense of the concentrated gains of those that stand to benefit from a lack of a better functioning marketplace. Interoperability would support market access, competition and open economies and hence be unfavourable to some of those who gain from the current situation.[11] Depending on how technologies and markets continue to evolve, incumbents may gain even more if barriers to market entry grow due to worsening technological lock-in. Blocking pressure for interoperability may therefore actually be in the interest of companies that provide security solutions. This may add to, or mix with, challenges in harmonising legal systems and business practices. It may also be that certain business models are applied in ways that are ineffective for introducing new technologies. In some business models, providers of digital transaction systems may aim to keep their centralised top-down approach to retain control. This might help them to strengthen their security, reduce competition and make it easier to defend market share. Such models should, in principle, be expected to lose out in the medium to long term. Three features of the ICT sector tend to lead to dominant-company markets with immense first-mover advantage (Anderson, 2003). The first is *network externalities*, as described by Metcalfe's Law, which stipulates that the value of a network is the square of the number of users since each additional member increases the market's value disproportionately. Network effects tend to lead to dominant company markets where the winner takes all. The second feature is *high fixed costs and low marginal costs*. Competition can reduce prices to the marginal cost of production, which makes it hard to recover capital investment (unless it is aided by patent, brand or other means of compensation, which also lead to dominant-company market structures). The third feature is *high switching costs*. Shifting from one product or service to another is expensive. For instance, switching from Windows to Linux means retraining staff, rewriting applications, and so on. This is reflected in *the Shapiro-Varian theorem* – that the net present value of a software company is the total switching costs. In ICT markets, time to market seems to be critical. The behaviour of many ICT companies that try to dominate markets or to ship products with lower quality in order to catch the market (and fix any problems later) may therefore be logical.

[11] Olson noted that actors are more able and prone to organise themselves so as to defend their interests where returns are concentrated, whereas when diffused they tend to be relatively passive. Private associations and lobbying thereby tend to be dominated by narrowly defined interest groups looking to maximise their own rents.

The presence of externalities normally indicates that regulatory standards or taxation are needed to enforce the internalisation of social costs or benefits, as in the case of environmental damage and the value of cutting pollution respectively. In that particular area, moreover, costs are often inflicted on the majority of citizens whereas the benefits of foregoing protection accrue to a small group of polluters. Given that consumers/citizens become better informed and start articulating their interests, however, firms may find it worth while to take the lead in establishing a "clean brand" – the previous externalities are then internalised. The security risks inherent in authentication processes may or may not present a similar situation. Often they cannot be subscribed to any particular transaction or criminal act of behaviour. Simply asking market actors to change behaviour is unlikely to represent a viable way forward to reduce risk. However, the overall outcome may be subject to "tipping behaviour", such as when a company that occupies a strategic niche induces others to follow its lead. Even if no single company exists that can exert such leverage, a small group of companies may be able to do so. This has significant implications for policymaking, since it suggests that markets may be in a position to potentially fix the problem, but that it may still be important to persuade certain key actors to take the lead (Kunreuther et al., 2002). This kind of strategy has been more or less explicitly applied by various countries, for example in Sweden where the government encouraged some domestic banks to jointly develop a solution for authentication, namely BankID.[12] Governments may also themselves attempt to set an example and employ strategically essential solutions, such as e-procurement using authentication mechanisms that are interoperable.

Some countries perceive the authentication service or the provision of identification as part of the national infrastructure, implying that it should be provided by the government. One rationale is that it represents a service of vital importance to information about citizens and hence should be protected by public interest. In many countries that take this view, governments have issued national identity cards from early on.

In principle, government intervention is motivated by the inability of markets to initiate or sustain linkages that are potentially favourable from a societal perspective. However, government action is not without challenges. The role of government, and its problems, is discussed in the following section.

Government approach

Governments basically have two measures, or a mix thereof, to guide the governance framework for authentication services. They can regulate and set the legal framework or they can take on the role of service provider and actively set up an authentication service. Both approaches face government failure problems.

The "regulation approach" includes challenges, including with respect to determining the degree to which market frameworks should be regulated. *Overregulation* can strangle markets,

[12] See http://www.bankid.com/index.jsp for more information.

a phenomenon that can be observed in Europe with regard to qualified certificates, which through over-regulation has lead to little deployment of the particular solution and actors opting for less secure solutions. On the other hand, lack of regulation can create a framework plagued by many market failures, and suffer from dominant actors and weak competition.

The second case is about dealing with challenges, such as white elephant projects that prove excessively complex and expensive. Such projects are launched by public actors with little market knowledge and which lack the right references to design adequate solutions due to improper incentive structures.

As was well understood long ago, governments and other public bodies are not necessarily efficient or impartial. Clearly, market failure should only be addressed if governments can be presumed to do better than markets. This includes not only taking account of administrative costs and policy errors within individual programmes, but also the risk that public involvement is influenced by *vested interests*, which distort private behaviour in a wider sense and/or perpetuate themselves over time.

It is often relatively easy for limited groups of vested interests in specific regions or sectors to organise themselves so as to exert pressure on governments to favour their special interest. This is particularly so when the benefits of policy intervention are concentrated and come at the expense of broader groups that must bear costs that are spread relatively thinly (Olson, 1965). In fact, resulting deficiencies in public choice mechanisms make government or policy failure occur relatively frequently, which in turn creates needs – and additional justification - for corrective measures. Some of the answers have to do with re-organisation of public responsibilities – between ministries or between national and local levels. A closer connection between decision-makers and those affected by the decisions is often warranted. On the other hand, care is needed to ensure that any such reorganisation does not increase the dominance of specific interests.

> *"The major reason companies do not worry about the externalities of their security decisions … is that there is no real liability for their actions. Liability will immediately change the cost/benefit equation for companies, because they will have to bear financial risks borne by others as a result of their actions."*
>
> Bruce Schneier, testimony before the US House of Representatives (2003)

Several examples of attempts to create public authentication solutions, without immediate demand (for these, often high cost, solutions) exists, sometimes with the result of costly market distortions. A point in case is Finland, which in 1999 launched a high-level digital certificate solution (based on PKI) for national e-identification. The system was, however, initially too expensive and complex for general use and has changed over time.

One way for governments to address the issue of governance is through rearrangement of incentives and liabilities. It is commonly claimed that the liability for this should rest with the actors that have the greatest capacity to respond to a problem as it arises, as well as with those that can integrate the costs from failures into transactions. Ross Anderson (2001*a*)

examined cases of fraud at ATMs in the UK and found that almost all involved human error. The security problems were a result of deficient installation, misconfiguration and mismanagement of the systems by the local banks. Anderson claimed it was due to how the liability was assigned. He compared the UK with the US, where the burden of proof is with the bank in the event of a customer dispute. The reverse applies in the UK. Since it is almost impossible for a customer to provide evidence, UK banks had little incentive to address problems, which led to an increase of ATM fraud. In the US, companies invested in risk management techniques and banks there ultimately spent less on security than their UK counterparts because they dealt with it more effectively.

A conclusion from this example is that policymakers should try to assign the liability to the party that can do the best job of managing risk. In the case described, the banks are in a better position than the users. However, liability should not be vested solely with one party as this would encourage complacency and could also lead to unwanted distribution effects. A sound balance is desirable, with outcomes reflecting the extent to which the different players are susceptible to key risk factors. As a result of the liability allocation, the responsible parties will most likely be interested in acquiring *insurance*. This might seem contradictory: if you are perfectly insured against liability, why invest in risk management? However, the incentive for the insurers is to deal only with clients who implement good security practices. This in turn provides a strong incentive to educate clients on optimal behaviour (Varian, 2000). To calculate the costs of risks and probabilities is not a trivial matter, however, because the challenges in the field of ICT security and authentication are changing by the day. New threats and usage rates are constantly evolving and comprehensive data is not widespread. A complicating factor is the lack of successful PKI implementations; the few that exist have little track record on which to base risk and liability assessments.

Legal liability is a complex topic, which – if not dealt with properly – may prevent interoperability. If demands on systems are set too high, service providers may be reluctant to interact with other service providers because the costs of failure are greater than the possible gains.

Designing an appropriate authentication framework for international transactions by changing the incentive structure may be difficult since governments' reach is mainly national in scope. Some issues are handled in different *international forums*, such as the EU, APEC or the ITU. A number of global forums and working groups,[13] such as Liberty Alliance, APEC TEL Working group, EU - CEN/ISSS, and the ITU Study Group 17, are also addressing authentication issues. Aspects that come under consideration include the development of potential interoperability models and the execution of pilots so that both technical and legal interoperability for authentication services can be achieved. Still, coordinating and implementing better solutions is not unproblematic.

[13] See more on this in Section 3.2.

Mixed approach

Conventional command and control strategies no longer suffice for governments since much is increasingly beyond government control due to deregulation, privatisation or international factors. Hence, governments require new and innovative ways of addressing failures and inconsistencies to respond to the changed setting. On the increase is the use of a more systemic approach and provision of governance through a mixed framework.

Both the market and the policy failure approaches serve to identify individual suboptimal outcomes that motivate policy correction. However, governments and policymakers impact on the economy in multiple and partly interrelated ways and it is becoming increasingly vital to understand the systemic interplay and pitfalls.

Systemic failure arises when there is a mismatch or inconsistency between the interrelated institutions, organisations or playing rules (Metcalfe, 1995). An example of a systemic failure is the electricity sector in California, where faulty market designs and regulations have resulted in an extremely costly loss of system reliability. Public and private institutions provide components for authentication that are of a public as well as of a private nature. Shaping appropriate and effective conditions for the two kinds requires interaction and coordination between different types of institution (Nelson and Romer, 1997). A positive example of international interoperable networks employing a decentralised systemic approach is the establishment of roaming[14] between mobile telephony networks, which is an example of decentralised, loosely coupled, organisational units that so far have managed to meet market demands satisfactorily (Heuvelhof et al, 2004).

Authentication should not be overly regulated centrally, but instead there is a need of working out solutions in a decentralised manner, to enable experimentation and the application of competing models in search of resource-effective and transparent solutions. Public-private partnership may represent a good way to bolster appropriate responsibilities for actors within an authentication framework. ICT is now critical infrastructure, on which the demands are becoming as high as for water and telecommunications. But needs diverge – and so should solutions. In cases where demands are lower, it is essential that the authentication framework can make top-down and bottom up requirements meet and make room for cost-effective solutions.

Security researchers have often tended to focus on the hard issues of cryptography and system design. However, soft issues revolving around the use of computers and the creation of incentives to avoid fraud and abuse also merit attention. Odlyzko (2003) argues that it is more productive to think of security not as a way to provide ironclad protection, but rather as the equivalent of speed bumps, and to decrease the velocity and impact of attacks to a level at which other protection mechanisms can operate. As previously stated, risk estimations are very hard and probably impossible for governments to make, but are more feasible for those that are closer to the risks. Insurance is solvable on an international scale,

[14] Roaming is a general term in wireless telecommunications that refers to the extending of connectivity service in a network that is different than the network with which a station is registered.

though it is harder (but not impossible) for a government to address liabilities and conflicting frameworks for international transactions. For long-term stability, it is essential that systems can incorporate and manage externalities. From a government perspective, it is desirable to strive for a proper balance of responsibilities and a sound mix of incentives, promoting actors to choose appropriate technologies and security levels and to support this through the regulatory system.

1.2 BASIC REQUIREMENTS

This section summarises some of the challenges described above and what demands are relevant when designing an appropriate framework for authentication services:

- Cost efficiency (e.g. low entry costs)
- Interoperability (separate systems should be able to communicate with each other in a secure manner)
- Works on the open Internet
- Non-dependence (no dependence on one specific technology or technology provider)
- Meets basic requirements of security
- Trustworthiness (which may be achieved by implementing dependable computing)
- Flexibility
- Scalability
- Usability
- Protecting user privacy (i.e. private data may not be transferred between countries or parties without the explicit consent of users)

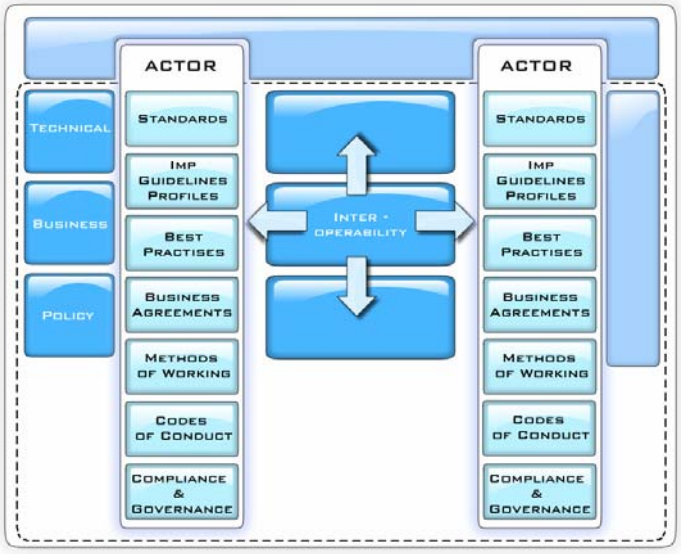
Authentication technologies can be designed to include interoperability features but the methodologies used to authenticate people may differ from country to country. Future authentication systems will need to include interoperability in their design to allow user mobility and to build trust and fight fraud and privacy abuse. A system should incorporate wider demands than a single sector application with a geographically limited scope, and should consider potential cross-sector and cross-border usage. Authentication solutions must be scalable and this is where problems, although generally of a predictable nature, arise. These tend to relate to the complexities of key revocation requiring the management of large and highly available revocation lists, and the distribution of liabilities in the case of abuse between certification authorities and businesses using certificates.

A complicating factor is the lack of a general understanding of the meaning of interoperable services. Interoperability is multilayered and not restricted to purely technical specifications. Many other conditions are needed to reap the benefits of interoperable technologies. Figure 2 illustrates various generic requirements for interoperability, for which technology alone does not provide the solution.

For interoperable solutions to be developed and adopted in a coordinated manner, actors' incentives need to be harmonised. The relationship between government and banks is one example of an inherent conflict whose easing might allow for a considerable acceleration in the development of new solutions. In this sense, enhanced cooperation between key actors in the public and private sectors may enable considerable progress. In a similar vein, overcoming the contrasting interests of, say, customers and service providers, patients and suppliers of health care, or contenders and tender providers, might represent the key to success in some cases.

Less hierarchical, demand-driven governance structures are likely to serve as key drivers for establishing frameworks conducive to the development of secure digital transactions. Solutions should follow the inherent Internet logic of connecting different authentication domains so as to underpin a comprehensive playing field.

Figure 2: Interoperability



Source: Athena[15]
Diagram: IKED 2006

1.3 GENERAL APPROACH AND METHODOLOGY

This report is based on material gathered through literary reviews and interviews with leading actors and stakeholders involved in authentication of digital transactions. They contributed to the mapping of available technologies and legal framework and also

[15]http://www.athenaip.org/components/com_docman/dl2.php?archive=0&file=Q2x1c3Rlcl9CdXNpbmVzc19Nb2RlbHNfQVRIRU5BX0IzX3YwLnBkZg==

responded to questions regarding the feasibility of a possible clearing house structure, as envisioned in the GTC concept.[16] The report reviews a limited number of actors and sectors and draws notably on experience from Australia, the European Union, (and the individual member states Austria, Belgium, Denmark, Estonia, Finland and Sweden), Hong Kong and the United States. These countries, selected by the Global Trust Center Steering Committee, represent systems from various parts of the world and specific conditions that help to generate insights into the role of various factors in shaping outcomes. Both common law and civil law countries are included, as well as markets featuring varying degrees of regulation.

In the empirical examination, some respondents to a survey questionnaire answered orally, whereas others provided information in writing. The questionnaire was structured according to the four principal perspectives mentioned above and contained questions related to each of the included sectors (see above). The questionnaire is attached to this document as Appendix B.

Finding comparable data covering relevant countries and sectors gives rise to a host of challenges. Overall, obtaining data on financial and most government sectors is fairly straightforward. However, corresponding information on health and institutions engaged in higher education is hard to come by. While the survey distinguished between sectoral features, respondents did not necessarily apply the distinction when answering the questionnaire. Mixed levels of data in part follow from the broad scope of the project. As a result, some respondents provided feedback on a wide range of authentication methods, used both in private and public sectors at national and international levels. The variation in respondents' backgrounds, expertise and focus further complicated comparisons. A compilation of the survey responses can be found in Appendix C.

On the sample countries

Australia is among the most advanced countries not only in terms of technology for ICT use, but also because it is known for high competency in designing public policies conducive to market solutions. Sweden and Denmark are geographically close but have different standards and are already in the process of harmonizing various structures. Some co-operation takes place with Finland, which was one of the first countries to regulate and promote authentication services by the public sector. Much of the EU work is inspired by the Finnish setup. Estonia has managed to roll out quite a substantial number of digital certificates in proportion to its population and in an economy that is not nearly as advanced as the others in the sample. Austria has combined public and private initiatives in a promising way and Belgium has great ambitions and has embarked on rolling out a National eID that will provide all citizens with a certificate for online authentication by 2009. In certain respects, the US is the most advanced player and home to a majority of the actors that provide solutions for authentication services on the international scene. Hong Kong

[16] see appendix A

has succeeded quite well and is considered the most advanced country in Asia, with an ambition that all citizens will have an eID by 2008.

On quality-assurance

The work on the report was overseen and guided by an international steering committee consisting of several leading players active in providing trust in digital transactions.[17] The committee includes representatives from private companies, the financial sector, technology providers, trust operators, standards organisations, ministries in charge of technology issues, and universities. Several conferences and workshops have addressed the topic over the last few years and helped advance and diffuse the understanding of what could be done to address the outstanding issues. In the meantime, practical pilot programmes have been developed under the framework of the steering committee to address specific issues, for example in the financial sector. Additional planned events will provide further impetus. An associate body encompassing a large number of representatives may be instituted to support the implementation of the trust center itself, if deemed practically feasible.

A range of leading security and authentication experts provided input to the report by preparing background studies and country data.

1.4 ON THE REPORT

Objectives

The report aims to assess ways in which it will be possible to improve security and enable trust in the information society. The most basic issue concerns the need to strengthen the market for the provision of authentication services. Based on the findings of empirical surveys, methods are structured for how to put in place more effective cross-recognition and cross-certification of services, spanning the gaps between national jurisdictions as well as institutional and sectoral frameworks. A fundamental observation concerns the presence of a public good component, which is presently unheeded but which needs to be addressed in any strategy hoping to succeed in enhancing trust and security in digital transactions.

The report provides a map and sets out to analyse a range of national and international activities of relevance to the implementation of authentication services – including their legal and regulatory frameworks and security perceptions of dependent parties and individual countries. It describes various countries' implementation strategies and gathers factors influencing transactions under the heading of a Global Authentication Framework. This framework may be viewed as a model to advance processes, issues, institutions and actors that affect the outcome of authentication services in international digital transactions. Market and government failures, technological choice, interoperability aspects, legal systems, governments that provide identification services, and so on, all play a role.

[17] To learn more about the group, see webpage: http://www.globaltrustcenter.org

In brief, the study presents:

i) Analysis of varying authentication services, resulting in:

- A description of selected services in individual countries
- An analysis of fragmentation of these services;
- Recommendations on possible ways to overcome such fragmentation.

ii) Analysis of similarities and differences between legal frameworks in various countries, resulting in recommendations on steps to advance common terminology.

iii) Reflections on the feasibility and viability of current and evolving practices for achieving orderly conditions for authentication services, followed by recommendations on how to facilitate the use of ICT and electronic commerce globally, by:

- Defining the regulatory strategies employed by countries in the implementation of authentication services
- Analysing perceptions of electronic transactions by relevant parties and countries
- Detailing country requirements regarding interoperability with respect to online transactions and digital certificates
- Describing markets and sector requirements for interoperability
- Exploring how a clearing house structure can be established to facilitate dialogue and the application of coordinated solutions on a continuous basis, including analysis and conclusions on how the GTC could support this kind of function.

Positioning the document

The report aims to provide a structured theoretical basis of the issues relating to authentication and collects an extensive body of empirical reference material based on the experiences of a global sample of countries, including representative examples from Asia, Europe, North America and Oceania. National and sectoral experiences are compared and brought together. The report represents a first attempt to examine various national and economic setups for authentication, and to compare them in terms of technological, economic and legal aspects, keeping in mind the importance of organisational and operational viability.

Structure of the report

The report seeks to analyse the feasibility of the GTC and thereby aims to remain objective. Nevertheless, the contents are organised around the GTC, as can be seen in Figure 3. A compilation of the interview questions, respondents' answers and some background data

can be found in the appendices. Appendix A includes further presentation of the GTC concept.

Figure 3: Structure and contents of the report

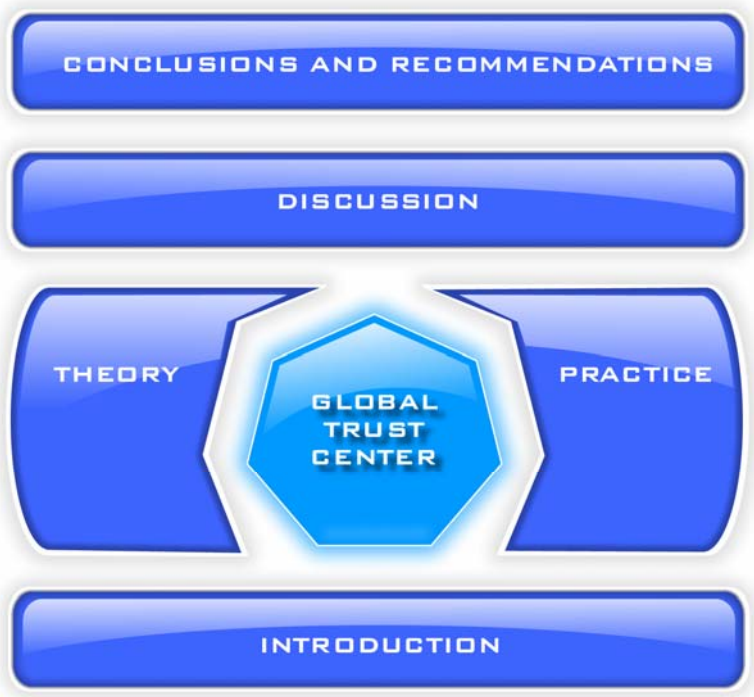


Diagram: IKED 2006

2. AUTHENTICATION ASPECTS

Security issues are often closely connected to the concept of authentication. A range of factors and perspectives are relevant in this context. This report addresses four principal views that combine to form an environment for authentication, depicting driving forces as well as impediments.

The Internet is currently characterised by numerous threats and risks that accentuate the need for authentication. Risk analysis, security engineering and privacy-enhancing methods form driving forces that separately and collectively impact on the development of authentication mechanisms. Here, the underlying idea is that a sounder and more effective platform for enhancing trust will be possible if the dangers and fears of utilising the Internet are managed. Figure 4 illustrates how these four principal drivers are treated within the report. In order to give authentication and its influencing factors a relevant context, organisational, legal, economic and technical aspects are also included in the analysis.

Figure 4: Authentication and the environment

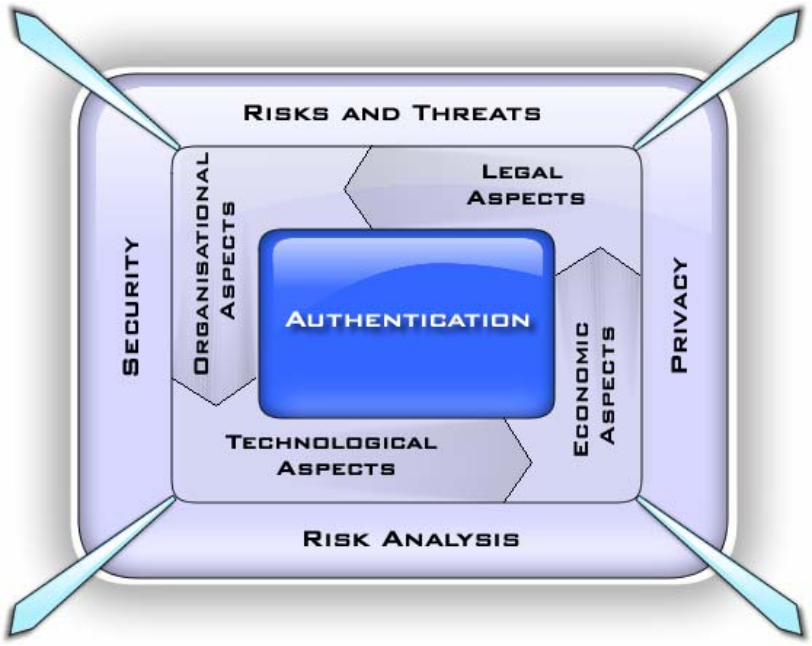


Diagram: IKED 2006

2.1 INTRODUCTION: THE WORLD IS FULL OF RISK

The increasing volume of private, business and government services and transactions that are in the process of turning digital, combined with the rapid introduction of new ICT

technologies, creates increased risks of disruption, fraud and crime. Some cyber crime resembles traditional crime. But new forms of crime are also evolving, targeting ICT infrastructure and the properties and contents of information (for example, the modification of data and denial of service attacks). ICT and electronic commerce are now becoming viewed as increasingly susceptible to misuse, especially in the case of online payments over the Internet (Computer Security Institute, 2001). There appear to be mounting risks associated with:

Data confidentiality, integrity and availability

i) Authentication
ii) Costs of failure
iii) Interoperability requirements
iv) Non-repudiation and liability

The digital world is an environment which is conducive to fraud, as it provides anonymity, low access barriers and rapid exchange of resources from hacking programs and credit card numbers. This is further worsened by the possibilities for automation of fraud on a larger scale and transnationality that creates challenges for national preventive resources in dealing with perpetrators (Calloyanides 2003). Fraudsters also benefit from the overall low security skills of Internet users and lack of appropriate tools and from increasing Internet connectivity from homes (such as always-on broadband connections) that provide more opportunities for crime. Prosecutions are complicated as transaction amounts in general are not significant, for most regular users, and existing electronic evidence tools and skills are very limited. Further, legislation has not yet adapted to the Internet environment and in a case of cross-border transactions, complex jurisdictional and procedural issues may arise.

When using the Internet, common risk factors are fraudulent behaviour, identity theft, malware design and distribution, abuse by insiders and a lack of methods to ensure digital evidence. The following subsections will examine these problems.

Malware

Malicious code, or malware, planted on computers has grown drastically in volume and sophistication in recent years (Skoudis 2004). Viruses, worms, spyware and Trojan horses are the most common examples of malware. Malware infections can, among other things, corrupt files, alter or delete data, distribute confidential data, disable hardware, deny legitimate user access, and cause a hard drive to crash (Rubin 1999). Frequently, malware is designed to send itself from email accounts to all the contacts in an address book. The results of malware infection include wasted resources, compromised systems, lost or stolen data and loss of user and client confidence (Szor 2005). Although each type of malware has its own defining characteristics, the distinctions are becoming blurred because blended threats are becoming increasingly common (Skoudis 2004). Blended threats combine the characteristics of more than one type of malware to maximise damage and speed of

contamination. Typically, malware is distributed in one of three ways (Skoudis 2004, Szor 2005):

i) By email, either in a virus-laden attachment or in the message body code
ii) In an infected application
iii) Through infected code on a website

Many security experts believe that the newer communications channels, such as instant messaging (IM) and Voice over Internet Protocol (VoIP), pose a very serious threat to networks (Townsend 2003). According to Gartner Group research, 58 per cent of network security managers stated that IM poses the most dangerous security risk to their enterprise. Symantec Security Response predicts that the next major worm hazard will be IM-based. There are no indications that the number and severity of attacks will do anything but increase, as illustrated in Box 1.

There are numerous reasons why malware continues to increase (Bishop 2004, Skoudis 2004). The ongoing rise in computer literacy is one. More and more people around the world have the technology and knowledge to create and distribute malware. Tools required for attacks are ever more widely available over the Internet, so that even people with only very rudimentary knowledge can launch attacks without much difficulty. Older threats often remain active for an extended period of time, or enjoy resurgence, so that while new malware is constantly being released, it supplements older threats rather than replacing them. Some reports from the underworld of malware creators suggest there is intense competition among virus writers to see who can wreak the greatest havoc. Also, the complexity of modern software makes it harder for developers to detect and correct vulnerabilities (Szor 2005). According to many experts, spam[18] – which has grown exponentially in the last few years (Ferris Research) – and malware are being used in tandem to maximise the distribution power of commercial messages (Jacobsson 2004). Naturally, this is not to say that defences are not advancing as well. With the much-increased diffusion of continuously upgraded firewalls in the last few years, some of the problems mentioned have in fact been quickly overcome, and there are signs that some types of problem may be disappearing. All the same, there is a growing need for counter-measures – and this need may take on new guises as the nature of attacks changes.

[18] Spam is typically defined as unsolicited commercial and/or political email.

Box 1: Malware incidents and effects

- Code Red infected every vulnerable computer on the Internet within 14 hours – Slammer did the same in 20 minutes. An IM exploit could spread to half a million computers in just 30 seconds (*Symantec Security Response*)
- In 2001, one in 300 email messages contained a virus and for 2004 that number was around one in 100 (*MessageLabs*)
- Attacks have increased tenfold in the past ten years, from 1,334 reported attacks in 1993 to 137,529 in 2003 (*CERT Coordination Center*)
- 20-40 new or variant virus threats were reported daily to Trend Micro in 2003
- Ninety-two out of 300 randomly selected companies suffered a major (more than 25 computers affected) virus attack in 2003 (*ISCA Labs, 2004).*
- Spyware is estimated to be present on about 90 per cent of computers with a broadband connection and they are responsible for about a third of all Windows application crashes (*Scott Culp, Microsoft*). Enterprise SpyAudit scanned nearly 60,000 systems. The infection rate remains above 80 per cent. During 2005, the number of spyware distribution sites quadrupled. In the second quarter of 2005, at least one form of unwanted programme (Trojan horse, system monitor, cookie or adware) was identified on more than 80 per cent of the PCs scanned. The frequency of malicious spyware on an infected PC rose 19 per cent in the last quarter. Reportedly, there has been an increase in the more malicious types of spyware, which are smarter at avoiding detection and removal, and capable of ensuring survival through a constant renewal of tactics (Webroot, 2005).
- Viruses cost businesses around the world US$ 55 billion in 2003, up from US$ 13 billion in 2001 (*Trend Micro*). The most expensive virus so far was the Love bug, which caused almost $8 billion dollars of damage worldwide. The effects of malware incidents and disasters arise in multiple ways, e.g., the loss of productivity, unavailable PCs, the loss of data, the loss of access to data, and corrupted files (McManus, 2005).
- According to available surveys, more than 3.9 million virus incidents were reported on more than 900,000 desktops, servers, and perimeter gateways during 2004. This translates into 392 encounters per 1,000 machines, and represents a 12 per cent increase since 2003. Another point of significance is that some recovery times appear to have increased. While recovery time had risen only slightly in 2003, the rise in 2004 represented an increase of almost 25 per cent. For the second year in a row, there was a significant jump in cost related to recovery, which rose to more than $ 130,000. This brought, for the second year in a row, sharply increasing costs (although, historically, there may be an under-estimation of recovery costs due to a mostly technical focus on security and recovery). (ICSA Labs, 2005).
- In the summer of 2003, Sobig.F infected 200 million e-mail messages across the Internet during its first week of activity. Estimates indicate that Sobig.F impacted 15 per cent of large corporations, and 30 per cent of SME organisations. Sobig.F was the biggest/most virulent virus over the last four years. Because Sobig.F also fits the properties of a worm, it infected the host computer when an enclosed file was opened by the user. Inside the computer, Sobig.F used addresses from the local address book for further spreading. As part of the payload, harmful software was downloaded and installed on the infected computer, which also permitted further installations of new malware and reconnections of network traffic. The original idea behind Sobig.F was to install a spam proxy-server on the targeted desktop in order to use the infected computers as distribution nodes over the Internet. The Sobig.F's outbreak pointed to a convergence between the burgeoning threats of email viruses and spam. The recent Sobig.F outbreak is the fastest-growing email virus ever. The initial seeding of Sobig.F was posted on an adult-oriented website, using an account created with a stolen credit card (MessageLabs, 2005).

Identity theft and Internet fraud

Identity theft is when someone's identity information is stolen in order to misrepresent the owner for the benefit of the perpetrator. Examples include theft of bank statements, incoming mail with bank or credit card statements and pre-approved credit cards, and then using this information to open a new credit card account or take over an existing one, to contract phone or wireless services, to open a bank account or to ask for a loan (Smith 2002). Businesses may transact with a consumer using stolen or fake identification and payment data which will ultimately lead to repudiation by the rightful owner of the payment data, or denial by a consumer of a performed purchase.

Identity theft in the virtual world is a growing problem and appropriate countermeasures need to be introduced (Ferris Research). Risks are exacerbated by disparate regulation and business practices that make consumers trade in their identities in exchange for commercial benefits (Cavoukian and Hamilton 2002). Identity theft is a major threat to the security of the identification process and is raising increasing concerns as it is a threat to the development of the information society (Fischer-Hübner 2000). Due to the present situation with coexistence of heterogeneous systems, identity systems attract much attention from cyber crime. Identity theft is facilitated by the lack of a clear risk management system for the identification process and also by the use of identification support for purposes other than those for which they were designed (Smith 2002).

Identity theft has thrived over the last few years and has been estimated to cost banks US$1 billion a year. The US Federal Trade Commission reports that 43 per cent of consumer fraud complaints in 2002 were about identity theft, with more than 161,000 reported cases – an increase of 88 per cent from 2001. Some 10,000 victims had home loans of US$300 million taken out in their name in 2002 and another 68,000 had new credit cards issued in their name.[19] Star Systems found in a survey of 2,000 US adults that 5.5 per cent had been victims of identity theft. Of the victims, 29 per cent reported having credit cards in their name issued to another person, 23 per cent had bank accounts in their name opened by another person, 21 per cent had loans taken out in their name by another person and 18 per cent had their currently existing bank account taken over. In the UK, banks, building societies and financial institutions reported more than 40,000 cases of identity fraud in 2002 compared with fewer than 13,000 cases in 2000.[20]

Consumer security concerns may be justified, as indicated by the 50 per cent increase of identity theft reported by the US Treasury's Financial Crimes Enforcement Network in 2001/2000. Experts estimate that this type of fraud has tripled between 2000 and 2005, with 1.5 million cases expected in the US. Furthermore, bank systems and services are reported to be central targets among fraudsters, with 42 per cent of cases being related to credit card fraud (26 per cent to new accounts and 10 per cent to existing accounts), 20 per cent to phone or utility bills, 13 per cent to bank fraud, and 7 per cent to loan fraud.

[19] MSN, 27 March 2003. http://www.msnbc.com/news/891186.asp?cp1=1
[20] Sunday Times, UK, *Ministers to act on huge rise in stolen identities*, 5 January 2003.

The superstructure of the Internet and the availability of means to remain anonymous online has resulted in multiplied increase of online fraud in both volume and extent (Garfinkel 2001). Statistics from the US Internet Fraud Center reveal a drastic increase in 2002 compared to 2001. Reported losses in the US totalled US$54 million, versus US$17 million the previous year and law enforcement complaints in total rose from 16,755 in 2001 to 48,252 the year after. Of the different kinds of Internet fraud the top two reported crimes were auction fraud and non-delivery of merchandise (see Table 2).

Table 1: Internet scams – fraud trends 2004

Top ten scams – category and % of all complaints	*Average loss*
Auctions 51% – goods never delivered or misrepresented	US$765
General merchandise 20% – sales not through auctions, goods never delivered or misrepresented	US$846
Nigerian money offers 8% – false promises of riches if consumers pay to transfer money to their bank accounts	US$2,649
Phishing 5% – emails pretending to be from well-known sources asking to confirm personal information	US$182
Information/adult Services 3% – cost and terms of services not disclosed or misrepresented	US$241
Fake cheques 3% – consumers paid with phoney cheques for work or items sold, instructed to wire money back	US$5,201
Lotteries/lottery clubs 3% – requests for payment to claim lottery winnings or get help to win, often foreign lotteries	US$2,225
Computer equipment/software 1% – non-auction sales of equipment or software never delivered or misrepresented	US$1,401
Fake escrow services 1% – criminals direct buyers or sellers to false escrow services, pocket the money or get goods free	US$2,585
Internet access services 1% – cost of Internet access and other services misrepresented or services never provided	US$1,187

Source: http://www.fraud.org/2004-internet%20scams.pdf

Another common type of Internet swindle is credit and debit card fraud.[21] Consumers face the risk of engaging in a transaction with a fake or fraudulent vendor who bills the transaction but never delivers the goods purchased. Alternatively, they may receive recurrent or unauthorised debits for a service subscription they never agreed to or risk having card or account data stolen and used for unauthorised purposes. Payment scheme statistics (Europay International, May 2001) show that Internet fraud with credit cards mainly takes place at transactional sites that collect payment data and disappear after fraudulently charging the cardholder (for instance, adult sites) or through unauthorised access to insufficiently protected payment data stored on vendors' servers. Market research estimates that credit cards are used for 93 per cent of Internet online payment transactions (Gartner, March 2001), of which 1.1 per cent are fraudulent. Following current credit card

[21] Internet Fraud Complaint Center, 11 April, 2003. http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf

rules, however, vendors assume liability for 90 per cent of them (CommerceNet, May 2001).

