GLOBAL IDENTITY
NETWORKING OF
INDIVIDUALS

The Individualised Digital
Identity Model

Research and Implementation Roadmap for Establishing a User-Centric INDI Ecosystem

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

Title:	Research and Implementation Roadmap for Establishing a User-Centric INDI Ecosystem
Authors:	GINI-SA project team.
Main editors:	Herbert Leitold and Bernd Zwattendorfer (TU Graz); Thomas Andersson and Lefteris Leontaridis (IKED); Pasi Lindholm (NorthID); and Shuzhe Yang (Goethe Universität Frankfurt).
Published:	Malmö, July 2013

SEVENTH FRAMEWORK
PROGRAMME

Table of Contents

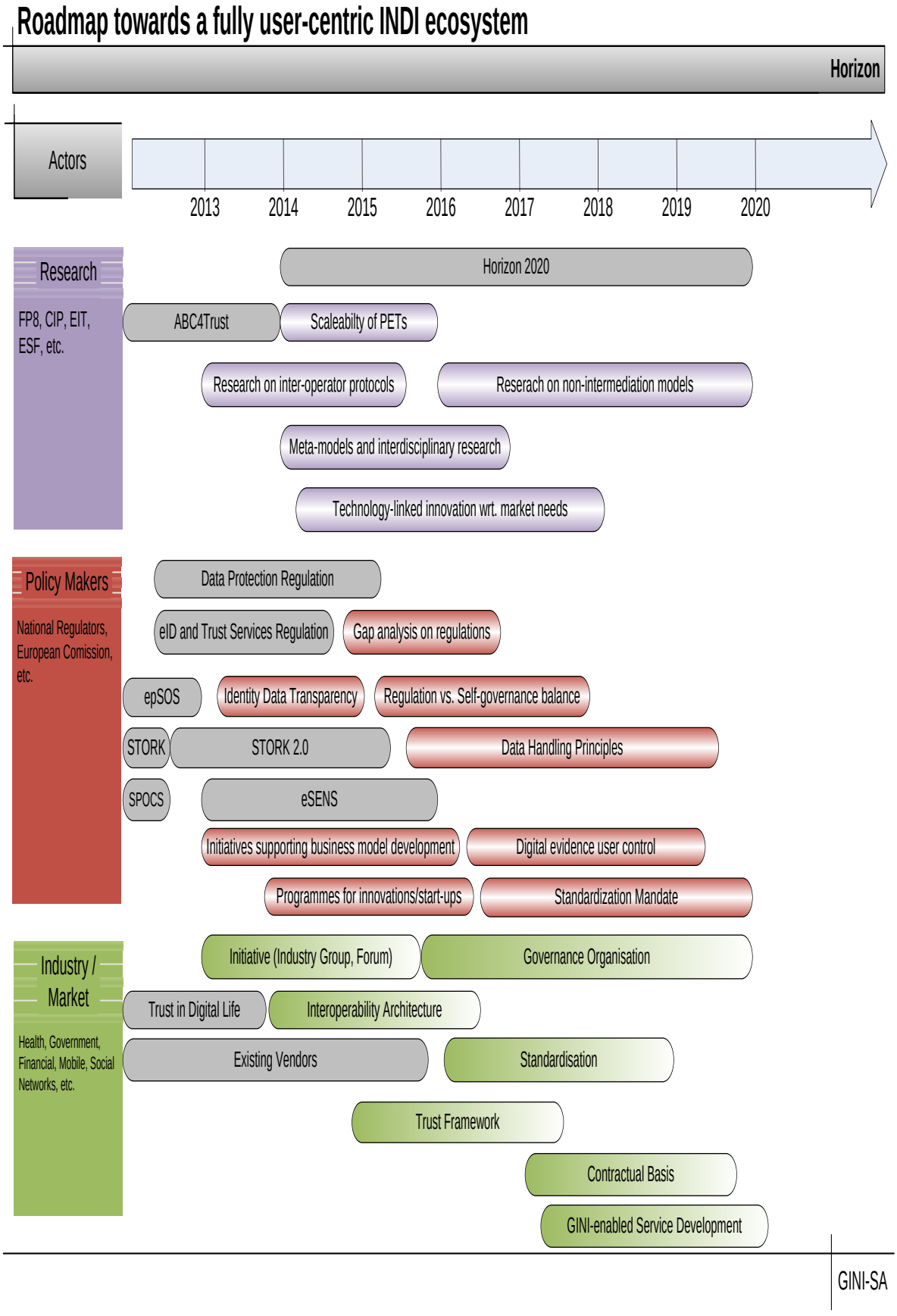
1 Executive Summary[1]

GINI-SA has elaborated on a user-centric identity ecosystem. In working towards such an Individual Digital Identity (INDI) space, research directions have addressed legal, technical, privacy, and business streams. We identified gaps between the existing conditions and the envisaged ecosystem in each of those different – but entangled – streams. The actions identified in this document, the Roadmap, have been identified as required for overcoming those gaps.

Electronic identities and identity management can now only be characterised as a hot spot of great importance for a range of electronic services as well as for the wider directions of our digital future. A plethora of actors is active in the field; representing commercial interests, policy making, the research community, and various user communities. Some are looking for profit or tuned to focus on sectorial issues; others aspire to protect consumer interests or the well-being of citizens.

Rather than just picking up on each gap identified, for the purpose of assigning "further work" for each in accordance with a timeline, and declare the result of that a *roadmap*, we have attempted to engage stakeholders and paid attention to their diverse interests and concerns. Therefore, the Roadmap has taken on board input received at various stakeholder consultation initiatives. We thus de-coupled work on this document from the original GINI-SA research streams on Technology-, Legal and Regulatory-, Privacy-, and Business-Dimensions. Instead we put the focus on the way in which prime stakeholders, such as Regulators, Sectors making use of identity data, Standardisation bodies, Research communities, and Civil society, could be engaged as actors in implementing the Roadmap. Actions to be taken have been aligned with on-going initiatives. The figure below illustrates the main result – an INDI Roadmap with an end-of-decade implementation horizon.

[1]This document has produced by the GINI team collectively. The main editors are: Herbert Leitold and Bernd Zwattendorfer (TU Graz); Thomas Andersson and Lefteris Leontaridis (IKED); Pasi Lindholm (NorthID); and Shuzhe Yang (Goethe Universität Frankfurt).


Roadmap towards a fully user-centric INDI ecosystem
Horizon
Actors
2013
2014
2015
2016
2017
2018
2019
2020
Research
FP8, CIP, EIT, ESF, etc.
Horizon 2020
ABC4Trust
Scaleabilty of PETs
Research on inter-operator protocols
Reserach on non-intermediation models
Meta-models and interdisciplinary research
Technology-linked innovation wrt. market needs
Policy Makers
National Regulators, European Comission, etc.
Data Protection Regulation
eID and Trust Services Regulation
Gap analysis on regulations
epSOS
Identity Data Transparency
Regulation vs. Self-governance balance
STORK
STORK 2.0
Data Handling Principles
SPOCS
eSENS
Initiatives supporting business model development
Digital evidence user control
Programmes for innovations/start-ups
Standardization Mandate
Industry / Market
Health, Government, Financial, Mobile, Social Networks, etc.
Initiative (Industry Group, Forum)
Governance Organisation
Trust in Digital Life
Interoperability Architecture
Existing Vendors
Standardisation
Trust Framework
Contractual Basis
GINI-enabled Service Development
GINI-SA

2 Introduction and Methodology

GINI-SA set out to develop a series of research results on technology, legal and regulatory, privacy, and business aspects of a user-centric identity ecosystem. While results in each of those areas may motivate their specific follow-up, the prime strength of the overall approach resides is the linkages between the different parts and the insight what integrated approach is required to enable realizing our vision. Still a sound methodology is needed to identify the various steps to be taken and to communicate them to stakeholders. This section discusses the chosen methodology while also providing an introduction to the Roadmap and its intended audience.

