GLOBAL IDENTITY NETWORKING OF INDIVIDUALS

The Individualised Digital Identity Model

White Paper on the Establishment of an INDI Operator Market

This document is published by the International Organisation for Knowledge Economy and Enterprise Development (IKED) on behalf of the GINI-SA Consortium.

Title:	White Paper on the Establishment of an INDI Operator Market
Authors:	GINI-SA project team.
Main editors:	Herbert Leitold and Bernd Zwattendorfer (TU Graz), Thomas Andersson and Lefteris Leontaridis (IKED) and Shuzhe Yang (Goethe Universität Frankfurt)
Published:	Malmö, July 2013
Publisher:	IKED

SEVENTH FRAMEWORK
PROGRAMME

Table of Contents

1 Problem Statements[1]

Main Problems:

- Citizens have little control over how and where personal data is collected, stored, and processed.
- Citizens are overwhelmed with a bulk of different digital identities.
- There is a mismatch in the balance between usability/comfort and security/privacy.
- Users are dependent on digital communication and have limited means to fully understand privacy implications, make choices and articulate informed identity management preferences.
- The potential for significant commercial gains from a more user-controlled utilisation of personal data is unmet by current implementation efforts.
- No international market has yet evolved for user-centric identity services with viable business models for protecting privacy.

Information and communication technologies (ICT) are in the process of transforming virtually all economies and kinds of industrial and service activities around the world. Our daily lives are fundamentally impacted in a myriad of ways. New applications and services are continuously becoming available online. Their maturity varies from simple informational services to sophisticated online transactions in e-Commerce, e-Government, e-Learning, e-Health, and so forth. Significant benefits of ICT have been demonstrated since decades at the level of firms, industries and aggregate economies. Despite the evidence of positive impacts, however, yet unresolved issues lead to frustrating inefficiencies and unwanted effects.

Although identity management in digital communication matters to almost any industry, the public sphere and for individual users, comprehensive progress in this area has been strikingly absent. The resulting patchwork of half-hearted identity solutions is interrelated with the presence of a range of other outstanding challenges, in regard to data governance, security, privacy, accountability, and lack of trust.

Personalised services must fulfil special requirements in these respects which generally are not fulfilled online. For instance, more personal data are often requested from users than is actually necessary. At the moment, there is a growing tension between the rapidly expanding benefits from massive collection, storage and processing of personal identity data, on the one hand, and the lack of responses on the part of users or service providers to protect privacy on the other hand.

Historically, the need of means to establish trusted identities was interwoven with cultural practices that helped define and prove societal belonging and credible loyalties. As societies evolved, the need increased for identities to be properly created, managed, maintained, used,

[1] The White Paper is the result of collective work by the GINI-SA project team. The main editors are: Herbert Leitold, Thomas Andersson, Lefteris Leontaridis, Shuzhe Yang, and Bernd Zwattendorfer.

and eventually deleted. A range of approaches to identity management solutions are now in place offering optional ways to organise these processes. However, the management of this hodgepodge becomes increasingly complex.

Over the years, digital identity management mainly grew out of the simple management of employees and services operated by individual organisations. As networks kept growing and became more and more interlinked, however, the presence of unresolved issues has become increasingly damaging. This includes violation of minimum disclosure principles, data-use beyond its original purpose, and lack of user control for privacy preservation.

Many users feel uncomfortable with a situation in which they are lacking knowledge which data is kept by service providers, for which purpose, and whom it is shared with. The consequences of such unease increase the more valuable the transactions are and the more dependent we become on online services.

The complexity of identity management in the digital world derives from the inherent involvement of several stakeholders. Users interact in various capacities, as citizens, customers, employees, employers, service providers or identity providers, with a whole lot of specific needs and requirements at stake. On this basis, lack of trust in digital communication may result in increased transaction costs and distortions to behaviour. This prompts finding ways of enabling users to acquire better control which personal data are transmitted to which service providers and how these data are processed or used. User control constitutes an essential aspect in online services which must gain more attention in future identity management systems.

Contemporary identity management systems are marked by serious gaps in security, privacy, trust, and usability. As users are often forced to register at each service provider as a condition for various transactions, they are left with a multitude of different partial identities, many of which will soon be outdated. Mechanisms are lacking for enacting the removal or invalidation of such identities and associated information. This is particularly problematic in cases when service providers store an extensive amount of personal data, as is commonly the case with social networks.. Most systems do not support the complexity of identity aspects, e.g. the use of one identity for different contexts, partial identities or the need of managing updates and expiration. Partial identities or the separation of identities offer users a higher level of privacy because, e.g., the full identity information does not have to be disclosed to the provider, hindering further unwanted data collection. Additionally, users should have the option to stay anonymous or pseudonymous in online services.

Typical identity management architectures usually consist of one identity provider, one or more service providers, and a user. More complex architectures, e.g. for identity federation, aim on interconnecting various identity providers for sharing or distributing identity information. In all architectures, the user has to rely on the service providers and the identity provider. In addition, a trust relationship must always exist between the service providers and the identity provider. Identity federation systems usually build a so-called circle of trust where each participating entity trusts each other. All these trust relationships must be assured on technical and organisational grounds. This, however, does not define a trivial task, as trust is a subjective state of condition that can be supported by technical or organisational means, but still needs to be earned.

Although privacy or security aspects are very important in identity management, usability should not be ignored or even hinder the fulfilment of these aspects. An identity management system which considers privacy and security concerns and additionally user friendliness, is not easy to implement. A balance between usability/comfort and security/privacy has to be found. One important aspect is location independence when users want to manage or use their digital identities. Hence, users should be able to access identity related systems independently of their location or device. This requirement cannot be fulfilled by most actual identity management systems.

Summarising, in current identity management systems individuals are not fully aware of what and where identity information is stored or processed. As a consequence, they experience a lack of privacy, control and trust, resulting in unease, distortions in behaviour and economic inefficiency. In contrast, future identity systems must enable individuals to gain control over their digital identities and use of their private data.

Problem Summary: In practice citizens only have limited knowledge of and control over how and where identity data are collected, stored and processed digitally, resulting in severe problems with privacy, lack of trust, high transaction costs and economic inefficiency. It is the objective of GINI to outline a digital identity ecosystem that enables citizens to exercise control over their digital identities and to exploit the commercial potential of more effective utilisation of user data.

2 Vision

Main Messages:

- The INDI ecosystem encompasses individuals, relying parties, data sources and INDI Operators as its main actors.
- Individuals manage their personal data by means of an Individual Digital Identity (INDI) which is self-created, can be presented to relying parties, and is verifiable against various data sources.
- The INDI users are enabled to exercise control over their digital identities.
- Multi-corner identity services should be enabled between individual users and relying parties, and be supported by intermediary Operators.