Other more sophisticated attacks exist, such as Internet Protocol spoofing (IP spoofing). This is the fraudulent behaviour of creating IP packets with a forged (spoofed) source IP address (Anderson 2001a). The header of every IP packet contains its source address. By forging the header, an attacker can make it appear that the packet was sent by a different machine. Network intruders have used this attack to overcome network security measures, such as authentication based on IP addresses. The attack is most effective when a trust relationship is established in a network. For example, many corporate networks are connected to internal systems so that users can log in without a username or password. By spoofing a connection from a trusted computer, an attacker may be able to access the target without authentication (Smith 2002). Spoofing is often mentioned in relation to phishing, which is a type of social engineering attack.

Insiders and social engineering

The insiders of an organisation – its own employees – have been identified as the potentially largest risk to security since human failings can undermine the best security measures. The Economist (2002c) records the example of PentaSafe Security, which conducted survey at London's Victoria Station in which two-thirds of commuters shared their computer password in exchange for a ballpoint pen. Another survey, also reported by The Economist, revealed that 50 per cent of UK office workers used their own name, the name of a family member or that of a pet as their password. Further failings include writing passwords down on adhesive notes attached to the computer monitor or nearby whiteboards; leaving machines logged on while out at lunch; and leaving laptop computers containing confidential information unsecured in public places. Also end-users often do not protect their home PCs properly, leaving them vulnerable for external persons to enter and acquire critical information or to hijack as a point of attack on critical systems. The lack of protection and knowledge of how to protect home PCs was reported by bankers as a critical problem that complicates the design and implementation of secure systems.

One of the most famous hackers, Kevin Mitnick, relied heavily on human vulnerabilities to access computer systems, which he refers to as social engineering attack (Bishop 2004). Mitnick manipulated people over the phone through deception and was so successful that he rarely had to use a technical attack. The human side of computer security is easily exploited and constantly overlooked. One of the quickest growing threats is phishing, which is a process whereby a perpetrator by deceptive means tries to acquire sensitive personal information such as passwords, user names, credit card numbers, and so on. (Bishop 2004). In phishing, the malevolent actor tries to acquire this information by masquerading as someone trustworthy who has a genuine need for the information and sends his requests in an official-looking email, IM, or similar message. Companies spend large amounts on firewalls, encryption and secure access devices. But this is money wasted unless it is complemented by correct social procedures because none of these measures address the weakest link in the security chain (The Economist 2002*b*).

Opportunities for Internet fraud and identification theft are overwhelming, and so far the techniques for preventing them are limited.[22] Also, there is a lack of methods that can provide digital evidence to prove criminal actions. The development, standardisation and diffusion of new digital evidence tools is required. Such methods are much-needed, and it is important to get them legally accepted in judicial processes and courts of justice. Furthermore, there needs to be an acceptable level of efficiency in crime prosecution processes, including the need for accountability and transparency. Current EU privacy regulation lacks horizontal effect, meaning that it is impossible for citizens to lodge a complaint against other citizens, their employers or commercial organisations based on Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedom.

Within the corporate sector, large companies tend to over-spend on security and small companies tend to under-spend. Research shows that this may be the result of an adverse selection effect, whereby the most risk-averse people end up working as corporate security managers and more risk-prone people seek posts as sales or small business entrepreneurs (Anderson 2001a). This is further enhanced by effects from due diligence, government regulation and insurance market issues. Nevertheless, risk analysis and information security are central aspects of computerised systems and networks. These domains will be explored in the following section.

2.2 INFORMATION SECURITY AND THE RIGHT TO PRIVACY

Most organisations recognise the critical role that ICT plays in supporting their business objectives. But today's highly connected ICT infrastructures exist in an environment which is increasingly hostile. Organisations are often unable to react to new security threats before their business is impacted. The primary concern for ICT departments has become to manage security of infrastructures and the business value that those infrastructures deliver.

Furthermore, new legislation that stems from privacy concerns, financial obligations and corporate governance is forcing organisations to manage their ICT infrastructures directly and effectively. Many government agencies and organisations that do business with them are required by law to maintain a minimum level of security. Failures may put executives and whole organisations at risk due to breaches in legal responsibilities. However, security issues are never black and white, and context matters more than technology. The role of technologies in overall security strategies differs depending on the security objectives that have been defined.

Information security

Information security is not confined to computer systems or to information in an electronic or machine-readable form. It applies to all aspects of safeguarding or protecting information or data, in whatever form (Pfleeger and Pfleeger 2003). As a concept,

[22] See more on the Electronic Privacy Information Center, www.epic.org

information security is problematic to work with. People use the term security in many ways in their daily lives. Security can be regarded as a context-dependent concept: its meaning is defined by the context in which it is intended to be used. Here are some examples:

i) Information security is the protection of information systems from unauthorised access to or modification of information, whether in storage, processing or transit, and from the denial of service to authorised users or the provision of service to unauthorised users, including measures necessary to detect, document and counter such threats (Bishop 2004).

ii) Computer security[23] is the process of creating a secure computing platform, designed so that users or programmes cannot perform prohibited actions but can execute the actions for which they have permission. The actions in question are operations of access, modification and deletion (Gollman 2001).

iii) Network security[24] is the protection of networks and their services from unauthorised modification, destruction or disclosure and provision of assurance that the network performs its critical functions correctly and that no harmful side effects will occur. Network security typically includes providing for data integrity (Kurose and Ross 2002).

The key problem in defining security is the inherent fuzziness of the concept. Most security measures also involve compromise. If you want to be safe from poisoned cigarettes, you must also accept that you will lose access to free cigarettes from strangers. If you want to be even safer, you must stop smoking. Security has to be compared and contrasted with other related concepts such as safety, continuity and reliability. The key difference between security and reliability is that security must take into account the actions of active malicious agents attempting to cause destruction. A simple and clear definition of effective security might be: a secure system is a system which does exactly what is desired and nothing that is unwanted, even when someone else tries to make it behave differently (Anderson 2001*a*).

In the context of this report and its objectives, security is examined in a digital setting represented by both computers and networks. From here on, security will be treated in the context of information security. Although information security is by no means strictly a technical issue, its technical aspects (firewalls, encryption and the like) play a key role. Information security is an increasingly high-profile problem as hackers, malicious actors and rival competitors take advantage of the fact that organisations are opening parts of their systems to employees, customers and other businesses via the Internet.

Most definitions of information security tend to focus, sometimes exclusively, on specific usage and/or particular media, for instance "protect electronic data from unauthorised use". In fact, it is a common misconception that information security is synonymous with computer security. The various guises of computer security – computer and network

[23] Computer security is not a synonym to information security, but can actually be regarded as a subset to information security, because the concern is the security of information in some form (electronic in this case).
[24] Network security can, in conformity with computer security, be regarded as subset to information security.

security, ICT security, information systems security and ICT security – each has a different emphasis. The common concern is the security of information in some form (electronic in these cases). Hence, all are subsets of information security.

Conversely, information security covers not just information but all infrastructures that facilitate its use: processes, systems, services, technology, and so on. These include computers and voice and data networks. It is a central point that information security is neither hermetic nor watertight nor perfectible. No one can ever eradicate all risk of improper or capricious use of information. The level of information security sought in any particular situation should be proportional to the value of the information and the loss, financial or otherwise, that might accrue from improper use: disclosure, degradation and denial. Bruce Schneier (2000) makes the point that information security is about risk management. Three widely accepted elements (or services) of information security are (Gollman 2001, Bishop 2004):

i) Confidentiality: prevention of unauthorised disclosure of information
ii) Integrity: prevention of unauthorised modification of information
iii) Availability: prevention of unauthorised withholding of information or resources

Other aspects might also be included. For instance, some regard authentication, non-repudiation and privacy to be relevant security services of computerised systems (Gollman 2001). Exactly which service to include in a security strategy depends on the overall underlying purpose, the risk factors involved and the nature of the asset that requires protection? Figure 5 shows the relationship between the three typical concepts that define security. A balanced combination of the three terms normally results in system/computer control, which suffices for security (Pfleeger and Pfleeger 2003). This implies trade-offs between the services. Certainly, the vulnerabilities and threats of the particular computing system under review must be analysed.

Figure 5: The relationship between the three goals of information security

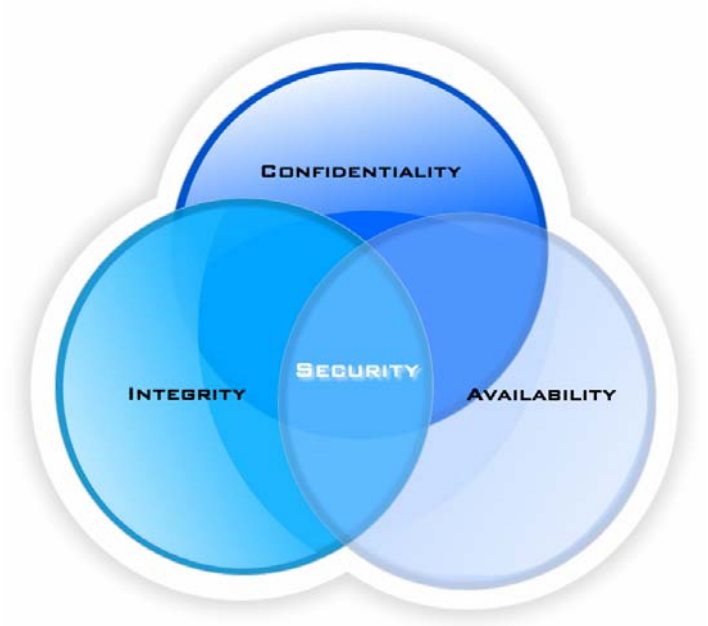


Diagram: IKED 2006

Information security consists of two principal processes. In the ideal scenario, these are conducted in the order in which they appear below:

i) *Risk analysis*. This is the process of defining what asset/information to protect and, more essentially, why. This topic will be returned to in Section 2.4.

ii) *Protection*. This process involves choosing, implementing, maintaining and evaluating the best possible means of protection. In short, protection is about safeguarding. Typically, protection is a process that involves three separate sub-processes (Gollman 2001):

- Prevention. Take measures that prevent assets from being damaged. This means that an attack will fail. Typically, prevention involves implementation of mechanisms that users cannot override and that are trusted to be implemented in a correct, unalterable way so that the attacker cannot defeat the mechanism by changing it. Preventive mechanisms are often cumbersome and interfere with systems to the point that they hinder normal use.
- Detection. Take measures that allow for detection of when an asset has been damaged, how it has been damaged and who has caused the damage. Detection mechanisms accept an attack because the objective is to identify

its launch and report it. Typical detection mechanisms monitor various aspects of a system and search for information indicating an attack.

- Response/reaction. This process has two forms. First, to stop an attack and to assess and repair any damage caused. This involves identification and overhauling the vulnerabilities used by the attacker to enter the system. In the second form the system continues to function normally while an attack is under way. This type of recovery is generally difficult to implement due to computer system complexity. In summary, this process deals with taking measures that allow for recovery from damage to assets.

Privacy

When designing ICT systems and online services to which illegitimate actors may gain control of personal and sensitive data it is vital to heed individuals' right to privacy – "the right to be let alone" (Warren and Brandeis 1890). Privacy violations occur in numerous forms throughout the Internet (Garfinkel 2001, Fischer-Hübner 2000). A large number of privacy-invasive and malicious software which can give an attacker a truly alarming degree of control over systems, networks and data is readily available for downloading, execution and distribution. Malware can be distributed and planted without the awareness or control of users, system administrators, companies and organisations. This provides opportunities for malicious actors to control an alarmingly large share of the Internet community.

Privacy is the ability of a person to control the availability and exposure of personal information (Schneier and Banisar 1997). Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of, privacy in the collection and sharing of data (Salomon 2003). Privacy problems exist wherever uniquely identifiable data relating to a person or persons is collected and stored in digital form or otherwise (Fischer-Hübner 2000). Improper or non-existent disclosure control can be the root cause of privacy issues (Rotenberg 2002). The most common sources of data affected by privacy issues are health, criminal justice, financial and genetic information (Garfinkel 2001). The challenge is to make data available while still protecting the personally identifiable information. Privacy as a phenomenon is composed of a variety of aspects that can exist on different levels at the same time (Jacobsson 2004). Thus, privacy is problematic to capture and define, making the context in which it appears greatly important. It may be given this working definition:

> *"Privacy is the claim for individuals to determine for themselves when, how and to what extent personal information is communicated to others."*
>
> Alan F. Westin (1967)

From a general perspective, the definition of privacy is typically not limited in scope as a right for individuals, but also as an entitlement of institutions and/or groups of individuals (Westin 1967, Fischer-Hübner 2000). However, this report has chosen a narrower approach. Considering the existing definitions of privacy and the context in which they are normally used, it may be contradictory to claim that privacy is a right for institutions since

they are usually the beneficiaries of access to personal information about individuals (Jacobsson 2004).

In the legal area, several regulatory frameworks exist to ensure individuals' right to privacy.[25] Ensuring privacy through legal frameworks is problematic since the criteria for privacy protection are often based on the legal view of privacy in a particular country, whereas enforcing personal privacy in information networks is a global consideration. Opinions vary between countries on where the boundaries for privacy invasion should be drawn. Also, it is seemingly more difficult to police the data shadow cast by individuals than it is to protect the data. To this day, the Code of Fair Information Practices (FIP) is said to constitute the most significant Western thinking on computers, privacy and legal frameworks (Garfinkel 2001). The FIP is based on five principles (1973):

i) There must be no personal data record-keeping systems whose very existence is secret.
ii) There must be a way for a person to find out what information about him/herself is on record and how it is used.
iii) There must be a way for a person to prevent information about him/herself that was obtained for one purpose from being used or made available for other purposes without his/her consent.
iv) There must be a way for a person to correct or amend a record of identifiable information about him/herself.
v) Any organisation creating, maintaining using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take precautions to prevent misuse of the data.

Other privacy frameworks are constructed more or less in consensus with the FIP. However, voices have called for the FIP to encompass a further statement. Since it is user information that is in focus, it should be a right for a user to be able to erase his/her own personal data from the database in question. So far, the business community appears to have paid little heed to this request.

2.3 IDENTIFICATION AND AUTHENTICATION

In this section the primary focus is on authentication. In order to comprehend the issues and opportunities on that topic, other aspects must also be addressed. Apart from information security, risk analysis and privacy, validation and identification aspects are also relevant.

[25] See for example the "EU Directive on Privacy and Electronic Communications" or the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data".

Identification

Identification is the process by which the identity of an individual or organisation is established. In other words, that it is established that the individual or organisation is truly represented. In the digital world, identity is embedded in the definition of personal data:

> "*An identifiable person is one who can be identified, directly or indirectly, by means such as an identification number or by other factors specific to his physical, physiological, mental, economic, cultural or social identity.*"
>
> European Commission (1995)[26]

In the real world, various national mechanisms for identification are provided, and practices continue to evolve. In Sweden, the use of social security numbers, in combination with passports and identity cards issued for a broad range of government and private services, is widely accepted and viewed as a key to high levels of precision in identification. In many countries, such as the UK and Germany, there are, however, significant concerns about privacy and these have resulted in alternative means of identification that are seen as less intrusive.

On the Internet, the traditional definition of identity is challenged. ICT use tends to fragment identity and produce partial identities. This raises challenges in overcoming the gap between a physical subject and the information which defines the identity. Historically, this has been addressed through the use of tools such as a picture, fingerprint or national "trusted" ID card, for instance passports, drivers' licences and so on. The focus has now shifted from trusting the individual to trusting the identity support/platform presented and to the definition, design and value of these platforms.

On occasions when the identity of an individual *per se* is less interesting to manage than the actions (which are determined by the appointed role of the individual) performed by these individuals, it is preferable for identity management to remain role-based. Within many organisations, roles are created for various work functions. The permission to perform some operations may then be assigned to specific roles. Members of staff (or other system users) may be assigned particular roles through which they acquire permission to perform particular system functions. The concept of *role based identity*[27] has fostered debate on how to design authentication systems that provide access, document signing or proof of transactions. The discussion is considered by some as pointless because there will always be a person behind a transaction and, accordingly, all authentication mechanisms can be tied to a personal identity (Salomon 2003). In some cases, individuals want online credentials to remain *anonymous*. In other cases, a company wants specific processes to be ongoing regardless of the staffing situation and is consequently less interested in switching authentication credentials only due to a shift of personnel. Yet other companies want to

[26] European Commission Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (art. 2 a).

[27] Role-based identity management is closely related to the Role-Based Access Control (RBAC), which deals with assigning certain permissions to certain persons, not based on who they are, but what role they are representing.

issue authentication credentials for employees or visitors, although they may be uninterested in the person's identity outside of his/her specific work task.

The growing use of ICT for social and economic transactions has created pressure for new forms of identification and authentication. However, traditional methods are still being used for new applications even though they may be inadequate, mainly because of lack of confidence in the new forms of digital identity support. A range of human characteristics used for real life identification, such as human behaviour and biometrics, will be reflected in electronic identification and some of them will possibly replace traditional information such as name, address and telephone number.

The new solutions will face challenges in respect of proof, theft, loss of identity and multiple identities and will represent attractive targets for illegal activities, generating new risks that have to be identified and controlled. These risks will be exacerbated by the increasing pervasiveness of interconnected computing devices. The Internet is growing at increasing speed and witnessing the addition of domestic and mobile networks and the multiplication of new network access technologies. This convergence is making the individual the primary entry point to services, which in turn indicates that identity management will be the key to accessing the information society.

Authentication

Authentication is the process by which a party attempts to confirm that another party from whom he or she has received some communication is, or is not, who he or she claims to be (Smith 2002). Computers use authentication to confidently associate an identity with a person. Authentication is one of the basic building blocks of security (Bishop 2004). A well-designed authentication system allows users to prove their identities conveniently and gain access to the network without threatening the organisation's security. For example, most systems distribute passwords to authorised users to allow the system to distinguish between legitimate users and others. The passwords and other authentication mechanisms used with today's computers cover a broad range of techniques and technologies.[28] Website designers, e-commerce planners, and other system developers must choose from numerous products and make numerous configuration decisions with each product. Systems like Windows by themselves incorporate several password alternatives to provide interoperability with other products. Some organisations need the extra security of smart cards or authentication tokens.

Regardless of whether an authentication system is computer-based or not, several elements are normally present, and certain things usually take place (Smith 2002). See Table 2:

i) First, a particular person or a group of persons will be authenticated;
ii) Next, a distinguishing characteristic is needed that differentiates that particular person or group from others;

[28] See Section 3.5.

iii) Third, the presence is required of a proprietor who is responsible for the system's management and who relies on mechanised authentication to distinguish authorised users from other parties;

iv) Fourth, an authentication mechanism is needed that verifies the presence of the distinguishing characteristic; and

v) Finally, some privilege is granted when the authentication succeeds by using an access control mechanism. The same mechanism denies the privilege if authentication fails.

Table 2: Examples of the five elements in an authentication system

Authentication element	*Ali Baba and the 40 thieves*	*Password login*	*Teller machine*	*Web server to client*
Person, principle, entity	Anyone who knew the password	Authorised user	Owner of a bank account	Website owner
Distinguishing characteristic, token, authenticator	The password "Open Sesame"	Secret password	ATM card and PIN	Public key within a certificate
Proprietor, system administrator, owner	The 40 thieves	Enterprise owning the system	Bank	Certificate authority
Authentication mechanism	Magical device that responded to the words	Password validation software	Card validation software	Certificate validation software
Access control mechanism	Mechanism to roll the stone from in front of the cave	Login process, access controls	Allows banking transactions	Browser marks the page "secure"

Source: Smith (2002)

The problem of authorisation is often thought of as identical to that of authentication. Many widely adopted standard security protocols, obligatory regulations and even legislation are based on this assumption. However, in many cases these two problems assume different shapes. One familiar example is that of access control. A computer system which has been designed to be used only by those who are authorised must attempt to detect and exclude the unauthorised. Access to it is therefore usually controlled by insisting on an authentication procedure before access is granted (Bishop 2004, Smith 2002). Although the problem of authenticating people poses a real challenge to computer systems, they are not the only entities that need authentication. For instance, there is also a need to authenticate unattended computer systems like web servers involved in monetary transactions between consumers and businesses.

Note that much of the discussion on these topics is misleading because terms are used without precision. Part of the confusion may be due to the legal tone present in much of the debate. Tricky issues lurk under what appears to be a straightforward surface. True identification over the Internet is extremely complicated and normally the only possibility is to apply one or more tests which, if passed, have been previously declared as sufficient to continue. The problem is to determine which tests are sufficient; several have proven to be

inadequate. Still, a lot of people continue to regard the tests, and the decision to regard success in passing them, as acceptable and blame failures on sloppiness or incompetence on the part of an individual. However, it is the test which has failed in such cases because as it did not work in reality. Consider the common case of a confirmation email which must be replied to in order to activate an online account of some kind. Since email can easily be arranged to go to or come from false and untraceable addresses, this is just about the least-reliable authentication possible. Success in passing this test means little, with no regard to sloppiness or incompetence.

Certain risks are involved in digital transactions. These can be estimated from previous experiences of how often they have arisen or the size and consequences with regard to the losses involved. Some systems are more secure than others, though none is totally secure. However, there is a balance to be found between the costs of a system and how secure it needs to be. It should be borne in mind that fraudulent behaviour also occurs in the non-cyber world and has not prevented transactions from taking place. In many countries, a signature or other classified information is considered safe to send by fax even though many experts regard fax machines as less technically secure than Internet-based applications.

In the early stages of the Internet, service providers recognised identification and authentication as key obstacles to the enabling of more online services. Much of the literature on digital transactions and security focuses on identification and authentication. While clearly representing central components, they are not the sole parts requiring attention in order for orderly routes for digital transactions to be established. Most industrialised economies have implemented or begun to implement some sort of national infrastructure for digital identification, using asymmetric encryption methods.[29] Such technology, which many scholars have considered sufficiently secure, may not be appropriate, effective or applicable in all situations. There is a need to address organisational, economic and legal aspects to overcome recurrent issues of insecurity and distrust. These are aspects that will be examined in section 2.6.

2.4 RISK ANALYSIS

Risk analysis is broadly defined to include risk assessment, risk characterisation, risk communication, risk management and policy relating to risk (Bishop 2004). Managing information security risks is very different from managing risks in traditional markets like the financial market (Peltier 2001). In today's highly connected environment, survival and growth involve managing a whole range of risks posed by external stakeholders.

A risk is the combination of the likelihood and the consequence of a specific hazard being realised (Peltier 2001). Or more delicately expressed: "Risk is an action that leads to one of a set of possible specific outcomes, where each outcome occurs with a known probability" (Luce and Raiffa 1957). Risk is therefore the product of the probability that an adverse effect or event will occur under specific circumstances and the probability that those

[29] See further section 3.2.4.

specific circumstances will happen. In quantitative terms, risk is typically expressed in values ranging from zero (the certainty that harm will not occur) to 1 (the certainty that harm will occur). However, this quantitative approach is seldom useful in analysing risks conveyed by Internet participation. The definition of Luce and Raiffa implies that the probability that an adverse event will occur and the probability of those specific circumstances should be known. This is, however, hardly the case in a setting as complex as the Internet. It is possible to compile data on threat realisation, but numerous numbers and types of impacting factors and their importance remain unclear. There are simply too many uncontrollable parameters available, while risks are changing by the day amid the constant emergence of new challenges. Even though it is virtually impossible to predict the future by utilising quantitative risk analysis, risk analysis generally plays a vital role. A range of organisations need to work systematically on generating better-founded knowledge and awareness about the risks, vulnerabilities and threats they face in the digital world (Bernstein 1998). On that basis, better informed decisions can be made.

Risk analysis is the process of defining what asset/information to protect and, more importantly, why. The objective is to mitigate risks to an acceptable level (Peltier 2001). A thorough risk analysis is a tool for preventing redundant expenditure, keeping expenditure on corrective measures at a sensible level. Risk analysis is a process for assuring efficiency and productivity in the security strategy, and for ensuring that security requirements match overall business objectives.

Risk analysis can be undertaken in numerous contexts, at many levels and with varying degrees of complexity. It is a generic concept that can be utilised to explore the actual need of a project, system or investment (Peltier 2001). Often, risk analysis is corporate managers' method for understanding and ensuring security. By reviewing and controlling the vulnerabilities, risks and threats relevant to an organisation, an acceptable level of security can be obtained. In reality, risk analysis is the key to enabling strategic security management. Many organisations conduct risk assessment methods based on the Technical Report ISO/IEC TR 13335-3 of 1998, entitled *Guidelines for the Management of ICT Security* (GMITS), published by the International Organization for Standardization, or derivatives thereof. ISO/IEC TR 13335 provides guidance on safeguards, taking into account business needs and security concerns. It describes a process for the selection and implementation of safeguards according to security risks and concerns and the specific environment of an organisation. One of the most influential standards on information security management systems is BS 7799,[30] which guides organisations on how to identify, manage and minimise risk related to information systems. This standard has earned much respect worldwide and both national and international standards have sprung from it.[31] One of the reasons is the holistic perspective on information security matters that is attributed to it through its description of organisational, economic, legal and technical aspects. In 2000, BS 7799 became a global standard (ISO 17799) that gives recommendations to information security managers. ISO 17799 is intended to provide a common basis for developing organisational

[30] See http://www.bsi-global.com/HigherEducation/Information_Security/intro.xalter, for more information.
[31] See, for instance the Swedish SS 17799 or the international variant ISO 1 77 99.

security standards and effective security management practice and to provide confidence in inter-organisational dealings. This standard has been upgraded by the ISO/IEC 17799:2005. The standards have nevertheless been criticised for being too general, too expensive and overly focused on goals that need to be fulfilled instead of methods for achieving them. Even though the criticisms may be partially justified, BS 7799, ISO 17799 and their offspring are valuable efforts since they can be applied in any organisation regardless of size, business activity or requirements. These standards may be regarded as risk-driven managerial tools fit for private as well as public organisations on both international and national levels. In the end, the results are increased risk awareness among decision-makers and personnel, and a more thorough level of security in organisations.

When it comes to the application of risk analysis, numerous models, methods, tools, processes and frameworks are available to choose from. This abundance of options makes it a challenge to know which tool or method to adopt. Selecting the right one depends on what asset or object is going to be reviewed and the context in which it is intended to function. Yet even knowing all these factors in advance, it is still a challenging task. Having an understanding of the nature of risk analysis helps and often suffices for making the right choice. In most risk analyses, the method more or less remains the same (Peltier 2001):

i) Identify the information asset to be reviewed;
ii) Ascertain the threats, concerns or issues in respect of that asset;
iii) Prioritise the risk to determine the vulnerability of the asset to the threat;
iv) Choose which corrective measures, controls, safeguards to implement or accept the risk; and
v) Monitor and assess the effectiveness of the measures, controls and safeguards.

A number of governments are providing guidelines for risk analysis and which authentication method to choose based on this analysis. These recommendations vary in complexity from relatively simple and straightforward models, as provided by the Swedish Agency for Public Management[32] (which divides risks into three levels with few explanatory factors), to more complex versions, like the Australian Government's e-Authentication Framework[33] (which provides a risk analysis framework that divides risks along the lines of outcome and damage resulting from a security breach into four levels). Another equally usable version is the US National Institute of Standards and Technology's E-Authentication Guidance for Federal Agencies[34] and the supplementary Electronic Authentication Guideline[35] that also defines four authentication levels. Levels are classified in terms of the consequences of the authentication errors and misuse of credentials. When determining assurance levels, it is recommended that agencies follow a process to identify the potential risks, their likelihood of occurrence and costs arising from failure based on the potential impact of an authentication error on:

[32] Statskontoret (2000)
[33] http://www.agimo.gov.au/infrastructure/authentication/agaf/overview
[34] http://csrc.nist.gov/policies/m04-04.pdf
[35] Burr, W. E. et al. (2004)

i) Inconvenience, distress or damage to standing or reputation;
ii) Financial loss or agency liability;
iii) Harm to agency programmes or public interests;
iv) Unauthorised release of sensitive information, personal safety; and/or
v) Civil or criminal violations.

Risk analysis is one of the key processes for defining an appropriate security and authentication structure for a company or government organisation. However, the risk analysis in itself is not sufficient to decide which system to use because other factors need to be considered: availability, privacy, legal requirements, user friendliness, possible mobility needs, transaction volume and so on. All these factors together affect the decision about which solution to use. This will be explored further in the ensuing chapters.

2.5 TECHNOLOGICAL ASPECTS

Electronic identification has been possible ever since electronic means of communication, such as the telephone and the Internet, first emerged. For example, identification can be based on the link between a caller and his phone number or on the association between the email address and the sender. Over time, the identification techniques available have evolved as responses to risks and challenges. They have become more sophisticated and a range of them are now widely used. Also, the business models being applied demonstrate disparities in design and cost structures and should reflect customers' demands. This has not always been the case, though. Some PKI installations, for instance, have been clearly excessively supply-driven.

It should be kept in mind that current technologies are considered sufficient to provide the required security level. Many customers are currently content with the security mechanisms provided by companies like Visa and MasterCard when using credit cards. Protection for email messaging is also apparently regarded as generally sufficient. Even lawyers send classified material over the SMTP protocol, although in reality sending email messages is like sending postcards: they can easily be read by anyone.[36] However, security-enhancing email software such as Pretty Good Privacy (PGP) now exists to lower the risk of confidentiality and integrity breaches.[37] While it is vital to identify the relevant systems for the users' needs, there is a need to define the levels at which users appreciate the system as being safe enough for use it and also what requirements apply.

A diverse range of e-identification mechanisms are in current us and a multitude of sectoral (banking, health, government) and geographically located (national, regional) identification card schemes have emerged. This section will explore and try to structure the available technologies. Section 3.1 will provide a more in-depth picture of available services in the

[36] Simple Mail Transfer Protocol (SMTP) is a protocol for sending electronic mail messages between computers.
[37] For further reading, see Section 4.2.

sample countries for this report and Section 3.2 will highlight the most widespread global initiatives.

Digital and electronic signatures

Digital and electronic signatures are common means of security and privacy enhancement. In cryptography, digital signatures are a method for authenticating digital information and often treated as analogous to a physical signature on paper. The two types of signatures show similarities and dissimilarities. A *digital signature* is one sort of electronic signature that uses cryptographic transformation of data to provide the recipient of the data with proof of the origin and integrity of the data and protect it against forgery. The term *electronic signature*, though sometimes used for the same thing, has a distinct meaning. It refers to mechanisms for identifying the originator of an electronic message and it is not necessarily cryptographic. Hence, an electronic signature is data in electronic form that is attached to or logically associated with other electronic subject data and serves as a means for authentication. The definition includes scanned images, signatures produced by devices to capture a hand-written signature and digital signatures.[38]

A digital signature is in itself simply a sequence of data conforming to one of a number of standards. It is the generation of this data, and the interpretation at a later time or place, and the cryptographic protocols and algorithms used to govern both which give a digital signature bit-sequence meaning, in contrast to just any sequence of data. Most digital signatures rely on public key cryptography. This method depends on the fact that anyone can transform a message into *ciphertext* using a public key, but that a matching private key is needed to reverse that transformation. A vital feature of public/private key pairs is that their functions are interchangeable. A message encrypted with the public key can only be decrypted with the private key, whereas a message encrypted with the private key can only be decrypted using the public key. It is this feature that digital signatures are based on. The ciphertext message is the digital signature for a message because anyone can use a public key to verify that the private key holder created it.

Authentication techniques

Authentication techniques are often based on cryptographic algorithms. A number of technologies exist for authentication, as presented below. The methods are broadly divided into four categories, based on:

i) Evidence of what an actor *knows* (for example, a password, a pass phrase or a personal identification number)
ii) Evidence of what an actor *has* (such as ID card or token)
iii) Evidence of what an actor *is* (such as fingerprint, retinal pattern or other biometric identifier)

[38] In common law, such electronic signatures have included cable and Telex addresses, as well as FAX transmission of handwritten signatures on a paper document. For example, see Cloud Corp v Hasbro in the US legal cases section (Section 3.1.10).

iv) Evidence of what an actor *does* (for example, a dynamic biometric identifier such as voice pattern or signature recognition) [39]

Systems that can use only one of the techniques are commonly referred to as one factor authentication, of which an example is typing in a password on a website. By contrast, two factor authentication is when the user provides two of the methods, such as inserting an ATM card in a teller machine and then typing a password. Security increases with the number of factors required, but the usability for the end-user decreases.

Figure 6: Identification technologies' relationship between security and costs

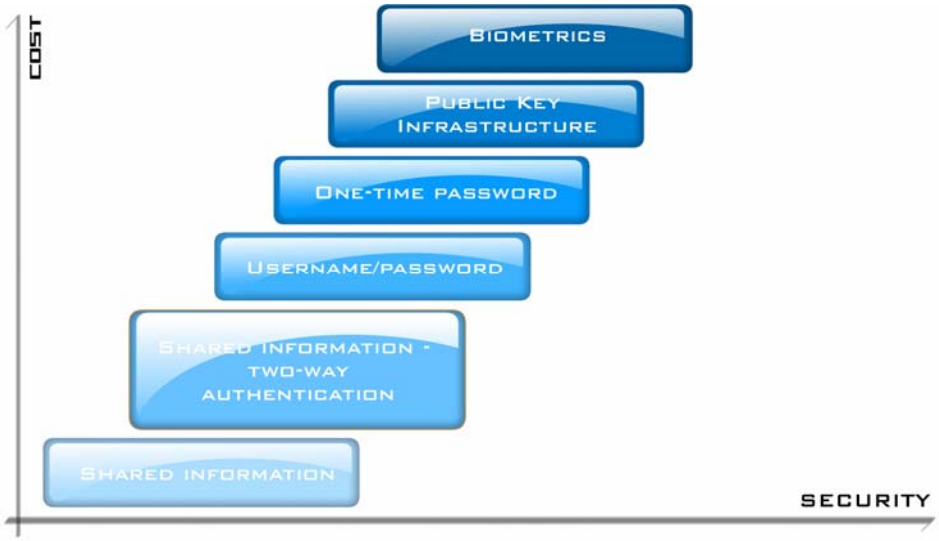


Diagram: IKED 2006

Historically, fingerprints have been used as the most authoritative method of authentication. Recent court cases in the US and elsewhere demonstrate, however, that its reliability is doubtful. Other biometric methods, such as retinal scans, show great potential but have not been fully developed, and/or have experienced fraud-related problems. However, cryptographic methods, such as digital signature and challenge-response authentication, have been developed and are currently not spoofable (forgeable) if the originator's key has not been compromised.[40] It is also common to use a combination of

[39] Adams and Lloyd (1999).

[40] That the originator (or anyone other than an attacker) knows (or does not know) about a compromise is irrelevant. It is not known whether these cryptographically based authentication methods are provably secure since unanticipated mathematical developments may make them vulnerable to attack in the future. If that were to occur, it may call into question much of the authentication in the past. In particular, a digitally signed contract may be questioned when a new attack on the cryptography underlying the signature is discovered.

technologies to raise the level of security, such as a credit card and a personal identification number (PIN).[41]

The most common technologies used for identification are introduced below: *shared information, username/password, one-time passwords, public key infrastructure (PKI) and biometrics*.

Shared information

To be authenticated an actor needs to correctly answer a question or a series of them, posed by a counterpart. Normally, the question concerns some secret information shared by the two actors. For the purpose of Internet transactions, it is common to use a more sophisticated approach, namely two-way authentication, whereby both the user and the system must prove knowledge of the shared secret without it being transmitted clearly over the communication channel. Typically, the secret information is any of three types:

i) Fixed data on file (for example, date of birth)
ii) Variable data (for example, date and amount of last payment/receipt/claim)
iii) Specifically designed shared secrets (where the user provides a series of questions and answers to the counterparty).

Username/password

An actor is authenticated by presenting a username and a password or pass phrase (a combination of words or a PIN, which is a numeric value used in certain systems to gain access). This method has previously been used mainly for lower-risk applications but it is becoming more widely used in higher-risk applications, especially in conjunction with another authentication mechanism such as shared information.

One-time password

Another technology considered more secure and commonly used for Internet banking is the one-time password system. It is a system demanding unique and different passwords each time an application is accessed and a separate hardware device that generates the unique password to be provided together with the username. Users are required to pre-register with the service provider to acquire the username and the hardware device. When accessing the online service, the user will be asked for the latest password provided by the device and the service provider will know which password is valid at that time for that user.