2.1 Synthetic Approach

Several gaps were identified in various parts of the GINI-SA project, including the "technology gaps for longer-term research" document (D2.2). An interdisciplinary approach is required to achieve synthesis of the drivers and expectations that flow from each of the main stakeholder groups – in Figure 1 depicted as Research, Government, and Industry. The task is to spur future actions and developments associated with key projected outcomes, notably:

1. Putting users in control
2. Easy integration of privacy enhancing technologies (PETs)
3. Advancing regulation for Data Protection
4. The emergence of Privacy-focused Business Models
5. Achieving vendor neutrality

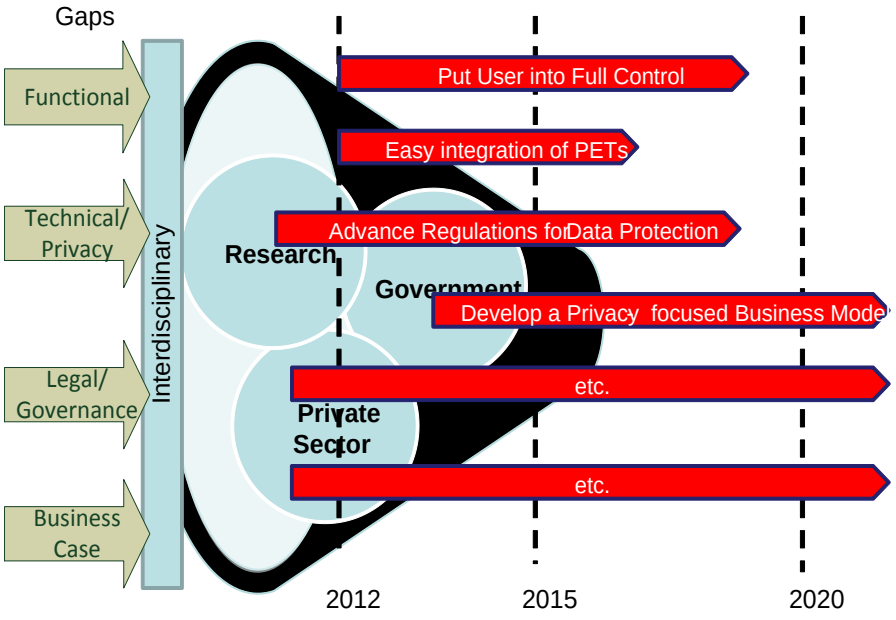


Figure 1 - Synthetic Approach to GINI Roadmapping

Our approach to roadmapping is actor-oriented and with timelines set up for achieving various objectives. As illustrated below, actions are structured along, and associated, with four main stakeholder groups: (1) Regulators and policy makers; (2) The user community making use of identity management are the service providers. Each may have specific Sector constraints (e.g., strict privacy in the health area, a security dominant in financial services, citizen rights in eGovernment, etc.); (3) Standardisation bodies leveraging industrialisation of ideas to interoperable products, and; (4) The research community devoted to building knowledge and creating new ideas. While we underline the importance of these four main stakeholder groups, each of which is strongly affected by issues of identity management and thus should play an active role in responding and contributing to our proposed actions, we organise our envisaged agenda around three actor groups (Research, Policy Makers, and Industry/Market), which should be involved in such a way that the relevant interests take part in fostering and implementing those actions that are required for making the GINI vision become reality.

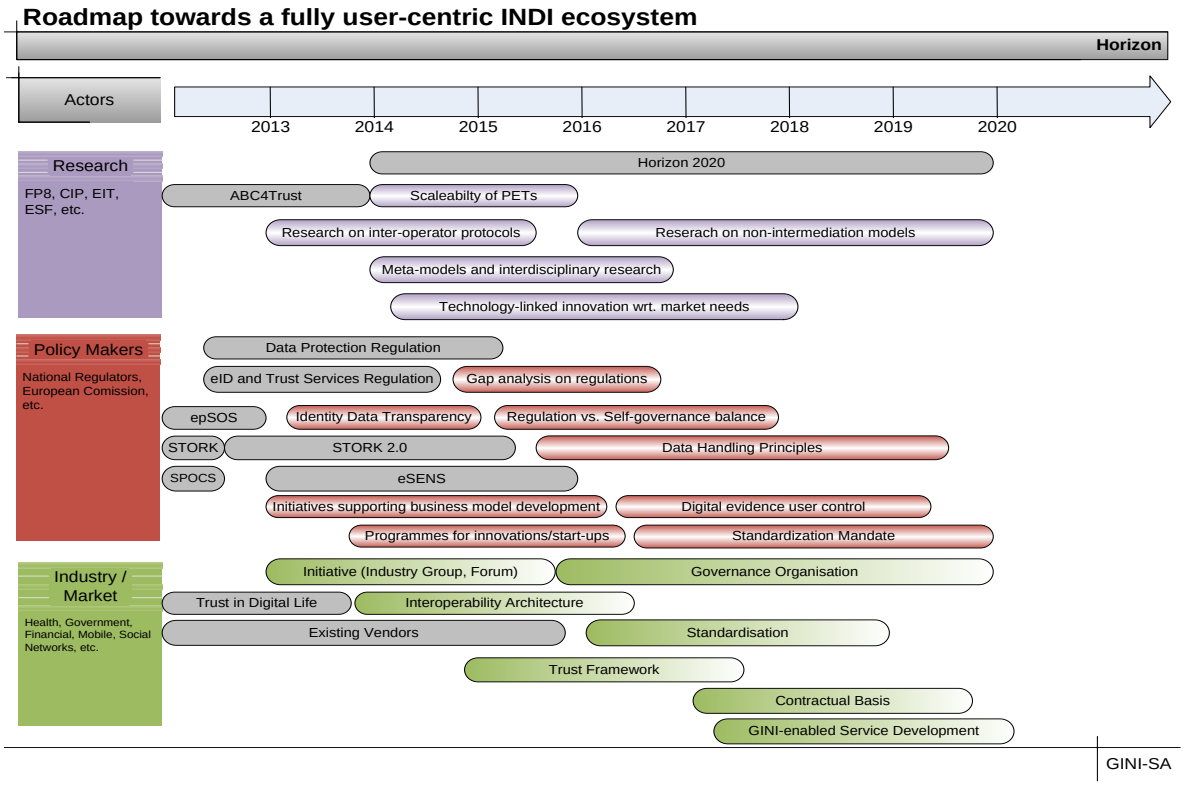


Figure 2 - GINI Roadmap towards a fully user-centric INDI ecosystem

The Roadmap presents on-going initiatives as grey blocks. These are not necessarily associated with immediate actions that stem from GINI-SA recommendations. They are listed as they are considered having major influence on the identity field. Thus, the roadmap aligns with major initiatives, such as the Draft Data Protection Regulation [ECa] and the Draft eID and eSignature Regulation [ECb]. Further relevant blocks are the Large Scale Pilots related to eGovernment, eHealth, or the Services Directive (STORK (2.0), epSOS, SPOCS), or the European Citizen Initiative on eParticipation.

3 Current Situation

The current identity landscape is discussed in this section. Three main pillars need to be emphasised: (1) government-driven initiatives that are mainly associated with the provision of high-quality identity credentials and authoritative sources of attributes; (2) private-sector initiatives that may be characterized as being driven by business needs and improving customer satisfaction; (3) research projects that are drivers of innovative ideas and scientific progress. A selection of relevant initiatives has been incorporated in order to reflect the state-of-the-art. We deliberately did not aim for an exhaustive list– a task that would anyhow most likely fail in a field as dynamic as that of Internet services in general, and electronic identity in particular. Rather this section should be interpreted as highlighting the various relevant flavours displayed by an identity, when observed from different angles.

3.1 Government Driven Initiatives

Identification of citizens represents a frequent process requirement in public administration but is also a core sovereign duty of governments. Thus, many electronic identity initiatives stem from leveraging traditional means of identification to the electronic world. Government issued electronic identification is associated with the data quality of public registers and with meeting the (often) high security requirements of its processes. Still, as electronic identification evolved from the realm of traditional identification it inherited national administration characteristics in its electronic substitutes, resulting in a complex and partly contradictory situation.

While there is no such thing as a common European approach to identification, the draft regulation on electronic identification and trust services [ECb]casts light on anticipated future developments in the EU. We therefore selected initiatives that may be seen as representative of what led to developments such as the Draft Regulation. Thereafter follow the US driven initiatives which may be said to have less of a regulatory focus but on market initiatives. The overview is completed by discussing international initiatives, such as those undertaken by the ITU or the OECD.

3.1.1 EU Driven

3.1.1.1 Public Sector issued IDs

Governments have placed great effort on transferring traditional and paper-based services into online services. Online services offer government customers (citizens, enterprises, or other governments) greater flexibility and easier access to public services. Governments are likely to save resources in part because personnel and process costs can be reduced.

Regardless whether paper-based or online public services are relied on, there is a need of unique identification of persons and authentication. Hence, most countries issue some kind of identification documents to their citizens. Examples for traditional means are national ID cards, passports, or driving licenses. The pendants of these IDs in the digital world are electronic IDs (eIDs). Electronic IDs can be used for eGovernment or eBusiness purposes or to

support any other service where applicable. Therefore, in parallel to traditional IDs, many countries issue eIDs to their citizens.