The purpose of GINI is to analyse and determine the requirements of a Personalised Identity Management (PIM) ecosystem in which individuals can manage their own digital identities and control any exchange of their personal information. Under the GINI vision, individuals manage their identities by means of an Individual Digital Identity (INDI). An INDI can be described as a self-generated and self-managed digital identity, which is verifiable against one or more authoritative data sources. Once created, users have the ability to link their INDI with authoritative identity data maintained by both public- and private-sector entities. The user will be in the position to control, and be informed of, any use of this data (or links thereto) towards relying parties. The user will be able to judge which transactional requirements (e.g., access control conditions set by a relying party) to meet with or how to underpin his or her trustworthiness towards others in various real life situations (e.g., verifying education or presenting skills when applying for a job).

The main objectives of GINI include:

- Decoupling the activation of digital identities from the use of any particular identifier, and to support the use of multiple identities and/or identifiers.
- Allowing users to exercise full control as to who is able to verify their identities and through which processes.
- Enabling users to control every phase of their digital identities’ life cycle (creation, change, management, revocation, etc.).
- Identifying the ways and means through which a separation of identifiers and other identity attributes can be implemented in a user-friendly manner.
- Outlining the main properties of a digital identity ecosystem that is efficient and yet capable of enabling maximum control of users over their digital identities.
- Determining the prerequisites for providers (Operators) so that a viable business model can be established.

Summarising, GINI envisions a personal and functional INDI ecosystem beyond 2020. This ecosystem considers fundamental requirements in terms of technological, legal, regulatory, and privacy aspects, devised so as to allow users to exercise maximum control over their digital identities in all online processes.

2.1 The INDI ecosystem

With an Individual Digital Identity (INDI), we refer to an identity claimed in the digital world by an individual who creates, manages and uses it. Individuals have the ability to establish and manage an INDI and to decide where and when to use it – while interacting with other individuals or entities. As a result, users are able to present their chosen, verified partial digital identity to other users or relying parties with which they wish to build trust relationships. This may be done so as to perform transactions for personal, business or official purposes.

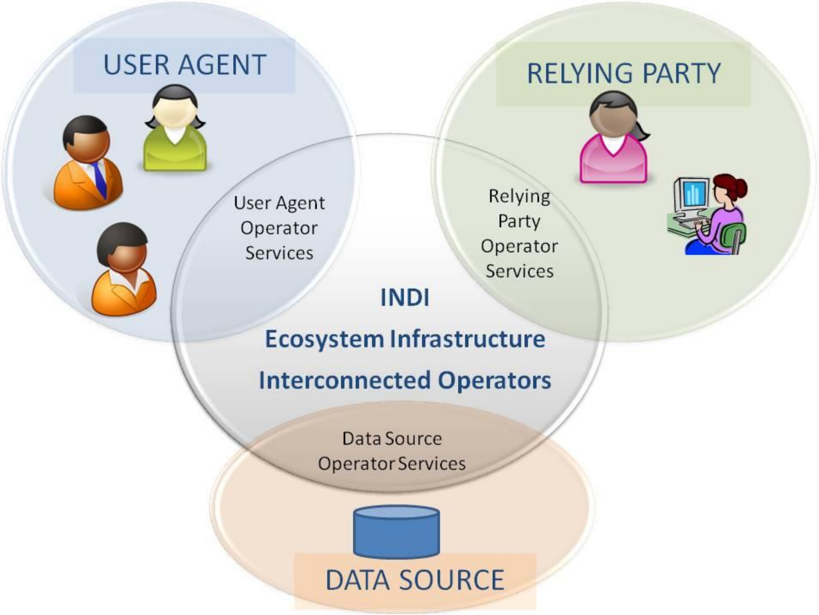
USER AGENT
RELYING PARTY
User Agent Operator Services
Relying Party Operator Services
INDI
Ecosystem Infrastructure
Interconnected Operators
Data Source Operator Services
DATA SOURCE

Figure 1 – The INDI ecosystem

The INDI is a digital identity that is:

- Self-created by the individual.
- Self-managed throughout its lifecycle.
- Presented to relying parties (entities or other individuals) partly or wholly, depending on interaction requirements and established trust relationships.
- Verifiable against varied and variable data sources chosen by the individual and trusted by the relying party.

Three types of actors constitute the outer corners of an INDI ecosystem:

- An individual is able to access and manage the INDI and its use in various types of context through a User Agent interface. Choices can be made about which data source to use and what identity attributes to disclose in each setting.

- A Relying Party is offered its particular interface through which it can accept and verify the use of an INDI and carry out its own side of the negotiation that establishes the trust relationship.
- Data sources such as authoritative identity registries or other types of identity service providers (e.g., from the financial sector, other business sectors, social media etc. are able to implement interfaces for attribute and assertion services to be used for verification and/or attribute exchange between individual users and relying parties.

GINI envisions these actors as plugged into an infrastructure that incorporates a community of interconnected INDI Operators. These are entities that provide INDI services and deploy INDI interfaces to the mentioned actors, as seen in Figure 1.

Inter-Operator functionality is a crucial manifestation of a viable infrastructure allowing for genuine interoperability in identity management. This in turn requires the presence of an inter-Operator interface that allows for the relay of identity claims and other attribute-related communication, meaning that service requests from an actor that is connected to one kind of Operator flow through smoothly to the actors that are connected to other Operators, effectively enabling multi-corner linkages and transactions. While relations between the main actors may be managed through different combinations of INDI Operators, it will be critical how the architecture for inter-Operator interphase is framed. An open and interconnected ecosystem that incorporates specialised Operators must critically spur a dynamic creation of diverse, innovative end-to-end services.

The INDI framework allows individual users to assume various roles, for instance as citizen, employee, or customer. The user must be able to choose which roles to act in and what information to reveal in the different roles. As such, an INDI Operator may serve to represent the user in many different kinds of context. Still the user is able to manage a set of partial identities, similarly to the situation in the physical world, by providing the information that is relevant for each situation. This includes those cases where anonymity, pseudonymity, and limited attribute provision are desired and acceptable.

2.2 Business Aspects of the INDI ecosystem

Users have limited awareness of their private data is used and possess few means to control the ways in which their identities are managed. While significant commercial gains can be attained from exploitation of user data, no effective market for privacy protection and user-driven identity management services has been developed thus far.

2.2.1 Business Models for INDI Operators

Establishing an INDI requires a new form infrastructure. With no INDI market or Operators currently in existence, what steps and measures are required to enable the rise of a market with viable INDI Operators? Not only the INDI ecosystem's technical aspects require consideration. Conditions must be such that financially viable INDI Operator business models fall into place. At present governance model is also greatly important for establishing user trust.