Public key infrastructure

PKI is a method for enabling users to authenticate their identity and to exchange information securely.[42] Central to a PKI is a trusted third party authority known as a certification authority (CA), which provides the users with public and private keys and a

[41] A personal identification number, i.e. a number entered into computer and/or telephone systems to authenticate the user.
[42] http://www.pkiforum.org/; http://www.pki-page.org/; http://www.pkilaw.com/

digital certificate. The CA links the public key to the digital certificate and vouches for the key holder's identity. The CA is in regular contact with a registration authority (RA) that collects evidence of the user's identity. If issues of concern have been indicated the RA will revoke the certificate from its list of approved identities. Certificates can be either soft keys (a piece of software on a computer) or hard keys that are stored on smart cards or in a token.

The user holds a public key available to everyone and a private key to encrypt information in order to prove the authenticity of the sender and the integrity of the information sent. The receiver of an encrypted message verifies it by comparing it with the sender's public key. If a message has been altered or another actor tries to impersonate the user the recipient will be unable to read the encrypted message or validate the signature. This provides secure information flows with a high level of non-repudiation between actors in PKI systems.

PKI is not only a digital technology, but requires secure physical organisation as well. In a global system for digital transactions, PKI is required to support the following services:

i) Registration, storage and maintenance of public keys owned by users of the service.
ii) Retrieval and delivery of public keys of participants.
iii) Archiving and retrieval of public key certificates for the lifetime of the documents to which they refer, in order to serve as evidence in the case of conflict.
iv) Authentication (or verification) of the ownership of specific public keys.
v) Creation and distribution of public/private key pairs and symmetric keys to users.
vi) Recovery of lost keys, revocation of stolen keys and, where appropriate, the provision of facilities for access to keys for law enforcement purposes (key escrow).

Biometrics

Biometrics is a group of technologies used for authentication that measure and compare a person's physiological or behavioural features. The generally used features are human physiological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements. A rarer route is to use recognisable behavioural characteristics, such as signature, gait, voice and typing. A biometric identifier can be used in a similar way to passwords to demonstrate ownership of a token or a smartcard.

It appears that encrypted validation technology alone is not sufficient for actors to engage in digital transactions over the Internet. Also, there appear to be organisational issues, such as the need for a trusted party. Actors tend only to engage with counterparties that have a certain degree of familiarity. For instance, it is easier to engage in transactions with the

familiar national bank than an unknown foreign one. A third party may also be needed when two actors are about to engage in a transaction such as a contract signing. In a case of conflict, it is important to be able to provide evidence of the actions that have taken place. This can be performed by an independent third party. Such organisational issues will be briefly explored in the next section.

2.6 ORGANISATIONAL ASPECTS

This section addresses the central aspects of how an authentication process is organised. Issues examined include how the physical infrastructure around the software system is set up, the size of the bank vaults that store the servers, physical security guards, and storage time for recorded transactions. Other topics considered relate to whether the authentication process is centralised or decentralised, the type of business model employed, availability, how trust is achieved, and how the number of actors involved affect the outcome.

Centralised and decentralised systems

In a *centralised* system, all personal user data (name, gender, and so on) from a profile is stored in a server not controlled by the user. One such system is Microsoft Passport, which acts as a gateway to numerous services such as those of Microsoft and Amazon.[43] Microsoft Passport offers a single sign-on service that offers users a convenient way to gain access to a system. This is also an attractive route for Microsoft, which can gather information and fees from users and sell the authentication service to other companies which sell online services. This kind of setup also offers advantages from a usability perspective but poses challenges in terms of privacy and how to handle international transactions from a legal perspective because the centralised entities may not come from the same legal jurisdiction. Furthermore, privacy issues stem from users' difficulty in monitoring or verifying that the identity provider respects local and international privacy laws. A centralised system is also likely to be a more susceptible target for malevolent attacks. This is in part because it may be slower in adjusting, and in part because it tends to gather all relevant data for numerous users in single locations and provide opportunities for theft of complete profiles with greater potential for misuse.

A *decentralised syst*em, on the other hand, provides storage and the processing of personal data under user control. Access to systems is arranged through PCs, PDAs, smart cards, tokens and mobile phones with an integrated identity management tool (which can be software or hardware). The access key and personal information is stored locally. The protection and possible diffusion of the user's data in these types of system are under personal control, which is a clear advantage with respect to the user's right to privacy.

The design of authentication systems is also linked to the character of the transactions undertaken. In a centralised system, *bilateral transactions* tend to be characterised by a top-down perspective, marked by an asymmetric power distribution between the actors involved. One example is the interaction between users attached to a certain bank, where

[43] eBay used to utilise Microsoft passport but has now launched a proprietary system.

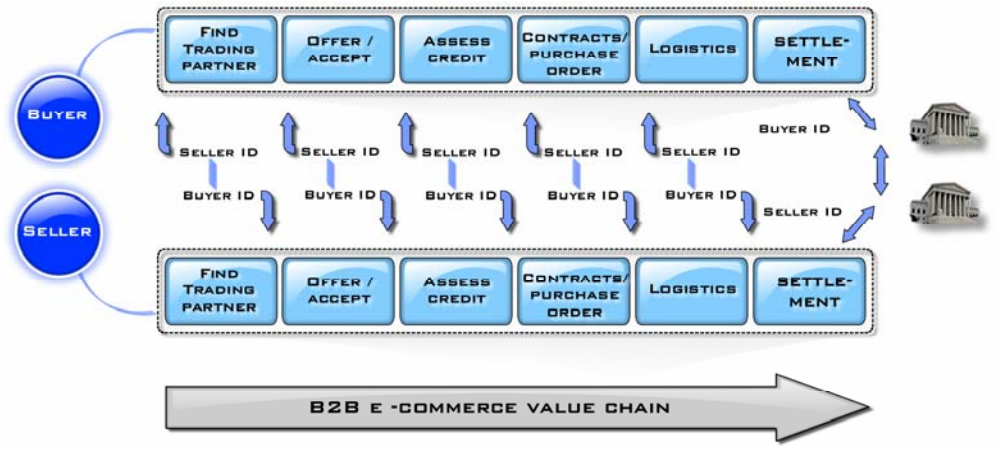
the latter controls the infrastructure. Bilateral transactions in a decentralised system are generally characterised by symmetric powers between the actors involved, but it is often logical to involve a *third party* actor to overcome distrust. While technologies such as cryptography may be used, it can be hard to provide good and secure schemes in a bilateral mode without the presence of a third party. Hence, it is likely that these technologies will tend to be used for transactions with lesser security needs.

In the case of symmetric relations within a decentralised system, it is often beneficial to involve a third party for security purposes. A local trading house or chamber of commerce can interact between two companies that want to engage in a businesses transaction and overcome the first hurdle of sorting out which actors to engage in business. A bank can handle payments between a buyer and a seller, as is the case with credit card systems. This is one of the most frequently used models for online transactions. In many cases, governments have started to issue different kinds of eIDs connected to certificates and identities.

Trust

The identity is a vital part of, and represents, a useful starting point in a business exchange, as shown in Figure 7. At the same time, it is generally insufficient for completing a business exchange. It is also central to acquiring trust in, and knowledge of, whether the counterpart is authorised to represent the interests he claims to represent, and that he indeed will be able to provide services as promised.

Figure 7: Trust is required in each step of a business-to-business relationship



Source: SWIFT (2002), http://www.swift.com/index.cfm?item_id=41792
Diagram: IKED 2006

In traditional business relations, actors have developed the means to overcome risks and create trust. These means in many cases go back generations or more, spanning cultural

traits, body language and other factors (Arrow, 1974; Bjerke, 1999). Trust is, however, not an empirical asset that you have or do not have but something that is gradually built up or lost. Actors can themselves be trusted to a certain degree on account of their reputation for trustworthiness from previous transactions. But trust is also fostered through interactions between multiple actors. These may start out with lesser engagements which are then gradually expanded over time.

For trust between actors in the digital world, the behavioural side is important in order to continuously prove trustworthiness in action. Actors are furthermore required to show they have adequate means to protect themselves and the transaction, meaning that they have a proper security setup. This includes technology such as firewalls and anti-spam software as well as evidence of a policy on how the actor treats data and ensures security and privacy protection in compliance with legal requirements.

Trust and possibly also a recognised trustworthy brand may be preconditions for actors to use an authentication solution, as explained by the discussion on *asymmetric information*. Akerlof (1970) provides key insight on this issue, describing in his paper on lemons a town that has 100 used cars for sale. There are 50 good ones worth US$2,000 each and 50 lemons worth US$1,000. In the absence of any specific means to distinguish between the two categories, the mean price of used cars in this town might be inferred to be US$1,500. But if this it is so, no good cars will be offered for sale and prices will slowly deteriorate. However, by introducing a fixed brand for the good vehicles, such as "Volvo certified used car", price levels can be maintained. Similarly, in markets for authentication provision there may be a need for recognised trustworthy actors to provide the solutions. It is much harder for a non-established actor with limited financial resources to establish itself as trustworthy enough for consumers or companies, which are frequently risk-averse, to start using them.

Trust-related issues are often overcome by the use of a (trusted) *third party*, such as a bank, a chamber of commerce or local trading house that can assist in sorting out and finding appropriate partners for payments, transportation, risk handling with escrow services and insurance. A third-party actor can also facilitate digital transactions by time-stamping transactions and providing this as evidence in a later case of conflict – a service provided by notaries and chambers of commerce. Banks can hold payments until certain criteria have been met in escrow processes. In non-digital relations, the engagement of trusted third parties is particularly developed in some industries and cultures. Southern Europe and East Asia offer multiple examples. In industries such as banking, telecoms or energy, specific practices have developed around institutions that are engaged in continuous relations with multiple actors. In the digital world there are centralised systems, such as the Microsoft Passport, and decentralised systems where third parties such as chambers of commerce function as intermediaries and can provide references for either party and time-stamp evidence in respect of transactions.

Business model

Business and organisational models are essential for the success and proliferation of services. Not all actors choose to set up their own authentication system, preferring instead to buy the service from, say, banks, postal services, dedicated CAs or telecommunications providers. The type of service that interests actors depends partly on the number of transactions and willingness to assume risk. For example, a company that has a high number of transactions per day will probably prefer a flat rate, whereas those with only a few will want to pay per transaction. Depending on the cost structure, competition and other such factors, either method may be preferable from a societal point of view.

Security activities differ with respect to the kinds of risk that can be tolerated, which in turn tend to depend on the nature of business relations and on the management strategy. Organisations have varying tolerance to the probability and urgency of risks and combinations thereof. For some, the main problem may be defence against the low probability versus high cost event, such as the total breakdown of a system or loss of a particular secret. For others, continual small interruptions may be of greater concern because everyday speed and reliability are important to customers. Most straightforward is the need to deal with high cost, high probability risks. But action is determined not only by these considerations but also by the feasibility of actually addressing the source of the problem and what it costs. This underlines the importance of examining and responding to priorities in countering various risks.

Availability

The proliferation of digitalised business systems and increased reliance on suppliers and outsourcing grows has coincided with growth in the number of users who will access a company's systems. Another aspect that enhances this process is that most modern companies have their business processes deeply embedded in their systems. This creates challenges with respect to access control privileges to the system, management of access control and monitoring and surveillance. The classic notion of perimeter security is becoming challenged and the focus is shifting from keeping people out to reliably providing access to trustworthy people (The Economist, 2002a). Security systems are increasingly depicted as airports rather than castles, with the emphasis on allowing people to enter some areas, clearly defining who can do what and requiring that people show credentials in order to access these areas or services. When designing systems that should permit mobility, it may be better to incorporate an authentication device that is portable, such as hardware tokens, mobile phones, USBs and smart cards. Overall, the conflict between availability and security requirements is a well-known problem. Often it is argued that it cannot be solved. But it is vital to recognise the conflict as a trade-off and treat or manage it in the best way possible.

2.7 LEGAL ASPECTS

This section explores authentication challenges with regard to specifications for how the original identification of an individual is undertaken, regulations concerning the right to privacy, legally valid frameworks for interoperability and liability claims.

Governments began recognising the potential of PKI for enhancing trust in electronic communications in the early 1990s. Digital signature laws emerged from the mid 1990s, but while PKI was generally considered the most appropriate technology for electronic signatures, the technology specificity of the digital signature laws was criticised.[44] It was argued that the law's focus on one technology would render it obsolete as technology evolved. This led to a change in the legislative approach and a trend towards more technology-neutral legislation.[45] However, despite this change, today's legislation is in many cases not truly technology-neutral. Regulation often aims at PKI but replaces the digital signature terminology with more technology-neutral terms.[46]

Electronic signature legislation generally aims to ensure legal recognition of all electronic signatures and to ensure equivalence between electronic and handwritten signatures, in some cases with presumptions for certain PKI-based signatures. Since 1995, all the world's leading trading nations have adopted or are in the process of adopting legislation rendering electronic signatures legally acceptable. These legislative efforts can be divided into three major approaches:

i) General recognising legislation which aims to ensure that electronic signatures are not denied admissibility as evidence or legal effect and that they can be used to meet form requirements (for example, for handwritten signatures). Examples are the US Uniform Electronic Transactions Act (UETA) and the US Electronic Signatures in Global and National Commerce Act (E-Sign Act).

ii) PKI-specific legislation, which is normally more detailed and also deals with liability issues. Examples are Japan's Electronic Signatures and Certification Authorities Act, Russia's Electronic Digital Signatures Act and Hong Kong's Electronic Transactions Ordinance.

iii) A combination of the above, which includes some general provisions, but also some PKI-specific ones, including liability. Examples are the EU E-Signature Directive and the UNCITRAL Model Law on Electronic Signatures.

---

[44] Utah Digital Signature Act from 1995 was the first regulation of digital signatures. Illinois Electronic Commerce Security Act from 1998 regulated both digital and electronic signatures. See also Washington Electronic Authentication Act, Missouri Digital Signatures Act and Minnesota Electronic Authentication Act.

[45] The UNCITRAL Model Law on Electronic Signatures removed the notion of "enhanced electronic signatures" from the drafts and now deals with electronic signatures. Also the political process leading up to the EU E-Signature Directive replaced the term "digital signature" used in early drafts with the more technology neutral "electronic signature".

[46] See e.g. the EU E-Signature Directive where the early drafts included "digital signatures", but were later modified to deal with "electronic signatures", although digital signatures obviously served as a model for the "advanced electronic signature". For a comparison of e-signature laws see Mason and Stephen (2003), Electronic Signatures in Law, LexisNexis Butterworths.

A number of countries have striven since the mid 1990s to institute legislation for the purpose of boosting electronic commerce and mandate the use of electronic signatures.[47] Regulatory approaches display considerable differences, however. In some cases, reforms have targeted digital signatures directly, even detailing a certain kind of digital signature, for example the EU qualified electronic signature. In others, approaches have been "technology neutral" and only mandated electronic transactions in a general sense, for example Australia's legislation. The observed variation in legislative approaches is not merely a reflection of varying attitudes in regard to electronic commerce and the use of PKI-based signatures, but also the result of fundamental differences in views on the role of government vis-à-vis markets, as well as the degree to which existing industry and other vested interests may be calling for measures that are more or less supportive of technology-specific solutions.

2.8 ECONOMIC ASPECTS

Economic factors are fundamental for understanding the need for authentication services and the problems that complicate their development and enforcement. The effectiveness of authentication, in turn, influences the viability and reliability of a range of ICT services. Whether satisfactory authentication is in place is likely to have far-reaching implications for the extent to which there will be continued cuts in the costs for diffusing, accessing and using information. In addition, there are implications for what products can be developed, which needs be satisfied, or which skills be upgraded with the help of ICT.

Markets characterised by severe forms of asymmetric information and skewed distribution of bargaining power, for instance, because of few providers and small, fragmented and poorly organised user groups, will be especially vulnerable to authentication problems. Relatively well-informed pioneers or high-end consumers (users) may work out their own solutions. When those who are uninformed understand neither the threats nor the need for security, there will be weak demand from these circles for solutions to problems.

It is possible that e-government and e-learning practices may cope relatively easily, either because of relatively good options for standardising practices or because some areas may be relatively uninteresting for fraud or other kinds of misuse. But the quality and effectiveness of e-business (especially as regards business-to-consumer transactions) is likely to be vulnerable and strongly dependent on the development of authentication services. Problems with interoperability and the absence of widely applicable international solutions can be assumed to result in market segmentation, with barriers to entry reducing competition and favouring market incumbents at the expense of newcomers. Such factors can contribute to the notion of a "digital divide" and social backlash.

Developing countries and SMEs have, for instance, relatively small means to handle, or mitigate, information-related problems through compensatory measures. Market imperfections and institutional failures may magnify the problems in many countries.

[47] See background report "Legal study on electronic signature legislation" by Anna Nordén (2005).

Rudimentary financial markets and limits on competition contribute to low demand for e-security as well as little effort to protect those that are affected. Remittances from diasporas abroad are greatly important for countries in Africa, South Asia and Latin America but receive little recognition or protection internationally. Subjected to strong fear of abuse and lack of trust among immigrants, the international banks managing their transactions have been able to extract exceedingly high charges while arranging scanty protection. With cellular technology on the brink of offering multiple technical opportunities for channelling the funds, internationally coordinated efforts to arrange secure transfers could lead to rapid, significant re-allocation of funds to poor regions and enable significant welfare improvements. Benefits for developing regions could be further enhanced to the extent that they are linked to policy programmes or other initiatives that facilitate complementary functions or services, for example in channelling funds to various productive savings and local investment opportunities in rural areas.

The potential value at stake in developed countries is equally huge. This can be exemplified by the magnitude of business-to-business e-commerce related to ICT-infrastructure, estimated at some US$2 trillion in 2003 and US$8.5 trillion in 2005.[48] Several studies have concluded that the level would have been much higher given stronger confidence in transaction security. How much business-to-consumer electronic commerce has been affected is much more difficult to estimate. Financial services, health services, logistics and transport, trade and other sectors are all subject to specific security-related costs and risks.

Indirect effects are likely to be more important than direct ones. Higher transaction costs due to a lack of security may, for instance, hamper the effectiveness of SME networks. This may reduce the ability of small companies to focus on core business and use professional external services in areas such as finance, trade and legal matters. Since orderly digital transactions give SMEs a unique opportunity to reach out to distant markets and broaden their uptake of resources and skills, such problems are also likely to reduce the extent to which ICT enables SMEs to benefit from the globalising economy. Such impacts may thus reduce SMEs' dynamism and limit their ability to exploit globalisation opportunities.

Network effects influence security engineering in multiple ways. Technological lock-in and path-dependency represent two costly risks, not least for SMEs, as companies often use obscure proprietary architecture to increase customer lock-in and increase the investment that competitors have to make to create compatible products. Interoperability between applications, decentralised system architecture and open-source software may play a mitigating role.

The difficulties in addressing authentication issues emanate from a number of fundamental imperfections that hinder straightforward matching between the demand for, and the supply of, effective solutions. Markets and public institutions alike need improved services

[48]Technology Administration 21st Century Policy Challenges for American Innovation Leadership, Remarks by Bruce P. Mehlman, Assistant Secretary for Technology Policy United States Department of Commerce, Before the Georgia Institute of Technology, Atlanta, GA, Oct. 23, 2003,
http://www.technology.gov/Speeches/BPM_031023.htm.
For further information on estimations for 2005 refer to http://www.gartner.com.

to enjoy trust in broad-based interactions. While the challenge is a global one, solutions are worked out within narrower groups of like-minded actors, where coordination is relatively easy. Coordinating a joint initiative between authorities and interested parties across different societal spheres, and among different countries, requires time and resources that are not easily raised. When, in addition, some countries view this as the responsibility first and foremost of government, whereas others wish the private sector to take care of the issue, the problem risks remain unresolved.

Work to develop appropriate solutions encounters problems for the following reasons:

i) Conflicting interests and agency problems that lead to inefficiency, delays and exclusion of some parties.
ii) Hold-up problems, for example emanating from lack of critical mass.
iii) External effects, as there is a tendency to push costs onto other actors, e.g., specific regions, sectors or spheres, where social costs are unaccounted for.

With the advance of ICT and more rapid diffusion of information, competition is sharpening in a general sense. Actors that are technologically sophisticated are faced with the need to keep specialising and developing new ways to maintain their lead. Technological advancement is swift and if actors are not up to date with the latest standards and requirements they may be confronted with formidable barriers.

Meanwhile, vulnerability incidents in societal functions and organisations increase at a similar pace. A computer malfunction might have been capable of causing minor disruption in 1993, whereas a virus in 2006 cost billions. The inherent superstructure of the Internet lets perpetrators selfishly abuse other network nodes anonymously without the risk of suffering consequences for their own actions. At the same time, the negative effects are shared by innocent network participants. The ability to remain anonymous on the Internet fuels temptations to misuse, threatening privacy, security and trust. These aspects influence the scope and utility of digital transactions and their future development. As opportunities for online transactions spread into new areas, the means to selectively control and manipulate digital transactions accumulates great power in destructive hands and may undercut confidence in legislation. The potential consequences indeed reach far and well beyond the digital domains themselves.

Among other aspects that are relevant for the costs and benefits of authentication, immature markets in particular are marked by high information costs and agency problems in contractual arrangements. The limitations as well as the opportunities confronting individual actors in part depend on their ability to gauge and rely on information on new technological advancements. Returns on investment in new technologies are highly uncertain and authentication weaknesses mean costs may be even higher.

For security to be seen as a strategic investment, rather than a cost, security managers must find ways to present executives with "hard numbers" that justify security spending. Since investment returns are highly uncertain, current research in the security industry aims to

explore security investment measurement and to define methodologies for calculating returns on security investments.

2.9 STRUCTURING AUTHENTICATION SERVICES

Authentication services can be structured for many purposes. These may include creating an overview of existing solutions so that a company can choose an appropriate authentication model based on its security needs and functionality. Other purposes may include determining if authentication services can provide support in a legal case or whether a service provider's systems meet interoperability requirements so that authentication systems can communicate with each other.

The public reports that provide recommendations on how to design authentication services (mentioned in Section 2.4) also provide the means for classification of authentication solutions. These recommendations often rank authentication solutions according to ideal (and theoretical) methods. The recommendations of the Australian government and the US divide authentication means in a four-level matrix based on minimal, low, moderate and high risk levels. The Swedish Agency for Public Management divides risks into high, medium high and lower levels.[49] It also highlights opportunities to sign legal documents, protection of codes and security levels for issuing identity tools.

The matrix in Table 3 includes aspects that may separate and distinguish solutions that are of relevance when evaluating an authentication system. The table builds on the analysis in Chapters 1 and 2 and may serve as a point of departure for further discussion.

[49] See Statskontoret (2000)

Table 3: Structuring authentication services

Aspects	*BankID*	*Microsoft Passport*
Original identification	Eye-to-eye	No
Open system	Moderate	No
Interoperable	Moderate	Moderate
Flexible	Moderate	Moderate
Scalable	Yes	Yes
Meets basic requirements of security	Yes	Yes
Centralised/decentralised	Central	Central
Bilateral or trilateral	Bilateral	Bilateral and trilateral
Supported by legal framework	Yes	No
Cost-efficient	No	Yes
Protecting privacy of users	Yes	No
Physical protection	High	High
Third-party actor	No	No
Availability mobility	Medium	High
Identity or role-based authentication	Identity	Both
Identification tool – evidence	Possession/knowledge	Knowledge
Provides means for legal signing	Yes	No
Risk assurance level	High	Low
Business model	Strong	Strong

3. THE CURRENT STATE OF AFFAIRS

3.1 SAMPLE COUNTRIES

The purpose of this report is to understand authentication in international transactions. This is determined largely by national frameworks. The current chapter presents an overview of the national framework for authentication solutions in the sample countries Australia, the US, Hong Kong, the EU (and its member states Austria, Belgium, Denmark, Estonia, Finland and Sweden). It describes legal frameworks and provides information on authentication in government services, the health and finance sectors and in the university world.

Finding comparable data on the different countries and sectors was challenging. Generally speaking, however, data on financial and government sectors were not problematic (though data on the health and university sectors were harder to come by). The survey distinguished between the four sectors throughout, but respondents did not necessarily apply this distinction when answering the questionnaire. The broad scope of the study contributed to mixed levels of data. Thus, some respondents provided feedback on a wide range of authentication methods from private and public sector and national and international settings. The respondents' different backgrounds, skills and focus areas had an effect on the data supplied, adding to the rich variety of information received. Some material was also acquired from Internet sources.

National practices may provide insights into how international solutions can be developed through best practice or identification of gaps and omissions. This section is followed by a review of existing international efforts encompassing service providers, standard and governance frameworks and global technology providers. Major actors are also analysed and structured according to economic, organisational, legal and technical aspects that impact on the enabling of digital transactions. A compilation of the data gathered is included in Appendix C.

3.1.1 AUSTRALIA

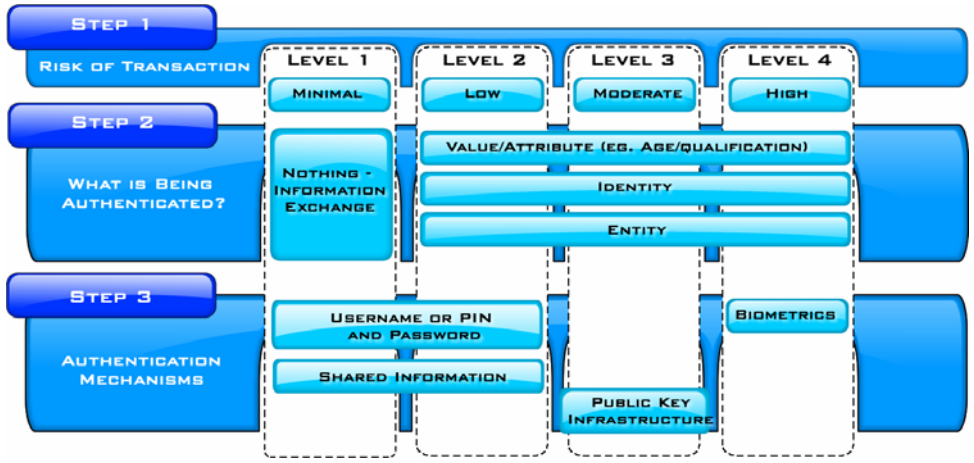
The Australian government is working towards the implementation of an Australian Government eAuthentication Framework (AGAF) to provide a comprehensive government approach to authentication. According to this strategy, successful authentication infrastructure requires the availability of several authentication techniques and the ability to apply these to different types of transactions, depending on the risk levels involved. The specific technology to be used should be assessed through a cost-benefit analysis which should take into account the costs and benefits for all respondents – governments, businesses and citizens.

Figure 8 illustrates the different types of risk levels, authentication categories and authentication methodologies that the Australian government recommends. It outlines

three steps that government agencies will go through when determining the sort of authentication mechanism they will use.

Although the Australian legal framework does not specify any one technology, much emphasis has been put on developing a national PKI scheme. The main Australian strategy for PKI use in government is the Gatekeeper.[50] It was established to assist the development of e-commerce for the exchange of government information and the procurement of services for government.

Figure 8: The AGAF



Source: AGIMO (2004)
Diagram: IKED 2006

Along with the Gatekeeper, a *cross-recognition* policy has been developed to encourage PKI interoperability, both domestically and internationally, in other words Australia is cross-recognising Gatekeeper with other domains at a harmonised policy level. The policy is consistent with the Asia-Pacific Economic Corporation (APEC) paper "Achieving Interoperability in PKI".[51] Certificate users in each domain can be confident in relying on certificates issued by approved certification authorities (CAs) in the other domains because it employs comparable and rigorous standards when approving organisations to issue certificates. However, the recognising domain does not guarantee the status and reliability of foreign certificates. The Gatekeeper certificate (or any certificate) remains with the relying party, based on that person's knowledge of the other domain's rules and trust processes and the recognising domain's assessment of those.

Cross-recognition is, however, not the same as *cross-certification*. The APEC paper states that *cross-certification* occurs when CAs from two separate PKI domains are, in effect, merged into

[50] http://www.agimo.gov.au/infrastructure/gatekeeper
[51] http://www.apectelwg.org/

one larger CA through an elaborate process that involves harmonisation of their certification policies and practice statements (the terms and conditions on which they issue and manage certificates). In practice, this almost equates to *technical* interoperability for cross-domain certificates and would mean that reliance could be placed on foreign (non-Gatekeeper) certificates as if they were Gatekeeper certificates.

Legal framework

Australia's Electronic Transactions Act (ETA) of 1999[52] has its roots in the UNCITRAL Model Law on Electronic Commerce (UNCITRAL MLEC).[53] The ETA aims to remove any existing legal impediments to the use of electronic transactions but is far from a detailed electronic signature regime due to the fear that technology-specific legislation might stifle innovation.

As to the validity of electronic signatures, the ETA has chosen, in order to keep technology neutral (the legislation is written in such a way that it is applicable whatever technology is in use) to deal with the larger concept of electronic *transactions*. The implication is that a transaction is not invalid simply because it took place by means of an electronic communication.[54] This rule has the same non-discriminatory effect as article 5 of the UNCITRAL MLEC.

The ETA further deals with legal requirements of a person's signature,[55] with the purpose of establishing that electronic signatures are functionally equivalent to handwritten signatures. A personal signature requirement is taken to have been met if (a) a method is used to identify the person and to indicate the person's approval of the information communicated, and (b) the method can be considered reliable. This provision is very close to the UNCITRAL MLEC, emphasising the identification and approval aspects as well as relative reliability.

An interesting feature of the ETA is that it includes an additional requirement when the signature is demanded by a Commonwealth entity, namely that it must meet the entity's technological requirements. If the signature is required to be given to another person, that person must consent to the use of a particular method.

The E-Transactions Act's technology-neutral approach means it includes no definitions of electronic signature or digital signature. Nor does it include any international acceptance provisions or regulations on the issue of digital certificates or CAs (and therefore no liability aspects either).

---

[52] Act No. 162 of 1999.

[53] See Section 3.2.

[54] "Electronic communication" means: (a) a communication of information in the form of data, text or images by means of guided and/or unguided electromagnetic energy; or (b) a communication of information in the form of speech by means of guided and/or unguided electromagnetic energy, where the speech is processed at its destination by an automated voice recognition system.

[55] Clause 10 of the E-Transaction Act.

Government services

Australia is a leading ICT nation with high levels of user activity. Its public and private sectors provide numerous online services and the government has adopted a progressive national framework. The Australian government provides many kinds of services and government entities have, with the support of the AGAF, chosen different authentication means for users to interact with these services. A number of services are listed and explained below.

Current government applications using *shared information (also called a challenge/response system)* method include the application for an Australian Business Number (ABN). This is an 11-digit business identifier that facilitates easier transactions with the Australian Taxation Office and other areas of government. Businesses can apply for an ABN online using secure sockets layer (SSL) to ensure security and privacy. The tax office requires applicants to provide proof of their own and their associates' identities. The office compares applicants' information to existing government agency data as a means of verification, such as Australian Company Numbers (ACNs) with the Australian Securities and Investments Commission (ASIC). Once an ABN is issued, a business must use a digital certificate issued by the tax office to access their details.[56]

Username/password: Current government applications include, for example, customs lodgements and payments, some Job Network transactions, business visas, patent applications and the Business Entry Point Transaction Manager Facility. The Business Entry Point (BEP) is an online government resource open to members of the small business community or the public. It allows businesses to access services and information about company start-up, taxation, licensing and legislation, as well as online transactions such as taxation compliance and licence applications. Businesses employ a username/password to authenticate and gain access to their information stored on the Transaction Manager Facility.[57]

One-time passwords: Members of the Australian Parliament use one-time passwords.

Public key infrastructure (PKI): Current government application include defence suppliers, healthcare provider systems, a pharmaceutical benefits scheme, the ATO business portal and electronic commerce interface for lodging business activity statements and a range of other business transactions.

Biometrics: Current government application spans several fields. New passports have to have high quality, machine readable photos embedded in them for facial recognition purposes as an aid to manual face recognition.[58] Important pull factors for the implementation of biometrics with regard to passports include international requests. Australians wishing to visit the US on business or leisure without a visa have been required to have a biometric

[56] For further information see http:// www.abr.gov.au.
[57] For further information see http:// www.business.gov.au
[58] For further information see http:/ / www.dfat.gov.au/dept/passports/

identifier in their passports since the end of 2004. In addition, Customs and Immigration are trialling "Smartgate", a biometric facial recognition system for international air passengers and crew.[59] Moreover, a number of agencies use biometrics, such as hand/fingerprint readers, for entry to secure areas. The Department of Immigration, Multicultural and Indigenous Affairs is introducing biometrics in some processes, and at least one state prison uses iris recognition technology for visitors wanting to see prisoners.[60] Also, *The Age* newspaper has reported that Centrelink, a government agency that delivers a range of Commonwealth services to the Australian community, is trialling new biometrics initiatives for some of its business lines, for example trials of fingerprint scanning (see below), and is experimenting with a voice biometrics system for students that recognises the voice as well as what the voice says.

"*Staff at the social security agency Centrelink are set to be fingerprinted as part of a new computer security crackdown. Centrelink has released a request for tender for 31,000 fingerprint scanners. The scanners would be used instead of passwords to access the agency's computers in its national support office, area support offices, call centres and customer centres, the tender documents said. They would also enable staff to securely access Centrelink computers using laptops from remote locations."*[61]

E-health

The SecureNet-HeSA Health PKI provides PKI for the Australian healthcare sector. PKI is used for the transfer of health-related information over the Internet and ensuring that patient information is not compromised. Healthcare providers interested in obtaining their own digital keys and certificates need to register through the Health eSignature Authority (HeSA). HeSA offers two types of certificate:

i) "Individual" certificates allow a user to encrypt and exchange messages electronically with other certificate subscribers. They also allow for electronic signing at the individual level, which provides a strong measure of security about the identity of the person sending the information.

ii) "Location" certificates allow a number of users at the same location to encrypt, sign and exchange messages electronically with other certificate subscribers. Signing a message using the location certificate reveals the location from which the message came, but not which individual.

Applicants must register for digital keys and certificates on HeSA's website and use a user ID/password approach during the application process. Applicants respond to a series of questions to provide information necessary for HeSA to arrange for certificate issue. The

[59] For further information see http:// www.customs.gov.au/site/page.cfm?u=4243

[60] For further information see http:// www.zdnet.com.au/insight/security/0,39023764,39191986-3,00.htm

[61] Extracted from article at http://www.theage.com.au/news/Breaking/Centrelink-to-move-from-passwords-to-fingerprints/2005/03/16/1110913633890.html?from=moreStories).

registration process is completed when applicants provide hard copies of identity-related documentation, as indicated during the Web-based application process.[62]

Finance

Australia and New Zealand Bank uses a user number and password combination with SSL for login in to its services. The bank promises customers that they will not be liable for any unauthorised transactions. It uses a cross-recognition facility with Gatekeeper.

Westpac Bank uses a combination of password and PIN with SSL as its authentication method. Westpac guarantees that customers will not be personally liable for unauthorised transactions provided they were i) in no way responsible for the unauthorised transaction, ii) did not contribute to the loss, or iii) complied with Westpac's Internet banking terms and conditions.

Commonwealth Bank uses a combination of user name and a password with SSL for authentication. It covers losses if an external actor makes an unauthorised transaction on a customer's account using his Internet bank, provided the customer protects his client number and password.

National Bank Australia requires customers to enter a personal ID number issued by the bank and an Internet banking password to access the bank's services online. The connection is protected by SSL.

Universities

While universities and other research agencies maintain institutionally based authentication schemes, Australia does not have a national scheme, such as the UK's Athens system.[63] The existing consensus favours a scheme based on federated rather than centrally managed identity. There are some regional authentication schemes. However, the Council of Australian University Directors of Information Technology (CAUDIT)[64] has been founded to develop policies and standards to enable the collaborative use of PKI among and between Australian universities and research groups and to implement a prototype system. It is intended that it will provide a basis for establishing a National Certification Authority for international operation, which is likely to be run by the Australian Computer Emergency Response Team (AusCERT).[65] AusCERT already has a trusted relationship with each university and with CAUDIT.

[62] For further information see http:// www.hesa.com.au.
[63] The Athens Access Management system provides users with single sign-on to numerous Web-based services throughout the UK and overseas. http://www.athens.ac.uk/
[64] http://www.caudit.edu.au
[65] http://www.auscert.org.au

3.1.2 EUROPE

Under the E-Signature Directive, qualified certificates issued by a CA in the EU are automatically accepted by the other member states. Foreign CAs are accepted if they fulfil criteria to ensure a similar level of quality as the EU's CAs. However, interaction between countries is at a low level due to interoperability problems (of organisational, technological and legal character). National implementations and standards lack a semantic view of interoperability, which is a challenge that should be addressed. The terminology in use within the EU displays great variance and there are difficulties in agreeing what types of certificates should be valid for individual sectors. In Germany, there is high demand for qualified e-signatures, whereas in the Nordic countries only simple e-signatures are required. Different countries take different positions on identification and authentication. The Nordic countries had, however, agreed internally to solve this question by 2005.