The currently dominant technology for government issued eIDs is smart cards, which offer strong security features for identification, authentication, or electronic signatures. Many countries, especially in the European Union, have already rolled-out national eIDs based on smart cards. However, other technologies such as mobile phones or USB token scan also be used. Although many countries rely on the same underlying technology, differences exist on organisational aspects or the legal basis. A survey of the various national eID solutions across Europe can be found in the Modinis-IDM study [Modinis] or the IDABC eID country reports [IDABC].

Although many eIDs rolled-out have already been rolled out across Europe, the rate of acceptance gives rise to concerns. Issues are usually related to low take-up by non-governmental service providers, limitations caused by domestic or sectoral requirements, and the specificities of particular user cases. On the other hand, distinct benefits have been achieved emanating from enhanced authentication and quality assurance in user data.

3.1.1.2 Secure Identity Across Borders Linked (STORK)

In 2008, the European Commission launched the large scale pilot project STORK[2] (Secure Identity Across Borders Linked) to bypass differences in national eID solutions on organisational, legal or technical level and achieve eID interoperability across Europe.

STORK was propelled by the vision to facilitate cross-border administrative services within the European Union by providing secure identification and authentication for service providers and citizens. The general idea was not to re-invent the wheel by introducing a new identification and authentication system for all European Union citizens. Instead, STORK took the existing national solutions as they were and built an interoperability framework on top of it. Through the STORK framework, citizens from one Member State have become able to access online services offered by another Member State by simply using their own national eID. For the citizen's experience, there is no difference in authenticating at a national or at a foreign service provider.

Cross-border applicability of eID authentication constitutes the main feature of STORK. Service provisioning across borders is facilitated and allows greater movements across Europe by strengthening the internal market at the same time. Nevertheless, STORK mainly demonstrated eID interoperability at technical level. Some legal or governance questions still remained unsolved and need to be taken up in follow-up projects, such as the succeeding STORK 2.0[3] project.

[2] https://www.eid-stork.eu/

[3] http://www.eid-stork2.eu

3.1.2 US Driven

3.1.2.1 National Strategy for Trusted Identities in Cyberspace (NSTIC)

The National Strategy for Trusted Identities in Cyberspace (NSTIC) [NSTIC]has been published by the White House in 2011. The US Government stated objectives and a strategy to proceed. Main reasons were encountering and hampering identity theft and online fraud. Such identity theft and online fraud has its roots to a large extent in current unsecure authentication mechanisms, such as username/password schemes. Also businesses and governments struggle with and suffer from these unsecure mechanisms in this respect. On the one hand, managing user accounts individually for each service is costly. On the other hand, more sophisticated online services require unique identification which cannot be achieved by most of the current offered methods.

The emphasis of the NSTIC strategy is to strengthen trust in online identities and build an appropriate "Identity Ecosystem". In general, the vision of this strategy is: *"Individuals and organisations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation"* [NSTIC]. The resulting identity solutions should be secure and capable of combating identity theft. Additionally, citizen's privacy should be protected by having personal data treated in a trustworthy manner. Adopted technologies should be easy to use and operate. Finally, the identity ecosystem should reduce paper-based processes.

As an important element of the strategy, the private sector is expected to take the lead in the development and implementation of the proposed identity ecosystem. The government only acts as a supporting entity and should not over-regulate the emerging market for future identity and authentication systems.

In summary, the NSTIC pushes for the rise of an identity ecosystem with the potential of benefitting citizens, government, and businesses. Citizens are set to profit from more secure and easy-to-use authentication mechanisms and an increasing number of online services. Governments and businesses will gain from reduced costs and less probability of online fraud.

3.1.2.2 American BarAssociation (ABA)

The American Bar Association (ABA)[4] is a union of lawyers, judges and law students in the United States. ABA was founded in 1978 and has currently approximately 410.000 members. By this, ABA is the biggest association of professionals on voluntary fellowship in the world. The general aim of ABA is representing the interests of legal professionals and promoting justice. The work carried out is divided into several task forces.

One of these task forces constitutes the "Federated Identity Management Legal Task Force"[5] which was established in 2009. This task force consists of lawyers, identity management technology experts, business persons, and any other persons who are interested in this topic. This task force especially focuses on legal issues in connection with federated identity

[4]http://www.americanbar.org/aba.html

[5]http://apps.americanbar.org/dch/committee.cfm?com=CL320041

management. In particular, legal identity aspects in the field of eCommerce are discussed. Legal issues are identified and evaluated to develop appropriate legal models for encountering these issues. Furthermore, common contracts or terms are developed to be used by various parties in the identity areas.

Working groups have been established for defining identity related terms, legal issues, privacy aspects, ID proofing, legal structures, or model contracts. There, the focus lies on the applicability of legal frameworks and which factors affect the application of law.

3.1.3 International Initiatives

3.1.3.1 Organisation for Economic Co-operation and Development (OECD)

The Organisation for Economic Co-operation and Development (OECD)[6], founded in 1960, constitutes an international organisation with 34 current members. In order to be eligible for membership, countries should be democracies with free market economies. Most of them can be seen as developed countries having a high per capita income.

The OECD Secretariat, based in Paris, works closely with its member countries to share experiences, identify good practices and frame solutions to common problems. At the same time, the OECD increasingly collaborates with non-member countries, and particularly emerging economies. It serves as a platform to help governments improve their understanding what drives economic and social change.

In regard to the information economy, OECD has addressed various issues that relate to identity management. For instance, it has published "policy guidance on online identity theft" and "national strategies and policies for digital identity management in OECD countries". Among other relevant studies, OECD (2011) analyses and compares national strategies for digital identity management across OECD countries. This work examines to what extent policy approaches in this area are conducive to innovation and supportive of the broader Internet[7].

3.1.3.2 Trust Frameworks with Global reach

The Kantara[8] initiative is a joint initiative that emerged out of several projects or communities such as the Liberty Alliance project, the Data Portability Project, the Internet Society (ISOC) or the Information Card Foundation (ICF). The Kantara initiative brings together enterprises, governments, mobile operators, and Web communities for the purpose of addressing issues in the field of identity management, e.g., with regard to interoperability, compliance, privacy, or usability. To foster industry-wide adoption and provision of interoperable identity systems, Kantara provides the so-called Identity Assurance Framework (IAF). The idea behind this framework is to facilitate for relying parties to understand and trust the identity credentials they receive from other parties. All parties are thereby meant to follow common and agreed levels of assurance. Since Kantara is not the only organisation addressing trust frameworks, it

[6] http://www.oecd.org

[7] http://www.oecd-ilibrary.org/science-and-technology/national-strategies-and-policies-for-digital-identity-management-in-oecd-countries_5kgdzvn5rfs2-en

[8] http://kantarainitiative.org/

also tries to establish a so-called Trust Framework Meta Model (TFMM). This meta model is intended to serve as a point of reference for any community conceptualizing a trust framework. Additionally, it aims to provide mechanisms for comparing different trust frameworks and make them interoperable.

3.2 Private Sector developments

Industry developed countless products, methodologies or standards reliant on or related to identity management. To illustrate the various flavours of the private sector achievements, we present a few examples that are interesting from a market penetration perspective (e.g., Facebook), or through its attempt to support interoperability and federation (OAuth, OpenID).

3.2.1 Facebook Platform

The so-called Facebook Platform (formerly Facebook Connect) [FB]exemplifies the classical identity triangle, where a user, an identity provider, and one or more service providers are involved. Authentication is usually required for accessing a certain protected service at a service provider. Instead of authenticating the user directly with the service provider, identification and authentication are delegated to the identity provider. Hence, in this scenario the user first has to be authenticated with the identity provider. The identity provider subsequently assembles a security token which contains all relevant identity and authentication information of the user. This security token is finally transmitted to the service provider which, based on the information contained therein, will either grant or deny access to its resources.

With this kind of set-up, no explicit prior registration is required at the service provider. The identity provider – in this special case Facebook – stores all the identity data and only transfers those data to the service provider in case an authentication process is needed. The identity provider can also serve multiple service providers which enables the possibility for single sign-on (SSO). Single sign-on defines the ability to gain access to multiple service providers performing just one authentication process. No further re-authentication is needed as long as the security context of the first authentication process remains valid.

The advantage of using an identity model such as that of the Facebook Platform is simplicity. Identity data needs to be stored only at the identity provider and the user needs to remember only the credentials for that identity provider authentication, in this case the Facebook username and password. Privacy concerns nevertheless arise as users' identity data are centrally stored at the identity provider. In addition, through every authentication process, the identity provider gains knowledge of service providers accessed by users. This facilitates user tracking and profiling on e.g. preferred services.

3.2.2 OAuth

OAuth[9] defines a standardized and open protocol for applying authorisation processes in web, desktop, or mobile applications. OAuth provides an API (application programming interface) allowing applications to access certain user data of another application.