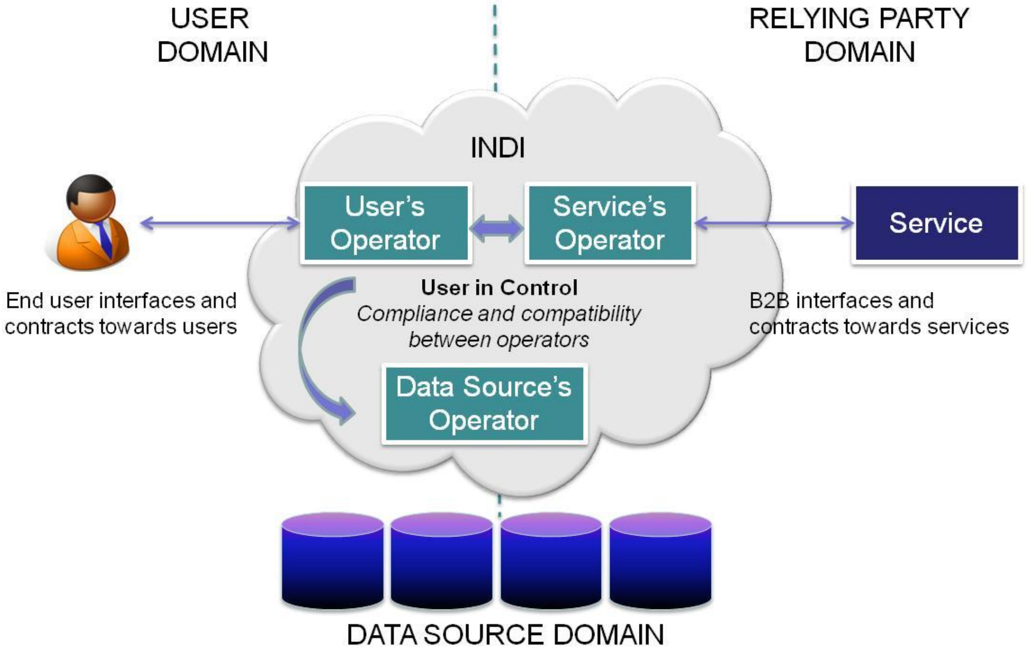
USER DOMAIN
RELYING PARTY DOMAIN
INDI
User's Operator
Service's Operator
Service
End user interfaces and contracts towards users
User in Control
Compliance and compatibility between operators
B2B interfaces and contracts towards services
Data Source's Operator
DATA SOURCE DOMAIN

Figure 2 – The multi-Operator model within the INDI ecosystem

The rationale for an Operator network model as the basis of the user-centric INDI ecosystem is as follows:

- Independent trust anchors are needed to enable trust within the INDI environment and provide added value beyond users' self-asserted claims.
- From a risk management and privacy point of view, it is important to avoid centralised single points of failure which also present threats for privacy-compromising data aggregation and/or profiling. INDI management and data should be de-centralised and decoupled from each other.
- The INDI Operator concept and associated business models leverage possibilities for creating a truly global and competitive market conducive to diversity and innovation in the development of INDI services.
- Without appropriate supporting services, users struggle to manage their own trust decisions. If they would have to evaluate large numbers of potential third parties, the situation becomes unmanageable. Users want entities which they can trust and which can "represent" the "whole infrastructure". Users must, however, be able to enjoy sufficient technical assurances and legal warranties, if they are to be able to undertake well-founded "trust decisions" and be expected to pay for associated services.
- The Operator Network model can be standardised and regulated more easily than a model that is based on strongly heterogeneous, uneven entities.

Some key assumptions about business models can serve as a starting point in this respect:

- An Operator can choose to deploy one or more interfaces according to its business scope. When multiple interfaces towards more than one actor category are in place, additional privacy safeguards are warranted. The GINI project explores these privacy constraints and requirements.
- Entities which are already active at either end of the INDI ecosystem (e.g., existing service providers, banks, telcos, social networks and large relying parties) may opt to deploy INDI interfaces and inter-Operator interfaces, thereby becoming Operators themselves.
- In any and all business models, certain requirements should be met in order to enable trusted relationships between Operators and Users:
    - The INDI Operator should act as a trust anchor, helping to verify the User's identity data in the INDI ecosystem – the whole ecosystem has a trust relationship with the User through the INDI Operator.
    - The INDI ecosystem is global, which means that the INDI Operator and the User need not to be from the same country or identity domain.
    - The relationship has a contractual and legal dimension and not just a technical side.
    - The User should be able to have several parallel relationships with INDI Operators, while being able to switch from one to another, as can be the case with mobile telcos.

2.2.2 Business Value for Actors and stakeholders

The INDI ecosystem could be built upon a one-sided market, where the service provider and customer interact directly with each other, or a two-sided market, where different business models and pricing schemes are involved in a unified set of business transactions. Creating a two-sided market is much more complex and often requires transfer fees and other types of pricing models.

It is essential that the INDI ecosystem can provide market conditions that allow for the creation of viable business models. In order to pave the way for such a development, it is important to understand which potential business models can arise and what is required for such a development to unfold. The search for solutions should be guided by concerns for realising a user-driven market, where services are designed to resolve real issues and meet genuine demand in the market place. It is also important to take the necessary steps for creating a competitive open market and avoiding vendor and technology lock-in. Operator business models should allow competition whilst promoting synergies in order to avoid "gated communities", "islands" or "silos".

Value of INDI services for Users:

- Enhanced privacy, conditionality of attribute disclosure control, reduction of uncertainty and behavioural distortion.

- Possibilities for building up their reputation when given the possibility to wilfully disclose verified and verifiable attributes of their own identity (e.g. professional status in a social network).
- Personalised services within the INDI ecosystem can offer behavioural simulation of real-life control of basic life processes:
    - Users can push desired information to relying parties and pull filtered information according to their own preferences, thereby controlling information exchange with relying parties such as internet merchants, social networking sites and other vendors with an online front.
    - Users can negotiate trust relationships based on the assumption that they want to share data and that valuable privacy lies in controlling what they share, how and with whom, rather than just blocking access to information according to traditional data protection models.
- Individual privacy can be enhanced by using consistent privacy policies as a basis for negotiating trust relationships with relying parties:
    - It should be a conscious decision by the user to release data, not an obligation to avoid denial of service.
    - Negotiated privacy levels and secondary use of data may add additional benefits in consumer relationships online.
    - Under such conditions, privacy can be safeguarded through an active choice by users, thereby opening for business value in offering privacy-enhancing services like PETs, resulting in possibilities for innovative companies to gain a competitive advantage through technological leadership, while enabling the establishment of an operational market.

Value of INDI services for Relying Parties:

- Online vendors and service providers will build stronger relationships with their customers and users of their services, if they offer them control over their side of trust relationship negotiations:
    - Data provided through wilful disclosure as a result of informed consent and free user choice will be much more useful and reliable.
    - Tailor-made trust relationships are likely to increase customer loyalty.
- INDI services would offer confidentiality for the Relying Party:
    - With current API-based interfaces of identity providers such as social networks, sensitive commercial information regarding the customer base of online vendors and service providers is at the hands of online identity providers who might be acting as competitors to those Relying Parties already existing or evolving in the future (on the basis of data aggregation).
    - A win-win situation in negotiated trust relationships gives benefits of privacy, confidentiality and directness to Users and Relying Parties.

- The INDI ecosystem should offer new opportunities to make implementation easier for Relying Parties:
  - With emerging models of Identity-as-a-Service, Claims-as-a-Service, the holy grail of Relying Party simplicity may be at reach.

Value of INDI services for Data Sources:

- For registries in the public domain, value relates to the public sphere:
  - Civil society goals such as freedom of information and release of control to the legitimate information owners can be realised.
  - Potential revenue streams resulting from some Operator models may help maintenance of public records if attribute access is chargeable.
- For directories in the private domain:
  - Revenue streams in identity-supply service can create a market for Cloud services directed at data sources.
- An individual can also act as a data source within the INDI ecosystem, thereby facilitating ways to monetise on data and privacy.