Within the EU authentication framework there seems to be confusion about the concepts involved. Lack of unity is putting a brake on development. Despite the existence of the EU's *Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Businesses and Citizens programme* (IDABC),[66] there is no unified international view. And a unified international view must stem from a unified national view, which is also often lacking.[67]

IDABC focuses on security-related actions, dealing inter alia with identity management.[68] IDABC has undertaken the development of specifications and procedures for a bridge certification authority. The goal of this bridge/gateway CA is to provide an intermediate trust infrastructure between the PKIs of Europe's national public administrations. A pilot is currently under development, involving IDABC and CAs from eight member states (Germany, Italy, Belgium, Finland, Estonia, Czech Republic, Slovenia and Slovakia) and one EEA country, Iceland. An extensive test programme, with functional and interoperability tests, was scheduled during 2005.

IDABC has also developed a basic policy for establishing the appropriate authentication mechanisms in sectoral networks and projects.[69] The IDABC Authentication Policy aims to provide an instrument that helps managers to assess and establish appropriate authentication mechanisms for their projects. The document foresees a certificate practice statement that describes different policies for the four levels of assurance defined – minimal, low, substantial and high. These policies relate to both registration and electronic authentication phases, and to the choice of token type and authentication protocol for each level of assurance.

Another major European actor that affects the market for authentication mechanisms is the European Committee for Standardisation (CEN/ISSS). CEN/ISSS has set up a workshop[70] to obtain consensual agreement on the essential organisational and operational rules and

[66] IDABC was formerly known as Interchange of Data between Administrations (IDA).
[67] An analyst at the Swedish Agency for Public Management.
[68] http://europa.eu.int/idabc/en/document/3784
[69] http://europa.eu.int/idabc/servlets/Doc?id=18227
[70] http://www.cenorm.be/CENORM/BusinessDomains/BusinessDomains/ISSS/activity/ws-mmust.asp

processes to enable interoperability between multi-application multi-issuer schemes from local to international level.

CEN/ISSS has also launched a focus group to determine the role that standards should play in e-government,[71] in particular as a means of achieving interoperability at all levels of public administration throughout the European Union, including at national, regional and local levels. The group will identify what measures are required to achieve this goal and will contribute to the debate on how to ensure a permanent framework for pan-European e-government standards that are as harmonised as possible with general ICT standards.

The European actors working on electronic identity and authentication include the WS eAuthentication working group of the CEN/ISSS and the Porvoo Group.[72] The objective for the CEN 224 WG 15 European Citizen Card working group is to develop a technical standard for a European citizen card. The European countries considered to have made the most progress in implementing electronic identity systems are Finland, Estonia, Norway, Belgium, Slovenia and Italy. Spain, France and Austria also have projects that are well on their way and the UK has commenced development work.

All the same, there remains no unified view within the EU on authentication matters and no de facto standards have been established.

Legal framework

The E-Signature Directive[73] was adopted partly in reaction to national legislative efforts on e-signatures in some European countries during the latter half of the 1990s. The range of national legislation was perceived as a possible obstacle to e-commerce in the internal market and the purpose of the E-Signature Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition, and to open up the European market for electronic signatures and certification services. In addition to rules on legal effect and liability, the directive also addresses voluntary accreditation and supervision of CAs.[74]

The directive defines an *electronic signature* as "data in electronic form, which is attached to or logically associated with other electronic data and which serves as a method of authentication". This is a very broad definition, covering a digitised image of a handwritten signature as well as a digital signature, and is meant to be able to cover future data authentication technologies.[75]

[71] http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/e-government.asp
[72] The Finnish government initiated the Porvoo Group that is promoting the use of smart ID-cards for online transactions.
[73] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[74] See The Legal and Market Aspects of Electronic Signatures (Leuven, 2003) for a thorough analysis of the E-Signature Directive and its implementation.
[75] The term "electronic signature" relates to "data authentication" and does not cover methods and technologies for "entity authentication", see The Legal and Market Aspects of Electronic Signatures (Leuven, 2003) p. 27.

The directive further defines a second level of electronic signature – the so-called *advanced electronic signature*. An advanced electronic signature is an electronic signature that is:

i) Uniquely linked to the signatory;
ii) Capable of identifying the signatory;
iii) Created using means that the signatory can maintain under his sole control; and
iv) Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The E-Signature Directive includes a non-discrimination rule that states that electronic signatures may not be denied legal effectiveness or admissibility as evidence in legal proceedings solely on the grounds that they are in electronic form or that the signature in question is not a so-called *qualified electronic signature*.[76]

The E-Signature Directive assumes that qualified certificates issued by a CA within the EU are automatically accepted by other member states. It regulates how qualified certificates issued in countries outside the EU should be treated and states[77] that member states shall ensure that certificates which are issued as qualified certificates to the public by a CA established in a third country (one outside the EU) are recognised as legally equivalent to certificates issued by a CA established within the EU if the following conditions are met:

i) The CA fulfils the requirements laid down in the E-Signature Directive and has been accredited under a voluntary accreditation scheme established in a member state; or
ii) A CA established within the EU which fulfils the requirements of the E-Signature Directive guarantees the certificate; or
iii) The certificate or the CA is recognised under a bilateral or multilateral agreement between the EU and third countries or international organisations.

For other types of signatures the non-discrimination principle applies, which means the issue of regulating cross-border acceptance does not arise. Instead, a judge will, from case to case, decide whether the signature is good enough for the purpose it is used for, with the only restriction that he or she may not deny it legal effect just because it is an electronic signature.

The E-Signature Directive includes liability provisions for issuers of qualified certificates, when such certificates are issued to the public.[78] The directive has no liability rules for other types of certificates or electronic signatures.

[76] The E-Signature Directive Article 5.2.
[77] The E-Signature Directive Article 7.
[78] The E-Signature Directive Article 6. The E-Signature Directive uses the term Certification Service Provider (CSP) instead of CA

Health sector

The health sector is highly complex and needs to overcome many regulatory aspects in order to develop effective schemes for transferring services online. One interesting initiative is the European Health Insurance Card, which is intended to replace current paper forms needed for health treatment in another member state. Initially, the E111 form will be replaced for holidays, temporary stays abroad, and later for employees, students, and so on (EC COM (2003) 73 final).

CEN/ISSS also have held workshops on e-health that have pinpointed a number of critical applications to achieve a more effective health sector. These include: electronic health/patient records; health record and business architectures; electronic transfer of prescriptions; electronic health data messages between hospitals and primary care (particularly communication of service requests and reports for laboratory investigations, discharge summaries and patient referrals); digital imaging and associated service requests and reports; e-prescribing with decision support; and core data sets, for example for public health and assessing clinical care quality.

It was concluded a number of critical infrastructure elements should be pursued to bring about these applications. They include: management of patient identification (with the possible inclusion in the EU Health Insurance Card of medical emergency data set and controlled access to data in a patient's country of residence); a common approach to patient identifiers; access control and authentication; protecting personal information (with emphasis on PKI and data cards for identifying and authenticating professionals and citizens/patients); terminological systems for clinical records and medicines; and data cards and portals.

Financial sector

Banking identification systems are used for a multitude of purposes, including commercial and public sector applications. Analysis of the role of the Internet in banking operations suggest that online banking is becoming a complementary channel to branch and call centres and is mostly used for simple transactions.[79] Consequently, the Internet is changing banks' role and organisation and, in some cases, the number of branches because these will tend to concentrate on advisory and selling functions (ECB, 2002). Bughin (2001) also points at bank-specific factors such as cost-effectiveness (characteristic of banks which have already established a large electronic channel base, measured by ATM density/customers) as having a significant leverage effect on customer conversion to Internet banking. Customers seem to prefer conventional banks with an established brand identity, that offer online services and conventional multi-channel delivery, providing customers with a higher degree of comfort, convenience and security as compared with online-only banks. While marketing efforts have a positive impact on e-banking use, low quality service at branches, insufficient numbers of branches and high pricing of branch services have also been proven to

[79] See: Bank of Korea, 2002; Datamonitor, 2002; Fundacion AUNA, 2002 and the Swedish Banking Association.

stimulate the adoption of Internet banking. This is the case, for example, in Estonia (Kerem, 2003). Internet banking may also be an enabling instrument for cross-border bank expansion. Initiatives, however, remain limited, partly because the Internet is often used as a complementary channel to the branch network, which is, by definition, local.[80]

It can be observed that banks or bank card operators are acting as identification/ authentication gateways in their operating countries and offer, through their portals, access to e-commerce and third party services, such as tax payment, insurance services and electricity bill management. In these cases, banks are acting as trusted parties. This may indicate that banks have a significant role to play in building security and trust on the Internet.

3.1.3 AUSTRIA

In Austria, it is not obligatory to carry an identity card, and thus the country has not developed an electronic ID card. Austria has instead deployed the Citizen Card ("Bürgerkarte"), which can be considered world leading when it comes to the interoperability of authentication providers.

The *Bürgerkarte*[81] launched by the Austrian government in November 2000 is not so much a card per se but a concept which defines a bundle of functions and minimum requirements relating to e-government perspective. It is a system that allows for electronic signatures and authentication through the creation of online "electronic identities" by a citizen. The basic attributes are the secure identification of the citizen and the digital signature function. It also offers confidentiality in communication by encryption facilities.

In principle, it is a federated identity management system that can cover various media, including smart cards, mobile phones and banking cards. The concept is based on open standards and open interfaces that allow for interoperability of a multitude of authentication initiatives. The strength of the Austrian approach is its technological neutrality. Several private sector and public sector projects already issue cards or are planning to do so.

The concept fulfils the requirements of e-government and can be implemented in an interoperable way by several solution providers. Some of these are:

- Membership card of Austrian Computergesellschaft (OCG)
- Signature card from certification service providers
- National ID card with chip
- Social security e-card
- Various student cards
- Banking cards with signature capability
- Chambers of commerce card (several notaries)

[80] ECB, 2002
[81] http://www.buergerkarte.at

The objective is for all citizens to have at least one electronic identity (the health insurance card), approximately 80-100 electronic-identity-based services are available. The possibility of using a so-called multi application smart card has been taken into account, for example to combine electronic identity with banking functions. Under the federal government programme, all administrative services to citizens and businesses were set to be enabled for electronic delivery by the end of 2005.

The main issue that had to be solved was a unique identification that capable of use both by e-government and by the private sector in a secure manner and with a technology-neutral interface.

No bilateral agreements with other national CAs for mutual recognition of cards have been signed, but a prototype integration of Italian and Finnish electronic identities has been piloted.

Legal framework

Transposition of the E-Signature Directive into federal law took place in January 2000 with the Federal Law 190/99 on electronic signatures.[82] The act defines two types of electronic signatures: *basic* and *secure electronic signatures*. The latter are defined as advanced electronic signatures that are based on qualified certificates and are created using technical components and procedures which comply with the security requirements stipulated by Austrian regulations. A secure electronic signature can thus be described as a kind of qualified electronic signature, but with the *qualified signature creation device* requirement of the E-Signature Directive replaced by national Austrian rules.

According to the act, secure electronic signatures meet the requirements of handwritten signatures, though a special law or agreement between the parties may specify otherwise. There is no obstacle to using non-secure signatures for other types of transactions. Austrian civil law imposes no restrictions on the use of electronic signatures and indeed has explicitly adopted a general non-discrimination clause for all forms of signatures from the E-Signature Directive.

The liability provision is an explicit transposition of the E-Signature Directive. CAs that issue qualified certificates are liable vis-à-vis persons who rely on certificates. Certification Authorities that supply secure electronic procedures are liable for the legal conformity and suitability of the signature creation products they supply or recommend. As in the E-Signature Directive, the burden of proof is reversed: the CA must prove that it or its personnel did not act negligently. The possibilities to limit liability are also the same as in the E-Signature Directive.

As for international recognition, the validity of all foreign certificates (issued by CAs established within the EU or not) shall be verifiable. EU qualified certificates are deemed equal to Austrian ones, provided that their validity can be checked. For non-EU certificates

[82] See also Federal Ordinance n°. 30/2000 on Electronic Signature, entered into force February 3, 2000.

the following applies: common certificates are recognised without conditions if their validity can be verified. Non-EU qualified certificates are accepted under the same conditions as in the E-Signature Directive but, in addition, the validity of the qualified certificate must be verifiable from Austria.

E-laws

i) *Freedom of Information*: Constitutional Law on Access to Information 1987.[83] It contains provisions on access to public information for the federal and regional levels, and stipulates a general right of access, in so far as this does not conflict with a legal obligation to maintain secrecy. On the basis of the provisions of this constitutional Law, the 9 Austrian States have enacted laws on access to information (setting mostly the technical details).

ii) *Data Protection/Privacy*: Data Protection Act (Datenschutzgesetz – DSG) 2000.[84] In implementation of the EC-directive on Data Protection 95/46, the Data Protection Act 2000 provides for a fundamental right to privacy with respect to the processing of personal data which entails the right to information, rectification of incorrect data and reassurance of unlawfully processed data. It regulates the preconditions for the lawful use and transfer of data, including necessary notifications, registrations with the examinations by a Data Protection Commission. It finally provides for judicial remedy in case of breach of its provisions. It lays down the respective procedures before the Data Protection Commission and civil courts as well as penal and administrative sanctions for its infringement.

iii) *E-Commerce/E-Signatures*: Electronic Signature Act 1999[85] made Austria the first member state of the EU to implement the Directive on Electronic Signatures. The Act legally recognises electronic signatures satisfying certain security requirements and provides some evidential value to less secure electronic signatures. It is complemented by an Electronic Signature Ordinance (Order) that was published in the "Bundesgesetzblatt" (Official Journal) in 2000.

Government Services

In Austria, some 80–100 e-services are available to citizens, for which a Citizen Card authentication may be required. Among these are electronic filing of tax returns, electronic declaration of corporation tax, filing of VAT, payments of family allowances, online business registration, transmittance of statistical data, paperless foreign trade, etc.

Finance

All leading Austrian banks; Bank Austria Creditanstalt, Erste Bank, Raiffeisen Zentralbank Österreich, Bank für Arbeit und Wirtschaft BAWAG-PSK, provide online banking. So far,

[83] http://oeh.tu-graz.ac.at/dokumentation/materialien/ausk.htm
[84] http://www.bka.gv.at/datenschutz/dsg2000d.htm
[85] http://www.signatur.rtr.at/en/legal/sigg.html

the solutions used for authentication have mainly been username and password, with some kind of tokens. These technologies have been used mainly for accessing banking functionality. However, recently the Maestro bank card was released in Austria that can be set to function as a citizen card. This new functionality is among other things aimed at increasing the uptake of e-services provided by the Austrian public sector and could ultimately be extended to all bank cards. Most common services are corporate e-banking and notary archiving.[86]

E-Health

The Austrian Social Security runs an e-Card project;[87] the idea is to issue smart health insurance cards to all Austrian citizens, where the e-Card is prepared for a digital signature function. The central element of the e-card project is to connect 12,000 medical doctors to the computing centre network of the Federation of Austrian Social Security Institutions. Austrian privacy and data protection organisations have questioned the project due to vulnerability to data abuse.

Universities

Some institutions have developed online enrolment systems (e.g. University of Vienna) and some types of student services are provided (e.g. University Network West, Linz, Salzburg, Innsbruck, Vienna University of Economy and Business, University Network South)

3.1.4 BELGIUM

The royal order creating the legal basis for an electronic ID card was published in the Belgian Official Journal on 15 September 2004. Following a successful test distribution of about 70,000 cards in 11 municipalities, the country's remaining 578 municipalities will have to complete the transition before the end of 2009. By then, every Belgian citizen will be required to own an electronic ID card and close to 10 million cards will have been issued. The new card is called BelPIC, an acronym for Belgian personal identity card.

The principal aims of the eID launch were to provide Belgian citizens with a means for online authentication and to generate digital signatures. It appears that the eID has evolved beyond the strict boundaries of an e-government tool into an economic, social and political driver. Many consider it a spur for the development of a safe electronic infrastructure, in which individual companies and organisations do not have to adapt and set up ICT-solutions for multiple online transactions. The use of the eID for secured online transactions generates considerable budget savings for the federal government. Moreover, greater security and trust lessen the risk of abuse and fraud, allowing for higher pick-up of

[86] "Notary" in this document refers to the definition used by Encyclopaedia Britannica. ***Notary,*** *"… also called* ***Notary Public,*** public official whose chief function…is to authenticate contracts, deeds, and other documents by an appropriate certificate with a notarial seal" (http://www.britannica.com/eb/article-9056330).
[87] http://www.e-card.or.at/

more cost-efficient online services. The government estimates that the card will save the public sector, private sector and the citizen approximately €100 million per year.

There are still some questions as to what extent the solution is demanded by the market, and it appears that Belgium's banks have yet to buy in to the project. The initiative is clearly supply driven, but the initiators are confident that it will generate the necessary framework for new services. They have received some support from the interest shown by Adobe and Microsoft in Belgium and the incorporation of the eID system in some of their services and pilot projects.

The eID card contains a digital certificate that enables remote authentication of the holder and transaction signing. Authentication takes place via a card reader connected to a computer. Initially, the ID card will not contain biometrics though it is sufficiently flexible for such data to be included at a later stage. Card readers are publicly available in electronic terminals in Belgium's municipalities. Suppliers have agreed to deliver 90,000 payment terminals which will accept the card. In the banking sector 8,000 readers will accept the card in the near future.

The network infrastructure linking the communities using the electronic ID card is provided by telecom operator Belgacom,[88] while ICT services company Steria[89] is supplying the infrastructure and services required to deploy the system. The federal government will provide 780 people to help the communities manage card deployment over the next three years.

In a bid to further strengthen e-government, the Belgian government has launched the Belgian Government Interoperability Framework (BELGIF) and published a first list of open standards to be used by public authorities. BELGIF is the result of a cooperative project bringing together the federal government and the federated entities (regions and communities). The launch of an interoperability framework for e-government stems from the need to promote interoperability at national and European level, and follows the federal government's June 2004 decision to promote the use of open standards.

Leading proponents of the Belgian infrastructure have expressed needs for improved communication to citizens, more cooperation with banks (buy-ins) and increased availability of card readers to make the system more effective.

Legal framework

Belgium has passed two pieces of legislation that enact the European Directive of 13 December, 1999, on a union-wide framework for electronic signatures. They give legal value to electronic signatures and electronically signed documents and establish a legal framework for certification services. All documents signed electronically will have the same legal value as those with a written signature.

[88] http://www.belgacom.be/
[89] http://www.steria.com/

The legislation assumes that qualified certificates issued by a CA within the EU are automatically accepted. Certificates which are issued as qualified certificates to the public by a CA in a third country (outside the EU) are recognised as legally equivalent to certificates issued by a CA in Belgium if certain conditions are met.

The following laws regulate the authentication mechanisms in Belgium:

i) E-commerce/e-signatures:

- Law on the use of Electronic Signature in Judicial and Extra-Judicial Proceedings, 20 October 2000.[90]
- Law on Electronic Signatures and Certification Services (Legal Framework – Miscellaneous Provisions), 9 July 2001.[91]

ii) Data protection/privacy:

- Law on the Protection of Private Life, 8 December 1992.[92] This was modified by the law transposing European Directive 95/46/EC on data protection, 11 December 1998. The modified version entered into force on 1 September 2001.

Government services to citizens

The eID card can be used for a number of e-government services, such as online tax filing, submission of VAT declarations, e-procurement, e-identity, e-justice, social security services, and online request and payment of civil certificates (birth, marriage, death, residence and nationality). The card also acts as a European travel document.

E-health

The government has launched Be-Health, an integrated platform aiming at delivering all health and healthcare-related information and services online through a single portal. The portal will provide services to health professionals as well as to the general public and the government.

Finance

The country's largest banks, Fortis, Dexia and KBC, still largely use password and username technologies for login. The banks' technologies can be used as authentication mechanisms beyond pure banking services, such as ordering of tickets. Fortis Bank, for example, has two systems for its clients. An older system is based on a smart card and a reader connected to a PC. It is used for logging in but also as a cash card, with the smart card being chargeable with lesser amounts of cash. The newer system is based on a user name and a digipass

[90] http://mineco.fgov.be/information_society/e-signatures/law_e_signature_001.pdf
[91] http://mineco.fgov.be/information_society/e-signatures/law_e_signature_002.pdf
[92] http://www.privacy.fgov.be/textes_normatifs.htm

which, once activated by a PIN code, generates a one-time code that is entered when logging in to Internet banking services. Identification is required for any user wanting to register with the system.

Universities

Universities are considering using the national ID-card as a student card.

3.1.5 DENMARK

In Denmark, there is an ambition across state, county, and municipal government to use the potential of an e-society to make the public sector more flexible and efficient so it can deliver higher quality services to citizens. The national e-government strategy states: "The e-government vision is to systematically use digital technologies to introduce new ways of thinking and to transform organisations and work processes to improve quality of service and efficiency."

All Danish citizens have a legal right to communicate electronically with central government bodies. The authenticity of all messages is certified through the use of digital signatures. Public authorities have established secure e-mail solutions and rearranged work practices to comply with Danish Data Protection Agency guidelines.

The Danish government has launched an ambitious programme to issue digital signatures[93] to all citizens, with a view to accelerate the take-up of e-government services. Each Danish citizen will receive a free software-based digital signature, issued by the Public Certificate for Electronic Services (OCES),[94] to provide sufficient security for most public sector and private sector transactions. Approximately 320,000 Danes out of a population of 5.4 million have a digital signature from OCES. Some 43,000 have acquired their digital signatures through work. The major issuer of OCES is TDC, the former national telecom operator.[95]

In Denmark, the OCES standard has not been adapted – or even supported – by financial institutions, which have instead launched a product known as Net-ID. This is based on the authentication process supported by various Internet banks, has approximately 2.2 million users[96] and is an important alternative to the official certificate.[97] The major difference between the certificates, except for pricing, is that secure e-mail messages can be sent with OCES, which can also provide certificates to organisations and role-based certificates.

Another certificate – the "KMD fælles pinkode" – is also in use in Denmark and as of April 2006 it had been issued to 800,000 Danes.[98] This certificate is part of a government single

[93] http://www.digitalsignatur.dk/
[94] https://www.signatursekretariatet.dk/forside.html
[95] http://tdc.dk
[96] For a comparison between OCES and Net-ID, see http://www.finansraadet.dk/danish/menu/faktaomsektoren/pengeinstitutterneisamfundet/Net+ID/Fakta+om+net-ID+og+OCES/.
[97] Henrik Elkjær, Business Development, Post Danmark.
[98] http://www.netborger.dk

sign-on solution to government services. Citizens acquire a PIN code that is used to log in to government services and sign documents through a common entrance portal. The OCES certificate can also be used to log in.

The available mechanisms for authentication are typically priced on a per-transaction basis. Cost is incurred per authentication, which is considered problematic for an information service but not for a business transaction.

Denmark has participated in a project with the other Nordic countries to enable interoperability between national authentication services. However, a number of challenges have arisen, among them the issue of original identification and having to cope with different requirements. In Denmark there is no need for face-to-face original identification, which has been the case in Sweden.

Legal framework

The EU directive has been implemented in Denmark and digital signatures have legal validity. Like other European jurisdictions, Denmark accepts foreign certificates under certain conditions.

i) Freedom of information/use of public sector information: Act on Access to Public Administration Files, 19 December 1985.[99] Amended in June 1991, June 1993, May 1998 and May 2000.
ii) Data protection/privacy: Act on Processing of Personal Data, 31 May 2000.[100] The act entered force on 1 July 2000 and implements Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data.
iii) E-commerce/e-signatures: Act on Electronic Signature, 31 May 2000.[101] This act entered force in October 2000 and implements the European Directive on Electronic Signatures.

Government services

A number of e-government services are available where there is a need for online authentication. For these services, citizens can use either one of the three major authentication solutions: OCES, Net-ID or KMD fælles pinkode. However, the last of these is not considered as secure and cannot be used for all types of services. For example, filing of tax returns is almost 100 per cent automated in Denmark. Most information is collected electronically from the relevant sources (employers, banks, mortgage lenders and so on) using citizens' ID numbers. Citizens can change their draft statement online using the official digital signature or another PIN-code-based identification system. Moreover,

[99] http://www.cfje.dk/cfje/Lovbasen.nsf/ID/LB00000597?OpenDocument
[100] http://www.datatilsynet.dk/include/show.article.asp?art_id=443&sub_url=/lovgivning/indhold.asp&nodate=1
[101] http://www.fsk.dk/cgi-bin/doc-show.cgi?doc_id=34226&doc_type=22

some services are administered by private funds and managed online. These include unemployment insurance; social and health services, and state educational grant and loan schemes. Citizens and residents can access and amend their records in the Central Population Register, including their address. Statistics Denmark, the Danish central statistics agency, Danish companies and public authorities can also submit wage and salary information electronically.

E-health

The purpose of the National IT Strategy for the Danish Health Service[102] is to establish a common framework for the full digitisation of national healthcare system during the period 2003-2007. It replaces the former National Strategy for IT in the Danish Hospital System 2000-2002. The National Strategy Group is in charge of developing the new IT strategy. Its task is to monitor, disseminate and develop the National Strategy for IT in the Danish Hospital System. The group consists of representatives of the Ministry of Inferior and Health, the National Board of Health, the Association of County Councils, the Copenhagen Hospital Corporation and the National Association of Local Authorities in Denmark.

One of the goals is to explore the possibilities of sharing data between the many ICT solutions currently in use in Denmark's health service, thus enabling the implementation of the strategic goals and the vision for citizens, for healthcare professionals and for society in general. The creation of a common public health portal is a central initiative. The portal is intended to become the common vehicle for communication and information in the health service and is also intended to be the electronic access point for the citizens.

The majority of initiatives from the first phase of the ICT strategy (1 January 2003 to 31 December 2005) bear on the development and implementation of electronic health records (EHRs). The focus is on initiatives aimed at the development of common standards, concepts and classifications, and on initiatives ensuring good integration between EHRs and the other ICT systems available in the healthcare service.

MedCom[103] is a cooperative venture between authorities, organisations and private companies linked to the Danish healthcare sector. In the 1999 budget agreement between the counties and central government, it was decided that MedCom would be made permanent to "contribute to the development, testing, dissemination and quality assurance of electronic communication and information in the healthcare sector with a view to supporting good patient progression".

Denmark is also, together with Estonia, Lithuania, Norway and Sweden, involved in the Baltic eHealth project, which will promote the use of e-health in rural areas of the Baltic Sea region by creating a substantial international infrastructure for e-health.

[102] http://www.sst.dk/publ/Publ2004/National_IT_strategy.pdf
[103] http://www.medcom.dk/

Finance

The Danish financial institutes undertake joint R&D and the provision of electronic payment services through an organisation called Payment Business Services (PBS). The three largest Danish banks (Nordea Bank Danmark, Den Danske Bank and Den Jyske Bank) hold the three seats on the PBS board. PBS has developed and launched Net-ID, currently being used by approximately 2.2 million Internet bank users for Internet identification and signing of documents and contracts.

Universities

UNIC is the Danish IT Centre for Education and Research[104] and is an IT organisation run by the Danish Ministry of Education that aims to provide a platform for the implementation of IT in education in Denmark. UNIC's objective is to be a leading provider of IT solutions for the entire educational sector. It specialises in all aspects of IT integration, such as the creation of educational material, educational websites, and connection of schools to the Internet. Other areas covered are training of teachers in the use of IT in education, and administrative systems for vocational schools, teachers training colleges and agricultural colleges. UNIC's customers are the educational and research sector, government ministries, organisations and companies. UNIC has specialised in advanced security solutions for more than ten years and its expertise covers a varied number of services, ranging from analysis of security solutions to design and monitoring.

3.1.6 ESTONIA

The first Estonian eID[105] cards were issued in January 2002. The card fulfils the requirements of Estonia's Digital Signature Act and is mandatory for all Estonian citizens and permanent resident foreigners over 15 years of age. It is meant to be the primary document for identifying citizens and residents and to be used in any form of business, governmental or private communications. Besides being a physical identification document, the card has advanced electronic functions that facilitate secure authentication and legally binding digital signature for nationwide online services. In the first year more than 130,000 cards were issued, and the total figure had grown to 745,920 as of 28 April 2005 – more than half of the population. The transformation to the new ID card was much helped by the fact that it replaced the ordinary passports for use within the EU (and some other countries). The card is used in many kinds of companies and organisations, such as banks, law firms, local government, ministries, municipalities and companies. The Finnish Population Register Centre and the Estonian Certification Service Provider have signed a memorandum of understanding stating that they "will cooperate to make legally binding digital documents a reality within and between Finland and Estonia". Estonia is also cooperating with Finland, Austria, Italy, Belgium and a few other countries in pilots to make their national eID systems interoperable.

[104] http://www.uni-c.dk/generelt/english/index.html
[105] http://www.id.ee/pages.php/0303

The ID cards are bought and distributed by the Estonian government that fund them by taxes, but the certificates are provided by Estonian companies. Estonians pay around €10 for the card (with identification and digital signature included) and then buy the certificates from the service providers. New markets (not only for CAs but also for multiple services) have been created as a result of the government's investment in the ID cards. Interoperability and certificate problems are managed by making the ICT infrastructure acceptant of different certificates.

The ID card is founded on two principal mechanisms: an identification scheme and a digital signature. The card supports strong signatures (which is also a prioritised requirement). Most e-services only require the identification scheme, so the whole product (with the digital signature) is not always used.

Strong authentication is required for around 10 per cent of the electronic services. For lesser needs, users utilise the banks' ID mechanisms, and around 90 per cent of all transactions are executed this way. If there are no services available requiring higher levels of security or there is no great demand for them, one might argue that maybe then there is no true need for a more complex system. However, one manager at the State Information Systems Department responded to this observation by saying: "In Estonia, people asked: 'Why have an ID card when there are no services available and no users that demand them?' The answer is that the ID card has promoted more services that have then been demanded by users and attracted new users as well. It's like the chicken and the egg – which comes first?"

Legal framework

The E-Signature Directive was enacted domestically through the Digital Signatures Act in 2000, though this statute is more PKI-focused and more detailed than the E-Signature Directive.[106] The legislation regulates only one type of electronic signature – the digital signature, defined as a data unit, created using a system of technical and organisational means, that a signatory uses to indicate his/her connection to a document.[107]

A digital signature has the same legal effect as a handwritten signature under two conditions. These are that this effect is not restricted by law and that it is proven that the signature in question fulfils the requirements of a digital signature. The requirements of a digital signature are a) unique identification, b) preservation of data integrity, and c) determination of time of signing. It is considered as a general rule in the Estonian legal system that any digital signature compliant with the Digital Signatures Act is equivalent to the handwritten one in any private, business or administrative relationship, unless a specific law expressly stipulates otherwise.

[106] Digital Signatures Act of 8 March 2000 (consolidated law). Entry in force on 15 December 2000. The last law having amended this act entered in force on 01.08.2002.
[107] Article 2 (1) of the Act.

The digital signature can be said to be equivalent to the advanced electronic signature of the E-Signature Directive, with the additional requirement that it should be possible to determine the time at which the signature is made.

The non-discrimination rule of the E-Signature Directive has not been explicitly incorporated in domestic legislation. E-signatures not compliant with the Digital Signatures Act have no explicit legal value and their use is unregulated. However, any piece of information and document (signed or unsigned) may have a legal value recognised on an ad hoc basis. Use of electronic signatures may be restricted in certain circumstances (as defined by special law or acts requiring the involvement of a notary).

As for liability aspects, the E-Signature Directive has not been incorporated into Estonian law. There is instead a general liability clause holding CAs liable for damage resulting from violation of their responsibilities. Also the certificate holder can be held liable if his private key is abused due to his intent or gross negligence.

Foreign certificates are deemed to be equivalent to Estonian certificates if at least one of the following conditions is met: i) a foreign CA complies with requirements of the Digital Services Act and Estonian legislation, ii) the foreign certificates are guaranteed by a CA acting on the basis of the act, and iii) the certificates are recognised by an international agreement entered into by Estonia.

The Estonian laws and regulations that constitute the authentication framework mechanisms are:

i) Freedom of information and use of public sector information – Public Information Act[108]
ii) Data protection and privacy – Personal Data Protection Act[109]
iii) E-signatures – Digital Signatures Act[110]

Government services

The Estonian government uses the national ID card as an authentication solution for many kinds of e-services, and the number of services is increasing. The following services can be accessed with the eID card: online tax services (enables taxpayers to file, view and correct their income tax returns online and also to view their VAT returns and submit VAT refund applications, to calculate their social insurance contributions and to view their tax account balances); health card; contact information with schools between parents and teachers; tickets; e-invoicing; unemployment benefits; family allowances; and reimbursement or direct settlement of medical costs.

[108] http://www.esis.ee/ist2004/106.html
[109] http://www.esis.ee/ist2004/103.html
[110] http://www.esis.ee/ist2004/101.html

E-health

Estonia is also, together with Denmark, Lithuania, Norway and Sweden, involved in the Baltic e-health project to promote the use of e-health in rural areas of the Baltic Sea region by creating a substantial international infrastructure for e-health.

Finance

Estonia's largest banks, including Hansabank, AS Sampo Pank and SEB Eesti Ühispank, apply different systems. Normally they provide username and password versions with or without hardware tokens. Also, they provide the opportunity of using the national eID. Banks seem to prefer their proprietary systems and to promote them.

For instance, Hansabank has three separate authentication systems:

i) The first is the oldest, imposes the fewest requirements and has the lowest level of functionality. It is a system with a username and changing password, which allows the user to make transactions of up to €268 (equivalent to SEK 2,500. The system is free of charge.

ii) The second system has been in use for three years and allows transactions of up to €5,355 (equivalent to SEK 50,000). It is based on username and a hardware token that generates new codes. All businesses are required to use the system and approximately 40,000 businesses are connected to it. It costs approximately €10.70 (equivalent to SEK 100) to purchase the hardware device.

iii) The third system is based on the national eID. Use requires a card reader. The card costs €16 (equivalent to SEK 150), but the bank has no price for the card reading system as it did not provide it.

From the discussion it was evident that Hansabank preferred users to keep using the second system. Using Hansabank's authentication mechanisms, the customer could utilise a range of other services, such as tax declaration, health card, contact information with schools between parents and teachers, information on homework, bus tickets purchase, e-invoicing and utility payments.

Universities

The Tiger University programme seeks to support the development of ICT infrastructure and academic ICT staff and the infrastructure for postgraduate training. However, no particular focus on authentication has been expressed.[111]

[111] http://www.eitsa.ee/inenglish/tigeruniv_program.asp

3.1.7 FINLAND

Finland was among the first countries to launch a national eID-card.[112] The Population Register Centre issued the first certificates in Finland in 1999. In April 2003 the Population Register Centre became the country's first qualified certifier. The identification card is issued by local police departments, while the Population Register Centre supplies the onboard certificates used in electronic identification. In addition to the card, a card reader is needed for online use. A total of 61,200 electronic ID cards, bank cards and mobile SIM cards had valid citizen certificates as of 31 March 2005. The card is also an official travel document for Finnish citizens in 29 European countries.

The Finnish government recently complemented the online authentication system with a system based on the existing online standard. The Finnish electronic ID card was originally the universal method for e-government services, but its uptake has been modest due to issues of over-complexity in relation to security needs and low numbers of services available. The new system provides more flexibility as it offers the possibility of accessing some public services online with a card reader.

The vision for the development of e-government in Finland is for public administration to provide secure and user-friendly online services. Achieving this vision involves dealing with a number of constraints, such as inadequate awareness and user skills in SMEs, poor availability of networks in remote regions and slow progress in services using strong authentication (electronic ID card). In order to address the issues, the national government has committed to promoting "a flexible and reliable system of electronic authentication by keeping authentication as light as is compatible with the nature of each online service, making it device-independent and making it possible to use alternative authentication services".

In Finland there is a general understanding of the challenges posed by a lack of de facto international standards and too many national standards and systems. Competition between systems and standards makes choosing one a gamble. The country is working pragmatically to address this, as it is working to amend authentication of bank applications. Finland also participates in many of the international working groups and pilots that promote online authentication and initiated the Porvoo Group, which promotes use of smart ID cards for online transactions.

Finland and Estonia signed an agreement in 2003 to harmonise their concepts and practices regarding digital signature and document format and exchange.

Legal framework

The Finnish legal framework for authentication mechanisms consists of the following laws and regulations:

[112] http://www.fineid.fi/

i) Freedom of information – Publicity of Official Documents Act 1951, Openness of Government Activities Act 1999[113]

ii) Data protection and privacy – Personal Data Act 1999[114] and Amendment of the Personal Data Act 2000[115]

iii) E-commerce/e-signatures – Electronic Signatures Act 2003[116]

iv) Other – Electronic Service in the Administration Act 1999[117]

Government services

The Finnish government provides e-services for which authentication is needed. Approximately 50 e-services require the card, including social and healthcare services; tax filing; change of address; e-identity; and customs and excise. Certain crimes (property offences or acts of vandalism) can be reported online.

E-health

Since the beginning of June 2004, Finnish citizens can request to have their health insurance data included in their electronic ID card. Citizens who take advantage of this new possibility carry one card instead of two.