In general, by the help of this protocol a user easily can allow a foreign application access to her data, which are actually managed by another application, by properly authorizing such a request. The advantage of OAuth is that such an authorisation request can be fulfilled successfully without revealing the user's credentials to the foreign application. The foreign application is awarded access only to the authorized data and not to, e.g., the user's passwords. Hence, sharing of secure user credentials with third parties is avoided. Authorisation is performed using tokens. Each token can grant access to a specific application for a certain defined time period. Before tokens are sent and user data are transferred to the foreign application, the user needs to state her willingness by giving her consent to this transmission.

A typical example for an application of OAuth would be user authorisation of an online printing service to access an online photo sharing service, where the user has stored her images. Moreover, it is assumed that the user wants to send some pictures from the photo sharing site to the online printing service for printing. In this example, the user authorizes the printing service to retrieve only photos from the photo sharing site without revealing any other credentials. If the authorisation process was granted by the user (through giving her consent), the printing service can continue its business processes.

The main advantage of OAuth defines the possibility of performing authorisation between applications without revealing user credentials such as usernames or passwords. This also leads to a decreasing number of user accounts since registration at each individual service provider is not required anymore. A decreasing number of user accounts means also less passwords to remember which in turn increases security. Disadvantages may again be found in the area of privacy. Although privacy is increased because not all data is shared between applications, OAuth providers can still track user preferences by saving users´ visited applications.

3.2.3 OpenID

OpenID[10]constitutes a decentralized authentication system for Web-based services. It also follows the classic triangular identity architecture, where a user, an identity provider, and one or more service providers are involved. In the context of OpenID, identity providers are called OpenID providers and service providers are named relying parties.

A prime feature of OpenID is single sign-on (SSO). In a distributed network, which is secured by OpenID providers, users just need to authenticate once at an OpenID provider and are further able to access multiple relying parties without re-authentication. Users typically authenticate by username/password authentication mechanisms and receive a URL-based OpenID identifier. This identifier can be used for seamless authentication at other relying parties without needing an additional authentication process again. Nevertheless, OpenID

[9] http://oauth.net

[10] http://openid.net

authentication mechanisms are not tailored to simple username/password mechanisms. Other and more sophisticated approaches e.g. based on smart-cards or biometry could be used.

The OpenID architecture is decentralized; hence everyone can become an OpenID provider and in principle install and deploy one´s own OpenID server. OpenID providers are responsible for registering OpenID identifiers and for communicating with relying parties. Currently, a lot of implementations of OpenID providers in various programming languages exist since OpenID is an open protocol.

The ability of SSO defines one of the main advantages of OpenID. Additionally, decentralisation has the advantage that OpenID providers can be switched easily. Disadvantages may also relate to privacy as public OpenID providers can track user's preferences and habits. However, due to its decentralisation everyone can install its own provider to lower this issue.

3.2.4 Private Sector issued IDs

Enterprises of the banking and telecom sector are the main drivers for private sector issued IDs. Although electronic identification and authentication does not define the core business of these sectors, in some countries they play a major role as identity providers. While banks are compelled to offer services online, high dependency on trust coupled with the high costs of identity theft or other kinds of fraud, this sector requires stronger identification and authentication than other services. Especially Scandinavian banks have a distinct foothold in this field. In some instances, their identification and authentication mechanisms are now offered to other service providers as a third party service. Bank-issued IDs tend to offer advantages of high reliability in part since they are usually backed by some under-lying non-electronic registration process. Other advantages emanate from the high degree to which bank customers can apply such IDs for other services at other providers. On the other hand, only the bank's own customers can usually obtain such IDs.

Besides banks, telecom operators have found electronic identities and authentication to represent a valuable and strategically important business. Similar to banks, telecom operators offer these services as third-party services. Since the number of online services from telecom operators increases steadily, stronger authentication mechanisms are required for more sophisticated and secure services. The rapid rise of mobile services likewise calls for enhanced identification and authentication services, motivating telecom operators to enter this market with an expectation of gaining access to new sources of revenue. Similar to banks, telecom operators have strong brands and are thus likely to enjoy high levels of trust from customers. Advantages of telecom-provided IDs include increased flexibility and tightness in connection with mobile services. Disadvantages may however follow from the limitation to customers of the specific telecom provider for use of such IDs and that every authentication request is routed through the user's operator. Such behavior can easily lead to user tracking which violates users' privacy.

3.3 Research Projects

Research serves as a major driver of innovation. The European research programmes are leading in the field of identity-related solutions, as well as in privacy enhancing technologies (PETs). In this section, we provide examples of such first-class research in these domains.

3.3.1 Trusted Architecture for Securely Shared Services (TAS^3)

Many system developments focus on a narrow niche sector and tend to be specific to their application context and environment. Systems designed and developed in this way do not naturally support cross-context services and interoperability. The resulting problems of isolation and complexity were addressed by TAS^3 (Trusted Architecture for Securely Shared Services)[11], a European Union research project which 17 partners which lasted between 2008 and 2011.

TAS^{3}aimed at the creation of a trusted network of Internet services and secure exchanges of personal data. It proposed an architecture aimed at handling the following challenges in a generic and scalable way:

- User and Service Provider Authentication and Credential management;
- Establishing Trust between Users, Information Repositories and Service Providers;
- Data Protection Policies;
- Transparency of Business Processes;
- Demonstrator Challenges.

Another important challenge covered by the TAS^3 project was the semantic coherence of data protection regulation. Interpretation of data protection regulation varies depending on the context. TAS^3 tried to optimize the use of procedures, policies, control, and contractual obligations with data elements and roles through automated solutions. Applications of TAS^3 have focused on e-Health and e-Employability. The results have been piloted in the United Kingdom, the Netherlands, and Belgium.

Besides the TAS^3 architecture, the project consortium designed a governance framework aimed to build the fundamental basis for secure exchange of personal data. Figure 3 illustrates this trust assurance framework which consists of three layers involving several actors. All layers require the compliance of a certain set of rules and policies in order to achieve a successful implementation of the TAS^3 architecture. In the top layer (Governance layer), policies or rules for the TAS^3 network are established. Those policies and rules are enforced by several actors of the Admin layer. Finally, the actors of the Operations layer realize TAS^3 transactions in compliance with the policies and rules established.

[11] http://www.tas3.eu

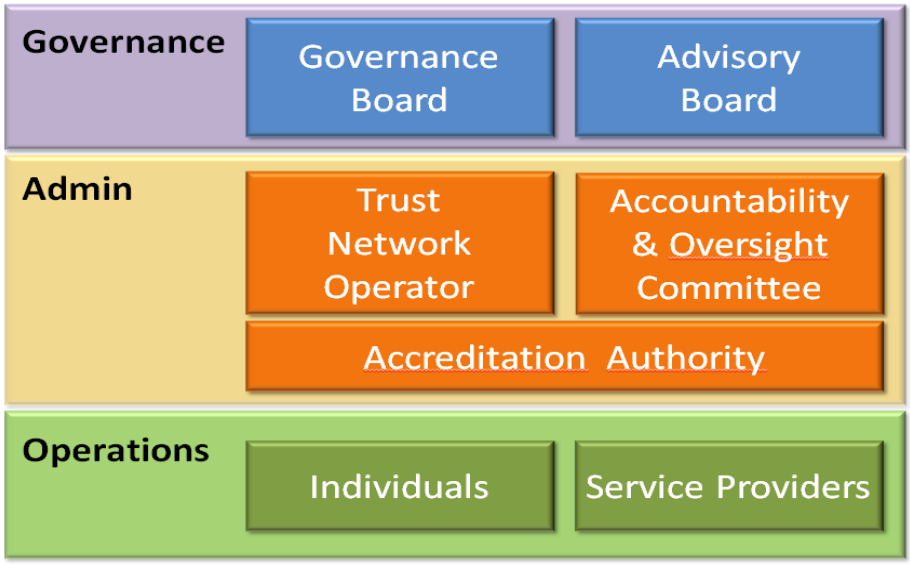


Figure 3 - Layers and Actors of the TAS^3 Ecosystem

3.3.2 PrimeLife

Individuals leave a life-long trail of personal data during their daily interaction on the Internet. Technological advances facilitate extensive data collection, unlimited storage and reuse of the individual's digital interactions. Today, individuals cannot retain control over personal information, as present information technologies hardly consider essential privacy requirements. This raises substantial new privacy challenges: how to protect privacy in emerging Internet applications such as collaborative scenarios and virtual communities; and how to maintain life-long privacy.