GINI Vision: Individuals' identities are self-created and self-managed throughout their lifecycle. Partial or full identities can be presented to any relying party (entities or other individuals) given the existence of appropriate trust relationships. The identities are verifiable against variable data sources chosen by the individual and trusted by the relying party. In the entire identity management system the individuals have maximum control of their digital identities.

3 Gaps

Main Gaps:

- How can user awareness of lacking control over personal data processing be increased?
- How can users be enabled to exercise control over their digital identities across a diversity of identity management systems?
- How can relying parties be induced to collect as little information as possible from individuals and use it for a predefined context only?
- How can new technologies be merged faster into the legal domain?
- What is the willingness to pay for enhanced trust and privacy-friendly services among users or relying parties? How can the benefits be appropriated by service providers?

Within this section, the main gaps relating to digital identities, which have been identified by GINI, are stated. The gaps are classified according to functional, privacy/technical, legal/governance and business gaps and are highlighted in the following sub-sections.

3.1 Functional Objectives

A plethora of identity management systems exist today. In most systems, identity information is directly exchanged between identity and service providers after user authentication. Other systems use claims for presentation to service providers, which have been obtained by the user from the identity provider before. However, a focus on the user perspective is still mostly lacking. In user-centric systems, the user is intended to exercise control what data are transferred or processed.

Many providers of digital services traditionally follow the “lock-in” principle concerning user’s data and information. Such practice is rendering the proposed user-centric approach ad absurdum by preventing users from taking their business elsewhere and thus from challenging the terms and conditions of service providers. Since decentralisation often hinders direct user control, further research is required what technologies and organisational models are best equipped to handle the kind of trade-offs that may exist between user-centricity and service provider-centricity. Further research is also necessary to clarify what initiatives and measures are needed to pave the way for the development of such user-centric digital solutions.

Traditionally, digital evidence was produced in and for the service provider domain, e.g., audit records and admission/access documentation. When shifting from service provider centricity to user centricity some collection of evidence can be moved into the user domain. The primary purpose of such digital evidence is user protection.

User Centricity:
How can users exercise control over their digital identities across a range of identity management systems?

How can the principle of a user-centric identity management be integrated into existing identity management systems and engrained into new ones to address privacy-by-design requirements?

The “user” needs to be empowered to take informed decisions and to be able to pursue potential violations of her privacy policy. Users must not exclusively rely on the evidence produced and owned by service providers.

Having a look at the world-wide eID landscape, various eID solutions or identity management systems are already in place. They usually differ at technological, legal and/or organisational levels. For example, some use simply username/password schemes; others rely on smart cards, which offer a higher level of security. As for organisations, the scope of some systems might only be one domain while others must achieve eID acceptance across multiple ones. Such differences lead to several challenges. For instance, many identity management systems are based on the combination of different services - all influencing the lifecycle of a user’s digital identity. Every interaction involving more than one entity requires a stable trust relationship. Hence, all services must have an appropriate trust relationship established amongst each other.

Interoperability:
How can multiple identities be combined most effectively?

How can cross-domain or cross-border interoperability be achieved (world-wide)?

What is the best way to establish trust relationships amongst various entities?

Building trust relationships is complex. Support can be provided at either technical or organisational level. Established or existing trust relationships usually require some kind of trust or digital evidence verification. Traditional means for gathering digital evidence and compiling evidence chains are challenged by today’s heavily distributed, possibly federated, and partially encrypted operating environments. This results in separate collections of digital evidences within a workflow. Compared to that, the seamless compilation of digital evidence chains that reflect the complete end-to-end workflow is almost impossible to attain.

Although many users are aware of the sensitivity of personal data, they are still mostly willing to expose personal information in order to gain economic or other advantages. This kind of voluntary personal data disclosure is frequently happening in social networks or lotteries of companies that further use the data for personalised marketing activities. This phenomenon, which emanates from the discrepancy between users’ privacy awareness and their actual privacy behaviour, is usually referred to as the “privacy paradox”. On the other hand, users lack information how data about them is being used today or might be used in future. They have imperfect options to express their preferences. For instance, if they have only the option to undertake a particular transaction in a way that does not protect their identities, or to not undertake it at all, this will not provide us with adequate information on their willingness to pay.

Usability:
How can user awareness on privacy be increased?

How can the right to demand deletion or correction of identity data be effectively fulfilled?

For such reasons, it is important both to raise user awareness and to grant users the means to express their demand for identity management pursued on their terms. User awareness and empowerment of this kind could be raised by increasing usability when developing or deploying new technological systems. Basically, usability includes navigation through the application, readability, as well as the design of the complete user interface. A privacy-friendly and useable application definitely raises user satisfaction and user acceptance. Moreover, a user- and privacy-friendly application can help users understand and follow what happens with their personal data. For instance, the prevailing legal frameworks grant users the right to request deletion or correction of their data. Today, unfortunately many providers do not oblige to this requirement. In practice, however, users are lacking the information that would be required for making this right operational. Therefore, users tend to have weak or no control in this respect.

In today's world, the period in which inventions and research are implemented into real-world software and international standards is significantly shortened. Traditionally, the "best-before" time of international best practices of approximately ten years was considered to be adequate. In the current reality, even "new" approaches and implementation processes are frequently subject to deprecation and disqualification (e.g. incidents that have been seen among certification authorities, flawed security protocols, or progress on breaking fundamental building blocks such as cryptographic services). However, new implementations should follow well-known security or privacy standards, i.e. when designing software, privacy aspects are usually covered by non-functional requirements only. Hence, future software developments should follow approaches where privacy-enhancing functions are considered and built-in throughout the design process.

Invention, Innovation, and Research Cycles:

What is required for ensuring that privacy-enhancing functions are integrated in the software design and development process?

3.2 Privacy/Technical

Although multiple identity management systems are already in place and they fulfil their basic functionality, most of them still lack in privacy protection. In most cases, they control or process more personal data than necessary. The current situation of collecting and storing as much personal data as possible should be avoided. Instead, only the minimum set of information should be processed. Technological advancements, such as attribute-based credentials, enable us to better address such fundamental privacy principles, e.g. data avoidance and minimisation. In practice, data controllers often obtain consent to collect information beyond what is necessary for the fulfilment of the core contract that constitutes their service. Additionally, personal data should only be used in the relevant and predefined context. This privacy requirement is defined as purpose binding for personal data. Purpose binding so far has been dictated with legal means. Technological solutions that would prevent a business service (i.e. relying party) from using personal data outside the context of its original purpose are currently dependent on the success of Digital Rights Management (DRM) systems for which many challenges remain. Moreover, in many digital interactions citizens

Data Anonymisation and Minimization:

How can relying parties be forced to collect as little information as possible from individuals and use it for a specific and predefined context only?