The National Research and Development Centre for Welfare and Health (STAKES)[118] is responsible for research on e-health in Finland. It produces information and know-how in welfare and health and sends it to policymakers and other actors in the field.

Finance

Finland has the highest per-capita number of online banking users. The country's largest banks – Nordea, Sampo and OKO Bank Group – have issued proprietary technologies mainly for authentication. Recently Finland accepted the use of bank authentication for a number of public services. However, some banks have also started utilising the public certification system, which is available for Visa Electron cards issued by OP Bank Group.

For example, Nordea has two proprietary systems for authentication. These include a PKI-based system with hard certificates which almost no one uses and a system with one-time codes which has 2.5 million users (and which is also used for eID in Finland and Denmark). This common interface, also used by other banks, allows customers to access a number of government services. They are, however, in discussion with BankID of Sweden and will most likely join that group during 2006. Nordea's system of one-time codes is considered beneficial and a good return on investment. It can be used in all channels, not only via the Internet, according to Nordea's IT strategy management department. It provides mobility

[113] http://www.om.fi/1184.htm
[114] http://www.tietosuoja.fi/uploads/hopxtvf.HTM
[115] http://www.tietosuoja.fi/uploads/p9qzq7zr3xxmm9j.rtf
[116] http://www.mintc.fi/www/sivut/suomi/tele/saadokset/telecom/norms/14-2003en.htm
[117] http://www.om.fi/2838.htm
[118] http://www.stakes.fi/english/

because it can be used for online and phone services and is inexpensive. Nordea's various relevant systems are based on proprietary technologies. Since banking is about trust, banks typically wish to provide secure technology over which they have firm control. They rarely use external technology vendors. Nordea operates in many countries but its systems are not interoperable between the countries and are hard to integrate. There are no major technical obstacles to establishing interoperability, though. The obstacles related to business considerations: companies compete with systems and solutions and there are political constraints on implementation.

Universities

The Finnish University and Research Network (Funet)[119] has the role of coordinating middleware activities in Finnish universities. Funet is a high-speed data communications network serving the Finnish research community. It connects more than 80 research organisations and 300,000 users. Funet services are maintained by the Finnish Information Technology Centre for Science (CSC), run by the Ministry of Education. CSC also coordinates Funet's network security and participates in developing services needed in information management for teaching and research. Membership of Funet is open to all Finnish university-level academies and public research institutions.

HAKA Federation is in a pilot phase and consists of Finnish universities. The members so far are the University of Helsinki, Tampere University of Technology, the University of Kuopio, Tampere Polytechnic and the portal of the Finnish Virtual University, the A&O learning management system at Tampere University of Technology and HUPnet at University of Helsinki. It is based on Shibboleth middleware.

3.1.8 SWEDEN

The goal of Swedish government policy is that public information and services should ideally be available electronically 24 hours a day and seven days a week. The government sets the overriding goals, removes obstacles in the form of legal barriers and supports government agencies by providing guidelines and methods and ensuring that the necessary common infrastructure for e-government comes into place. Government agencies have substantial freedom but some coordination is provided by the Swedish Agency for Public Management. Among the most popular agency websites is that of the National Tax Board. In recent years the number of people using the Internet to submit their income tax returns electronically has increased dramatically.[120]

The government has commissioned the National Tax Board to coordinate the administration of certificates for electronic identification and electronic signatures in order to ensure high security in electronic communication. The strategy is to establish an open solution in cooperation with the private market. A framework agreement has been reached with several banks, telecom operators, the Swedish Companies Registration Office and the

[119] http://www.csc.fi/suomi/funet/middleware/english/index.phtml
[120] See further, http://www.nyteknik.se/pub/ipsart.asp?art_id=40526

National Tax Board to offer electronic signature services and an electronic ID has been issued.[121] Using their eID, citizens can communicate with all government and some private sector e-services. Two channels provide eID and services, which are used by central and local government. The first is BankID, backed by a group of eight banks. The second is a certificate service provider joint venture between the Swedish Post, telecom operator Telia and Nordea Bank. Nordea has, however, indicated that it will join BankID during 2006.

Security solutions are complex and individual consumers mostly have incomplete information and therefore little ability to evaluate risks properly. This causes difficulties in facilitating trust. One solution to this issue might be incentive schemes. One successful initiative was a "carrot" offered by the National Tax Board which involved providing tax returns earlier to those who filed them online. In 2003, around 36,000 Swedes filed their taxes with e-authentication. In 2005, the figure was 350,000. Alternatively, Swedish banks have used a "stick" on customers by imposing costs for conducting bank transactions by traditional means rather than online.

According to a National Tax Board official, insufficient services are connected to the national eID. However, several new services are due to be added in the near future, such as extended banking services and income declaration. The initial investment in e-authentication per new user is quite significant (SEK 300[122]), which makes it vital to introduce new services to improve the cost-benefit ratio. However, more and more people are adopting e-legitimation.

The National Tax Board official further emphasised that services must be easy to use and that service providers must offer similar user interfaces to reduce confusion about what the ID is and what it is valid for. The underlying technical infrastructure should be treated separately, but the market needs coordination. Alternative solutions that support different technologies show up almost everywhere, which is a challenge for identification mechanisms that need to reach mass markets. Most actors support a unified and unanimously-adopted solution and PKI was thought to be it, but the market has so far responded coolly. Though some praise the trust model within PKI, it has so far not been successful. The official's conclusion is that something must be wrong, but exactly what is difficult to say.

Some actors contend that there is a lack of strategy and coordination. A representative of the Swedish Agency for Public Management said the lack of a common standard was a major problem and there was insufficient debate on solving this issue. The official identified the need for an actor capable of providing a strong voice on these issues. In the absence of such an actor, many small players are trying to grasp the initiative – often successfully. These players are often more interested in short-term personal results, raising question marks over achievement of a usable solution fit for the public. Some critics argue that a lack

[121] The Electronic ID can be hard and soft certificates, and are issued by a number of different actors. http://www.e-legitimation.se/

[122] Approximately €33.

of coordination has given rise to technological lock-in that hampers innovation. There are still few e-services that require authentication mechanisms, but they are steadily increasing.

Legal framework

Sweden has incorporated the E-Signature Directive into domestic legislation by way of the Qualified Electronic Signatures Act**.** The act applies only to certificate providers established in Sweden and that issue qualified certificates to the public. Thus all private entities which issue certificates for internal use or use within a closed user group are not covered. Neither are CAs that issue certificates to the public unless they are said to be qualified certificates.

The fact that all certificates issued in Sweden today are outside the scope of the act (no qualified certificates have been issued in Sweden) does not mean that they are denied legal validity. In most cases, an electronic signature has the same legal effect as pen on paper or an oral manifestation of will. Electronic signatures were already permissible as evidence prior to the directive because the principle of free sifting of evidence applies in Sweden and there are no rules denying legal effectiveness of electronic signatures.

Only in cases where the law requires a signature do qualified electronic signatures become relevant. Swedish law states that if a requirement in the law or regulation for a handwritten signature or its equivalent may be satisfied by electronic means, a qualified electronic signature (defined based on the requirements in article 5.1 of the E-Signature Directive) shall be deemed to fulfil this requirement.[123] This rule has had little impact, and from the Swedish government's report on form requirements in legislation (the FORMEL report)[124] it can be concluded that it will not gain any real relevance. The FORMEL report states that the intention is instead to remove requirements for handwritten signatures. This would remove obstacles to the use of electronic means and also facilitate application of the principle of free sifting of evidence, obviating the need for a qualified electronic signature. In cases in which handwritten signature requirements are still seen as valid (for example, for wills and other family law transactions), these will be maintained without opportunity for electronic signing.

The act defines electronic signature more narrowly than the E-Signature Directive. Its liability provision applies only to qualified certificates issued to the public, however. Since there are currently no such certificates issued in Sweden it is currently of theoretical value only in this context.[125]

As for foreign certificates, the act states that certificates which comply with the content requirements of a qualified certificate, issued by a provider that is not established in

[123] § 17 Act (2000:832) on Qualified Electronic Signatures.
[124] DS 2003:29.
[125] There is a presumption for liability in the circumstances listed in the law (as in the directive), in which case the certificate provider, in order to avoid having to pay damages, shall show that the injury or loss was not caused by the negligence of the certificate provider. However, the damaged party will have to prove the loss.

Sweden, will be deemed to be qualified under certain conditions.[126] The Swedish legal framework for authentication mechanisms encompasses the following laws and regulations:

i) Freedom of information – Freedom of the Press Act 1949.[127] Sweden was the first country in the world to introduce freedom of information legislation, with the Freedom of the Press Act of 1766. This statute was reviewed in 1949 and last amended in 1994.

ii) Data protection/privacy – Personal Data Act 1998 and Data Act 1973.

iii) E-commerce/e-communications – Electronic Commerce and Other Information Society Services Act 2002.[128]

iv) E-signatures – Qualified Electronic Signature Act 2000.[129] This act, which implements the EU Directive on Electronic Signatures, entered into force on 1 January 2001.

Government services

A number of authorities deploy e-services. Username and password, text message and PKI are the most common mechanisms. New work methods and organisational schemes have been established to handle the new technologies. The Infra Services programme has been launched to develop e-government by providing government agencies with standard e-identification and secure electronic messaging services on a pay-per-use or subscription basis. A new Swedish national ID card will also be released based on PKI technology.

Using electronic ID, citizens can file and alter their income tax declarations, download information from their tax accounts, file applications for change of tax base, register a company, print a personal certificate (paper), apply for family and other social security benefits, view information on their pension accounts, file change of address announcements and arrange transfers of post.

E-health

Carelink[130] facilitates cooperation and initiates and supports ICT development in healthcare in Sweden. Carelink was founded by the Swedish Association of Local Authorities and Regions, the Association of Private Care Providers and the Apoteket, the state pharmacy monopoly. Carelink has a decentralised structure, cooperating at local and regional level with public and private health service providers. It provides supportive services such as

[126] The conditions are the following: i) The certificate provider is established in another state within the European Economic Area, and is permitted to issue qualified certificates there; ii) The certificate provider satisfies requirements equivalent to those contained in §§ 9-12 (transposition of Annex II) and the regulations issued under § 13 (more detailed Government requirements), and is accredited in another state belonging to the European Economic Area; iii) The certificate is guaranteed as being qualified by a certificate provider referred to in point 1 or the first clause of § 6 (i.e. complies with the Swedish Act on Qualified Certificates).
[127] http://www.riksdagen.se/english/work/fundamental/press/index.htm
[128] http://www.notisum.se/rnp/SLS/LAG/20020562.HTM
[129] http://www.notisum.se/rnp/SLS/LAG/20000832.HTM
[130] http://www.carelink.se

directory services and security, information and the diffusion of best practices. Carelink is a coordination partner in national projects and networks and covers most of the perspectives that concern the development of ICT in healthcare. Classifications are, however, the responsibility of the National Board of Health and Welfare. Carelink is involved in numerous projects of interest when it comes to authentication in health.

Carelink has developed a system for secure email provision in the health sector that is more secure and cost-efficient than fax machines or mail clients, which are trusted channels today. Within the Baltic e-health programme, Carelink has examined how to connect Danish and Swedish ICT systems in the health sector and has identified a need for a gateway to connect the two. Also, a Swedish hospital has teamed up with Spanish actors that receive x-ray files for analysis and then return the results – a process that required the Spanish organisations to adapt to the Swedish system. There is a perceived need for international cooperation, primarily at EU level (where the IDABC programme may provide a way forward, even though it may take time). Interviewed experts did not consider authentication to be a major issue. Carelink is a CA but cooperates with other actors, one of which is BankID. Carelink does not see a need for these other actors to be CAs.

Some experts predicted that authentication solutions (specifically PKI) would relatively soon break through on a broad scale. Some regional health organisations have already deployed PKI systems. For example, in the region of Scania, more than 1,000 hospital employees use hard certificates.

Finance

BankID[131] is a service that offers secure online electronic identification and signature that is legally binding according to EU legislation. The service has been developed by a group of Swedish banks for use by public authorities, companies and other organisations. Currently, the banks that participate in BankID are Danske Bank i Sverige, Swedbank, Handelsbanken, Ikanobanken, Länsförsäkringar Bank, SkandiaBanken, Sparbanken Finn and Sparbanken Gripen. Other large banks, notably Nordea, have expressed serious interest and are expected to join the network in the near future. BankID can be used for a number of services, among them the e-government services mentioned above, and for logging in to the Internet bank. Customers of Ikanobanken, Sparbanken Finn and Sparbanken Gripen currently use BankID for login.

The participating banks had by early 2005 more than 2.7 million e-customers – over 70 per cent of the total number of e-customers in Sweden. Of them, 500,000 used the specific BankID technology and 370,000 were active users. They undertook between 2 million and 3 million transactions per week. BankID has recorded only 10 cases of fraud (and no pecuniary losses) during its existence.

[131] http://www.bankid.com/index.jsp

The participating banks set their price models themselves when providing authentication services to external parties. However, they pay per-transaction fees to BankID for online checks of the revocation list (OSCP), which they jointly own.[132]

An interesting application that BankID is rolling out with Ericsson, Telia and Vodafone is the WPKI,[133] which incorporates mobile phones in a two-factor authentication system.

SEB, one of Sweden's four largest banks, provides login with a password and a hardware token via a system it introduced in the mid-1990s. At the moment, the bank has no plans to switch technologies since the current system works well and establishing a PKI system is expensive. Low volumes of international transactions mean that SEB sees insufficient demand for such a service. SEB does not cooperate with other banks in e-signature but with telecom operator Telia.

SEB has branch offices in a number of countries, and each country has its own technologies. However, the central IT department sets minimum security levels for the local banks.

An SEB ICT strategy manager predicted that a variety of systems would continue to prevail and that no single one-stop authentication system would be established. He suggested that interoperability between banks would occur but would take five to seven years to achieve. One positive factor was the launch of the new EU passport, to which CAs will be able to download their certificates.

Banks are not necessarily interested in interoperability as such, however. Authentication is not primarily a way to acquire new customers. One view is that interoperability between systems makes it easier for customers to switch banks – a process to which a bank in a delimited geographical market may be reluctant to contribute. Some banks show greater interest in launching new technology whereas others tend to follow developments. In Sweden, Swedbank and Handelsbanken cooperated closely in launching BankID. SEB has preferred to follow its own track, while Nordea has declared an intention to join BankID during 2006. This pattern reflects divergent interests in coordinated solutions and may also reflect divergent assessments of what technologies will prove successful in the future. The future prospects of BankID will be influenced by the combined efforts, strategies and expectations of utility among market actors, on the one hand, and on the development of future security and authentication issues on the other hand.

Universities

SwUPKI[134] is the Swedish PKI for universities and university colleges operated by Stockholm University and Umeå University. SwUPKI is composed of the Policy Management Authority (PMA) and the Policy Certificate Authority (PCA). The PMA is responsible for SwUPKI certification policy and also approves membership applications.

[132] Senior Advisor, BankID.
[133] See further section 4.2.
[134] http://www.swupki.su.se/org.shtml

The PCA operates the CA, publishes certificate revocation lists and the CA repository for SwUPKI. The PMA is operated by Stockholm University and the PCA is operated by Umeå University.

3.1.9 HONG KONG

Everyone who holds a valid Hong Kong identity card issued on or after 1 July 1987 and before 23 June 2003 is required by law to apply for a smart identity card.[135] As there are about 6.9 million cards to be replaced, it is expected that the whole exercise will last for about four years. Groups of people will be called up according to their year of birth. Details will be published in the newspapers, announced on radio and television and posted on a website. The new card includes a chip containing an ID number and the person's name, date of birth and digital fingerprint reference data.

Apart from being an identification document, the smart ID card offers the option of an e-Cert, issued free of charge for one year by Hongkong Post[136]. In processing an e-Cert application, Hongkong Post is required to verify the applicant's identity. Hence, it is necessary for the applicant to complete a face-to-face identity verification process for delivery of the PIN envelope and to be able to issue the e-Cert. As of 1 August 2004, over 420,000 persons had chosen to embed their Smart ID Card with an e-Cert.

The e-Cert can be used to sign various kinds of documents and to access e-services such as email encryption, online entertainment, stock trading, payment and online banking. The e-Cert can be used via public or personal computers equipped with a smart card reader. Electronic services delivery (ESD) kiosks and public computers are used to perform e-government and e-commerce transactions. ESD kiosks are accessible in various locations, including supermarkets and shopping centres. More than 400 public computers are equipped with card readers to facilitate the use of the e-Cert stored in the smart ID Card. These public computers are provided in locations such as public libraries and Hongkong Post outlets.

Some critics have argued that Hong Kong focuses too much on PKI and that this will eventually prevent it from adopting more cost-effective solutions that will emerge, as well as lock the territory into a technology that might quickly become obsolete.

Legal framework

The Hong Kong Electronic Transactions Ordinance 2000[137] is not technology-neutral legislation but rather quite PKI-specific (like several other Asian e-signature statutes). It

[135] http://www.smartid.gov.hk/en/index.html
[136] The Hong Kong government's provider of postal, courier and other associated services to the public
[137] Electronics Transactions Ordinance (2000) Ordinance No.1 of 2000, Legal Supplement No.1 to the Government of The Hong Kong Special Administrative Region Gazette, 7 January 2000

authorises the use of electronic and digital signatures but only gives legal recognition to the latter. It defines electronic signature but ties no legal effect to the definition.[138]

If the law requires a signature from a person, that requirement can be met with a digital signature. However, the digital signature should be based on a so-called recognised certificate. A recognised certificate is issued by a CA that has been approved under a voluntary recognition system. Such a CA is called a Recognised Certification Authority (RCA).[139]

The main benefit of CA recognition is that the ordinance affords significant limitations on the potential legal liabilities of RCAs. For example, RCAs are not liable for loss caused by reliance on false or forged digital signatures supported by certificates issued by them, provided that they have complied with due requirements. RCAs may also specify reliance limits in their certificates.

The ordinance has no provisions in respect of acceptance of foreign Certification Authorities and certificates.

Government services

The government is trying to assist development of electronic commerce with the implementation of its ESD programme. The first phase of the ESD scheme was launched in the latter half of 2000 for the delivery of government services online to the public via the Internet and other electronic means. Under the first phase of implementation, ten government departments and public agencies provided a range of services, including submission of simple tax returns and tax payment; driver's and vehicle licence renewal; business registration certificate application; guides on investment in Hong Kong and advice on business licensing requirements; payment of rates; government rent and water charges; and job search and matching services.

This has been substantially extended and currently there are over 200 electronic public services (excluding more than 50 hyperlinks to departmental websites) provided by some 60 government departments and agencies. The government of Hong Kong has gathered all available e-services (ESD) in an easy-to-use portal, including a list of the 30 most popular services. Of these, 20 require some sort of signature for use.[140] Subsequent phases are to be implemented on an ongoing basis. In the long run, the government aims to include all public services amenable to electronic delivery.

[138] Electronic signature means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authentication or approving the electronic record.
[139] Regulatory authority is conferred on the Director of Information Technology Services, a government official, to 'recognise' CAs.
[140] http://www.esd.gov.hk/gov_dept_index/eng/all_depts.asp

E-health

Electronic health records[141] can be submitted via email conforming to the simple mail transfer protocol (SMTP) and the secure multipurpose Internet mail extension (S/MIME) standards promulgated by the Internet Engineering Task Force (IETF) provided they do not exceed 5MB. If digital signature is not applied, compliance with the SMTP standard suffices. If digital signature is required, compliance with the S/MIME standard is necessary.

Only a digital signature supported by a recognised certificate issued by a CA recognised in accordance with the ordinance is acceptable. A digital signature must be attached to an electronic record in compliance with the secure multipurpose Internet mail extension (S/MIME) and public key cryptography (PKCS) standards. For an electronic record which comprises multiple electronic files and which has to be signed, each individual file must be separately signed digitally.

Finance

Numerous financial institutions in Hong Kong provide online services, using the e-Cert and other authentication technologies.

Bank of East Asia[142] provides a service it calls corporate cyberbanking that enables users to conduct banking transactions and manage their finances. The Hongkong Post's Bank-Cert is used for authentication. Users can submit account enquiries, make transfers to local and overseas accounts, manage MPF contributions, apply for and amend letters of credit and submit payroll payment files.

CITIC Ka Wah Bank's[143] online service provides links to trade initiation and cash management activities via the Internet. It consists of the import and export trade transactions system Click2Trade Station and Internet cash management services that allow users to conduct cash transactions on the Web. E-Cert is used for authentication.

Dah Sing Bank[144] users can use Hongkong Post e-Certs or Bank-Cert (Dah Sing Bank-Personal) to log in to use online banking services such as bill settlement by credit card, fund transfers to Dah Sing Bank or other local bank accounts, e-deposits, balance information, scheduling of fund transfers and bill payments.

E-Cert enables a range of services including fund transfers, credit card and other bill settlements, account information and financial market information enquiries.

[141] http://www.info.gov.hk/dh/forms/manner.htm
[142] http://biz.hkbea-cyberbanking.com/index_eng.html
[143] http://www.ckw-b2beb.com/
[144] http://www.dahsing.com/

Shanghai Commercial Bank[145] corporate Internet banking system (CIBS) uses Hongkong Post e-Certs. Users can log in to use cash management, MPF, payroll and trade finance functions.

Universities

The Hong Kong University Certification Authority (HKUCA)[146], run by the HKU Computer Centre, issues HKU digital certificates (HKU-Cert) to current HKU staff and students (HKU members).

The HKU-Cert of a HKU member serves as a digital identity for authentication and electronic signing using HKU electronic services delivery (HKUESD) of digital signature applications.

Since February 2002, HKUCA has issued HKU-Certs (server) to administrators of approved computer servers. The server named in a HKU-Cert (server) can use the certificate in applications employing secure socket layer (SSL) encryption.

Note that HKUCA has not sought Recognised CA status, as defined in the Electronic Transactions Ordinance, from the director of the information technology services department of the HK SAR government.

3.1.10 UNITED STATES

The US federal government has launched an e-authentication initiative[147] that provides online identity verification to e-government services. The service is based on open standards and is organised as a federated approach that incorporates many service providers and technologies to meet the diverse authentication needs of government agencies, customers, citizens and businesses. It will deliver a uniform, government-wide approach to authentication while providing government agencies with a choice of technologies and interoperable products to achieve their authentication needs. The federated approach was chosen as a means to overcome trust issues, allowing individuals to use the authentication technology that is acceptable to government institutions.

The system works so that the application user selects the agency application and which authentication provider he wants to use (at an access point of his choice). The user is then redirected to the authenticating partner, where he is checked. If the user does not possess credentials he is offered the opportunity to acquire these before proceeding. After being authenticated, the user is redirected to the agency application. Authentication service

[145] http://www.shacombank.com.hk/EN/ibk_cibanking.html
[146] http://www.hkuca.hku.hk/
[147] http://www.cio.gov/eauthentication/

providers are classified according to varying risk assurance levels, where level four represents the highest and level one the lowest in terms of risk protection.[148]

Working together with the e-authentication programme is the Electronic Authentication Partnership,[149] which is a voluntary joint venture for digital authentication governance among stakeholders from all levels of government, the private sector and public interest groups.[150] The group establishes and maintains common policies and practices for authentication providers that will facilitate trust, interoperability and the easy evaluation and acceptance of various types of credentials issued by other parties. Those involved have international ambitions and want to work cooperatively with other nations' identity systems.

The federal government has also set up the Federal Bridge Certification Authority (FBCA), which is an interoperability mechanism designed to facilitate interoperability among US Federal PKI domains and between the US federal government and external PKI domains on a peer-to-peer basis. The US government will accept certificates if the issuing CA has cross-certified with the FBCA. The Federal PKI Policy Authority (FPKIPA) is the governing body for the FBCA and has by-laws and procedures under which the FBCA operates. At the FPKIPA's discretion, agencies may choose to interoperate among themselves without using the FBCA. Those agencies that elect to do so may nonetheless employ levels of assurance that mimic those set forth in the FBCA CP.

The X509 certificate policy defines five certificate policies for use by the FBCA to facilitate agency CA interoperability with the FBCA and with other agency PKI domains. The five policies represent four different assurance levels (rudimentary, basic, medium and high) for public key digital certificates, plus one assurance level used for testing purposes. The word assurance used in this CP indicates at what level a relying party can be certain of the identity binding the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the relying party can be certain that the individual whose subject name is cited in the certificate controls the use of the private key that corresponds to the public key in the certificate.

[148] The following service providers, sorted after assurance level and technology employed, are working with the programme; Level 4 and the highest level of security: Department of the Treasury, PKI; Department of Defense, PKI; Department of State, PKI; Federal Common Policy Framework, PKI; Level 3: Department of the Treasury, PKI; NASA, PKI; USDA/National Finance Center, PKI; Department of Defense, PKI; Department of Energy, PKI; ACES/DST, PKI; State of Illinois, PKI; ACES/ORC, PKI; Federal Common Policy Framework, PKI; Level 2: USDA E-Authentication Svc., Password ORC, Inc.; Password; OPM-Employee Express, PIN; Level 1: ORC, Inc., Password; USDA E-Authentication Svc., Password; NSF FastLane, Password.

[149] http://www.eapartnership.org/

[150] The new board of directors, which was elected in January 2005, is composed of 16 members from Microsoft Corporation, BITS, KPMG, State of West Virginia, representing the National Association of State Auditors, Comptrollers and Treasurers (NASACT), Wells Fargo, General Motors Corporation, American Association of Motor Vehicles Administration, VeriSign, Inc., NACHA – The Electronic Payments Association, Mortgage Bankers Association, Northrop Grumman, US Computer Emergency Readiness Team, Postsecondary Electronic Standards Council, Sun Microsystems, representing the Liberty Alliance Project, Health Information and Management Systems Society (HIMSS)

The FBCA provides documentation on how external entities can act to facilitate cross-certification and interoperate their PKIs with the FBCA. This information is provided in a document entitled US Government PKI Cross-Certification Methodology and Criteria.[151]

The US private sector has also been working actively to develop authentication methods and to facilitate interoperability. Major initiatives with global implications have been launched, such as the Liberty Alliance,[152] Identrus[153] and Web Services Federation Language.[154] Furthermore, Sun and Microsoft have jointly developed interoperability protocols that will enable browser-based single sign-on between Liberty Alliance and Web Services Federation Language solutions. Microsoft is also working on a system to wrap up identity management systems under a single identity metasystem. The interoperable architecture would allow for several digital identities based on multiple underlying technologies, implementations and providers.

Work is progressing and there are many great initiatives, though they tend to be supply-driven and end-users have not yet completely adopted the technology. Many respondents indicated that major security problems are attached to end-users who do not apply an appropriate infrastructure in the home to protect their PCs. Furthermore, there is also a lack of international recognised standards for authentication.

Legal framework

The US, like many other common law countries (including Canada, Australia, Ireland and the UK), has adopted e-signature legislation based on or influenced by the UNCITRAL Model Law on Electronic Commerce.

The Uniform Electronic Transactions Act (UETA)[155] drafted by the National Conference of Commissioners on Uniform State Laws (NCCUSL) has been implemented in many US states. It includes a non-discrimination rule stating that a signature may not be denied legal effect solely because it is in electronic form. The act further establishes the equivalence of electronic signatures and manual signatures by stating that an electronic signature satisfies legal requirements for a signature.[156] Execution of wills, codicils and testamentary trusts are exempted, however.

As for the definition of an e-signature, it is "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record". Thus, no specific technology is needed to create a valid

[151] http://www.cio.gov/fbca/documents/crosscert_method_criteria.pdf
[152] See Section 3.2.1
[153] See Section 3.2.2
[154] See Section 3.2.1
[155] Uniform Electronic Transactions Act, 1999 National Conference of Commissioners on Uniform State Laws (NCCUSL).
[156] These provisions are based on UNICTRAL Model Law on Electronic Commerce, Articles 5 and 7.

signature, though there is a need for an intention to sign. This is the differentiating factor compared to a purely technical use of an electronic signature technology.[157]

The US Electronic Signatures in Global and National Commerce Act[158] (E-SIGN Act) is a federal law intended to facilitate the use of electronic communications. It imports many of the provisions of UETA into the federal legislation and does not deviate from UETA in its electronic signature approach.

Since US legislation does not address any specific types of authentication mechanisms or electronic signatures, the issues of cross-border acceptance and which certificates should be accepted do not arise (cf. the case of non-qualified electronic signatures). Nor are liabilities or damages dealt with in the law.

i) Acts -

- Government Paperwork Elimination Act 1998 (GPEA)
- Uniform Electronic Transactions Act (UETA)
- Electronic Signatures in Global and National Commerce Act (E-SIGN)

ii) Legal cases – court decisions discussing the effect and validity of digital signatures or digital signature related legislation.

- In re Piranha Inc 2003 WL 21468504 (ND Tex), stating that UETA does not preclude a person from contesting that he executed, adopted, or authorised an electronic signature that is purportedly his.
- Cloud Corp v Hasbro, 314 F.3d 289 (7th Cir, 2002), stating that E-SIGN does not apply retroactively to contracts formed before it took effect in 2000. Nevertheless, the Statute of Frauds was satisfied by the text of emails plus an (apparently) written note.
- Sea-Land Service Inc v Lozen International, 285 F.3d 808 (9th Cir., 2002), ruled that internal corporate email with signature block, forwarded to a third party by another employee, was admissible over hearsay objection as a party admission, where the statement was apparently within the scope of the author's and forwarder's employment.

Government services

As mentioned above, the US government has launched an e-authentication programme as a key part of its drive to create an effective infrastructure for e-government services. The official federal government website provides an entry point to many government online

[157] Section 2 Definitions, Comment to 7. "Electronic Signature", Uniform Electronic Transactions Act, 1999, with Prefatory Note and Comments, National Conference of Commissioners on Uniform State Laws (NCCUSL) 1999.

[158] Public law 106-229 Electronic Signatures in Global and National Commerce Act, 2000.

services.[159] Government e-services include: contact with the US government; filing of tax returns; wage report filing; state business licence applications; export licence applications; online training; registration of employer ID numbers; verification of employee social security numbers; health plan comparisons; information on government benefits; government grant applications; government job applications; notification of address changes; driver's licence renewal; passport application and renewal; finding vital records; social security benefit applications; immigration case status checks and contacting elected officials.

Among the many pilots that have been launched are a Department of Transportation smart card pilot project, which aims to distribute smart cards to approximately 10,000 FAA employees and contractor personnel for access to the department's facilities. In July 2002, the Department of the Treasury announced plans to launch a pilot project to assess the use of smart cards for a variety of purposes, including physical and logical access. The Treasury plans to distribute smart cards equipped with biometrics and PKI capabilities to approximately 7,200 employees during the pilot. The Department of Defence started to prepare for a Common Access Card (CAC) programme in 2000 and expected to provide the device to about 4 million military, civilian and contract employees. According to DOD programme officials, the department will likely have expended more than US$1 billion on its smart cards and PKI capabilities by 2006.

E-health

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) aims to make the healthcare industry more efficient. Online services are an important part of HIPAA and there have been many discussions about national identifiers as part of a new infrastructure. The Secretary of Health and Human Services (HHS)[160] intends to publish a proposed rule on requirements for a unique health identifier for individuals. The plans have encountered strong objections from organisations concerned about privacy issues, and have been halted. A national provider identifier (NPI) has been launched, however. This is a unique health identifier for healthcare providers to use in filing and processing healthcare claims and other transactions.

An interesting pilot is the WGA Health Passport Project (HPP) in Nevada, North Dakota and Wyoming, which will service up to 30,000 clients. A report on that project acknowledged that it was complicated and costly to manage card issuance activities. The states encountered problems when trying to integrate legacy systems with the smart cards and had difficulty establishing accountability among different organisations for data stored on and transferred from the cards. The report further indicated that help desk services were difficult to manage because of the number of organisations and outside retailers (as well as different systems and hardware) involved in the project. WGA officials said they expected costs to decrease as more clients were provided with smart cards and the technology

[159] http://www.firstgov.gov
[160] http://www.os.dhhs.gov/

became more familiar to users. They also believed smart card benefits would exceed costs over the long term.

Finance

All major banks in the US provide online services. The majority deploy various username and password solutions, many with a token device to generate codes. A challenge for the banks, however, is that consumers have not indicated a willingness to pay for increased online security, even though there are indications that online risks are significantly affecting consumer behaviour. PKI, meanwhile, is faced by high costs and overly complex solutions. Gartner Group reports that nearly 30 per cent of those who bank online say that online attacks have influenced their Internet banking activities. Over three-quarters of this group log in less frequently and nearly 14 per cent of them have stopped paying bills online. Some 2.4 million online consumers report losing money directly because of phishing attacks.

Banks are launching new and improved solutions. Many are currently upgrading with different kinds of two-factor identification, using hardware token solutions for strong authentication from RSA. Also, Identrus and IBM have released new technology allowing banks to enhance security. Many of the initiatives in the US are global in nature and information is provided in Section 3.2.

Universities

Most US universities have deployed some kind of authentication technology for multiple purposes, ranging from very simple low-cost solutions to highly complex and costly ones. Nevertheless, these technologies are not yet interoperable. However, the Internet2 group has initiated the Shibboleth[161] project to create a federated identity management system. Shibboleth is an open-source, standards-based architecture providing trusted, inter-institutional access to Web resources. It consists of software resident on both the browser user's campus (the identity provider component, which authenticates the user and then provides trusted assertions about the person) and the resource provider site (the service provider component, which obtains and validates the assertions and makes an access control decision). When an unidentified user attempts to access services, Shibboleth initiates a handshake between the service and identity providers. During that process, the identity provider creates attribute assertions that describe the browser user to the service provider.

3.2 INTERNATIONAL ACTORS

Numerous initiatives around the globe provide authentication services and various regulatory systems influence the framework for transactions. There are indications of increased interaction between systems at national level. For example, authentication in bank systems is used for government services such as taxation and declaration. Also, it concerns the interaction between national systems, such as between Finland and Estonia, for cross-

[161] http://shibboleth.internet2.edu

recognition aspects between the APEC countries, or for the support of cross-recognition between European CAs. However, transaction distributors face challenges at international level because the nature of the Internet does not support one single jurisdiction, standard or technology. There are other challenges, too. This section describes current conditions for authentication of global digital transactions and analyses and assesses leading actors according to the economic, organisational, legal and technical factors that impact on the enabling of digital transactions.

3.2.1 ECONOMIC ASPECTS

A key element for reliable and high-quality e-service transactions is trust. Online authentication has been identified as a key enabler for trust. The technical building blocks are all there, and many authentication projects and providers are in active operation. The conditions are emerging for broad interoperable solutions, based on established common policies, best practice guidelines and international coordination. Effective and cost-efficient introduction of a global, accepted, easy-to-use system for online interactions requiring a certain level of authentication would provide economies of scale to governments and businesses and empower individuals to benefit directly from information society services and applications.

Governance depends on networks and actors (such as governments, legislators, standards organisations, private-public partnerships and private interest groups in many places) and on mixed geographical scales. There are a few global organisations for Internet management, but these are traditionally narrow in scope and functionally delimited to specific purposes (for instance ICANN[162]). These organisations have benefited from the involvement of dedicated enthusiasts and limited politicisation. So far they have been quite successful. With the convergence of the Internet and the addition of traditional networks and services, such as telephony, that have previously been subject to tighter regulation through bodies such as the ITU[163] and higher requirements on quality of service in delivery, there is increased impact from top-down interference and regulation. Different cultures and approaches also need to align. There has been criticism that existing arenas which address governance issues seldom incorporate the opinions and needs of consumers and citizens.

There are quite a few actors, as can be seen from the presentation of noteworthy ones below. Nevertheless, there is a proliferation of standards and solutions which are not interoperable. Whether this is temporary or will be overcome by existing initiatives will become clear in time.

- In 2000, the former APEC TEL Electronic Authentication Task Group developed the concept of cross-recognition, which can be defined as an interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a subject in the

[162]http://www.icann.org/
[163]http://www.itu.int/home/index.html

other PKI domain, and vice versa.[164] APEC has developed draft guidelines for schemes to issue certificates capable of being used in cross jurisdiction e-commerce.[165] APEC has also recently released guidelines for PKI.[166] The issue is how these interoperability approaches can be extended across jurisdictions. The APEC approach to this problem is for recognition to occur at the scheme level rather than the individual CA level. Thus where a scheme recognises another scheme, it automatically recognises any CAs accredited under the scheme.