PrimeLife[12] was an international research project, which brought sustainable privacy and identity management to future networks and services [CaFiRa11]. The PrimeLife consortium consisted of 15 partners from nine different countries and was funded by the European Community's 7th Framework Programme. PrimeLife was built upon and extended the FP6 Project PRIME, which dealt with enabling citizens to exercise their legal rights to control personal information in online transactions. PrimeLife aimed to support informational self-determination through user-controlled identity management. The main objectives included:

- Research and develop new concepts, approaches and technologies to protect privacy for Web 2.0 applications, such as social networks and blogs, and to achieve lifelong privacy protection and management;
- Make existing privacy enhancing technologies useable and improve the state of the art;
- Foster the adoption of privacy enhancing technologies by providing open source components and educational materials, doing that in cooperation with standardisation bodies during dedicated workshops.

PrimeLife developed a number of underlying technologies to meet these objectives. The project results further advanced state-of-the-art in the sphere of interface usability,

[12] http://primelife.ercim.eu/

configurable policy languages, federation of web services, privacy-enhanced identity management enablers, and privacy-enhancing cryptography. To make the result accessible to a broader public, PrimeLife worked together with relevant open source communities, standardisation bodies and other related projects.

3.3.3 Privacy and Identity Management for Community Services (PICOS)

According to the PICOS website, PICOS[13] is an international research project whose mission is to investigate mobile communities and their services. The PICOS consortium consists of eleven partners from seven different countries, supported by the European Community as a part of the Trust & Security thematic area within the ICT programme of the 7th Research Framework Programme. The objective is to advance the state of the art in technologies that provide privacy-enhanced identity and trust management features within complex community-supporting services that are built on Next Generation Networks and delivered by multiple communication service providers.

Currently, professional and private online collaboration via the Internet is rapidly becoming more important. Nowadays, many European citizens spend work and leisure time as part of online communities, and are also increasingly consumed in mobile environments. Although the benefits of mobile communications are well known, the risk of unconsciously leaving personal information traces is rising. PICOS addresses this issue by investigating:

- How trust and privacy are handled by providers of community services;
- Users' expectation about privacy and how they can be met; and
- Needs to be open for marketing activities of sponsors, advertisers and other actors.

To address these aspects, a community architecture including privacy-enhancing concepts were developed by PICOS and prototypically implemented in a community platform and exemplary community applications. The architecture was tested in a community of recreational anglers and online gamers.

One of the central concepts in PICOS is identity management, which enables users to manage their identity-related information in a convenient way. Users can build different partial identities for the usage in different contexts. Especially if users participate in sub-communities, partial identities support users in hiding and revealing personal information based on a particular usage context.

To increase the privacy protection of the users, PICOS provides multiple integrated tools. When founding a sub-community, users can decide if they want to make the sub-community public or private. The users have also a personal area for managing their private information and content. This area enhances users' privacy by enabling them to store and selectively publish their private information to a certain group of other users. The visibility of profile information can be controlled by selectively defined policies, which reveal the information to a certain group. These policies are built on rules, which consider as well context information. In a mobile environment especially location information is of interest (e.g. friends finder). The PICOS concept of Blurring gives users the opportunity to hide their exact position, without

[13] http://www.picos-project.eu/

being completely invisible, as the own position can be obfuscated in a previously defined radius. To increase the usability for the user, a Privacy Advisor has been introduced, which provides guidance to users (e.g., regarding disclosure or sharing of location information) to assist them in protecting their privacy. The Privacy Advisor helps build awareness of privacy related aspects within mobile communities based on users' current behaviour and context.

3.3.4 Attribute-based Credentials for Trust (ABC4Trust)

Anonymous credential systems continue to evolve rapidly. They have resulted in various cases of concrete implementation, such as IBM's Identity Mixer [IDE] and Microsoft's U-Prove [UPR], as well as extensive contributions to past EU projects (e.g. PrimeLife, cf. Section 2.3.2).But until now, the effort of understanding anonymous credential technologies has been rather theoretical and limited to individual research prototypes. The research projects have been demonstrated in a very limited number of actual production environments with real users. Furthermore, commonly agreed sets of functions, features, formats, protocols, and metrics to gauge and compare these technologies, are lacking. It is hard to judge the advantages and disadvantages of the different technologies so as to build an understanding which ones are best suited to match various scenarios.

Recently, the EU project ABC4Trust[14]was initiated to address these problems. It produces an architectural framework for Privacy-ABC[15] technologies that allows different realisations of these technologies to coexist, be interchanged, and federated. This enables users to obtain credentials following different Privacy-ABC technologies and use them indifferently on the same hardware and software platforms, as well as service providers to adopt whatever Privacy-ABC technology suits their needs the best. In particular, the ABC4Trust architecture [Kro11] has been designed to decompose future (reference) implementations of Privacy-ABC technologies into sets of modules and specify the abstract functionality of these components in such a way that they are independent from algorithms or cryptographic components used underneath. The functional decomposition foresees possible architectural extensions that may be desirable and feasible using future Privacy-ABC technologies.

Another line of research looks at interoperability issues between conventional identity management infrastructures and anonymous credentials. The identity management paradigm that is currently hyped by the industry uses only conventional cryptographic techniques as clear basic principles, as they already exist in large products and standards portfolios. Still, the interoperability issues between different vendors and different domains define it as a moving target. The ABC4Trust architecture takes a big step ahead in helping the integration of anonymous credentials, due to the unified format and specification of the corresponding artefacts. Deliverable D2.1 [Kro11] provides an analysis showing that the applicability of the ABC4Trust architecture to the popular existing identity protocols and frameworks such as WS-*, SAML, OpenID, OAuth and X.509 is not only possible but can also help alleviate some of the security, privacy, and scalability issues of the latter.

[14] www.abc4trust.eu

[15] Privacy-ABCs (or Privacy Attribute Based Credentials) is a more accurate term for anonymous credentials suggested by ABC4Trust.

4 Addressing the Gaps

This roadmap receives its input from two main sources: Firstly, research carried out by GINI-SA identified gaps. These are summarized in the sibling document "White Paper on the establishment of an INDI Operator Market across the EU" (D5.1). Secondly, extensive external input was received during the stakeholder consultation process. The latter included both stakeholder views that were similar to the GINI-SA results but complementary, as well as some important critique that helped address some of the gaps identified in the project itself.

In this section, we address the identified gaps. Actions concluded to be required in order to fill these gaps as well as for realising the vision of digital identities are described. These actions are divided into short-, mid-, and long-term. Furthermore, we present the actors deemed relevant for taking up the proposed actions.

Initially, however, we review the main features of the INDI vision, after which we discuss what actions are needed in order to make this vision reality. After considering what actors are relevant for carrying out these actions, we address the issue of what business models may be viable. Paving the way for such business models is fundamental for enabling a sustainable INDI ecosystem.

4.1 Vision

To illustrate the GINI-SA vision, in the following we use material from the main project reports – notably our Whitepaper "White Paper on the establishment of an INDI Operator Market across the EU" (D5.1):

> *We refer to an Individual Digital Identity (INDI) as 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 in order to perform transactions for personal, business or official purposes.*
>
> *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 trust relationships established;*
> - *Verifiable against varied and variable data sources chosen by the individual and trusted by the relying party.*
>
> *Within the INDI ecosystem three types of actors would interact with one another:*
>
> - *An individual would need to access and manage the INDI and its use in various types of context through a User Agent interface where choices can be made about which data source to use and what identity attributes to disclose in each setting;*

- *A Relying Party would need its own interface whereby to 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. would need to implement interfaces for attribute and assertion services in order to be used for verification and/or attribute exchange between individual users and relying parties.*

GINI envisions these interfaces to be provided to the main actors through an infrastructure of interconnected INDI Operators. These are entities that provide INDI services and deploy INDI interfaces to the relevant actors, as seen in the figure below:

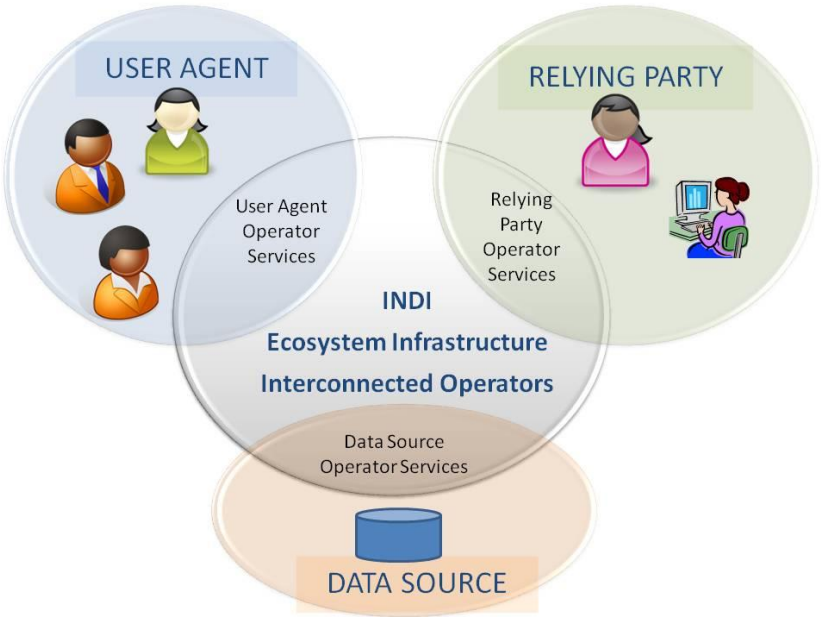


Figure 4 - INDI Ecosystem Infrastructure

In a nutshell, the vision has been summarized in the White Paper (D5.1), as:

> *GINI vision: Individuals' identities are self-created and self-managed throughout the whole lifecycle. Partial or full identities can be presented to any relying party (entities or other individuals) if appropriate trust relationships exist. 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.*

Legal aspects are critical since digital interaction keeps growing within as well as beyond national borders, raising issues of international technical/legal interoperability, and transparency. Neither national nor international frameworks of the current time are up to the task of tackling the outstanding vulnerabilities.