Can better anonymisation techniques be found?

should have the possibility to be anonymous. However, recent research has demonstrated that seemingly anonymised data can often be processed in such a way that it is possible to "re-identify" or "de-anonymise" individuals with significant accuracy. Given the theoretical limits of anonymisation techniques, scientists look for more holistic approaches, such as differential privacy.

For privacy-preserving reasons, entities that are involved in data collection or data processing are usually in charge of keeping these data safe and protected. Additionally, under certain conditions business services (i.e. relying parties) should be able to retrieve the identity of an anonymous user, who has misbehaved or has misused the service. Hence, the relying party is many times accountable for the data stored or processed. Accordingly, they usually tailor their terms and conditions to this requirement. The electronic representation of consenting into a new, potentially complex service in today's digital services is traditionally designed in a binary fashion: opt-in or opt-out concerning the basic terms and conditions of the service provider. Furthermore, while the process of consenting is usually realised by a one-click solution, the terms in which one is consenting into are quite exhausting (60+ pages on a mobile screen) and through that rarely promotes an adequate "informed" consent.

Accountability and Consenting:

Can cryptographic techniques be established that allow for the inspection of anonymous credentials by trusted third parties?

Would it be possible to consent only to parts of terms of conditions?

Currently, cloud computing represents one of the most important emerging new frameworks set to shape the IT sector. An effective implementation requires, however, that the issues related to electronic identification are resolved. Technology gaps arise when moving existing identity systems to the cloud or when designing an Identity as a Service Model (IaaS). Smart phones or tablets define another emerging technology where a lot of research is carried out or business applications are developed. Such mobile devices are usually not designed to support single functions only but provide a high number of features. Aside classical functions such as phone or organizer support they can use different communication channels or have built-in different sensors such as acceleration or position sensors or Global Positioning System (GPS) functionality. Additionally, installing third-party applications can enhance these mobile devices. A true user-centric operating environment is highly dependent on the availability of extraordinary mobile and highly versatile devices. However, in particular the currently available mobile devices have proven to be uncontrollable and assumed causes of privacy violations through manufacturer means, for example remote monitoring and localisation, remote device wiping, and the explicit prohibition of device software analysis (black box principle).

3.3 Legal/Governance

When processing or storing sensitive data this may have to occur in accordance with legal regulations or policies, e.g. in some cases data must only be stored in specific countries. It is still not clear what technical means are best suited to accommodate jurisdictional discrepancies.Traditionally, new technology and applications are advancing much quicker than the respective regulatory frameworks. However, due to a significantly accelerated development and swift derivation of formerly unavailable services within the technology domain, the legal domain is merely responding with "quick fixes" and specific addressing of details instead of bringing forward an "umbrella" under which new applications and technology may be implemented and operated.

A couple of nations, especially within the European Union, have already rolled-out qualified national eID solutions[2]. Where qualified eID exists, the recognition beyond their initial domain of application (e.g., outside the country, between public and private sector) is typically not ensured. Besides technological differences, legal acceptance is usually given on national level only. Hence, there exists a gap in cross-border applicability. Within identity management, underlying identity data can be of different quality. Identity data can be provided by users themselves, e.g. by registering at a web site. In contrast, data are usually of higher quality if retrieved from national registers which are maintained by a region or country. Thus, when using identity data as a certain claim, the level of assurance of the data is vital. In addition, at the moment, users have their digital identities stored across various providers. In many cases that data is duplicated. In social networks, users must provide their identity information for every social network Operator during registration. Consequently, the simple transfer of a social network profile to another provider is not possible. The same issue also applies to the public sector, where it is difficult for public authorities to share or transfer identity information between different sectors or domains.

The data protection directive of the European Union (Directive 95/46/EC, currently under revision)regulates the protection of individuals with regard to the processing of personal data and on the free movement of such data. This directive was published in 1995. Within this directive, actors are classified into data subjects, data controllers, and data processors. Besides legal regulations, organisations or systems have to follow a regulatory or governance

Compliance:

How can compliance with legal regulations or policies be achieved best?

How can new technologies be merged faster into the legal domain?

eID Mutual Recognition:

Which policy initiatives may be adopted to stimulate further mutual recognition?

How will liability be allocated in case of a breach?

What enforcement regimes should be put in place?

Regulatory and Governance Framework:

Is the data protection directive of the European Union (Directive 95/46/EC) still adequate in today's (and tomorrow's) information society?

Which arguments support regulatory intervention, what is the drawback?

Are all/some of these arguments covered with the draft Regulation revising the Directive 95/36/EC?

[2] We refer to "qualified electronic ID" as what might become "notified electronic identification" under the proposed Regulation on electronic identification and trust services for electronic transactions in the internal market, i.e. eID that Member States inter alia assume liability for. As at the time of writing, this Regulation is still in a draft status, we avoided using the term "notified eID" to not indicate that such cross-border schemes already exist. However, for several government eIDs, the characteristics of legal certainty and liability exist.

framework. Such governance frameworks can be self-regulated, government regulated, or co-regulated. In case of the implementation of user-centric identity management systems, the evaluation of various approaches is required.

3.4 Business Case

Identity management fulfils a range of purposes. Outcomes matter for user well-being, trust, transaction costs, communication and purchasing behaviour. Improved identity management will mean that processes can be simplified and there will be higher efficiency. For best possible outcomes, a market place conducive to the introduction of viable business models needs to be enabled, as well as for innovation and experimentation.

Although identity management has been a hot topic for years, no international commercial market for identity services has evolved to date. Many governments and individual companies have implemented new technologies, methodologies and services for prospective widespread diffusion, but the numbers of users and transactions has remained low. It seems that the market for identity services does not match well with the current technology driven online environment, which is lacking proper protocols and mechanisms for supporting orderly identity management.

Productivity and Costs:

How can future identity management systems help increase productivity or decrease administration efforts and costs?

Can the deployment of more secure and privacy-friendly identity management systems increase user satisfaction?

The basic idea behind the notion of a viable business case in identity management centres on the challenge how to arrive at a situation in which the benefits of removing distortions and inefficiencies can be appropriated by business developing and offering the best services. The value added that is captured needs at least be sufficient for outweighing the required investments and costs.

Because of the increasing scope of digital communication, coupled with the complexity and heterogeneity of modern organisations, traditional identity management systems have reached their limits. Individual users run into a myriad of diverse identity issues every day, frequently causing negative experiences as well as distortions in behaviour. This problem is compounded by the large benefits that can be reaped by organisations through exploitation of personal data among unknowing users. The prospect of offering users understandable services, reducing their uncertainty and increasing their control, carries the potential of leading to substantial benefits for business and for the economy.

As for modern organisations, identity management requires heavy administration, e.g. every employee owns one or more digital identity, which are used for various kinds of access control. However, most organisations tailor their identity management system implementation only to specific needs and limit the use of foreign identities. Hence, opening up these identity management systems as a business case can rationalise the organisation and help focus attention on core business. There is also a strong case for reducing costs, e.g. by improved authentication infrastructures, reduction of redundant infrastructures, or simplified administrations.