- The Asia PKI Forum[167] is an international non-profit organisation, established in 2001, whose purpose is to promote joint work to secure interoperability among national and regional PKI solutions in Asia and Oceania. The Asia PKI Forum working groups are divided into two areas: business working groups and technical working groups.
- ATHENA[168] aims to contribute to seamless interoperation among enterprises by providing reference architectures, methods and infrastructure components that solve interoperability difficulties, supported by a large, representative European community.
- The European Electronic Signature Standardization Initiative (EESSI)[169] was created in 1999 by the ICT standards board to coordinate standardisation activity resulting from implementation of the EU Directive 1999/93/EC on electronic signatures. Standardisation activities were carried out in the CEN/ISSS E-sign workshop and the ETSI TC SEC/ESI. The references to the required standards were published in the Official Journal in July 2003. These standards are part of a longer list of specifications defined by EESSI and included in its work programme. With the publication of this full set of standards, EESSI has fulfilled its mandate and ICTSB decided to dissolve the EESSI working group in October 2004.
- The eEurope Smart Card (eESC) initiative, launched by the European Commission in December 1999, aims to accelerate and harmonise the development of smart cards across Europe and to establish them in all shapes and forms as the preferred mobile and secure access key for citizen and business information society services. The Open Smart Card Infrastructure for Europe (OSCIE) is the result of three years of cooperation within eESC and has provided relevant deliverables in the areas of identification, authentication and electronic signature interoperability. Two demonstrations have been launched to prove the validity of OSCIE-produced documentation: ePOCH (national public

[164]http://webapps.apec.org/content/apec/news___media/media_releases/010405_secureintlecommerceguidelines.downloadlinks.0001.LinkURL.Download.ver5.1.9
[165]http://www.apectelwg.org:8080/admin/document/documents/Guidelines%20For%20Schemes%20To%20Issue%20Certificates%20Capable%20Of%20Being%20Used%20In%20Cross%20Jurisdiction%20eCommerce.doc
[166]http://webapps.apec.org/content/apec/news___media/media_releases/010405_secureintlecommerceguidelines.downloadlinks.0001.LinkURL.Download.ver5.1.9
[167]http://asia-pkiforum.org/NEW/01_aboutus/sub01.php
[168] http://www.athena-ip.org
[169] http://www.ictsb.org/EESSI_home.htm

identity and city-based e-services cards) and Netc@ards (a pan-European social services entitlement card).

- IATA/ICAO is a machine-readable document. Recently imposed security measures by the US government on foreign visitors require passports need to incorporate biometric information in their magnetic strip. As a result, it is possible to incorporate a digital identity into the passport. Passports will incorporate Rfid and identification technologies.
- The Internet Society (ISOC)[170] is a professional membership society with more than 100 organisations and over 20,000 individual members in over 180 countries. It addresses issues that confront the future of the Internet and is the organisational home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The Internet Society acts not only as a global clearing house for Internet information and education but also as a facilitator and coordinator of Internet-related initiatives around the world. The society's board of trustees is its governing body and is responsible for the organisation's affairs worldwide. IETF's by-laws state that the board of trustees must consist of no more than 20 trustees unless and until this number is changed by the board.
- The International Telecommunication Union (ITU)[171] is headquartered in Geneva, Switzerland. It is an international organisation within the United Nations system that brings together governments and the private sector to coordinate global telecom networks and services.
- Liberty Alliance is a US-based organisation that provides a platform for organisations to formulate and bridge the fragmented field of authentication. Its members include 14 large corporations from a variety of sectors and countries around the world. A number of leading organisations have deployed Liberty specifications to create interoperability, including AOL, Ericsson, HP, Nokia, Novell, NTT, Sun Microsystems and Vodafone.
- The OASIS PKI Member Section[172] was established as PKI Forum in 1999 to foster support for standards-based, interoperable PKI as a foundation for secure transactions in e-business applications. OASIS (Organisation for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence and adoption of e-business standards.[173] The consortium produces more Web services standards than any other organisation, along with standards for security, e-business and standardisation efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 4,000 participants representing over 600 organisations and individual members in 100 countries. The OASIS PKI member section brings member organisations together in a

[170] http://www.isoc.org/
[171] http://www.itu.int/home/index.html
[172]http://www.pkiforum.org/
[173]http://www.oasis-open.org/who/

neutral setting to increase knowledge about PKI and to initiate studies and to demonstrate projects that show the value of interoperable PKI and PKI-based solutions. The group collaborates and cooperates with appropriate standards and testing bodies to promote the adoption of open industry standards.

- The Porvoo eID Group, launched in 2002, is an informal international cooperative network of government and industry representatives from 16 EU and accession countries. The aim is to promote the potential of interoperable electronic public identities using PKI and smart cards in order to help ensure secure public and private sector e-transactions in Europe. The Porvoo Group is lobbying leading PC manufacturers to integrate a standard card reader in the motherboard as default in at least a selected range of new PCs. The Porvoo Group supports inclusion of interoperability aspects in international standards for smart cards, certification infrastructure and biometrics.
- World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software and tools) to harness the Web's full potential as a forum for information, commerce, communication and collective understanding.
- WS-Federation has partners including IBM, BEA, Microsoft, Verisign and RSA Security. It provides a specification for standardising the way organisations share user and machine identities among disparate authentication and authorisation systems (Web Services Federation Language). However, with IBM now being part of the Liberty Alliance, many observers predict that the competing standards will eventually come together.

3.2.2 ORGANISATIONAL ASPECTS

Just as there are few established international organisations for governance, so there are few trusted service providers. This deficit could perhaps be overcome by banks and actors such as chambers of commerce or law firms. Trusted organisations like banks have joined together to provide such services (for example, Identrus). Critics of the current solutions say they are too supply-oriented, too top-down and do not respond appropriately to existing demands. Interoperability is seen by many as a key to transacting data across sectors and borders, and solutions that enable interoperability need to retain a flat structure and be more organised towards the web of trust style.

An interesting approach, which nevertheless is top-down, is WISeKey, which is established in Switzerland, a neutral country with a history of providing trustworthy services like banking (which connotes trust). WISeKey has teamed up with trustworthy actors like ITU, but it remains to be seen whether it can establish itself as the root authority. There are challenges which need to be resolved but that may be difficult to overcome, such as political and cultural differences and desires. In particular, it is problematic for participating countries and organisations to give up autonomy to another country or organisation.

A common argument for low usage at national level is government demand for flat-rate authentication subscriptions, whereas service providers offer per-transaction cost models. Similarly, there may be issues regarding system interaction. Knowledge and inspiration could probably be gained from mobile phone roaming.

A number of service providers are presented below that are active internationally but which have varying organisational approaches. As can be seen, the majority are still restricted to one or a few different sectors.

- The Athens[174] Access Management System (AMS) controls access to Web-based subscription services. This service from Eduserv Technologies has been in active use since 1996, principally in the UK's higher education community, providing access to many centrally-funded Web-based services. Athens is the de facto standard for higher education in the UK. Furthermore, Athens has been utilised by education and research councils for access management. Athens has also been adopted by the National Health Service Information Authority to control access to the National Electronic Library for Health (NeLH). Athens now protects many of the services provided under this umbrella and is steadily gaining ground among health authorities. It is interoperable with Shibboleth.
- Bolero[175] is a platform that seeks to secure paperless trading between buyers, sellers and their logistics service and bank partners. The solution integrates physical and financial supply chains and aims to provide visibility, predictability, accuracy and security. Bolero was founded by SWIFT,[176] and the Thorough Transport Club (TT Club).[177]
- ChamberSign[178] was founded by Eurochambres, the Association of European Chambers of Commerce and Industry in 1999 with nine national member organisations. ChamberSign represents 579 local chambers of commerce. It aims to create a comprehensive architecture for secure B2B electronic commerce across international borders. The focus is to promote and enable strong authentication and digital signature technology, making it available and achieving international recognition and interoperability. ChamberSign sees implementation of an international CA covering the different national requirements for e-government as a major challenge.
- Identrus[179] is a company founded as a trust authority by ABN AMRO, Bank of America, Bankers Trust (since acquired by Deutsche Bank), Barclays, Chase Manhattan, Citigroup, Deutsche Bank and HypoVereinsbank in April 1999. Identrus today has approximately 60 participating financial institutions

[174] http://www.athensams.net/
[175] http://www.bolero.net/
[176] SWIFT is the industry-owned cooperative supplying secure, standardised messaging services and interface software to 7,600 financial institutions in 200 countries.
[177] The TT Club is the international transport and logistics industry's leading provider of insurance and related risk management services.
[178] http://chambersign.com
[179] http://www.identrus.com/

worldwide. It has developed a rule book and technology standards to enable banks to issue digital certificates to their customers and accept digital certificates issued by other member banks.

- SWIFT[180] is a not-for-profit association owned by banks. It operates the SWIFT private network which provides secure messaging between the majority of banks and other financial institutions. It is moving to IP via SwiftNet, which will be outsourced and managed by Global Crossing. This infrastructure may become the backbone for interoperability between banks.
- WISekey[181] is Swiss-registered company headquartered in Geneva and founded in February 1999. WISeKey provides a common global root certificate. The company believes this common global root should solve the problem of cross-certification as more and more countries, corporations and industry sectors set up certification authorities for their communities of interest. WISekey's solution to the discussion on whether to use a shared common global root certificate versus cross-certification is that a common global root is preferable and that the only realistic geopolitical solution lies in Switzerland, the home of almost all non-politically based inter-governmental and international organisations. WISeKey has partnerships with the International Telecommunications Union (ITU), HP, Microsoft and SUN.

3.2.3 LEGAL ASPECTS

Standards and the law

If digital signature implementations are to be meaningful they must get the technical and legal aspects right. Many of the technical and related legal issues surrounding PKI have benefited from a high level of standardisation. These standards can have real legal implications; industry standards that have developed over a long period of time are often seen as an expression of current practice and thus considered to represent a "norm" for a certain sectors or areas. An example of legal relevance of a standard is when assessing whether someone has been negligent or not. If a party has followed a standard (such as RFC 2527 or RFC 3647[182]), a judge will likely presume that the party was not negligent.

Bodies that develop and publish authoritative PKI-related standards include IETF at the international level and the European Committee for Standardisation (CEN) and European Telecommunication Standards Institute (ETSI) in the EU.

Standards may also assume legal importance if the law makes reference to them. An example is the European Directive on Electronic Signatures, which enables the European Commission to publish the references to standards considered "generally relevant" for its implementation. Such standards were drawn up by CEN and ETSI under the auspices of

[180] http://www.swift.com/
[181] http://www.wisekey.com/
[182] Even though the RFC are working documents, they are in effect used as standards.

the European Electronic Signature Standardisation Initiative (EESSI) and adopted by the European Commission. This means that meeting such standards entails a presumption that the applicable requirements of the e-Signature Directive have been met, although nothing prevents a party from meeting those requirements in another way.

International forums

At the global level, harmonisation efforts have been led by UNCITRAL.[183] In 1996, UNCITRAL adopted a Model Law on Electronic Commerce[184] that has become the basis for much worldwide e-commerce and e-signature legislation. The law does not specifically regulate digital or electronic signatures but includes more general rules that can be helpful in signature use. The basis is a so-called non-discrimination rule, according to which information should not be denied legal effect solely on the grounds that it is in the form of a data message.[185] This is also called the functional-equivalent approach, which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic commerce techniques. The model law further provides that a signature requirement in law can be met in relation to a data message if the method used is as reliable as was appropriate for the purpose. The method should identify the signer and also indicate the signer's approval of the information.[186] The law also includes a provision that data messages should not be denied admissibility in legal proceedings on the sole ground that it is a data message.[187]

UNCITRAL sought to provide further guidance on electronic signatures by developing a Model Law on Electronic Signatures.[188] It restates the rule from the Model Law on Electronic Commerce whereby an electronic signature can meet the requirements for a legally recognised signature.[189] This is a very flexible and technology-neutral provision that allows any electronic signature that is "sufficiently reliable" to replace a handwritten signature. The Model Law on Electronic Signatures further establishes a presumption that a signature with technical features corresponding to those of a digital signature shall be treated as equivalent to a hand-written signature.[190] Without mentioning the words PKI or digital signature, the model law includes basic rules of conduct that may serve as guidelines for assessing the liability of the CA, the certificate holder and the relying party.[191] However,

[183] http://www.uncitral.org/en-index.htm

[184] United Nations Commission on International Trade Law (UNCITRAL), UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996, with additional article 5 as adopted in 1998, note 16, found at http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm.

[185] UNCITRAL Model Law on Electronic Commerce Article 5.

[186] UNCITRAL Model Law on Electronic Commerce Article 7.

[187] UNCITRAL Model Law on Electronic Commerce Article 9.

[188] United Nations Commission on International Trade Law (UNCITRAL), UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001. http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf

[189] UNCITRAL Model Law on Electronic Signatures Article 6.1.

[190] In an effort to be technology neutral the term digital signature is not used. UNCITRAL Model Law on Electronic Signatures Article 6.

[191] UNCITRAL Model Law on Electronic Signatures Articles 8, 9, 11.

the Model Law on Electronic Signatures has not met with universal acclaim and has not been used as the basis for legislation to the same extent as the higher-level Model Law on Electronic Commerce.

The International Chamber of Commerce's (ICC) guidance document General Usage for International Digital Electronic Commerce (GUIDEC) includes best practice guidelines for authentication of messages and management of digital certificates.[192]

The American Bar Association is not an international organisation but has reached international reach through its digital signature guidelines, which aim to establish best practices for digital certificates and signatures.[193] The ICC GUIDEC is largely based on American Bar Association work in this area.

3.2.4 TECHNICAL ASPECTS

Countless technical standards exist for authentication. There are, however, a few core technologies that are at the basis of most authentication services, such as technologies based on the X509 standard, SSL or online payment solutions by the credit card companies. There are many providers of technical solutions and no de facto standard. Some companies, such as Microsoft, have the potential eventually to corner the market. Still, it is not only the technical aspects that determine outcomes in the governance framework. Some of the leading and most interesting technologies or standards are presented below.

- Adobe Acrobat Reader software incorporates the facility to digitally sign documents. This has been enhanced by combining Reader with different kinds of digital IDs. In Belgium, a new application has been launched to allow Belgian eID cardholders to authenticate PDF documents with their legally binding digital signatures. Adobe and the WPKI consortia are also cooperating on launching an application to enable mobile phones to sign PDF files.
- ITU-T and ISO jointly developed the X500 computer networking standard. The most widely spread specification of the X500 series is the X509. This is the specification of public key certificates. X509 specifies standard formats for public key certificates and a certification path validation algorithm. X509 was first issued in 1988 and assumed a strict hierarchical system of certificate authorities (CAs) for issuing the certificates. The X500 system has never been fully implemented and the IETF's PKI working group (PKIX)[194] has adapted the standard to the more flexible organisation of the Internet. In fact, the term X509 certificate usually refers to the IETF's PKI certificate and CRL profile, which includes the flexibility to support other topologies like bridges and

[192] International Chamber of Commerce (ICC), General Usage for International Digital Electronic Commerce (GUIDEC), 2nd Edition 2001. http://www.iccwbo.org/home/guidec/guidec_two/foreword.asp
[193] See American Bar Association (ABA), Digital Signature Guidelines (with comments), 1996. http://www.abanet.org/scitech/ec/isc/dsgfree.html
[194] http://www.ietf.org/html.charters/pkix-charter.html

meshes. It can be used in a peer-to-peer or OpenPGP-like web of trust, but is rarely used that way.

- Microsoft has numerous connections to authentication. Through Microsoft Outlook it is possible to sign emails and Microsoft's forthcoming new operating system, Vista (previously codenamed "Longhorn"), will contain a smart client for e-signature. Furthermore, Sun and Microsoft have jointly developed protocols that will enable browser-based single sign-on between Liberty Alliance and Web Services Federation Language solutions. Microsoft is also working on a system to wrap up identity management systems under a single-identity metasystem. Also, Hotmail and the upscaled Microsoft Passport service are Web solutions for authentication, though these services have had limited success. Microsoft has set up the European Microsoft Innovation Centre (EMIC), which participates in public-private research programmes in EU-prioritised research areas. EMIC will perform applied research in three areas, one of which is security and privacy technologies. One specific project is TrustCom, which will make possible ad hoc integration of systems across organisational boundaries. Microsoft has also indicated that it will work together with the Belgian government to pilot technology in Belgium in respect of the launch of the national ID. One new service is the integration of the Belgian eID technology into MSN Messenger for online identification.
- Pretty Good Privacy (PGP)[195] provides cryptographic privacy and authentication and is one of the most widely used standards for email encryption today, with millions of users worldwide. PGP uses both public key cryptography and symmetric key cryptography, and to a certain degree a PKI with some similarity to the X509 certificate standard. PGP uses asymmetric key encryption, in which the recipient of a message has previously generated a linked key pair, a public key and a private key. The recipient's public key is used by a sender to encrypt a shared key for a symmetric cipher algorithm. That key is then used to encrypt the plain text of a message. PGP has released an open Internet standards track specification known as OpenPGP.[196] It has further been standardised for interoperability between different pieces of software. PGPi is the international variant of PGP and differs slightly from the US versions (but is claimed to be completely interoperable). The PGP cryptosystem is a form of web of trust within which PGP users digitally sign each others' identity certificates and are instructed to do so only if they are confident that the person and the public key belong together.
- RSA Security[197] is one of the most successful e-security technology companies. RSA SecureID Authenticators is a system for accessing VPN and remote access applications with two-factor authentication consisting of a PIN and hardware token. RSA is a major provider of online authentication and provides solutions

[195] http://www.pgp.com
[196] http://www.ietf.org/html.charters/openpgp-charter.html
[197] http://www.rsasecurity.com/node.asp?id=1156

using hardware tokens for two-factor authentication. The technology is used by banks and by AOL.

- Secure Sockets Layer (SSL) is a protocol developed by Netscape for securely transmitting private documents via the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. SSL, in combination with usernames and passwords, is commonly utilised by service providers to obtain confidential user information, such as credit card numbers. IETF has developed an open protocol based on SSL version 3.0 and called Transport Layer Security (TLS).
- The Shibboleth system[198] offers a scalable and easy-to-use solution for identity and access management infrastructures to authenticate individuals for universities. Only information attributes are exchanged concerning the person requesting authentication, and the Shibboleth system allows institutions with different technology architectures and security systems to collaborate without using proxies or managing external or transitory accounts. This facilitates collaboration with other campuses, organisations and off-campus vendor systems.
- VeriSign[199] processes 30 per cent of North American e-commerce transactions and maintains the largest base of secure-payments customers on the Internet: more than 100,000 customers that process billions of dollars every quarter. VeriSign's Certificate Interoperability Service enables trust interoperability between digital certificates issued by privately-operated CAs and PKI. Verisign works actively in most international alliances and working groups that promote authentication technologies, such as Liberty Alliance and the WS-Federation.
- 3D Secure and EMV is a joint venture between Visa and MasterCard whereby banks deploy a specification known as EMV for chip cards. Businesses and consumers have started to receive a new card that can be enabled to carry a digital certificate. All European point of sales devices at vendors and ATM devices across Europe will be upgraded to read the new cards. The multi-application chip card can, through the PKI application, allow the cardholder to perform various e-business functions, such as securing access to private websites, digital signing of documents and email, and electronic message encryption. PKI provides a digital signature and complies with many legislative requirements.
- Wireless PKI[200] is a consortium created by BankID, Ericsson, TeliaSonera and Vodafone. Wireless PKI will provide secure transactions through login and identification using mobile phones (in the same way as hard certificates) and the Internet as information transport channels.

[198] http://shibboleth.internet2.edu/index.html
[199] http://www.verisign.com/
[200] http://www.wpki.net/

4. DISCUSSION AND ANALYSIS

Use of the Internet is today marked by massive new opportunities and by pressures and risks. As usage evolves so the complexity of the system grows and systematic deficiencies may worsen. A lack of orderly responses already hampers the deployment of digital transactions. Although continued rapid growth and more advanced use of the Internet appears inevitable, advances will be seriously impeded and distorted as long as proper security and trust is not in place. One of the most important requirements is the need to secure the validity of transactions and to build a proper framework for the provision of authentication services.

International perspective

While many countries provide a legal framework for recognition of electronic signatures, technical and even legislative implementation varies dramatically. Even within the EU, which has issued a common directive regarding authentication technologies and digital signatures, countries have been unable to provide an interoperable framework. Even greater hurdles must be overcome at wider international level. For instance, Europe is outspokenly geared towards PKI, whereas Australia and the US are open to a broad range of technologies. In contrast, Hong Kong has a complete focus on rolling out advanced PKI infrastructure. If transactions are to be orderly, both signers and relying parties need to overcome these obstacles.

Solutions to the current and future problems in the field will need to adopt a global approach. As shown in Chapter 3, it appears that most service providers are subject to limitations of a geographical and sectoral nature. Few service providers are able to offer a sufficiently wide reach to satisfy the relying parties' needs.

In this context, challenges arise also due to the convergence of infrastructures, applications and technologies above all between the fields of telecom and datacom, where regulatory traditions differ. The telecom sector has been governed in a more centralised manner that more broadly addresses governance issues; datacom has grown more step-wise and in an ad hoc manner. This challenges governance of the infrastructure, business models and what roles various actors should have in the value chain.

National perspectives

This current international status quo – marked by fragmentation despite the need for global solutions – is reflected in national frameworks. Though there are grand schemes for launching national ID cards and the like in many places, most countries display considerable diversity in their authentication frameworks. For instance, the Belgian bank Fortis continues to authenticate people using a token and a password. The same applies to banks in Estonia, such as Hansabank and SEB, although they have the option to authenticate customers using the national PKI system, and to Hong Kong Bank of China. Fragmentation similarly

prevails in Sweden, though most of the banks are currently moving towards an agreement to use the BankID solution. BankID is particularly interesting because it has the potential to be applied in a number of other areas, ranging from identification and authentication of people to e-government services. Interestingly, this means that the banks' authentication mechanisms can be used for a range of other private as well as government services.

The implementation of PKI-based digital signatures, eID or e-government services encounters a number of barriers. These include the lack of a global standard, the absence of interoperability and the risk of technological lock-in. Also, the services that have been provided have been more supply-driven than the result of real demand, which reflects severe information problems on the part of future users.[201] Elements of an appropriate infrastructure are missing, such as card readers (which leads to users not adopting complex PKI solutions). As a result, it is open to debate whether the systems are really needed or whether PKI is simply a white elephant.

Even though PKI occasionally can be too complex for some solutions, there are many indications that it is an interesting infrastructure solution that could serve as a multi-purpose technology and provide the answer to many of the issues regarding authentication if implemented.[202] "If there is a silver bullet, it is the PKI itself," as one of the respondents said in the survey.[203] But many banks with an online service have already invested in other systems. They want a return on investment and to use their technology until change is motivated from a business perspective. Several key actors also find PKI too difficult to grasp and too costly to use or are not interested in buying it from an external supplier.

There are numerous authentication systems and they respond to a universe of varying demands. Many of the legal requirements stem from government needs in application with respect to safety and authentication assurances required in the process of signing documents and agreements. The latter may require a more flexible system that incorporates another organisational setup. However, all sectors could benefit from an authentication system where a transaction is tracked and time-stamped by a third party. At the same time, a third party is not always necessary or desirable in all transactions. After all, ICT is a way to improve efficiency and an opportunity to remove intermediaries. Within this notion lies the attractiveness of improvements in this direction, for instance as a means to reduce corruption by disengaging public officials and various private individuals.

The current authentication map has a legal emphasis on solutions aligned with PKI and reflects the great influence and importance of e-government as a driver of the trust and security market. Most digital certificates released to the public by CAs in Europe follow national accreditation schemes with diverse policies and standards. Yet the fact that these schemes are non-discriminatory and comply with EU directives serves as an impediment to

[201] The Global Trust Authority (www.theglobaltrustauthority.org/) a consortia of major European banks trying to create a cross border initiative with a root authority for PKI implementations that was created with great enthusiasm, has since the introduction lost speed and is now run with limited efforts.
[202] Manager, SEB.
[203] Manager, RISO.

service delivery and increases costs. This is indicated by the fact that the different security levels included in the directives are not very widely deployed.

Paths forward

It is vital not only to focus on PKI as *the* technology for authentication but also to embrace other means which may concurrently serve as complementary keys to the successful implementation of PKI technology. PKI is a central environment for authentication, especially when high security is a prioritised requirement. But rolling out services and making people accustomed to using e-services will in the end create a critical mass of users that will probably generate sufficient demand for more e-solutions and more security. However, it might be of great value when setting up e-services to be able to switch between authentication technologies with relative ease. Different levels of security suffice for a broad range of e-services. Other technologies are more easily accepted in countries that have chosen to follow the UNCITRAL Model Law more closely, such as the United States and Australia. Australia's authentication framework provides an interesting example of acceptance of multi-level security for authentication solutions.

When providing authentication services, actors should focus on where the first income streams are likely to appear, and on designing business models that are relevant, cost-efficient and support the overall mission of the enterprise. The primary areas in which there is a will to invest in these systems typically enhance and facilitate business and government processes. One significant way forward is for actors with joint interests to share (and reduce) infrastructure costs or associated risks. At present, there appears to be an imbalance in that there are too many actors and too few users. This lack of critical mass creates a situation in which costs per transaction become too high. Coalitions of actors – private and public – are obliged to share costs and customers to deploy adequate technology. Further, common legal and policy standards need to be designed.

Authentication systems display various levels of security, depending on the requirements set for different transactional needs. It is vital that the "right systems" are used for the "right purposes". The Austrian model, designed to optimise different levels of quality, provides useful experience in this context. Its inbuilt acceptance function, which recognises authentication mechanisms regardless of origin, is of particular interest.

The presence of multiple systems and ways to establish trust offer a number of opportunities. By combining some of them it may be possible to create a functioning system in which a specific actor is identified and checked by numerous authentication systems. Together, these may then provide the required secure means of authentication (for instance, a person is not identified only by a driver's licence but by the combination of driver's license and a telephone bill). This is, in fact, common in many real life situations around the world, such as Australia's 100 point check.[204]

[204] http://www.austrac.gov.au/guidelines/forms/201.pdf

Creating a single sign-on solution in which all electronic transactions are undertaken with one framework of authentication mechanisms is likely to be a challenge. One obvious risk is identity theft; another is the threat of single point of failure (which is serious since the exploitation of such vulnerability can render the entire system unusable). There are also privacy considerations if personal data is to be made available to more organisations than the initial single link.

Government and financial institutions

Two of the most evident candidates to roll out authentication services are governments and financial institutions. How either of them assumes the role of trust leader is not obvious, though. Despite potential synergies, the partly contradictory interests and requirements of banks and governments raise obstacles to cooperation. Key factors appear to be reducing the likelihood that banks and governments will spontaneously succeed in deepening cooperation, as the incentives for using authentication vary between these actors and both parties wish to remain in charge and commonly prefer proprietary top-down approaches. Governments, while needing interoperability between various governmental bodies and sectors, have less motivation to build cross-border or international interoperability-based solutions. Banks do need to build globally interoperable solutions so they can offer e-payment services through worldwide open networks.

Banks are among the most trusted organisations since they manage a truly sensitive consideration for people and companies: money. Banks therefore need authentication solutions that meet high security goals. In a physical scenario, this is taken care of by face-to-face encounters, ID cards and personal relationships. In a digital setting, where there are no face-to-face encounters or personal relationships, it becomes more complicated. Existing ID cards can be used to some extent, but in most cases new solutions are needed – of which PKI-based eID may be one option. In many developed countries, banks already have many online banking users, making it easier to roll out eIDs. EIDs can also be used as authentication for other services, such as e-government services. This approach has been deployed in Sweden, where "e-Leg" is obtained from existing bank infrastructures. According to a leading technical expert at the Swedish National Tax Board (a pioneer of authentication in Sweden) e-Leg can be compared to the development of ATM cards.

Banks possess a number of capabilities that put them in a strong position to manage authentication schemes. These include extensive branch networks and customer knowledge, long service in the trust business, experience of mass-issuing of smart cards, secure infrastructures and risk management. At the same time, coordinated solutions are expensive, there is competition between alternative models and the need to cover the initial costs of innovations that will require widespread adoption ex post, and final outcomes will depend on the strategies of multiple actors.

Overall, the challenges for authentication schemes may be of a temporary character, or the result of implementation weaknesses, rather than the artefact of fundamental, lasting features of the system itself. There is a perceived lack of smart-card infrastructure, though

this could change swiftly with the planned migration to EMV bank cards, whereby credit cards can incorporate certificates for identification. Many countries are also rolling out national ID cards that can carry certificates (such as Spain, France and Italy). The next generation of passports will be implemented in conformity with the US's new demand for inclusion of biometric information.[205]

The infrastructure in general lacks embedded smart-card readers. However, the number of PCs with this feature is increasing in countries like Estonia, Belgium and Hong Kong. The Porvoo Group is encouraging manufacturers to make card readers a new PC standard. Another way forward for two-factor authentication with hardware tokens is the use of a wireless PKI that enables a mobile phone to be utilised as the identifier. An analogy can be drawn with the expansion of the Internet. Though the Internet has grown and spread at remarkable speed it still had to pass through delicate initial stages. Many early acts of implementation proved to be unviable but they still contributed to generating an infrastructural basis for which a host of later services were developed and provided.

Governments are essential to authentication for a number of reasons. They provide legal frameworks and guidance. In some countries they provide identification infrastructures, and in many nations they provide services via the Internet to citizens. They have an interest in buying services to reduce costs in areas such as healthcare, tax filing and tertiary education. If this can be managed electronically instead of on paper, governments can make substantial savings. Hence, governments need to have some sort of authentication mechanism in place.

The sample countries provide examples of quite divergent strategies for how to address authentication aspects. In some, national governments have taken much of the initiative and have rolled out national ID cards as part of public service provision. In a number of cases, this has been done in cooperation with banks and other key private actors. This has been the case in Hong Kong, Estonia and to some extent in Belgium. Interestingly, Estonia is content with its solution, which it claims has stimulated user volume and a market of services. The Estonians are looking for ways to make their solution interoperable and are planning for joint schemes with Finland and Sweden. In some countries, a legal framework exists but authentication service provision is left more or less to the market, as in the US. Even though this may be one plausible path forward, it seems that the European actors are rather sceptical about such a strategy. One explanation may be that European countries are more used to government regulation and control than the US.

Mixed approach

A model of great interest both from national and international perspective is the Austrian citizen card. It provides a technology-neutral framework for identification and authentication that accepts technical solutions provided by both the private sector (such as bank cards or mobile phone services) and the public sector (such as health insurance or public servant service cards). The government's goal was for almost every citizen by the end

[205] There is an ongoing discussion on this, where privacy advocates claim that the information that is generated by biometric solutions is in violation to international frameworks on privacy rights.

of 2005 to have a token capable of being enabled as a citizen card. The authentication aspect of the citizen card is provided by electronic signatures.

Public-private partnerships can be an interesting way to facilitate coordination and information sharing due to the fact that frameworks for government and business transactions are intrinsically complex. Information sharing and interoperation between agencies, businesses and governments creates opportunities to enhance efficiency, unify work and improve the governance framework. An interesting model is the Liberty Alliance's focus on the concept of identity management and its work to develop a standard that is open, interoperable and decentralised. The Liberty Alliance project was established to address the issues of standards and trust. It promotes federated identity implementations that allow the public and private sector to gain substantial benefits from areas such as improved alliances within governments and between governments through interoperability with autonomy. One objection to the project is that consumers and citizens are weakly represented – a problem that is prevalent in most kinds of international framework dialogue. It is often argued that governments represent their citizens in these discussions but at times there is clearly a conflict of interest. Hence, it is imperative to involve consumer organisations, such as Consumers International or the Trans-Atlantic Consumer Dialogue, in an appropriate fashion.[206]

Incentives

A senior official behind the Swedish government's ICT bill in 2004 emphasises the need for users to appreciate some kind of benefit in order to change behaviour. In countries where the government and financial institutions have offered proper incentives, results have been achieved. For example, the Swedish government offered citizens early payment of tax return surpluses if tax returns were filed electronically. Many Swedes responded positively to this incentive: 900,000 approved a pre-printed tax file with a security code online, 560,000 through a fixed-line telephone, 235,000 by SMS and 420,000 with a digital ID (the "e-Leg"), which also allowed them to change their returns. Apart from reducing red tape, the initiative virtually removed the traditional queues during the tax-filing period in 2005. Similarly, French taxpayers are offered a tax rebate of €20 if their returns are submitted online and their taxes paid by bank order or via electronic payment. By mid-April 2005, around 3 million French income declarations had been submitted which qualified under the electronic scheme.[207] Another example, again in Sweden, saw banks successfully raise prices for non-electronic transactions and introduced new fees for manual labour, while keeping online banking fees to a minimum.

Legal issues

When discussing legal issues, much revolves around PKI because most legal frameworks have dealt with or are focused on this technology. PKI and in particular digital signatures have been touted as the most appropriate way of making Internet communication secure. A

[206] http://www.consumersinternational.org/homepage.asp or the http://www.tacd.org/index2.htm
[207] http://www.minefi.gouv.fr/

more open trade over an inherently non-secured network increases exposure to risk. Certificates and the mechanisms for digitally signing and encrypting information are ideally suited to enabling the loosely-coupled model. For PKI to play this enabling role, its practice should work according to its theory. If parties that communicate over the open Internet cannot recognise each others' certificates, we are back to square one. As with so many aspects of the multi-disciplinary PKI technique, the aim of interoperability can mean very different things to different people. This lack of interdisciplinary interoperability (different aspects of, or viewpoints about, PKI stemming from different disciplines, such as legal, operational, technical, commercial) is, in a sense, the major interoperability challenge (Nordén, 2005). The interdisciplinary gap would be substantially reduced if a common classification of interoperability issues could be agreed upon. Among the most common interoperability issues are:

- *Format interoperability* of certificate, certificate revocation list (CRL) and other important technical PKI elements
- *Format interoperability* of certificate policy, certification practice statement, relying party agreements, certificate holder agreements and other rule-based PKI elements
- *Content interoperability* of certificates
- *Content interoperability* of rule-based PKI elements
- *Cross-jurisdictional recognition* of certificates by authorities
- Recognition of certificates used for compliance across different *regulatory domains*

Of these issues, *content interoperability* directs what kind of information should be included within certain certificates, for example limitations on responsibility, content of attribute certificate data and the person or role to which the certificate could be distributed. Many of these questions are specifically relevant in the context of e-billing; for instance, can e-invoicing certificates be assigned to organisations or to individuals, or is a combination of the two possible? Number v) concerns the level of acceptance among different countries' certificates, whereas number vi) deals with the possibility to use the same certificate to manage different legal requirements that belong to different areas. In conclusion, number v) addresses legal regulation on the matter of e-signatures and vi) applies to legal regulations that require e-signatures.

Past attempts at solving interoperability issues have often suffered because they did not appropriately differentiate among these different challenges. Their scope in terms of the interoperability issues to be tackled was too broad in relation to the available means and/or they did not set realistic or appropriate geographic and sectoral scopes. It is fair to say that:

i) Many of the format-level interoperability issues (numbers i. and ii.) in PKI have today been solved. Work is, however, ongoing and improvements will continue to be made.

ii) There is a lack of content-related standards (numbers iii. and iv.) and best practices. However, it should be noted that solving this will require a very

cautious plan of action and in particular an intelligent breakdown of issues to be solved at a cross-sectoral and international level. Also, more narrow sectoral and geographic definitions are required. A complicating factor is that content in these areas is the direct result of underlying operational processes, which in turn depends on established business practices and structures. This underlying fabric may also suffer from interoperability issues.

iii) The greatest lack of interoperability is in the regulatory sphere (numbers v. and vi.). Despite federal laws in the US, a directive in the EU, a model UN law and others, legislation regulating or requiring PKI continues to differ substantially between countries and regulatory areas.

Progress in the areas of content and regulation is expected to take place in the interplay between, on the one hand, developments in technology and real-world applications and, on the other, developments in the political sphere. These processes will most likely converge towards a level of interoperability at which the cost/benefit ratio of electronic signatures is acceptable to everyone. Due to the primacy of the national state in lawmaking and the lack of powerful global coordination mechanisms, such a solution will not be theoretically optimal from anyone's perspective. Due to the magnitude of these processes it is hard to make them change course fundamentally. However, focused efforts at appropriate levels can affect the processes and cause them to make some adjustments.

The first key to achieving positive changes is to set achievable goals, which in turn requires a sufficient understanding of realities in all fields of interest, including political, market and business processes and technical and business regulatory standards-setting. The second key to achieving such changes is to have them spearheaded by people with appropriate means and authority, which presupposes inclusiveness in terms of a multi-stakeholder approach, political recognition, transparency, and so on. While these actions are feasible, they may be costly and their effects will always remain relatively limited.

5. CONCLUSIONS AND RECOMMENDATIONS

This chapter outlines the report's key findings. It begins by addressing the overall conclusions, followed by economic, technological, organisational and legal findings and the results of the survey on the GTC concept, and ends with recommendations for enabling trust in the digital world.

5.1 OVERALL CONCLUSIONS

The report draws the following overall conclusions:

Markets are highly fragmented. Numerous governmental and corporate actors exist that all apply their own different technologies, business models, policies, protocols and legal imperatives.

A range of authentication methods is in use. The multitude of implementation initiatives available today confuses users and service providers as to which technology or method is likely to best fit their purposes (for example, in terms of efficiency and effectiveness, limiting key security risks or supporting strategic business options). There is also a risk of technological lock-in that may further enhance market fragmentation. The banking sector is a case in point. In some of the sample countries, banks hesitate to use national PKI solutions due to the presence of embedded investment in older (and, in some cases, obsolete) technologies still being deployed. This underlines the need for better reference tools that can be used for risk management purposes so as to make it possible to identify and engage appropriate expertise to assess the current standing and future prospects of various authentication techniques, and the degree to which their attributes can be anticipated to address requirements identified by application providers and/or users.