Governments have fundamentally different views on the role of governments versus markets in this sphere. Meanwhile, while the Internet is not bound by national borders, cybercrime along with various unethical behaviours may originate in any country and spread from there to others.

4.2 Actors and Actions

This sub-section outlines required future actions in the light of the gaps identified in the White Paper (D5.1).We structure the section along the main stakeholder groups poised to carry out these actions.

4.2.1 Policy Makers

The regulatory gaps identified by GINI-SA inter alia relate to compliance issues that arise due to the discrepancy between the speed of technical progress and the pace with which that is fed into legal action. Opportunities thus arise for the development of new services that are at odds with the existing legal environment. Mutual recognition of eID and liability frameworks is presently lacking, in particular related to government-issued credentials, or data protection and privacy aspects.

On the European level, recent developments such as the proposed Data Protection Regulation [ECa] and the proposed eID, eSignature and trust services Regulation [ECb] may address several such gaps. Implementation details, addressed through Delegated Acts and standards, will occupy policy makers beyond the enacting of both. The actors on the European level are Member States and EU institutions.

With the increasing importance of identity-related services at global level, action beyond the European Union is desirable but a prerequisite for the development of orderly identity management frameworks. The wider context for European trust services is partly discussed in the Draft Regulation [ECb] and the US NSTIC [NSTIC]. Actors that might facilitate coordinated global solutions include the ITU, the OECD and UNCITRAL[16].

Main Gaps to be addressed:

- Which arguments support regulatory intervention and what are the drawbacks? Are all/some of these arguments covered by the draft Regulation revising the Directive 95/36/EC?
- Is the data protection directive of the European Union (Directive 95/46/EC) still adequate in today's (and tomorrow's) information society?
- What enforcement regimes should be put in place for mutual eID recognition? How will liability be allocated in the case of a breach?
- Which policy initiatives may be adopted to stimulate further mutual recognition?
- How can new technologies be merged into the legal domain at higher speed?

[16] http://www.uncitral.org/

4.2.2 Major Sectors

Secure and reliable identification of both natural and legal persons is universally important in human activities and exchanges. This is naturally the case already in the non-digital world where identification is required in various processes. For instance, opening a bank account usually requires an official ID. Even ordering an alcoholic drink in a bar sometimes prompts the barkeeper to ask for an ID, e.g., to obtain evidence for the customer's age. Hence, identification is an important process, usually carried out prior to receiving some services. Since many offline services are mapped to the digital world, secure and reliable identification is also necessary in online processes. This requirement is not limited to any specific area but is relevant across a range of sectors.

Health service delivery to citizens exemplifies another area where digitalisation, in this case the offering of e-Health services, has led to significant improvements. Electronic access to patient data saves time and costs and allows for, e.g., issuance of medical prescriptions online. This is a strong added value for patients but also for doctors or pharmacists. Nevertheless, such online services require secure and unique identification methods to guarantee the same level of security as in the physical world.

A further sector includes government applications that have been massively moved to the Internet. By this, especially in government-to-government (G2G) transactions enormous cost savings are possible. Furthermore, citizens and businesses benefit from eGovernment services by having a faster and easier communication channel to public authorities. Again, unique and secure identification and authentication are essential for such online services to target the very person who is actually involved in online process with the government.

Besides health and the government sector, financial services such as online banking require secure identification systems. Since services where money is involved are preferred targets for attackers, identification and authentication systems must be heavily safeguarded to diminish the risk of identity theft or identity fraud.

Another sector, where identification is less critical is that of social networks. Currently, most social network implementation relies on self-registration and weak authentication mechanisms such as username/passwords. The providers or people using social networks are obliged to trust that the persons they communicate with are those they claim to be. In fact, each user of such social networks can typically create a self-issued identity without any requirement of verification.

More sophisticated and trustworthy identity management systems can help bypassing this issue. Most of these proposed sectoral services affect traditional Internet and web-based services. However, due to the continuous increase in mobility, digital identities gain importance in the mobile phone sector. Hence, users desire the use of more sophisticated services on their mobile phone or smartphone. Whereas web-based services usually can be more or less easily transformed into mobile applications on smartphones, less sophisticated and older mobile phones reach their limits. Therefore, to offer services on these kinds of phones, identity management must be taken into account in other networks, e.g. the GSM network widely used in Europe.

Main Gaps to be addressed:

- 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?
- How can users exercise control over their digital identities across a range of identity management systems?
- How can future identity management systems help increase productivity or decrease administration efforts and costs?
- How can compliance with legal regulations or policies best be achieved?
- How can the right to demand deletion or correction of identity data be fulfilled effectively?

4.2.3 Standardisation Bodies

Standardisation bodies play an important role in, e.g., achieving interoperability or compatibility of technologies or technical components. They possess extensive detailed knowledge of their areas of specialisation, are often highly influential and have well developed links with relevant research institutions as well as industry partners. The development and the implementation of standards furthermore support the independence of a specific product for customers. To close the gaps identified by the GINI consortium, standardisation bodies must become engaged. The development process for standards is invariably slower than the pace of technology evolution; hence the earlier standardisation bodies respond, the less time is lost before support of implementation and innovations can be put in place. Especially in the mid- and long-term, organisations responsible for standardisation could be strong partners in realising the GINI vision. Standards not only influence the long term strategy of industry but elements of current regimes tend to serve as the basis for later versions of the respective standards. Therefore, the relevant standardisation bodies should become acquainted with the GINI vision and be engaged in work to incorporate its elements into their standards. This will lead to a faster diffusion process and support acceptance by industry. The following sub-sections present a selected set of organisations engaged in standardisation, and especially with the development and the promulgation of technical standards in the field of identity management.

Amongst the various interest groups and standardisation bodies, in the following we list those reckoned most relevant in relation to GINI. These are already engaged in identity-related standards work, and also in several cases influential in regard to cross-sectoral and global impacts.

4.2.3.1 ISOC

One important example ensuring transparency and openness of the Internet constitutes the Internet Society (ISOC)[17]. Founded on the INET Conference in 1992 in Kobe, Japan, the Internet Society is a global Non-Profit and Non-Governmental Organisation (NGO), joining forces

[17] http://www.internetsociety.org/

ofmore than 130 organisations and over 55.000 members. ISOC's mission is "to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world" [IS12]. It engages in standardisation activities in the spectrum of the Internet and consults governments in making decisions to guarantee the future independence of the Internet. Basically, the main tasks of ISOC are the facilitation of Internet standards and infrastructure development, promoting open access, and organising events for collaboration. Nowadays, ISOC represents the organisational home for the standardisation bodies Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), Internet Engineering Steering Group (IESG), and the Internet Research Task Force (IRTF).

The overlap of GINI and ISOC lies in the broad field of identity management (IdM) and its privacy aspects. Its research on identity covers privacy policies, data transparency, and various aspects of online identity. One result of ISOC's research and implementation work is the "Identity Management Policy Audit System", launched in 2010, which was jointly developed with the department of Computer Science at the University of Colorado at Boulder (CU) [IPAS]. In the area of privacy, it is also a voice for the community. It brings the ideas, wishes, and concerns of the community into relevant discussions on revisions, modifications or new privacy frameworks.

To enable and disseminate the GINI vision, ISOC is one of the most important stakeholders. This is in part because of a shared view and understanding of IdM and privacy. ISOC has the possibility to transfer the elements of the GINI vision to the communities. Additionally, it has the power to bring the GINI vision into the aforementioned discussions on revisions, modifications or new privacy frameworks as well as on standards.