A lot of processes or transactions in public administration, banking, or health sector require identification information from users. Moreover, lacking assurance in the client's identity leads to "pay-in-advance" business models in the online world of a sort that consumers might not accept in traditional business. Compare, e.g., the way a book shop or "traditional" mail order shopping with cash on delivery has changed to advance payment or at least credit card guarantees. Less risky quality identification for service providers will allow for a broader range of models.

Traditionally, users prove their identity by showing an appropriate ID. As an example, users need to go personally to the bank and have to show their ID for opening a bank account. Such processes can be much improved when using digital identities, e.g. bank accounts can simply be opened online without any bank opening hours constraints. Hence, promoting qualified electronic IDs within the private sector could increase productivity and save costs.

Compliance describes the adherence to legal regulations or certain policies. In case of audit events, organisations are often required to prove that they behave compliant with certain regulations. Identity management systems can improve accuracy when responding to audit requests. By the help of digital identities they get, on the one hand, better visibility of user access rights and, on the other hand, they are able to retrieve user's identity in any case of misbehaviour. In typical identity management scenarios, one or more service providers interact with one identity provider and user. All these entities must have a proper trust relationship amongst each other, hence the user trusts the identity and service provider and the identity and service provider trust each other. However, there is still a gap if service providers act as intermediary for person-to-person transactions. In this case, each person trusts the service provider but the trust relationship between the two interacting persons cannot be directly achieved. Overcoming this gap in online person-to-person trust relationships could create new ideas for business case development. Additionally, businesses must work out the tools that can induce users to participate in enhanced trusted and privacy friendly services. This includes articulating and communicating the advantages such services offer to the user and how the higher value can be communicated best. Users must somehow value trust and privacy preservation and be willing to pay for it.

4 Recommendations

General Recommendations:

- Users should be enabled to exercise maximum control of their personal data.
- Privacy Enhancing Technologies should become state of the art in identity management systems.
- Regulations for data protection and privacy should be advanced to better address fundamental privacy principles.
- Conditions need to allow for the rise on business models that can thrive from the development of user driven privacy protection and identity management services.
- Multiple stakeholders need to be engaged in the development of a viable ecosystem for identity management services.

This section offers recommendations how to tackle the gaps identified in the previous section. On the one hand, this gives readers a vision on how eID related topics could and should be enhanced in the future. On the other hand, these bundled recommendations should help and support professionals (e.g. policy- or decision-makers, managers, researchers, etc.) as well as the broad community of users in making informed decisions when electronic identities are involved.

4.1 Functional Objectives

4.1.1 Enable User Control over Personal Data

Most of today's identity management systems follow the approach where user's identity data are directly exchanged between an identity provider and a service provider. This means that the user has less or even no control what data are being transferred or processed. To enable user control, the user perspective of identity management systems must be put in focus. Users should always be aware and have maximum control which personal data are processed or transferred by service providers or other connected entities.

4.1.2 Increase Interoperability

Various eID solutions or identity management systems can be found across the world. Some are driven by the public sector, others by the private sector. Offering users online access to services through different eID systems is important for allowing users greater usability and flexibility. Increasing interoperability (at functional, technological, legal, and organisational level) needs to assume high priority in future identity management systems.

4.1.3 Gain User-Awareness on Privacy

Many users are still willing to over-share personal information although they claim to care about privacy. This frequently happens in social networks or marketing lotteries of companies where users voluntarily disclose their personal data. Additionally, many service providers offer discounts or other not only economic advantages for collecting personal data. The collected personal data is commonly used for more personalised marketing activities to further increase revenues. Hence, one objective should be to increase user-awareness on privacy, show its advantages, and look for incentives to change user behaviour.

4.2 Privacy/Technical

4.2.1 Follow Data Minimisation and Minimal Disclosure Principles

In all relevant scenarios where personal user data are involved or processed, only a minimum set of data, which are really required for processing, should be disclosed. At the moment, many service providers obtain user's consent to collect data beyond this minimum required set. In general, collection of as much personal data as possible must be avoided and service providers should be obliged to. Additionally, personal data should be only processed in the relevant and predefined context.

4.2.2 Ease integration of PETs and TETs

For more privacy preservation, technology enhancements such as attribute-based credentials or any other PETs already exist. They can act as key enablers to better address fundamental privacy principles such as data minimisation or minimal disclosure. However, although such technologies are already available they still lack in practicability. At the moment, for service providers they are more complex to implement and integrate than not do so. Thus, an easy and less complex format can help to achieve mainstream adoption. Additionally, Transparency Enhancing Technologies (TETs) can also be a way to create and increase user-awareness for privacy. These technologies make data processing and information flows visible to users and thus enable transparency for sensitive data processing.

4.2.3 Privacy by Design in New Technologies

In practice, security or privacy does not play that important role in most online services as it should do. If privacy concepts are considered, they are usually covered by non-functional requirements only, e.g. by specifying appropriate general terms and conditions. However, to fundamentally consider and integrate privacy concepts from the very beginning, privacy-enhancing functions should already be built-in throughout the whole development and design process. The early integration of such concepts could additionally support especially new technologies such as cloud computing or mobile systems to gain more trust.

4.3 Legal/Governance

For the setup of electronic identification and correspondingly respecting privacy in a broad scope, usually some kinds of regulations are required to be considered by policy makers. Regulations can take many different forms. In general, there are two categories of measures available to EU policy makers: legislative measures and non-legislative measures. Legislative measures or so-called "hard law", which are directly binding, are regulations, directives or decisions. In contrast, non-legislative measures and referred to as “soft law” include e.g. recommendations or opinions, which have no direct binding legal effect.

Within future identity systems, the availability of privacy enhancing services will play an inevitable role. Although there are already data protection regulations in place, they mostly focus on ex-post securing of data rather than on ex-ante elimination of privacy risks. Counter-examples such as the Privacy Impact Assessment Framework for RFID applications are rather exceptions than the rule. Hence, single legislative measures do not produce the desired outcome, thus rather a combination of legislative and non-legislative measures seem to be more effective.

Because the costs of deficiencies in identity management are spread thinly on large numbers of unaware users that face difficulties to organise themselves effectively, the appropriate portfolio of measures should be worked out in a consultative process marked by effective engagement by multiple stakeholders, including among:

1. Civil society (e.g., consumer advocacy groups, activists, academia, and other experts).
2. Governmental entities, spanning authorities concerned with implementation as well as those to be affected by the outcome.
3. ICT industry (particularly those involved in the design and deployment of identity solutions, including large scale Operators as well as small niche players and potential innovators).

Since users’ awareness and behaviour will be linked to the options they are confronted with, and the incentives for different service providers to engage in efforts to, e.g., develop better privacy protection, will depend on the actions of other service providers as well as how users will respond. The drive for developing solutions will much depend on what active interface can be achieved between users, service providers and various kinds of public authorities and policymakers. There is a case not only for activating appropriate representatives of the latent “silent majority” to have a say on what needs to be done, but to initiate a process of continuous collaboration, entailing improved awareness creation as well as concrete problem-solving, between the key actors that need to be part of a viable solution.