Reaching critical mass of users is hard. There is typically an over-supply of e-services, though the volume of users is limited. Demand-driven solutions are more successful. When consumer demand grows the solutions are more widely deployed.

Differences in the governance of transaction services. In some countries (like Estonia, Finland and Hong Kong), it is the government which is relied upon to provide regulation for national and international transactions, whereas in other countries (like the US) it is up to the market to do so.

There is a national focus. In most countries, efforts are focused on setting up services that function nationally. This probably reflects an urgency to address a number of outstanding challenges while the driving forces and instruments for implementing broader solutions remain too weak at this relatively early stage of the e-transaction era. Despite a number of initiatives and pilots that enable international transactions with improved security, no widely perceived groundbreaking impact has been achieved. The Internet is inherently global and citizens and customers are affected by events and trends in the international context in which they are active. This implies a need for an international and inter-organisational structure for digital transactions.

Opinions differ on PKI. Actors do not agree to what extent an overall and secure enough infrastructure such as PKI should be utilised. In Hong Kong, for example, PKI is the only standard used, whereas in Australia and the US all available technologies are used.

The lack of interdisciplinary interoperability is an obstacle. This applies to the following contexts:

- *Format interoperability* of certificate, certificate revocation list (CRL) and other vital technical PKI elements
- *Format interoperability* of certificate policy, certification practice statement, relying party agreements, certificate holder agreements and other rule-based PKI elements
- *Content interoperability* of certificates
- *Content interoperability* of rule-based PKI elements
- *Cross-jurisdictional recognition* of certificates by authorities
- Recognition of certificates used for compliance across different *regulatory domains*

Over-supply of standards. There are numerous initiatives to establish authentication standards for digital transactions, but so far none can be deemed successful. SSL and PKI have achieved partial success, yet no single solution has been established as a de facto standard.

Lack of international and powerful alliances. Although some (market-driven) coalitions exist, they have not yet had any real impact on societies, organisations and users.

Privacy is important, but to a variable degree. In some countries and settings, the right to privacy is a high priority, whereas in others it is less contentious.

Enabling trust in the digital world is a complex task. As with most complex tasks, time and patience is required. Some argue that PKI's lack of success is due to impatience on the part of key actors.

5.2 ECONOMIC CONCLUSIONS

The report draws the following economic conclusions:

Financial limitations contribute to poor e-security practices. Financial limitations in some countries have a tendency to contribute to poor e-security practices or non-introduction of up-to-date and secure technologies.

Market coordination problems and myopia occur in the absence of leaders. Some market progress has been observed, however, with respect to certain international organisations such as the Liberty Alliance.

5.3 TECHNICAL CONCLUSIONS

The report draws the following technical conclusions:

Interoperability insufficiencies exist between systems. Few solutions exist today that could be considered interoperable (and which thus can function between different systems).

Path dependencies and technological lock-in are present in some areas. Banks are one example of businesses which are involved in digital transactions and which have invested in systems that they do not want to abandon until it is financially motivated – even if better technological solutions are available.

There is a need for common standards. It is not just standards that are needed. Protocols and generic languages are also required to enhance interoperability and optimise other factors.

Numerous technical authentication solutions exist today. The oversupply of solutions makes it difficult for actors to scan the market and locate the "right" solution (that is, one that fits corporate goals and satisfactorily secures transactions). This, in turn, puts customers at risk in that they may spend either too much or too little money on security mechanisms.

5.4 LEGAL CONCLUSIONS

The report draws the following legal conclusions:

A great lack of interoperability characterises the regulatory sphere. Despite federal laws in the US, an EU directive, a model UN law and other legislative requirements, authentication continues to differ substantially among countries and regulatory areas.

5.5 ORGANISATIONAL CONCLUSIONS

The report draws the following organisational conclusions:

Lack of coordination results in market fragmentation. Since there is no coordination (either market-driven or governmental), there is differentiation in services, languages, protocols, standards and cultures.

Trusted parties are not trusted. Some of the established and so-called trusted third parties are not trusted by key actors (in government, industry and the private sector) and economic agents.

Risk analysis is the key. Embedding risk analysis approaches in existing solutions improves prospects for more efficient and productive security solutions – and security enables trust.

5.6 SUMMARY OF FEEDBACK BY RESPONDENTS ON THE GTC CONCEPT

This section presents a summary of respondents' views on the GTC concept and their responses to whether a global brokerage organisation that gathers and organises the available market actors and conveys contacts and counselling would enhance authentication in international transactions or not.

In general, there seems to be strong support for the creation of such a GTC. However, opinions differ on the approach and visions involved.

There is agreement on the need for international coordination. This should, however, be based on national coordination.

International debate suffers from conceptual confusion. Appropriate terminology, protocols and risk evaluation methods need to be developed. There is no agreement at national or international level.

The GTC needs to answer two vital questions: what needs can it meet and is the volume of users high enough? For coordination, proper risk analysis is also needed. However, respondents doubted whether the GTC should assume this responsibility or not.

Pilots present a feasible future approach. By implementing small-scale projects and basing strategies on the conclusions of such studies, improvements can be made and problems straightened out before large- scale deployments.

It is easier to develop new systems than to adjust old ones. One possibility would be to use existing national solutions that can be managed by a central international coordinator with a technology that is built on top of existing and national technologies. The coordinator can receive and pass on messages to other national systems. The coordinator should be interoperable and investment costs and disruption can be minimised by designing a new system that is placed on top of existing ones.

A global brokerage and clearing house will require appropriate funding, time, knowledge and resources. The prospects of such a venture are not a given, but the promotion of viable means to enhance security in digital transactions will exert a positive impact on, for example, market openness, competition and the variety of services that can be deployed over global information networks. Thus, the potential is huge. In addition, an effective GTC would be in a position to add a valuable public good component.

One significant way forward is through standardisation bodies. The goal would be to influence the work of these organisations in order to coordinate the different standards.

Actors are already well positioned to take on the standardisation role. Organisations such as IETF, W3C, OASIS already exist and could assume a standardisation role. An additional challenge for the GTC would be to improve international recognition of authentication methods by lobbying towards and/or working with other relevant well-established organisations, such as the OECD.

5.7 GENERAL RECOMMENDATIONS BY RESPONDENTS ON THE GTC CONCEPT

Coordination is needed if the potential of digital transactions is to be achieved. Coordination should be enforced by leading and trusted private and public actors (both nationwide and

internationally). One critical task is to gather trustworthy and influential actors and have them use their influence in order to affect other parties to submit to the norms achieved through coordination.

Freedom lies in the plan, not in the realisation. Enhancement of secure digital transactions requires a plan. A systematic overview of the overall objective divided into sub-goals suffices to fulfil the potential of digital transactions. One helpful way forward would be to implement the plan on a small scale, for example in a pilot region. The banking sector would be well suited to that purpose since banks are typically well versed in digital transactions, have a critical mass of users, are rigorous about trust, security and privacy, are engaged in national and international cooperation, and have private as well as public and corporate customers.

Start with existing solutions. Utilising current systems, infrastructures, coalitions and standard organisations is a sensible way forward. Introducing a common protocol that is interoperable, risk-driven, scalable, flexible, cost-efficient and usable (and that addresses multilevel security) on top of existing solutions would minimise disruption to existing technologies, legal frameworks and organisational models. It would also strengthen financial incentives.

Complex matters take time. Enabling digital transactions is a highly complex task, and patience is vital.

6. THE ROAD AHEAD – RECOMMENDATIONS

As a point of departure, the action plan for the near future includes the following steps:

1. Decide on strategy	*2. Establish network*	*3. Test phase*	*4. Full launch*
Steering committee meeting	Hold conference	Initiate pilots	Provide full-scale web of trust services or back-up for federated identity management.
Decide organisational form	Create association	Provide knowledge	
Secure financing	Start development of protocol	Develop marketing strategy and tools	
	Develop risk management tools	Engage key stakeholders	

The next section presents suggestions for how to proceed with the GTC. The report identifies four alternative structures: i) international organisation, ii) public-private partnership (PPP), iii) company, and, iv) loose network. An analysis of these options, including final recommendations on the road ahead, is presented below.

6.1 A FEASIBLE PATH FORWARD

The overarching objective of the report was to examine strategies capable of enhancing the security of digital transactions by improving authentication mechanisms on a global basis. The report proposes the advancement of the GTC to address challenges facing existing authentication solutions. Our analysis is based on four categories of challenges and opportunities (see below). For each of these, the GTC could act in a number of ways to support sound institutional and market responses. Thus, the GTC could:

i) With regard to *legal aspects,*

- undertake analysis and provide recommendations on existing gaps, malfunctioning elements or coordination and development needs to regulators, service and technology providers as well as to potential new initiatives.

ii) With regard to *technological aspects,*

- either through partners, joint ventures or by itself develop and improve standards, protocols and technical solutions that help improve the functioning of the market. One such solution might be to develop a risk-driven protocol for interoperation between authentication systems; and
- analyse and advise on technological solutions. The GTC could function as a centre of excellence providing trustworthy and independent information on techniques, best practices, standards and solutions.

iii) With regard to *economic aspects,*

- help facilitate the coordination of supply and demand to address market inconsistencies that currently hinder the development of new and improved services and effective pick-up by users of digital solutions. By acting as a broker between existing solutions, it would provide bridging between systems and serve as a catalyst for the development of new services and solutions. The GTC could also facilitate the emergence of a web of trust or a federated identity management structure; and
- analyse direct and indirect effects on national and international markets, as well as assess incentives and the rationale for action of key stakeholders.

iv) With regard to *organisational aspects,*

- strengthen market signals by providing and coordinating risk management tools;
- assist private and public entities and develop policies for organisations as well as recommendations for legislation;
- organise actors and solutions to facilitate coordination of existing and new efforts towards enhanced interoperability; and
- assemble, package and disseminate information and recommendations on available and successful business models, technologies and standards.

6.2 ORGANISATIONAL STRUCTURE

The tentative conclusions of the study underline the seriousness of the security issue in the digital world. There is a clear gap between the needs to establish mechanisms and institutions in support of digital trust and what current and anticipated future driving forces (from the policy and market side alike) exist to generate these mechanisms and institutions.

Demand for digital trust mechanisms is disparate, encounters fragmented market conditions and is unable to articulate coherent incentives to put effective solutions in place. The authentication solutions available today are primarily supply-driven and there appears to be an over-supply of technology alternatives. Going forward, there is a risk of technological lock-in, with heavy investments made in obsolete technologies.

A few international initiatives can be noted in this sphere, including the Liberty Alliance, intergovernmental organisations such as the ITU, IDABC and APEC Tel Group, and partnerships between market leaders such as Verisign, Microsoft, RSA and IBM. All face hurdles, however. These include limitations on resources, a varying ability to adjust to changing conditions and user and market demands, political factors, competition and coordination difficulties. The lingering presence of information and coordination problems mans the gap between needs and responses may not be closed spontaneously, either by public institutions or market forces.

A GTC focused on enhancing security for international electronic transactions and which introduces means to develop interoperability could make a major beneficial contribution to link the defence of public goods with improved conditions for new professional services that respond to real demand. This report believes establishment of a global trust centre is based on a sound rationale. A range of different GTC models are conceivable, all with various pros and cons. Four alternative paths for the GTC are outlined in the study:

i) International organisation
ii) Public-private partnership (PPP)
iii) Corporation
iv) Loose network

1) International organisation

This option may in itself involve several alternative constructs, where the level of, and relationship between, the members defines what form of organisation is implemented. In the case of a supranational approach, numerous privacy and political obstacles may undermine success. The intergovernmental approach presents somewhat different prospects. Here, governments might be engaged so as to build a web of trust by developing a cross-certification scheme including each national authentication model, thereby enhancing interoperability. This is, however, somewhat uncertain on a global level because the intergovernmental approach shares some of the same challenges as a supranational structure. An international organisation with slightly increased flexibility, with a mix of the level of its members, might provide a practical approach in the initial phase. A more publicly oriented organisation would require public resources and political buy-in to proceed. At the same time, it might be shunned by market actors. Also, by appropriating service provision that market actors should be able to provide, there is a risk that such a body would become too supply-driven. The implications of the international organisation option are summarised below.

International organisation	
Pros	*Cons*
Potentially powerful and well-resourced	Too top-down
Well placed to establish a protocol	Supply-driven
Clout to back security in digital transactions	Lack of flexibility
Favourable position to achieve critical mass	Slow
Good position to establish a web of trust/federated identity management of public organisations at least	Susceptibility to political problems, e.g. where to locate, who will take final call, turf battles for influence
High ability to address public-good issues	Expensive
	Return on investment uncertain

2) Public-private partnership (PPP)

A PPP would aim to gather key stakeholders from public and private entities across different sectors. It may be relatively easy to establish confidence in this kind of operation, applying both to the market actors and the public sector side. A GTC on these lines may be in a favourable position to develop matching regulations and technological solutions that meet interoperability requirements. Success would clearly require public and private buy-in. Launching the process would most likely require significant public funding. For a PPP to avoid some of the political challenges related to location and influence, it could be organised as a network with decentralised national nodes, which could help spread the cost burden among participating actors.

Public-private partnership (PPP)	
Pros	*Cons*
Demand-oriented	Limited political powers
Impact on critical mass	Uncertain value proposition
Cross-sectoral bridging	Competition
Integrity preserving	Lack of ownership and commitment
Coordination function	
Can develop protocol	
Can establish a web of trust/ federated identity management	
Potential buy-in from key stakeholders	
Can address public good factor	

3) Corporation

A third option is to start a private company based on key stakeholders' buy-in to the organisation and perhaps facilitating joint provision of technology through the organisation. It would be more flexible and more market-oriented than the other two alternatives. An initiative on these lines would require some sort of venture or seed capital, which could be provided by the actors buying into it. Presumably, it would not have buy-in from governments. There is also a risk that this structure would be viewed as yet another competitor or consultancy firm and not perceived as a coordinator of digital transactions.

Corporation	
Pros	*Cons*
Potentially high return on investment	Less trust from market actors
Flexible	High risk
Independence	No public buy-in
Demand-oriented	Hard to handle the public good component
Business-driven	Fierce competition from technology and service providers as well as consultancy companies

4) Loose network

A loose network aims to form a light structure which still exercises sufficient connections to keep the organisation functional around the key actors, presumably represented in the steering committee. Such a body could be relatively flexible and able to focus and respond as important opportunities arise. The network would observe market developments and gather more knowledge from initiated pilots.

Loose network	
Pros	*Cons*
Low risk	No resources – few results
Flexibility	Loss of interest of actors
Independence	Weak coordination
Small resource requirements	No true ownership

6.3 RECOMMENDATIONS

The key criteria for recommendations are *relevance of the organisation's purpose*, *feasibility* and *funding*. The relevance of the organisation is reflected in the value added it can generate through its activities, including to what extent it can deliver on providing the public good of interoperability and succeed in facilitating an improved match between outstanding needs and actually available or potential solutions. Relevance further depends on the organisation's ability to generate buy-in from key stakeholders and become a trustworthy actor in multiple camps.

As for the organisational form, this report concludes that an international organisation (alternative 1) is the best model for dealing with the legal, economic and organisational aspects on a global level. It is crucial that the GTC achieves appropriate support and sufficient integrity so as not to be vulnerable to external interests. Naturally, there will be challenges, given the state of the e-political arena, the market, and the speed of the ongoing technological development. However, it is of utmost importance to maintain focus on the global tasks envisioned for the GTC.

Forming an effective public-private partnership (alternative 2) for the technological aspects involved would be less problematic in terms of rapid start-up. This kind of structure should lend itself to engaging key market actors and other relevant stakeholders, which may make it the best positioned alternative to deliver the public good of interoperability and give it the greatest ability to be constantly up-to-date on the latest innovative technological solutions. It would clearly require funding from both the private and public sectors.

A corporate organisational form (alternative 3) may be somewhat more expedient and "easier" to establish. Risks include being viewed as lacking credibility in terms of exercising influence, not being fully transparent and trustworthy in its objectives, and not being able properly to support the public good component. However, there might be opportunities to base it on incentives to deepen commitments as opportunities develop. The viability of this

option must be thought through carefully on account of the difficulties in fulfilling the "trust" factor that is a prerequisite for success in the GTC's core function.

If options 1 and 2 are preferred but there is a lack of initial clout to muster the necessary resources, it might be feasible to cultivate the GTC as a network that could subsequently be gradually developed into an association of key stakeholders based on the build-up of several country nodes coordinated under a central function. The respective national actors could bring together their respective interests and experiences while carving out a suitable path towards overall coordination in line with the jointly preferred strategy of the GTC to be followed by a full rollout of the GTC once critical mass of support, commitment and funding is achieved. The board and the associate body would have to have a sufficiently broad geographical and sectoral representation, while avoiding the development of excessively diverse interests within the network. The intended members should be invited to working group seminars and conferences to advance a common approach to the GTC concept and ensure collaboration in making it concrete.

The development of a protocol of risk management tools and experiences from pilot projects are important building blocks for further progress. Pilots should be advanced not primarily to derive final solutions or strengthen the financial basis of the GTC, but rather to accumulate practical experience and to demonstrate the organisation's mission. Nevertheless, launching such efforts requires sufficient resources and certainty of funding, including contributions from institutions that would volunteer to support and host certain functions. An appropriate division of labour between the participating parties would have to be worked out. The members would provide the various kinds of experience required for the GTC and help to generate the perceived trust that is key to success.

In going forward with work that involves promoting an increase in the use of authentication mechanisms, the GTC will need to remain mindful that there will be a corresponding global increase in the need for users to have ways to manage their digital identities. If the GTC is organised so as to address this need, its work would presumably include an assessment of the degree to which federated identity solutions can meet marketplace demands in this regard, as well as assessments of potential policy issues that these solutions would require. Exchanges, seminars and conferences on the theme of authentication and digital transactions might be needed to boost not only interest in online security and an enhanced awareness of Internet-related risks and threats, but also to help advance the community of interested parties towards sufficiently common perceptions and perspectives, in other words establishing more shared concepts. Although numerous such meeting places already exist, there is a need to widen the circle of those engaged and to bridge the interaction between public sector, industry and academia. There is also the need to involve consumer groups as the demand side is often omitted. Arguments in support of this vision of cross-sectoral exchange on authentication include:

i) Trust-enabling methods such as authentication are an agreed topic of importance to the Internet's security culture.

ii) There are a limited number of conferences devoted to cross-sectoral interested parties.
iii) Cross-sectoral representation at such conferences would provide opportunities for market forces to contribute to the development processes.

This report recommends the foundation of a frontline international research and policy body – a Global Trust Center. The GTC should ideally be organised as a combined international organisation and public-private partnership and should cover legal, economic and organisational aspects of e-security, authentication and e-integrity globally. The GTC should have a structure for incorporating practically useful pilots that aim to solve targeted technological aspects and are tailored to meet the needs of specific market sectors and/or regions. A development in this direction has already been initiated by the Australian group within the steering committee, which has taken the lead in the development of a financial pilot. Demands for new solutions to digital trust are currently in focus in the governmental and the financial sectors. Coordination within these domains may help greatly to enable a strengthening of joint authentication protocols. Experiences learned from the pilot may serve as inspiration for the development of a future protocol and may show the way towards the establishment of future pilots. The provision of good examples and a track record in promoting efforts which can help create trust will be key to underpinning the formation of an effective GTC.

Important initiatives will have to be taken to examine and advance solutions that can enhance interoperability and support the implementation of cross-cutting solutions. A range of initiatives may be needed to advance and explore approaches and methods that can support effective third-party engagement in authentication schemes. Work on the development of an expanded protocol would have to be matched by additional work on risk management tools in order to start planning for marketing strategies and engage private and public actors in tandem.

REFERENCES

Adams, C. and Lloyd S. (1999), *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations,* Macmillan Technical Publishing, Boston MA.

AGIMO (The Australian Government Information Management Office) (2004), "Australian Government Electronic Authentication Framework – An Overview for Australian Businesses (Exposure Draft)".

Akerlof, G. (1970), "The Market for Lemons: Quality Uncertainty and the Market Mechanism", in *Quarterly Journal of Economics*, No. 84, pp. 488-500.

Anderson, R.J. (2001*a*), *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, Inc., New York, NY.

Anderson, R.J. (2001*b*), "Why Information Security is Hard – An Economic Perspective", in *Proceedings of the Seventeenth Computer Security Applications Conference*, IEEE Computer Society Press, pp. 358-365. http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf

Anderson, R.J. (2003), *Cryptography and Competition Policy – Issues with Trusted Computing*, Workshop on Economics and Information Security.

Arrow, K.J. (1974), *The Limits of Organisation*, W.W. Norton, New York.

Axelrod, R. (1984), *The Evolution of Cooperation*, Basic Books, New York.

Bernstein, P.L. (1998), *Against the Gods – the Remarkable Story of Risk*, John Wiley & Sons, Inc., New York NY.

Bishop, M. (2004), *Introduction to Computer Security*, Addison Wesley, Upper Saddle River NJ.

Bjerke, B. (1999), "Business Leadership and Culture – National Management Styles in the Global Economy", Edward Elgar, Cheltenham.

Bughin, J. (2001). "E-push or e-pull? Laggards and First-movers in European On-Line Banking." Digital Economy Lab, McKinsey & Co, JCMC 7 (1), October 2001.

Burr, W. E., Dodson, D. F. and Polk, W.T. (2004), "Electronic Authentication Guideline – Recommendations of the National Institute of Standards and Technology", National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf.

Cavoukian, A. and Hamilton, T.J. (2002), *The Privacy Payoff – How Successful Businesses Build Customer Trust*, McGraw-Hill Ryerson, Ltd., Canada.

Centeno, C. (2003*a*), "Security and Privacy for the Citizen in the post-Sep 11 Digital Age: A Prospective Overview". http://www.jrc.es/home/publications/publication.cfm?pub=1118

CERT Coordination Center
http://www.cert.org/

CommerceNet, May 2001
http://www.commercenet.net

Computer Security Institute (2001), "CSI/FBI Computer Crime and Security Survey", Published in the *Computer Security Issues and Trends Magazine*, Vol. VII, No.1.
http://www.gocsi.com

The Economist (2002b), "The weakest link", in *The Economist*, Oct 24th.

The Economist (2002c),"Putting it all together", in *The Economist*, Oct 24th.

The Economist (2002*a*), "When the door is always open", in *The Economist*, Oct 24th.

Electronic Privacy Information Center.
http://www.epic.org

Europay International, Payment Scheme Statistics, May 2001

European Commission (1995), Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities of 23 November 1995 No L.281 p. 31*, Luxembourg

Ferris Research.
http://www.ferris.com

Fischer-Hübner, S. (2000), "Privacy in the Global Information Society", in *IT-Security and Privacy – Design and Use of Privacy-Enhancing Security Mechanisms*, Lecture Notes in Computer Science LNCS 1958, Springer-Verlag, Berlin Germany.

Garfinkel, S. (2001), *Database Nation – The Death of Privacy in the 21st Century*", O'Reilly & Associates, Inc., Sebastopol CA.

Gartner Group
http://www.gartner.com

Gartner Group (2001), "Online Fraud Prevention", (white paper) for the *E-Commerce Fraud Prevention Network*, March 14th.
http://www.gartner.com/webletter/amex/index.html

Gollman, D. (2001), *Computer Security*, John Wiley and Sons Ltd., New York NY.

Heuvelhof, E. Kuit, M. and Stout, H., (2004), "Dilemmas in Smart capacity Management of infrastructures", in *Innovations in Infrastructures – New Solutions to Increase Reliability of Vital Infrastructures*, pp. 18-24.

ICSA Labs 9th Annual "Computer Virus Prevalence Survey"(2004), Cybertrust, ICSA Labs.
http://www.icsalabs.com

ICSA Labs 10th Annual "Computer Virus Prevalence Survey" (2005), Cybertrust, ICSA Labs.
http://www.icsalabs.com

Jacobsson, A. (2004), *Exploring Privacy Risks in Information Networks*, Licentiate Thesis Series No. 2004:11, Department of Interaction and System Design, Blekinge Institute of Technology, Kalmar.

Jahankani, H. (2006), Information Security and cybercrime legislations in the global cybervillage. Mimeo, University of East London, School of Computing and Technology, London.

Kerem, K. (2003), "Internet Banking in Estonia", PRAXIS Working Paper no 7, PRAXIS Center for Policy Studies, Estonia.
http://www.praxis.ee/data/PRAXIS_Internet_Banking_in_Estonia0.pdf

Kunreuther, H., Heal, G. and Orszag, P.R. (2002), "Interdependent Security: Implications for Homeland Security Policy and Other Areas", the Brookings Institution, Policy Brief, No. 108, October.

Kurose, J.F. and Ross, K.W. (2002), *Computer Networking – A Top-Down Approach Featuring the Internet*, Addison-Wesley Computing, New York NY.

Luce, D.R. and Raiffa, H. (1957), *Games and Decisions – Introduction and Critical Survey*, Dover Publications, Inc., New York NY.

McManus, M. (2005), "Zotob: A Malware Event in Warp Speed", Computer Economics, 2005
http://www.computereconomics.com/article.cfm?id=1066

Mehlman, B.P., (2003) "Technology Administration – 21st Century Policy Challenges for American Innovation Leadership", Remarks by Assistant Secretary for Technology Policy United States Department of Commerce, Before the Georgia Institute of Technology, Atlanta, Oct. 23.
http://www.technology.gov/Speeches/BPM_031023.htm

MessageLabs
http://www.messagelabs.com

MessageLabs (2005), "The convergence of viruses and spam: Lessons learned from Sobig.F experience"
http://www.messagelabs.com/

Metcalfe, S. (1995), The Economic Foundations of Technology Policy: Equilibrium and Evolutionary Perspectives, in Stoneman, P. (ed.), *Handbook of the Economics of Innovation and Technological Change*, Blackwell, Oxford.

MSN News Bulletin, March 27, 2003.
http://www.msnbc.com/news/891186.asp?cp1=1

National Fraud Information Center, Infernet Scams - Fraud Trends 2004.
http://www.fraud.org/2004-internet%20scams.pdf

Nelson, R. and Romer, P. (1997), Science, Economic Growth and Public Policy, in Smith, B. and Barfield, C. (eds.), *Technology, R&D and the Economy*, Brookings Institution, Washington DC.

Odlyzko, A. (2003), "Economics, Psychology, and Sociology of Security", Digital Technology Center, University of Minnesota.
http://www.dtc.umn.edu/_odlyzko

Olson, M. (1965), *The Logic of Collective Action*, Harvard University Press, Cambridge, MA.

Peltier, T.R. (2001), *Information Security Risk Analysis*, Auerbach Publications, Boca Ranton FL.

Pfleeger, C.P. and Pfleeger S.L. (2003), *Security in Computing*, third edition, Prentice Hall, Upper Saddle River NJ.

PriceWaterhouseCoopers and UK Department of Trade and Industry (DTI) (2006), "Information Security Breaches Survey 2006 – Technical Survey.
http://www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16

Rotenberg, M. (2002), *The Privacy Law Source Book 2002*, EPIC Publications, Washington DC.

Rubin, A.D. (1999), *White-Hat Security Arsenal: Tackling the Threats*, Addison Wesley, Upper Saddle River NJ.

Salomon, D. (2003), *Data Privacy and Security*, Springer-Verlag, Inc., New York NY.

Schneier, B. (2000), *Secrets and Lies: Digital Security in a Networked World*, John Wiley and Sons, New York NY.

Schneier, B. and Banisar, D. (1997), *The Electronic Privacy Papers – Documents on the Battle for Privacy in the Age of Surveillance*, John Wiley & Sons, Inc., New York NY.

Skoudis, E. (2004) *Malware – Fighting Malicious Code*, Prentice Hall PTR, Upper Saddle River NJ.

Smith, R. (2002), *Authentication: from Passwords to Public Keys,* Addison Wesley, Boston MA.

Statskontoret (2000), Elektroniska signaturer och elektronisk identifiering för myndigheters tjänster, 2000:40.

SWIFT (2002), "TrustAct the Power of Managed Business Transactions", by Juanita Maes, Regional Conference, Warsaw, March 25th to 27th.
http://www.swift.com/index.cfm?item_id=41792

Symantec Security Response
http://www.symantec.com/security_response/index.jsp

Szor, P. (2005), *The Art of Computer Virus Research and Defence*, Addison Wesley, Upper Saddle River NJ.

Townsend, K. (2003), "Spyware, Adware, and Peer-to-Peer Networks: the Hidden Threat to Corporate Security" (technical white paper), PestPatrol.
http://www.pestpatrol.com/Whitepapers/PDFs/SpywareAdware P2P.pdf

Varian, H. (2000), "Managing Online Security Risks", in *New York Times*, June 1st.

Warren, S. and Brandeis, L. (1890), "The Right to Privacy", in *Harvard Law Review*, pp. 193-220.

Webroot, 2005, "State of Spyware Q2 2005", Webroot Software, Inc., 2005
http://www.webroot.com

Westin, A.F. (1967), *Privacy & Freedom*, Atheneum, New York NY.

APPENDIX A: GTC STRUCTURE

The notion of a GTC was born out of the experience of many years of rather ineffective international negotiations in various multinational organisations to agree to common playing rules and mechanisms in support of a digital playing field marked by conditions in support of security, privacy and trust. Although there has been agreement on various forms of nice wording, e.g. in OECD guidelines or ITU and UN declarations, there is little tooth to any of the international settlements. The lack of progress most likely emanates from partly contradictory interests among stakeholders and countries, the difficulty of signing on to legal documents spanning fundamentally unregulated virtual territory, and fundamentally different perceptions among countries what the role of government and authorities is vis -à-vis that of markets in this field.

In the context of discussions within ASEM, in the OECD and various other international gatherings ideas have been tested on various occasions to form an inherently international but more flexible and lighter structure in which governments as well as the private sector and civil society work together in an open and experimental manner to scan the development of new solutions in the rapidly evolving field, evaluate what works and what does not work and to diffuse experience of best practice. The operation should be in part analytical, in part practical in that it needs to attract the interest, experience and ambition of practitioners that are engaged in "hands-on" efforts to develop, implement or link various solutions. The GTC concept thus centres on facilitating the globalisation of trustworthy digital transactions, with a primary focus on e-integrity and authentication. The aim is to increase knowledge and support initiatives which can help pave the way for the introduction and diffusion of competitive and transparent markets for the application of relevant technologies and solutions to actual and anticipated problems in this area.

One of the envisioned roles of the GTC is to serve as a clearing house for different proprietary authentication systems. This could be done in different ways. A clearing house might aim to enable people with different authorisations (tokens, smart cards and digital certificates) to be able to achieve interoperable digital transactions between users (persons, organisations, government institutions, and so on) without expensive investments in diverse proprietary systems. Other potential roles would include being an advocate and spokesperson for the rights of the private citizen in digital transactions by serving as an authorised digital transaction receipt holder. Among examples that could be further enhanced, ChamberSign represents an example of a corporate-oriented organisation that has been initiated for the purpose of catering for the advocacy of the corporate sector. The objective here is to advance mechanisms for organisations to obtain trustworthy evidence in support of security – traceability and verifiability via a reliable electronic receipt stored and issued by a third party (the GTC) – in the event of a dispute, or other needs to present or evaluate the validity of the information provided and agreed upon at the time of the actual transaction. Similar opportunities might be at hand, and be potentially more important, for private individuals, which may then be facilitated by the functions of the GTC. Other roles ought to evolve from the knowledge and experience gathered in this area.

Strategies for overcoming fragmentation in the provision of global trust services may focus on paths for enabling interoperability. At present, however, the interoperability is somewhat confused. The interoperability concept is very broadly defined and refers to general features of compatibility and absence of conflict. In some other cases, though, it refers to very strict and partly technical requirements. In part, the solution will have to fulfil specific criteria on a case by case basis.

The key question is what interoperability issues are outstanding, are a source of friction and give rise to costs, and yet might be addressed effectively by available (or potentially available) means? What mechanisms could solve the problems? How could they be implemented as effectively as possible, and by whom?

It is likely that a process capable of generating answers to such questions will have to build on a set of competencies and functions that allow for the identification and demonstration of best practices, thereby facilitating the development of useful standards and the standardised interface for system interaction. Building on what is available today, the structure should depart from a user's perspective on effective and desirable means for linking actors over the Internet through secure transactions in which the participating actors are satisfactorily validated.

In a sense, the potential benefits of the GTC are associated with the outstanding need of strengthening demand perspectives. In order to obtain the appropriate orientation, the GTC should thus abstain from launching new proprietary technology. Rather, it would assist in bridging existing solutions, like a web of trust or a federated identity management system, to diminish the risk of technological lock-in and support openness to new tools and developments. It would take on the role of a trusted third party that indicates, directs and provides brokerage between actors in digital transactions. By providing or facilitating such primary linkages it would facilitate the deployment of secondary linkages in the market place.

A GTC of this sort would have to aim to become a centre of excellence on trust, security and authentication in the digital world. It would act as a spokesperson in global arenas on these issues. It would undertake research to facilitate the accumulation of knowledge and the processing and accumulation of institutional insights on effective ways to address trust and security issues.

The GTC should not aim to offer one universal solution, but rather provide a map and well-structured approach to developing and creating bridges between various solutions. Its work would not merely be abstract and theoretical, but it would cherish and promote a portfolio of practical real-world technologies and solutions. In other words, it would assume the role of a technology brokerage house with the aim of achieving real interoperability. In effect, the GTC would offer a platform and opportunity for actors from relevant initiatives to meet and collaborate in establishing and providing trust solutions. From that platform, it could facilitate knowledge transfers between actors from diverse sectors and regions. By improving

conditions for sharing of infrastructure costs, it could help facilitate the deployment and use of new technical solutions.

If the GTC is to carve out a unique niche it will need wide-ranging credibility and buy-in from several kinds of actors. It is vital to involve those actors most relevant to the issues at hand. Since certain types of technology or methods are expensive to develop and launch, it will be essential to gain and share knowledge and experience from others. This will be an incentive for actors to engage in the GTC. Public-private partnerships can serve as a useful starting point for finding out which actors can provide critical infrastructure services. And it may be a way of making bottom-up and top-down initiatives meet. Solutions vary in accordance with the transaction, and an organisation such as a GTC can explore that nexus.

The GTC is here conceived of as a non-profit organisation. The structure would be based on the mutual effort made by key national actors that represent different trust provision actors and interests in digital transactions. Public actors would form part of the circle. Some public core funding is envisaged – and viewed as essential for the integrity and long-term direction of the institutions. Public and private perspectives would be balanced, however. The organisation would further embrace a number of local nodes, which would form an international network. The national nodes would be organised bottom-up, again incorporating many different sectoral interests bridged in the nodes.