4.2.3.2 ISO IEC/JTC1

The International Organisation for Standardization (ISO)[18]is divided into several committees. ISO has a joint technical committee (JTC) with the International Electrotechnical Commission (IEC)[19], which is better known as ISO/IEC JTC. This joint program is necessary since electrical, electrotechnical and telecommunication standards are not in the portfolio of ISO. IEC is responsible for all international standards related to the electric and electrotechnical fields. The International Telecommunication Union (ITU)[20] has the competence for telecommunication standards. These three top-tier international standardisation organisations form an alliance called World Standards Cooperation (WSC)[21], whereas their mission is to "strengthen and advance the voluntary consensus-based international standards systems of IEC, ISO and ITU" [AWSC]. The role of ISO is often not carved in stone. It does not only standardize specifications or formats, but also acts as an integrator of the work of different standardisation bodies around the world. It can be seen as the "root" of standardisation bodies. This is grounded in its history, and might also be related to its structure as being strongly tied to only one recognized standardisation body on a national level.

[18] http://www.iso.org/iso/

[19] http://www.iec.ch/

[20] http://www.itu.int/en/Pages/default.aspx

[21] http://worldstandardscooperation.org/

Especially the Joint Technical Committee 1 (ISO/IEC JTC 1) can be relevant for the take-up of GINI actions. ISO/IEC JTC 1, formed in 1987, is the first JTC between ISO and IEC, which deals with the development of worldwide information and communication technology (ICT) standards for business and consumer applications [JTC1]. It has many sub-committees (SC), which again can have several working groups (WG). The SC27, which deals with IT security techniques, has a WG 5 with research focus on IdM and privacy technologies [SC27]. Its actual frameworks, architectures and concepts for IdM and privacy include:

- A Framework for Identity Management (ISO/IEC 24760);
- Privacy Framework (ISO/IEC 29100);
- Privacy Reference Architecture (ISO/IEC 29101);
- Entity Authentication Assurance Framework (ISO/IEC 29115 / ITU-T X.eaa);
- A Framework for Access Management (ISO/IEC 29146);
- Requirements on relative anonymity with identity escrow – model for authentication and authorisation using group signatures (ISO/IEC 29191).

Those frameworks are accepted, acknowledged and often referenced, which also has a link to the GINI concept and INDI model. Currently, most of the aforementioned frameworks, architectures and concepts do not cover the GINI vision or the INDI model. But the GINI vision and the INDI model can be a valuable extension, since they could possibly offer more flexibility, privacy and new business opportunity. It could be important for GINI to have ISO and its SC as a stakeholder since they enjoy a world-wide high level of recognition especially with national governments and international institutions such as the World Trade Organisation.

4.2.3.3 ITU-T

On the same level, the Telecommunication Standardization Sector (ITU-T) of the International Telecommunication Union (ITU) also works on standardisation in the field of identity management, especially in relation to telecommunication. ITU-T is a member of WSC and therefore it is one of the most important international standardisation bodies worldwide. Founded in 1865 in Paris as the Internal Telegraph Union [ITU-T], it is also one of the most traditional standardisation bodies. According to its own information, it has currently a membership of 193 countries and some 700 private-sector entities. Other sectors of ITU, such as ITU-Radiocommunication (ITU-R) or ITU-Development (ITU-D), deal with issues like managing radio-frequency spectrums or establishing information and communication technologies.

One of the most prominent and also oldest standards of ITU-T is the X.500 series for directory services, which can be seen as the originator of all directory services. This standard is still the basic for many wide spread technologies such as LDAP, OpenDAP, or Microsoft Active Directory. What X.500 is for directory services, is X.509 for public key infrastructures (PKI). Furthermore, ITU-U does not only work on standards for IdM, but also recommendations like X.1252 [X.1252], which defines the term IdM itself and other related key terms used in IdM. Other famous key standards developed and published by ITU-T are for example: Q.931 for Integrated Services Digital Network (ISDN) and the Digital Subscriber Line (DSL) series for broadband telecoms.

As we can see from the history of ITU-T, it has much experience in developing standards, makes them widely accepted and achieves long-term deployment in the industry (cf. DSL and ISDN). The so-called Focus Group on Identity Management (FG IdM) works on the facilitation and the development of a generic IdM framework. In more detail, the objectives of this group are maintaining a list of standardisation bodies dealing with IdM, analyzing general IdM requirements, and deriving appropriate IdM telecommunications/ICT use cases. Hence, it could be important for GINI to have ITU-T as a partner because they can incorporate the GINI vision in its standards and establish them appropriately. Since GINI has a long-term vision, ITU-T would be an optimal stakeholder for future development.

4.2.3.4 OASIS

The Organization for the Advancement of Structured Information Standards (OASIS)[22] is a non-profit consortium with focus on development and adoption of open standards, especially on eBusiness and web services standards. It was founded in 1993 under the name "SGML open", and the consortium changed its name 1998 to "OASIS" to show their expansion of technical work [OASIS]. According to its own admission, it has "more than 5,000 participants representing over 600 organisations and individual members in 100 countries" [OASIS]and its mission is to "promote industry consensus and produce worldwide standards for security, Cloud computing, SOA, Web services, the Smart Grid, electronic publishing, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology"[OASIS].

OASIS' portfolio contains several important and widely-adopted IdM related frameworks, specifications, and protocols such as:

Security Assertion Markup Language (SAML);

WS-Trust, or;

eXtensible Access Control Markup Language (XACML).

Most of the OASIS standards are widely used in many products and other IdM frameworks, e.g. Liberty Alliance's Identity Web Services Framework [LIWSF]. For the GINI vision, OASIS could be a strong partner. It has many industry partners, which already have adopted and implemented its standards. Having OASIS on board could significantly accelerate the diffusion process, especially in the industry.

4.2.3.5 Kantara

The Kantara[23] Initiative is an independent non-profit organisation which discusses and works on various issues in the identity management landscape. The Kantara Initiative, founded as a program of IEEE-ISTO [ISTO] in June 2009, is the successor of the Liberty Alliance Project[24], and all work as well as related materials of Liberty Alliance have been contributed to the Kantara Initiative. It has members across several areas such as governments, telecommunication

[22] http://www.oasis-open.org/org.

[23] http://kantarainitiative.org/

[24] http://www.projectliberty.org/

providers, financial service providers, research and education sector. According to its testimonial its vision is to "ensure secure, identity-based, online interactions while preventing misuse of personal information so that networks will become privacy protecting and more natively trustworthy environments"[Kantara]. The Kantara Initiative is not a standardisation body, but it helps to improve standards by submitting recommendations to standardisation bodies such as ISO or ITU-T. The main goal is to speed up the adoption of interoperable, secure and privacy-preserving identity solutions on various devices, irrespective of the applying sector (e.g. business or government). The members of this initiative discuss common goals by simultaneously taking advantage of already existing standards.

The Kantara Initiative can accelerate the diffusion process for GINI since they have members and partners in all relevant areas. With its strong network and its possibility to make recommendations to the important standardisation bodies, the Kantara Initiative can bring in elements of the GINI vision to the industry and into the standards, which can result in faster adoption, implementation, and acceptance of the GINI vision.

Main Gaps to be addressed:

- How can the principle of a user-centric identity management be integrated into existing identity management systems?
- How can cross-domain or cross-border interoperability be achieved (world-wide)?
- How can multiple identities be combined most effectively?
- What is the best way to establish trust relationships amongst various entities?
- What is required for ensuring that privacy-enhancing functions are integrated in the software design and development process?

4.2.4 Research

This section briefly overviews research programmes or research institutions which may be relevant for consultation to take up the proposed actions within the Roadmap. Only European programmes and institutions are considered.

Some of the most important research programmes within the European Union are the so-called "Framework Programmes for Research and Technological Development", or often simply called Framework Programmes (FP). Those Framework Programmes are funding programmes of the European Commission and aim to foster the strengths of European research activities. Currently, FP7 is running. The next framework programme (FP8) will start in 2014 and will last until 2020. Hence, the proposed and derived actions resulting from the GINI project can strongly contribute to the research and development priorities of FP8.

While the Framework Programmes' aims are strengthening the European research area, the Competitiveness and Innovation Framework Programme (CIP) targets a better take-up of information and communication technologies within the European regions. This should encourage a growing information society and provide European citizens easier access to finance and business support services. Because of these objectives, the main interest groups for funding and support are small and medium-sized enterprises (SMEs) for improving innovation. CIP is actually divided into three programmes, the Entrepreneurship and

Innovation Programme (EIP), the Information Communication Technologies Policy support Programme (ICT PSP), and the Intelligent Energy Europe programme (IEE). However, the CIP programme will end in 2013 and will be superseded by COSME, the Programme for the Competitiveness of enterprises and SMEs. COSME also targets SMEs to increase competitiveness of EU companies beyond national borders and to promote an entrepreneurial culture in Europe.