On this basis, we propose that the preparations for launching an INDI architecture and/or INDI services should be accompanied by the establishment of a consultation and communication platform. Such a forum could be developed on a European basis, but should be global in nature (or extend to other parts of the world from a European base). This is important both because the global nature of the digital exchange means that technical, market and policy developments in any single region can affect other parts of the world. This would facilitate exchange of information what works and what does not work under varying circumstances, and help identify best practices. This further helps supporting a more widespread understanding and agreement on what measures are required for attaining solutions that are both effective in the short term and susceptible to innovation and gradual improvement over time.

4.3.1 Enhance the Data Protection and Privacy Framework

Privacy Enhancing Technologies have already been discussed in the privacy/technical section by describing the lack of practical applicability. Service providers themselves have only low incentives to minimise data sets, as this would be against their existing business models. Hence, certain regulations can help in stimulating the adoption of PETs. However, the sole use of legislative measures will have limitations; hence efforts should be made a work out a combination of legislative and non-legislative measures capable of acting as a driving force.

At the moment, taking user account and attribute information from one service provider and transfer it to another service provider is nearly impossible. Actually, users should have the possibility to choose their desired provider and data should be made available towards the user or other providers for a possible and authentic transfer. Although the European Commission (EC) has considered a general right on data portability within its proposal of the amended data protection directive, open issues still remain which need to be taken into account in future. For instance, this implies the application of a different legitimate basis (not based on consent or a contract) for data portability or the ability to designate recipients without revealing more information than necessary.

Within a future legal framework accountability is also worth mentioning. In general, accountability means the responsibility of an entity to explain how and why it has acted in a certain way. Accountability is a basic principle of data protection law. In the upcoming new data protection regulation of the EU, accountability is interpreted as ensuring that data controllers comply with data protection rules, and that effective policies and mechanisms for achieving that are in place. However, although there is a strong correlation between accountability and data protection, additional accountability mechanisms may be required in future systems. In order to find the right accountability mechanisms, the individual context needs to be investigated by considering the nature and scope of trust framework policies or the economic interests of the participants.

4.3.2 EnableRe-Use of Public Sector Information (PSI)

The re-use of public sector information (PSI) is adopted in Directive 2003/98/EC, the so-called PSI Directive. The aim of this directive is to harmonise policies and practices of the Member States for the re-use of data available from public sector bodies. In terms of legal recommendations, a regulatory framework which enables and promotes the re-use of PSI pursuant to a data subject request is required. Additionally, public authorities must recognise the benefits of opening their data and share this added value also to the private sector. Open issues for further research remain on data portability for PSI, legal and technical safeguards or verification of compliance.

4.3.3 Achieve Cross-Border Acceptance of E-Signatures

Within the Digital Agenda for Europe, the European Commission proposed a revision of the signature directive. The proposed regulation includes a legal framework for achieving interoperability of secure electronic authentication systems. Furthermore, the mutual recognition of notified electronic identification means across all EU Member States is aimed at. While the implementation of a solid and common legal base within the EU may be appropriate for the public sector, the private sector does not require legal measures per se. Hence, other forms of regulatory invention (non-legislative measures) are likely to be more suitable for the private sector, including for the purpose of catalysing viable demand for identity management services and for stimulating innovation and experimentation. Still the proposed regulation requires that notified electronic identities can be used by the private sector. This gives legal certainty for private sector players if they choose to do so.

4.4 Market Development

4.4.1 Apply a two-sided Market Model

A new identity management system could be built upon a one-sided market, where the service provider and customer interact directly with one another. However, such a scenario lacks network effects and economy of scale. We therefore recommend that INDI would be based on multi-Operator business models, which could foresee multi-sided pricing between Operators and users, relying parties, even data sources. In order to promote competition, INDI implementation could be based on open pricing from the outset, without transfer or roaming fees taking place between Operators. On the other hand, some models appearing in the market do incorporate transfer fees while abstaining from charges at the outer ends of the multi-corner transactions.

Under such a multi-Operator model, there is no need for Operators to negotiate fees. Operators can then be anticipated to collaborate primarily on the basis of standard Service Level Agreements. However, a contractual or regulatory set-up capable of promoting standardisation and definition of responsibilities is required.

In order for the INDI network to work out, orderly conditions need to be in place to support effective co-operation contracts between the various INDI Operators. On this basis, the infrastructure initiated by the EU could be extended globally. We recommend that a rule book is developed through which the fundamental principles, standards and rules of the INDI network can be defined. Such a rule book could be a recommendation or the parties may contractually agree to follow it.

4.4.2 Pave the Way for Privacy-enhancing Business Models

Although PETs such as anonymous credential systems are technically available, they have still failed to inspire mainstream adoption. One reason might be that service providers do not have the incentive to limit functionality of data or cease collecting as much user information as possible. Privacy-related and user-centric identity models and technologies still suffer from a gap in business adoption. We recommend research and experimental policy action how to catalyse that concerns for privacy can generate value for service providers and Operators. By providing a basis that allows for the rise of innovative and economically viable business models in the area of privacy, beyond sole compliance considerations, we assume that concerns for privacy, user control and trust can evolve as a competitive advantage. Hence, PET can be seen as a factor in the value chain of electronic service the same way as productivity increasing tools are seen in a production plant.

4.4.3 Enable the Rise of a Competitive Market

Competition in the market place is an important prerequisite for pushing businesses and entrepreneurs to develop new technologies and to innovate in new processes, goods and services. In the field of digital identities, whereas the present situation brings high costs, the creation of a competitive market would speed the development and the adoption of a range of PETs, adapted to resolve outstanding issues and create value in a range of service domains.

How do we get to that kind of state? A comprehensive strategy should be adopted to create incentives for each of the key players to contribute to the rise of new demand-led ventures from their end. Part of the task is to overcome coordination problems in the development of mutually interdependent but inherently separable parts of the GINI architecture, such as the parallel development of diverse but compatible identity services and attribute services.

There is a specific need for initiatives that can serve to make users more aware and spur the currently lacking demand for control of their identities and privacy protection. Real options need to be introduced so that users can be confronted with orderly choices in behaviour, allowing them to articulate their preferences and demonstrate willingness to pay for privacy and higher levels of trust. To achieve that we need diversity in initiatives, innovation and experimentation, featuring public-private partnership and procurement strategies for promoting the rise of services that do not exist today while maintaining the requirements for interoperability.

4.5 GINI Recommendations to the main stakeholder groups

4.5.1 Recommendations to Industry

1. Concerted collaboration should be initiated between ICT market players and potential service providers such as Cloud Operators and various identity intermediaries to build consensus and common understanding on what is required for broad industry-wide agreements on issues such as:
    a. Requirements for ensuring user-centricity and user control to identity and attribute provision.
    b. Ways forward to stake out the extent to which an INDI-like ecosystem can be built around existing infrastructure, or what new infrastructure components need to be developed.
    c. Privacy-enhancement principles and rights of individuals including, but not limited to, the requirements of the upcoming privacy-related regulation in the EU, so that the trust framework underpinning an INDI-like ecosystem may take shape.
2. Industry-wide standardisation initiatives should be undertaken, supported by major technology and service providers in order to define various dimensions of inter-Operator interfaces concerning:
    a. Interoperability and data handling processes ensuring privacy for users and confidentiality for relying parties.
    b. Portability specifications, aiming for compliance with upcoming EU regulation.

   c. Protocols, APIs, auditing and security for cross-Operator relaying of claims and assertions.