Figure 9: GTC – brokerage house

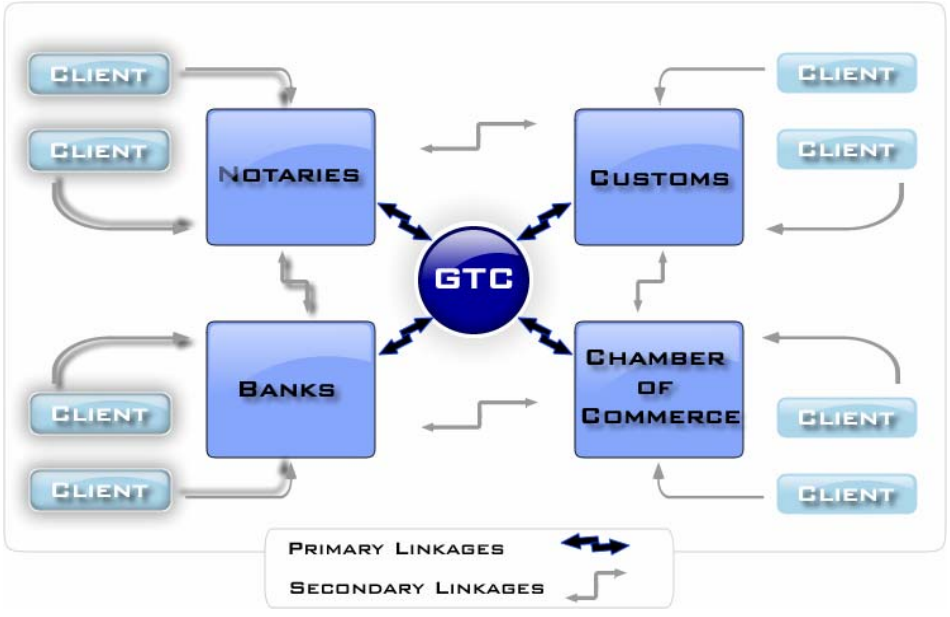


Diagram: IKED 2006

Figure 10: GTC – global network with national nodes

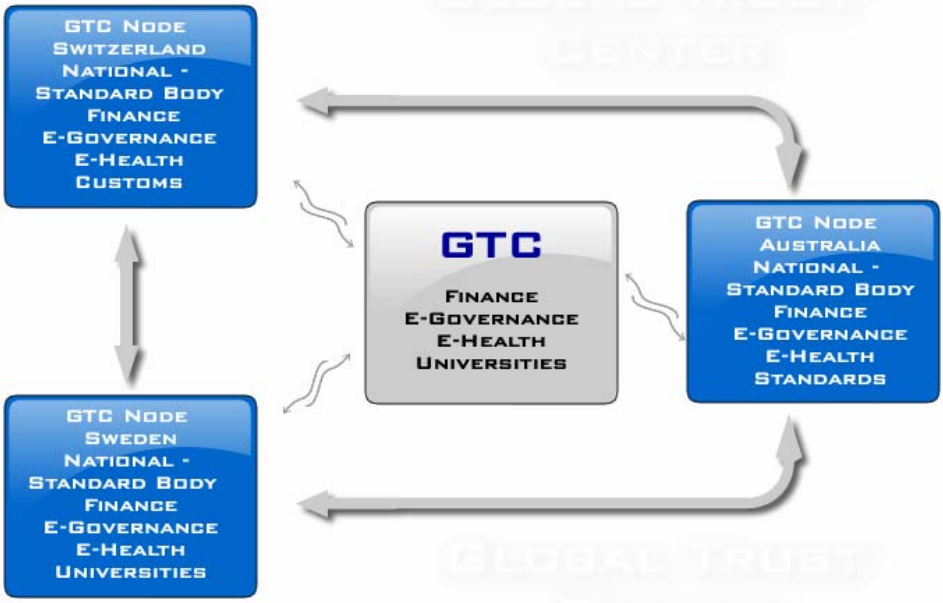


Diagram: IKED 2006

The envisioned members of the GTC fall within four different categories.

i) *Trusted third party actors.* Organisations whose role is to provide trust as a third party in digital transactions, such as law firms or chambers of commerce. Among the early adopters would be actors that already work digitally and have reached critical mass, such as governments and banks. It might also be of interest to include third-party actors that are not digital at present but that play a vital role in the non-digital economy and that can potentially provide significant digital services (international law firms, for example). The motive for these organisations to join is that they can receive international recognition. The GTC would provide a channel for acquiring new technology and learning business models and best practices as well as giving them access to third-party support (see below).

ii) *Users.* This category would include governments, banks and other sectors of industry along with other kinds of private or public institutions or organisations. These seek ways to develop or influence technology and appropriate regulations, for which the GTC could be relevant. They might also benefit from the development of a channel for acquiring new technology, learning new business models and identifying best practices and drawing lessons from them. Consumer

organisations, such as Consumers International and Transatlantic Consumer Dialogue might also be relevant participants.

iii) *Regulators.* Organisations responsible for regulations, standards and best practices (such as policymakers, lobby groups and standards organisations).

iv) *Technology and service providers and system integrators.* The motive for these organisations to join would emanate from their striving to receive international recognition. They might also benefit from obtaining a channel for acquiring new technology and learning about business models and best practices. They would gain new ways of influencing relevant technologies and legal frameworks.

Activities

For the GTC to succeed in its role of acting as an independent third party among other players it would need to be trustworthy. It should be "organisationally trustworthy", which would also apply to the technology it uses. The organisation would have to be as independent and free as possible from the influence of vested interests in the form of specific organisations or technology providers.

Trustworthiness would be achieved by gaining buy-in from other trustworthy actors. While performing its core functions and services, the GTC would also have to perform certain functions that are key to earning a reputation. For this purpose, the GTC could serve as a platform for:

i) *Development of an interoperability protocol* between actors and technologies with different national and sectoral origins.

ii) Policymakers and companies, and other relying parties, *to meet and work on clearing fragmentation and enhance the development of interoperability* by setting up pilot projects. These should create commercially viable opportunities and provide knowledge and input to policymakers.

iii) *Conferences and workshops.* The GTC would, on its own or in conjunction with associated actors, create opportunities for actors to take part in processes to strengthen the development of future systems or the diffusion of existing good practices. This would help to provide access to policymakers, standards organisations, relying parties and facilitate interaction with other parts of the broader information. Companies that develop new technology would themselves gain acquaintance with and inspiration from leading-edge technology, while policymakers would come into closer contact with users and developers and thereby obtain information relevant to policy design.

iv) *Creating knowledge databases and structural information for other actors.* The GTC would undertake knowledge gathering, create best practice documents and establish a common terminology and possibly a higher order standard for interoperability. It would provide information, including requirements for national or regional legislation on validation, examples of best practices and information on standards and regulation of trust issues.

v) *Process supportive services.* More complex services, where a global trust centre can take part in the process to partially verify a flow, decision or activity, in the process to integrate services into an application, and to do research or consultancy to explore the needs to meet international requirements. Also, the GTC would provide suggestions on how to design systems and which actors to involve in processes to create an environment of trust with secure technology. It would also be involved in integrating and implementing tools to transfer services online.

vi) *Brokerage of technologies.* The GTC would help service providers to provide technology and information on how to create a secure environment.

vii) *Classification of validation services.* Two vital tasks for the GTC would be to provide classification of validation and certification services and to provide information on how different service providers meet different security levels (and whether these accord with various national standards).

viii) *Support for national actors.* The GTC could provide support and reinsuring services in a few different areas to support national actors in transnational transactions. These services might also provide a way for newly established third-party actors to become more trustworthy, if they can refer to the GTC. The GTC Authentication Service could pave the way for, or itself include, a function such as a third-party authenticator (a somewhat modified modern version of a notary public). The aim would be to establish a service capable of verifying the identity and validity of parties, transactions and related documents. It would also be able to store these digital verifications for future reference in the event of disputes:

- Contract signing. The GTC can certify certifiers, the process and independent certifiers at different stages of a transaction.
- Contract authentication. The GTC can certify time stamping and also provide double time-stamping.
- Digital rights services. The GTC can certify the validity of a time stamp and also provide extra time-stamping.
- Escrow processes. The GTC can assume the role of an independent intermediary between a third party and a person/subject that has assigned it to handle the escrow process. The GTC can register that a document was sent as agreed. It can also verify that a certain document is available vis-à-vis the party receiving the document.
- Actor validation. If chambers of commerce are involved in the organisation, the GTC can bridge between these organisations on an international level to provide the linkages for transnational actor validation.
- Verification of documents. The GTC can verify that contracts have been certified.

ix) *Technology-driven certification.* The GTC would provide a technology-driven certification package that includes other audit criteria.

Financing

It is envisioned that the GTC could be financed by:

i) *Membership fees*: Will be divided along the lines of different levels of memberships, or members of management group. Hosting countries or regions may be induced to contribute to core funding.

ii) *Third party actors supporting and reinsuring services*: Charged in accordance with market prices.

iii) *Transaction fees* per transaction from members' use of the GTC Authentication and Validation Service.

iv) *Process support*. Teams can be put together from GTC personnel but also involve GTC member organisations.

v) *Income from setting up pilot projects*: When setting up pilots, the GTC will facilitate processes that generate income for the organisation.

vi) *Provision of classification/Validation of trust-based legal technical solutions according to national legislation:* Information that GTC members receive as part of membership. Can be transferred to other interested actors in return for remuneration.

APPENDIX B: EMPIRICAL SURVEY IN THE "ENABLING TRUST IN THE DIGITAL WORLD" PROJECT

Questions:

1. We believe that the implementation of ICT imposes severe security problems. One central aspect in increasing ICT security is authentication. Do you agree that authentication is important for increasing global ICT security between buyers and sellers in a digital market?

   [ ] YES, then proceed to question no. 2.

   [ ] NO, then proceed to questions no. 9.

2. What are the problems and opportunities associated with authentication in transnational transactions (for example, in international trade, public services and contract distribution)?

3. What are the problems and opportunities associated with authentication on a national level?
   Please describe the various authentication services in your country and their main advantages and disadvantages.

4. What do you see as the legal issues or obstacles relating to transnational authentication?

5. What do you see as the technical issues or obstacles relating to transnational authentication, and what are the main (technical) authentication solutions?

6. Are today's authentication mechanisms sound from a business perspective? How?

7. How would you characterise the market for authentication mechanisms where you are? How do you think it will develop going forward?

8. Could a global brokerage organisation that gathers and organises the available market actors and provides contacts and advice enhance authentication in transnational transactions? How?

9. If authentication is not the key to increasing global ICT security between buyers and sellers on a digital market, then what is? What do you think are the main security obstacles to enhancing global ICT?

Could these ICT security aspects be addressed on an international level? If so, should the market solve the problems by itself or should governments put in place regulations or in other ways provide the public with the means required for enabling digital security?

APPENDIX C: COMPILATION OF SURVEY RESPONSES FROM THE "ENABLING TRUST IN THE DIGITAL WORLD" PROJECT

AUSTRALIA	
1. Aspects of authentication in international transactions	Have addressed the issue by leaving it open for discussion. It is up to service providers to choose technology (foreign service providers are accepted). Are not restricted to PKI. (See, e.g. AUS framework.)
2. Current authentication solutions	For instance, user-name, password, SSL, PKI and shared information.
3. Legal aspects	Legal system is technology-neutral, deals with the wider concept of electronic transactions, stating that a transaction is not invalid simply because it took place by means of an electronic communication.
4. Technical aspects	Main service providers are banks. None uses PKI technology. Instead, banks use username, passwords and SSL. Have invested in Gatekeeper and PKI technology, but there has not been any noticeable pick-up by market actors.
5. Organisational aspects	Questions about security level of existing username and password solutions. PKI technology has been introduced but so far met with limited success. It has been considered too complex and costly. Telstra (the former national telco) has pulled out of this business.
6. Economic aspects	Current market fragmentation, leading to inadequate critical mass of users to enable sound return on investment for more complex and secure solutions. However, substantial implementation by banks of authentication systems for online banking.
7. Government services and needs	Public guidelines for choice of security solutions exist with risk recommendations on how to choose technology based on risk estimation. The public has used shared information or a challenge/response system, username/password and PKI.
8. Health services and needs	The SecureNet-HeSA Health PKI provides PKI for the Australian healthcare sector.
9. Financial services and needs	All major banks offer Internet banking, for which a combination of passwords and user names are used for authentication and identification. Major challenges with respect to fraud, which costs banks more than A$100 million per year.

HONG KONG	
1. Aspects of authentication in international transactions	Contrary to the technology-neutral regulation in the US and Australia, one would expect to find some regulation in Hong Kong law as to whether and how foreign certificates and signatures are accepted. But Hong Kong Electronic Transactions Ordinance 2000 is silent on the issue of cross-border acceptance of foreign certification authorities and certificates.
2. Current authentication solutions	Hong Kong is launching its new mandatory ID card to 6.9 million people. The new card contains a chip that contains an ID number, the person's name, date of birth and digital fingerprint reference data. Apart from being an identification document, the smart ID card offers the option of e-Cert.
3. Legal aspects	The Hong Kong Electronic Transactions Ordinance 2000 is not technology-neutral legislation but rather quite PKI-specific, in keeping with several other Asian e-signature laws. It authorises the use of electronic and digital signatures but only gives legal recognition to the latter.
4. Technical aspects	Hong Kong is possibly excessively centred on PI. This will prevent the region from picking up more cost-effective solutions and lock it into a technology that could become obsolete.
5. Organisational aspects	Hong Kong does not wait for citizen pick-up, but is rolling out its authentication service with the launch of the new identity card. This card can be loaded with a certificate. Through an incentives scheme it is almost for free to integrate an e-cert to the id card.
6. Economic aspects	The new id-card with the e-cert have managed quite will in fostering new applications and services. Numerous financial institutions in Hong Kong provide online services, using the e-Cert as authentication means, but also other authentication methods.
7. Government services and needs	The government is trying to assist development of electronic commerce with the implementation of its Electronic Services Delivery (ESD) programme. Under the first phase of implementation, 10 government departments and public agencies provided a range of services. Now 210 electronic public services provided by 56 government departments and public agencies exist. Of these are twenty such that you require some sort of signature to use the service.
8. Health services and needs	Electronic health records can be submitted through email. If digital signature is not applied, compliance with SMTP standard will suffice. If digital signature is required, compliance with S/MIME standard is necessary.
9. Financial services and needs	Numerous financial institutions in Hong Kong provide online services, using the e-Cert for authentication along with other authentication methods.

EU	
1. Aspects of authentication in international transactions	Banks have an important role to play in building security and trust on the Internet. They serve the purpose except for traditional financial services as identification/authentication gateways in their operating countries and offer, through their portals, access to e-commerce and third party services, such as tax payment, insurance services, e-bill management, etc.
2. Current authentication solutions	The main obstacles are not technological, but organisational. Great variance in terminology within the EU. Difficulties in agreeing what level of certificates that should be valid for different sectors within the union. Through the E-Signature Directive, qualified certificates issued by a CA in the EU are automatically accepted by the other member states. Foreign CAs are also accepted if they fulfil requisite criteria to ensure a similar level of quality as the EU's CAs. However, there remains little interaction between countries, due to interoperability problems (of an organisational, technological and legal character).
3. Legal aspects	(See each country separately.) Username/password/SSL with and without tokens, PKI solutions, EU passports and biometric solutions. The future Visa Information System (VIS) will include biometric data and will be introduced by the end of 2007.
4. Technical aspects	Different aspects of secure digital transactions have different value among EU members. The purpose of the E-Signature Directive is i) to facilitate the use of electronic signatures and to contribute to their legal recognition, and ii) to open the European market for electronic signatures and certification services. But the legislative focus remains mainly fixed on PKI and is not addressing other solutions that can provide authentication.
5. Organisational aspects	National implementation and standards lack a semantic view of interoperability. A few initiatives to address these issues are around, such as CEN/ISSS. CEN/ISSS has a project to determine the role of standards for e-government applications, in particular to achieve interoperability at all levels of public administration throughout the EU. IDABC is also addressing the issues, is creating middleware solutions and is running pilots to achieve interoperability.
6. Economic aspects	Some interesting cases of pilots and projects to overcome national fragmentation, including BankID in Sweden and Bürgerkarte in Austria. Fragmentation is increasing in other countries. The banks consider their authentication solutions to be sound from a business perspective but they are rarely accepted for government purposes. There are complaints from the public sector that the business models offered by the banks (and which feature per-transaction fees) are ill-suited to high-volume customers. However, some banks have started to offer services with fixed fees.
7. Government services and needs	Most member states have additional requirements for e-signatures in the public sector. Communicating electronically with public authorities is possible only through qualified certificates. The main danger of the public sector exception, is that it could lead member states to adopt additional requirements that may be detrimental to basic EU competition rules and the internal market.
8. Health services and needs	The EU has a programme called Interoperable Delivery of Pan-European E-government Services to Public Administrations, Businesses and Citizens (IDABC). It raises some of the issues, and in the work of the CEN/ISSS on standardisation of digital signatures and e-authentication there is no unified view within the EU.
9. Financial services and needs	The health sector is quite complex and needs to address many different regulatory aspects in order to transfer services online. One interesting initiative is the European Health Insurance Card, which aims to replace current paper forms needed for health treatment in another member state. CEN/ISSS also runs workshops on e-health, examining the need for authentication as part of infrastructure.

AUSTRIA	
1. Aspects of authentication in international transactions	No bilateral agreements with other national CAs for mutual recognition of cards exist, but there is a prototype integration of Italian and Finnish electronic identities. Uniquely, the Austrian system does not transmit citizen-identifiable data to e-service applications. It instead uses the concept of "sector-specific identifier numbers" that are generated for each service.
2. Current authentication solutions	The Bürgerkarte allows for electronic signatures and authentication through the creation of different online "electronic identities" by a citizen, and using different media such as smart cards and mobile phones. The concept is also to be applied to credit and debit banking cards. It allows various technical solutions that have been taken up by both the private sector and the public sector. By the end of 2005, each citizen will have a "citizen card".
3. Legal aspects	The EU E-Signature Directive has been incorporated into domestic legislation. The secure electronic signature meets the standards for the qualified signature creation device replaced due to Austrian security requirements. Austria's civil law system imposes no restriction on the use of electronic signatures. A general non-discrimination clause for all forms of signatures was explicitly incorporated into domestic legislation from the E-Signature Directive. As for cross-border recognition, the validity of all foreign certificates must be verifiable.
4. Technical aspects	Austria has managed to create a federated identity management system incorporating, health, bank and government cards. The technology-neutral concept turns out to be the strength of the Austrian approach; various private-sector issuers have taken up the concept (banks, mobile phone providers), emerging technologies have been integrated (mobile phones) and citizens can choose which eID they prefer. One hundred per cent coverage is expected in 2005.
5. Organisational aspects	The issues have been: unique identification that can be used in both e-government and by the private sector in a data protection compliant manner; representation and mandates; and a technology-neutral interface so that the various technologies can follow the concepts.
6. Economic aspects	In Austria, it is not obligatory to carry an identity card and it will not become obligatory to do so. Instead the citizen card (The "Bürgerkarte") has been introduced and this has contributed to good progress in in coordinating authentication technologies.
7. Government services and needs	So far, some 100,000 cards have been issued to approximately 70,000 individuals. Between 80 and 100 e-services are available to citizens (for which citizen card authentication may be required).
8. Health services and needs	The Austrian electronic health insurance card (e-card) is enabled for a digital signature function and is the central element of the e-card project to connect 12,000 doctors to the central computer network of the Federation of Austrian Social Security Institutions.
9. Financial services and needs	Maestro bank cards issued in Austria can contain a 'citizen card' function, which allows for online authentication. This new functionality is among other things aimed at increasing the uptake of e-services provided by the Austrian public sector and could ultimately be extended to all bank cards. Most common service is corporate e-banking and notary archiving.

BELGIUM	
1. Aspects of authentication in international transactions	The Belgian government has launched the Belgian Government Interoperability Framework (BELGIF) and published a first list of open standards to be used by public authorities. BELGIF is the result of a joint venture bringing together the federal government and the country's federal entities (regions and communities). The launch of a Belgian interoperability framework for e-government stems from the need to promote interoperability both at national and European level, and follows the federal government's June 2004 decision to promote the use of open standards.
2. Current authentication solutions	By 2009 every Belgian citizen will be required to own a Belgian personal identity card. The card can be used with services like tax filing and e-banking, but also as a European travel document. Initially, the ID card will not contain biometric data. It will, however, be possible to include such data at a later stage. Banks have username and password solutions, with and without hardware tokens.
3. Legal aspects	Two acts that incorporate the European directive into national law substantially amend the Belgian civil and judicial codes. The acts give legal value to electronic signatures and electronically signed documents and set up a legal framework for certification services.
4. Technical aspects	The general use of the card will introduce an increased level of security and trust for the users of online applications. The question is whether the solution is demanded by the market. The Belgian project is clearly supply-driven but the initiators are confident that the new infrastructure will generate the necessary framework for new services. They are somewhat supported by interest from Adobe and Microsoft in the initiative.
5. Organisational aspects	The need for improved communication with citizens, greater cooperation with banks (buy-in) and increased availability of card readers has been emphasised.
6. Economic aspects	The principal aims of the eID were to allow Belgian citizens to authenticate and generate digital signatures. Since then, the eID has evolved from a tool for e-government into an economic, social and political driver. The eID is a spur for the development of a safe electronic infrastructure. Individual companies do not have to set up an infrastructure for multiple online transactions, which cuts costs. These savings are far exceeded by the fact that the added security and trust minimises the risk of abuse and fraud. The use of the eID for secure online transactions of various kinds generates considerable savings for the federal government.
7. Government services and needs	E-identity, e-VAT, e-justice, social security services and others use authentication solutions. The Belgian federal government will deploy an identity management system allowing civil servants from across more than 30 government agencies and citizens to securely access a wide range of e-government applications through a single sign-on solution.
8. Health services and needs	The government has launched Be-Health, an integrated platform to deliver all health and healthcare-related information and services online through a single portal. The portal will provide services to health professionals, the general public and the government.
9. Financial services and needs	Online banking is the commonest service that requires authentication. Banks use username and password solutions based on smartcards and on digipass solutions. The banks can be used as authentication mechanisms beyond pure banking services, such as for ticket ordering.

DENMARK	
1. Aspects of authentication in international transactions	A problem that arose in the harmonisation process for publicly provided authentication solutions in the Nordic countries was the issue of original identification. In Sweden it had to be face to face, whereas in Denmark it could be performed over the phone.
2. Current authentication solutions	There is a national digital signature programme, Public Certificate for Electronic Services (OCES), that provides sufficient security for most public sector and private sector transactions. Approximately 320,000 Danes have a signature from OCES. Then there is the bank system Net-ID, 2.2 million users. Furthermore there is the "KMD fælles pinkode", which has been issued to 800,000 Danes. It is part of a government single sign-on solution for government services.
3. Legal aspects	All Danish citizens have a legal right to communicate electronically with central government bodies. The authenticity of all messages must be certified by the use of digital signatures. Public authorities have established secure e-mail solutions and have re-arranged their work practices to comply with guidelines from the Danish Data Protection Agency.
4. Technical aspects	The national PKI solution has not been taken up by Danes to the same extent as either the banks' Net-ID or the less secure public single sign-on solution.
5. Organisational aspects	Available mechanisms are priced on a per-transaction basis. Cost is incurred per authentication which is a problem for public information services, but not for a business transaction. Public information services have large number of transactions, with low revenue per transaction.
6. Economic aspects	At a national level, the main issue is that OCES public standard is not adapted or even supported by the banking sector, which has launched its own authentication product, Net-ID.
7. Government services and needs	The Danish national digital signature enables citizens to access numerous government services, send secure messages and file applications. Technology offered by the banks allows users to do much of this and perform financial transactions online.
8. Health services and needs	Denmark will establish a common framework for full e-healthcare service. One of the goals is for data-sharing between the many ICT solutions currently in use in the Danish healthcare service. Denmark is also together with Estonia, Lithuania, Norway and Sweden involved in the Baltic eHealth project. This will promote the use of e-health in rural areas of the Baltic Sea Region by creating a large transnational infrastructure for e-health.
9. Financial services and needs	Danish financial institutions undertake joint R&D and electronic payment services provision through Payment Business Services (PBS). PBS has developed and launched the Net-ID solution for Internet identification and singing of documents and contracts. NetID is the major authentication scheme and has 2.2 million users.

ESTONIA	
1. Aspects of authentication in international transactions	In distributing trust it is critically important to establish who is in charge of what parts and levels of transactions. Here, views diverge widely between countries. Estonia has sought to overcome interoperability and certificate problems by setting the ICT framework to accept different and foreign certificates. Hence, trust is enabled between the certified parties. Finland and Estonia signed an agreement in 2003 harmonise the concepts and practices between the two countries regarding digital signature and document format and exchange.
2. Current authentication solutions	Most Estonians have the national ID card, which supports strong signatures. Around 730,000 ID cards have been distributed to the people of Estonia (which has a population of 1,360,000). For approximately 10% of total authentication use, strong security is needed. For less strong security needs, users utilise the banks' ID mechanisms, and around 90% of all transactions are executed this way.
3. Legal aspects	A digital signature has the same legal effect as a handwritten signature under certain conditions. Foreign certificates are deemed to be equivalent to Estonian certificates if certain conditions are met.
4. Technical aspects	Following a political debate, PKI is now the legal standard in Estonia Estonia also has a number of registered CAs but only two certified PKI service providers (due to high qualification levels).
5. Organisational aspects	Technology development has been supply driven. However the national PKI solution has fostered new services which has in turn attracted new users. Overall, the programme is considered successful, though the banks still prefer their proprietary technologies.
6. Economic aspects	The government supports the idea of co-operation between government and industry. The two have agreed on the concept of a national ID card and divided key activities between them. The result is a joint ID card that has user volume and a market for services. Estonia is also cooperating with Finland, Austria and a few other countries in different projects to make their national ID systems interoperable.
7. Government services and needs	The Estonian government is using the national ID card as an authentication solution for many kinds of services, such as tax returns, health card, parent-teacher-school contacts, tickets, e-invoicing and utility invoices.
8. Health services and needs	Estonia, together with Denmark, Lithuania, Norway and Sweden, is involved in the Baltic eHealth project to promote the use of e-health in rural areas of the Baltic Sea Region by creating a large transnational infrastructure for e-health.
9. Financial services and needs	Estonian banks have different systems. Normally they provide different versions of usernames and passwords with or without hardware tokens. They also provide the opportunity of to use the national eID. Banks seem to prefer their proprietary systems and to promote them.

FINLAND	
1. Aspects of authentication in international transactions	In Finland there is a lack of international standards and too many national standards and systems. These competing systems and standards make choosing one a gamble. Finland and Estonia signed an in 2003 to harmonise the concepts and practices between the two countries regarding digital signature and document format and exchange. Finland is actively participating in many working groups and pilots. For example, Finland initiated the Porvoo Group, which promotes use of smart ID cards for online transactions.
2. Current authentication solutions	Finland has a national eID-card based on PKI. Banks have other authentication solutions as well, based on usernames and passwords with soft and hard tokens. The Finnish government is to start issuing biometric passports that will store the holder's personal details and biometric identifiers.
3. Legal aspects	The EU directive has been implemented (and indeed the directive was based on many ideas stemming from Finland). From an international perspective the needs of different countries with regard to privacy issues poses legal challenges.
4. Technical aspects	No major technical issues. Finland is a pioneer country, being among the first to launch national eIDs. However, initial pick-up was low, due to few services being available. The situation is improving. Finland is participating in many of the international working groups and pilots that promote online authentication. Finland is one of the first countries to launch mobile authentication solutions.
5. Organisational aspects	Banks see their password and username systems as being sound from a business perspective and offering a healthy return on investment. They also believe they have attained a sufficient critical mass of users. The key to success is easy-to-use solutions, participation of social and health services, private and public sector co-operation, appropriate service content and provision of supporting and guiding services.
6. Economic aspects	The government has just introduced a new online authentication system based on the existing standard used for Internet banking. It will be available to all government authorities. Originally the Finnish electronic ID card was the universal method for e-government services, but the uptake was too slow due to issues of over-complexity in relation to security needs. The new system provides more flexibility as some public services can be accessed online without card readers. A number of e-government services will be made available for the system.
7. Government services and needs	Government services include social and health-related services, tax returns, changes of address, crime reporting and e-identity.
8. Health services and needs	As of June 2004, Finnish citizens can request to have their health insurance data included in their electronic ID card. Citizens who take advantage of this will carry one card instead of two.
9. Financial services and needs	Finland has the highest per capita penetration of online banking. So far the banks have mainly used their proprietary technologies for authentication. As banking is about trust, the banks are keen to provide secure technology over which they have control. For example, Nordea's users can choose between two systems: a PKI-based system with hard certificates which almost no-one uses; and one with one-time codes which has 2.5 million users. This is also behind the eID in Finland and Denmark. The common interface is used by other banks and customers can use it to access a number of government services.

SWEDEN	
1. Aspects of authentication in international transactions	The regulatory framework points towards PKI, and foreign certificates are deemed to be equivalent to Swedish ones if certain conditions are met. The banks are rolling out one joint PKI solution, BankID, and at the same time most banks have invested in other technologies. The number of international transactions remains low and as there are problems with fragmentation on a national level, these are being addressed in priority. However the Nordic countries have stated an ambition to overcome fragmentation before 2006. Lack of understanding of interoperability is an international and national challenge.
2. Current authentication solutions	Most authentication technologies are used. Most still centre on username and password with soft certificates and hard tokens (as used by the banks). Large PKI introductions are in the offing and major actors are Telia, BankID, Nexus and Verisign. Biometrics are used in pilots and in some internal company processes, and will probably feature in the forthcoming EU passport. Emerging technologies are authentication with mobile phones, and wireless PKI.
3. Legal aspects	Sweden has free sifting of evidence and there is no clear legal ruling on e-identification (e-leg) and identification theft. There is no structured, approved and common approach to these factors. There is also a lack of consensus on who is supposed to push these questions forward. In Sweden, the laws are not formulated in such a way as to tie tied to specific technologies. This may act as a disincentive to adopt new technology. On the other hand, the qualified certificates are more strictly regulated and PKI has not been deployed in Sweden, mainly due to that they imply strict liability.
4. Technical aspects	There is no set of common standards. This raises questions regarding usability of available technologies. Differences exist in respect of user interfaces and terminology, possibly making for higher barriers to potential users. Users do not understand the technology and therefore have problems trusting it. Different committees are trying to address these issues to create a common interface and terminology.
5. Organisational aspects	Incomplete information raises challenges for trust. Consumers see risks attached to e-transactions. Since there is little possibility to evaluate risks there is no ground for enabling trust at the moment. Incentives – such as charging consumers more to use branch services – have been used successfully by banks to encourage consumers to migrate online. The National Tax Board has had some success by returning tax refunds earlier to people who file their returns online. In 2003, around 36,000 Swedes filed their taxes using "e-leg"; in 2005 some 350,000 did so.
6. Economic aspects	Many actors want clearer coordination, both inside the government and also between public and private players. Some critics argue that a lack of coordination creates technological lock-in that is hampering innovation. There are still only a few e-services around that require authentication mechanisms, but they are increasing steadily.
7. Government services and needs	A number of authorities are deploying e-services. Username and password, SMS and PKI are the commonest technologies. New work methods and organisational schemes are being put in place to fuel adoption of the new technologies. A new Swedish national ID card will be introduced founded on PKI. A framework agreement on "infra services" aimed at developing e-government by providing government agencies with standard e-identification and secure electronic messaging services on a pay-per-use or subscription basis has also been launched.
8. Health services and needs	Carelink is a cooperative company set up by public and private actors in the health sector. Carelink is a CA and is working with other Nordic countries to improve interoperability. It sees the need for a gateway but accords relatively low priority to international transactions and believes there are sufficient challenges at national level.
9. Financial services and needs	Most Swedish banks offer online services and authentication solutions based on user name and passwords. Many also have a combination featuring hardware tokens. More than 4.5 million people do some of their banking online. The PKI joint venture BankID is gaining increasing popularity and it was expected that it would break even in 2005. The BankID authentication scheme can be used for a number of public services. Banks consider their standard authentication mechanisms for bank login to be sound from a business perspective. However Swedish Post has withdrawn from this business.

USA	
1. Aspects of authentication in international transactions	Differences arise in relation to legal structures and PKI structures. Mutual authentication, using some form of federated identity may help move this forward.
2. Current authentication solutions	The Federal Bridge Certification Authority (FBCA) facilitates interoperability among US Federal PKI domains and external PKI domains in a peer-to-peer fashion. The US government will accept certificates if the issuing CA has cross-certified with the FBCA.. Major private initiatives include the Verisign Unified Authentication, the AOL and RSA Passcode. Sun Microsystems and Microsoft have jointly developed the Web SSO MEX and Web SSO Interop Profile, which will enable browser-based single sign-on between the solutions of Liberty Alliance and Web Services Federation Language (VeriSign, Microsoft, IBM, BEA and RSA Security). Microsoft is also working on a system to wrap identity management systems under a single identity metasystem. The interoperable architecture would allow several digital identities based on multiple underlying technologies, implementations and providers.
3. Legal aspects	Many US states have a rule on non-discrimination, stating that a signature may not be denied legal effect solely because it is in electronic form. There is also a federal law to facilitate the use of electronic communications. Since US regulations do not address any specific types of authentication mechanisms or electronic signatures, the issues of cross-border acceptance and which certificates should be accepted do not arise. Nor are liabilities or damages addressed by legislation.
4. Technical aspects	Most technical protocols are in place. There are, however, issues with regard to end users that do not apply an appropriate infrastructure in the home to protect their PCs. Furthermore, there is a lack of an international recognised standard for authentication. There are numerous private and public PKI schemes. Banks use usernames and passwords with soft and hard keys. Some biometric applications are used, both by public actors and some banks. Also, all new passports for visitors to the US must carry mandatory biometric data.
5. Organisational aspects	PKI has offered a mixed response to the challenges of high fees and excessively complex solutions. However, US banks have been quite successful in providing other authentication solutions that meet their needs. The American Bankers Association is one such solution provider. Strict PKI solutions do probably need to reduce their fees. However all e-commerce sites involve authentication in some form, and are probably sound in business terms.
6. Economic aspects	Fraud and other risks are posing serious threats to the market. Gartner Group reports that nearly 30 per cent of those who bank online say that online attacks have influenced their Internet banking activities. Over three-quarters of this group log in less frequently and nearly 14 per cent of them have stopped paying bills online. Some 2.4 million online consumers report losing money directly because of phishing attacks.
7. Government services and needs	The e-Authentication Initiative aims to provide online identity verification services to federal e-government services. This common e-authentication service under the US Federal Enterprise Architecture is based on open standards and a federated approach will allow it to meet the diverse authentication needs of the federal agencies. It will support multiple technologies and interoperable products. It will deliver a uniform, government-wide approach to authentication while providing government agencies with a choice of technologies and interoperable products to achieve their authentication needs.
8. Health services and needs	The Secretary of Health and Human Services (HHS) intends to publish a proposed rule on requirements for a unique health identifier for individuals. This has encountered objections from organisations concerned about privacy issues. A National Provider Identifier (NPI) has been launched. It is a unique health identifier for healthcare providers to use in filing and processing healthcare claims and other transactions.
9. Financial services and needs	The challenge for banks is that consumers have not indicated a willingness to pay for increased online security

INTERNATIONAL ACTORS	
1. Aspects of authentication in international transactions	One of the key elements for reliable and high quality e-service transaction is trust. Online authentication has been identified as a key enabler for trust. The technical building blocks are all there and many authentication projects and providers are active. The conditions for broad interoperable solutions, based on established common policies, best practice guidelines and international coordination, are emerging. A worldwide, accepted, easy-to-use system for online interactions requiring a certain level of e-authentication might be feasible.
2. Current authentication solutions	Liberty Alliance, a group of more than 150 companies, non-profit organisations and government agencies from around the globe is developing an "open federated identity standard" and business tools for implementing federated identity and identity-based Web services. The alliance's members include AOL, Ericsson, HP, Nokia, Novell, NTT, Sun Microsystems, Vodafone, IBM and Adobe. Web Services Federation Language (WS-Federation) has partners including IBM, BEA, Microsoft, Verisign and RSA Security. It provides a specification for standardising the way organisations share user and machine identities among disparate authentication and authorisation systems. However, with IBM now being part of the Liberty Alliance, many observers predict that the competing standards will eventually come together.
3. Legal aspects	One market trend that has emerged in the last two years is the universal acceptance of standards supporting X.509-based PKI. Version X.509 appeared in 1988, while the current version 3 for PKI certificates and version 2 for CRL was adopted by the Internet Engineering
4. Technical aspects	Task Force (IETF) in 1996. Acceptance of this standard by most vendors has provided the groundwork for interoperability of the technology. More work is needed, however, in the area of CPs and CPSs.
5. Organisational aspects	Lack of coordination. Trust and political issues are preventing a top down solution with one central node. More likely that a web-based trust solution will emerge.
6. Economic aspects	
7. Government services and needs	While enabling Governments to offer e-government services, in co-partnership with commercial uses of public e-identity. By introducing this in an efficient and cost-effective way government and commercial enterprises will benefit from economies of scale and at the same time individuals will be empowered to directly benefit from information society services and applications. Standardisation efforts such as by CEN and ETSI (or W3C or OASIS on the global level) are assumed to improve interoperability.
8. Health services and needs	
9. Financial services and needs	

APPENDIX D: MEMBERS OF THE GLOBAL TRUST CENTER STEERING COMMITTEE

The Steering Committee members are:

Thomas Andersson, President International Organisation for Knowledge Economy and Enterprise Development (IKED), President Jönköping University, Sweden.

Keith Besgrove, Chief General Manager, Information Economy Division at the Australian Department of Communications, Information Technology and the Arts, Australia.

Michael Coomer, Director, Westpac Banking Corporation, Australia.

Rob Craig, General Manager, Product and Channel Transformation, Westpac, Australia.

Peter Fritz, Group Managing Director, TCG Group, Member of the Australian Consultative Committee on Business Opportunities Arising from Security and Risk Issues, Australia.

Peter Höjerback, President, Öresund IT Academy, Sweden/Denmark.

John Ketchell, Head of Corporate Services, CEN/ISSS, Belgium.

George Metakides, Advisor Enisa, Greece.

Anders Orre, STG/ChamberSign, European network of Chambers of Commerce, Sweden.

Elly Plooij, Former Member of the European Parliament, Chair of the Council of Experts for National Standards.

IKED
INTERNATIONAL ORGANISATION
FOR KNOWLEDGE ECONOMY
AND ENTERPRISE DEVELOPMENT

PO Box 298
SE-210 22 Malmö
Sweden
info@iked.org
www.iked.org

GTC
Global Trust Center
Sweden

PO Box 298
SE-210 22 Malmö
Sweden
info@globaltrustcenter.com
www.globaltrustcenter.com

GTC
Global Trust Center
Australia

53 Balfour St, Chippendale
NSW 2008 Sydney
Australia
tcgadmin@tcg.net.au

ISBN-10 91-85281-08-5
ISBN-13 978-91-85281-08-4