3. A governance framework for self-regulation of industry should be agreed, addressing the necessary elements of ecosystem-wide operations based on:
   a. A trust meta-model underpinning user-centricity and privacy-enhancing requirements (see point 1 above).
   b. Inter-Operator agreements for relaying of claims and assertions, including possible charges (or lack thereof) and other conditions.
   c. Infrastructure interoperability around standardised inter-Operator interfaces (see point 2 above).

4.5.2 Recommendations to Policymakers

1. Data handling principles and decisions by governments will be pivotal for the emergence of an INDI-like ecosystem:
   a. Governments should allow their citizens to own their identity data, which resides in public registries, and should give those individuals the right and the facilities to control, under conditions that satisfy the public interest, the whole life cycle of identity data including insertion, access, modification, re-use, or erasure. Apart from the obvious public good of respecting what can be considered as a basic human right, such moves by governments will actually facilitate the provision of eGovernment services by the public domain. It will further increase the productivity of the public sector by reducing bureaucracy, minimise regulatory complexity and turn regulatory requirements into an enabler rather than an obstacle to cross-border interoperability, while at the same time reducing identity-related errors.
   b. To fulfil this vision, governments should build INDI-compliant Attribute Services on top of public data registries, so that these become accessible from other relevant actors within an INDI ecosystem. Policies must be put in place, as part of the ecosystem governance, in order to allow only privacy-respecting parties to gain access to those Attribute Services.
   c. Governments should begin to accept INDIs for eGovernment services. There are already such providers but a move by governments to accept INDI-type eIDs for some eGovernment operations will dramatically increase the market scope, foster innovation and supply more choice for citizens and consumers.
   d. Governments should put pressure on business to be transparent in the enrolment and transfer processes of identity data.
2. The best combination between government regulation and industry self-governance should be analysed and a process capable of underpinning the evolution of the best mix should be defined.

3. Governments should foster and support initiatives that foster innovation and experimentation in the development of new business models while taking action to support interoperability among Operators (see Recommendations for Industry above).
4. Governments should ensure that digital evidence also protects the user, in contrast to today's situation where they are forced to rely on the evidence produced and owned by the service provider, thus preventing them from pursuing potential violations of their privacy. Creating user awareness of privacy issues can enable them to make informed choices. This is especially important since users seem willing to disclose personal information to gain an economic advantage.
5. Governments should work out the best way of fostering innovative start-ups motivated by developing and taking new services and business models to market. While already existing EC programmes could be used or adapted to fill this purpose, needs to complement them with new programmes and also national government initiatives as well as schemes promoting cross-regional and global collaboration should be explored.

4.5.3 Recommendations to the Research Community

1. Further R&D work is needed as follows, in regard to:

   a. The scalable use of privacy-enhancing technologies, such as anonymous credentials, to support privacy in multi-corner models with more than one intermediary Operator present in the transaction flow.

   b. Development work in regard to basic protocols. Given its original purpose to support the corporate paradigm of identity and access management, will SAML be sufficient for supporting an INDI ecosystem? What may be the roles of OpenID, OAuth, or other new protocols?

   c. The drivers of user demand and acceptance in regard to technology-linked innovation around identity management. What is required for raising user awareness of identity management and privacy issues?

   d. The development of trust meta-models. This includes the architecture for inter-operator relations as well as non-intermediation ecosystems allowing the participating entities to interact directly without the involvement of intermediaries.
2. Collaborate with stakeholders from other social spheres, including government, industry and civil society, and engage in devising and examining practical pilots that can support innovation around new research-based models to identity management and test their acceptability to different stakeholders.
3. Embrace international collaboration and also interdisciplinary approaches that go beyond technology to include social sciences, so as to pursue collaborative research work that spans geographical boundaries and takes appropriate account of cultural factors in identity management.

5 Abbreviations

Table 1 Abbreviations

DRM	Digital Rights Management
EC	European Commission
eID	Electronic Identity
EU	European Union
GINI	Global Identity Network of Individuals
GPS	Global Positioning System
IaaS	Identity as a Service
ICT	Information and communication technologies
INDI	Individual Digital Identity
IT	Information Technology
PET	Privacy Enhancing Technology
PIM	Personalised Identity Management
PSI	Public Sector Information
TET	Transparency Enhancing Technology

6 List of Figures

7 References

This document – the White Paper on the establishment of an INDI Operator Market – is summarising work carried out by the GINI-SA project and scrutinised stakeholders in a consultation. As such, it is based on predecessor work and comprehensive deliverables on the GINI conceptual framework as well as its legal and regulatory, technical, and privacy dimensions. For the sake of readability, we omitted direct reference in the text. Detailed coverage of various aspects is found in the predecessor documents, including:

- D1.x on the GINI Conceptual Framework
- D2.x on the Technology Dimension of the INDI Domain
- D3.x on the Legal and Regulatory Dimension of the INDI Domain
- D4.x on the Privacy Dimension of the INDI Domain
- D.5.1 providing the GINI Roadmap outlining the steps and timelines for implementing the recommendations of the GINI project
- D6.x reporting on feedback from stakeholder consultation that influenced the findings of the project and the present document

Table 2 Table of References

[D1.1]	The Individualised Digital Identity (INDI) Model: A User-centric Framework of identity management; version 1.2, 06/2011.
[D2.1]	Logical Outline of the INDI Service Framework; version 1.0, 06/2011.
[D2.2]	Technology gaps for longer-term research, amended version 1.1, 07/2012.
[D3.1]	Legal Provisions for Deploying INDI Services, version 1.0, 07/2011.
[D3.2]	A Regulatory Framework for INDI Operators, version 1.2, 04/2012.
[D4.1]	A Privacy Policy Framework for the INDI ecosystem, version 1.0, 06/2011.
[D5.1]	Research and Implementation Roadmap for Establishing a User-centric INDI Ecosystem, revised07/2013.
[D6.3/6.4/6.5]	Interim Reports (6.3/6.4; 2011-2012) and Final Re-port (6.5) on Stakeholder Engagement and Community of Interest. 10/2012.

GINI Consortium

- International Organisation for Knowledge Economy and Enterprise Development (IKED) –**Sweden**
- Fraunhofer Institute for Open Communication Systems, Fraunhofer FOKUS - **Germany**
- The Catholic University of Leuven - Katholieke Universiteit Leuven (KUL) - **Belgium**

  KUL participates in the consortium with two departments

  1. Department of Electrical Engineering, research group (COSIC)
  2. The Interdisciplinary Centre for Law and Information & Communication Technology (ICRI)

- Graz University of Technology - Technische Universitaet Graz (TUG) - **Austria**
- Johann Wolfgang Goethe-Universität Frankfurt (GUF) - **Germany**
- Government to You (Gov2U) - **Greece**
- NorthID Oy (NorthID) - **Finland**

Project website: http://www.gini-sa.eu/

Revised version, July 20, 2013

SEVENTH FRAMEWORK
PROGRAMME