An institution supporting research within the European Union is the European Institute of Innovation and Technology (EIT). This institute was founded in 2008 with the aim on encouraging the collaboration between high performing institutionsof the higher education, research and business sectors. In fact, its mission is to increase the competiveness of the EU by reinforcing innovation. To achieve this, the EIT has generated so-called Knowledge and Innovation Communities (KIC) which focus on research topics with societal impact (e.g. climate change mitigation, ICTs, or sustainable energies). In short, the main objectives are to facilitate the following transitions: from idea to product, from lab to market, from student to entrepreneur.

The European Science Foundation (ESF) is an independent and non-governmental organisation and currently consists of 72 member organisations of 30 countries. One of its main goals is to achieve cooperation between European research institutions and to mediate between various research cultures. It coordinates common research activities within Europe and promotes scientific interests across Europe. Nevertheless, international collaborations are not fixed to Europe only but can also go beyond. In addition, in this context the ESF carries out scientific workshops or gives science policy advices.

Main Gaps to be addressed:

- Can cryptographic techniques be established that allow for the inspection of anonymous credentials by trusted third parties?
- Can better anonymisation techniques be found?
- How could an Identity as a Service Cloud Computing model look like?
- Can location independence for identities fully be achieved with mobile devices?
- Can the deployment of more secure and privacy-friendly identity management systems increase user satisfaction?

4.3 Business Models and Business Development

A sustainable INDI environment needs business models. To discuss these, we start with the current situation. From that, an intermediate operator-driven model is discussed that is further developed to a full operator driven model.

There are several reasons why the identity service market has not evolved on its own:

- The discussion about identity management has mostly concentrated on strong authentication and security – however, strong authentication is seldom needed and does not offer users any new applications;

- Although identities of persons and organisations are distributed, they are still very often local, which makes identity management market domestic – however, the revenue potential for strong authentication services is quite limited in one single national market, and;
- Identity management was not very well considered in the original design on Internet, which means that the most important Internet protocols and end-user devices support identity management poorly – this makes implementations clumsy and difficult to use.

The INDI vision could, however, be realised through the rise of an international market for identity services. Such a development would require a coordinated effort to put in place conditions allowing for the establishment of a set of complementary operators, specialising in providing the range of services required in identity management.

In this document, potential operator business models are analysed from two different viewpoints:

- Operator cohesion, what does the market look like depending on service offering with / without co-operation between the operators, and;
- Contractual offerings towards different customer / service user groups.

4.3.1 Multi-operator Market

For the evolution of INDI, a multi-operator market model is required. In this section, we initially describe the predominant existing business model. We then compare that with the multi-operator model by listing benefits and drawbacks.

4.3.1.1 Operator Centric Business Model

If an operator or a service provider opts to implement a new service, it generallyrealises that adopting an operator-centric approach. It is the operator that establishes contracts with users and builds the critical mass which is required for the service to be sustainable. Often, businesses are targeted with different business-to-business offerings.

In cases when the operator enables an exchange between users, or between users and businesses, the approach is often labelled a “three-corner model” (cf. Figure 5). In order to interact, both the user and the business entity need to agree on a contractual arrangement with the operator. Irrespective of the kind of contract, its purpose is merely to enable access to other parties who have a contract with the same operator. The operator is central to the model and is the one who decides whom to charge.

Most new Internet businesses apply a three-corner model. Google, Facebook and Skype may serve as examples. They might create two-sided markets for users, services and marketers, but the operator maintains full control of the business and shuns away from co-operation with competing services or operators.

It is also common that Identity Providers, particularly authentication service providers, apply a three-corner model. Users are given credentials and the relying parties must establish a contractual relationship with the IdP. The relying party contract typically gives access only to the users of the IdP.

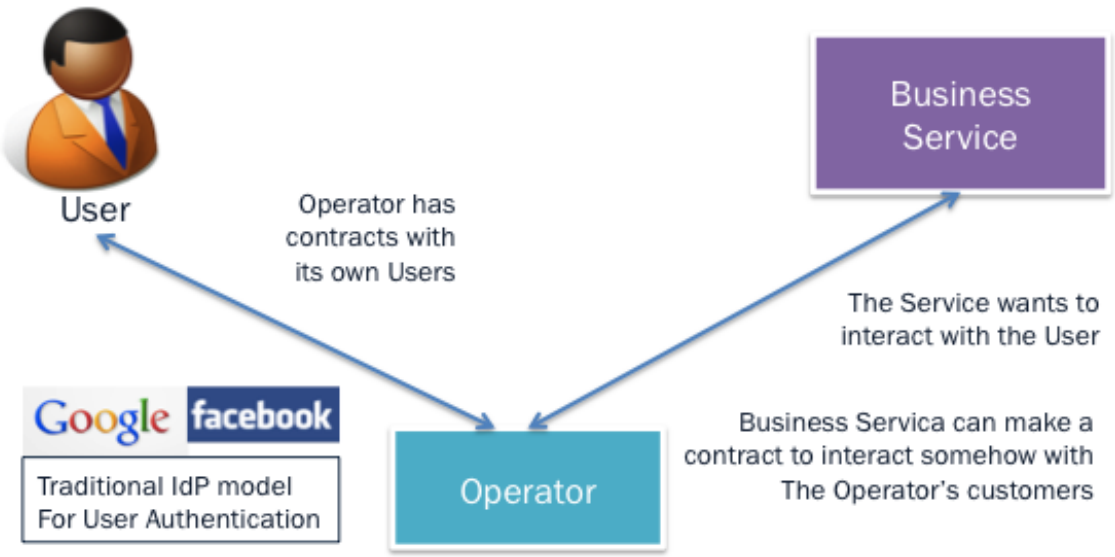


Figure 5 - Operator Centric Business Model

4.3.1.1.1 Benefits and Drawbacks

Operator-centric business models are characterised by some distinct benefits:

- Development work is straightforward and new services or features can be taken to market with little delay;
- Standardisation work can proceed with relatively great speed, because everybody uses the same service interface;
- If an operator manages to create a position as global market leader, its value is prone to sky-rocket with great speed.

Operator-centric business models also have clear drawbacks:

- Operator infrastructure is closed and does not allow easy customisation;
- Competition is hampered because coverage of a market requires entering a contract with relevant operators;
- Relying parties may have to enter a contract with 5-10 operators;
- Small operators may face a difficult position, because it may suffice for relying parties to establish a contract only with the biggest ones;
- Specialised operators may face difficulties in reaching a critical mass for their services.

4.3.1.1.2 Possible Development Scenarios

The following characteristics are common in markets that are driven by operator centric business models:

- One operator gains most of the market share;
- Technical and service development is pursued in a "silo format" for the purpose of boosting the agenda of the operator, not necessarily to grow the market as a whole;

- Operators with smaller market shares tend to focus on differentiated market segments;
- Standardisation work tends to be limited to market niches while operators segment the overall market and may refrain from competing as well as co-operating among each other;
- End users and customers benefit little from innovations and the service development of other operators, but only from those made available by their own operator.

4.3.1.2 Multi-operator Business Model

Sometimes operators co-operate to create more attractive markets. The basic idea is to connect the operators in such a way that the whole network is reachable with one single contract. This is often referred to as a "four-corner model", since users and service providers (or other users) may establish contracts and interact with different operators (cf. Figure 6).

A classic example of operator co-operation is the international telephone network, where local operators co-operate internationally to enable long-distance calls (currently, it would be very difficult to imagine that - with a normal telephone - you would need to know the operator of the receiver of the call). Although the general business model for Internet connection service providers complies with a multi-operator business model, for many specialised Internet services it is common that interactions are lacking between competing operators.

Another example of a multi-operator network is the international card payment network. The user can get the credit card from his local bank and use it in a foreign shop, which has a contract with their local banks. The banks have agreed on a four-corner model and process for money settling between the banks, and created a global infrastructure which can be accessed with a single contract.

Although credit card payments represent another great example of the four-corner model, they also highlight one of its challenges. As the card payment fee is always charged from the merchant, the banks have created a transfer fee system where the card issuer bank gets part of the fee. Although competition for consumers as well as for merchants is fierce, the transfer fee mechanism sets a fixed fee, which always forms part of the transaction. That fee has not changed much over time which has prompted calls from authorities to put a cap on credit card industry transfer fees. Similar discussions have taken hold in the case of the mobile operator roaming fees.

The solution to the transfer fee problem is typically the introduction of open pricing, without any transfer fee related to the actual service fee. Once a transfer fee has been used for a while, however, it is generally difficult to make the shift in regime in favour of open pricing.

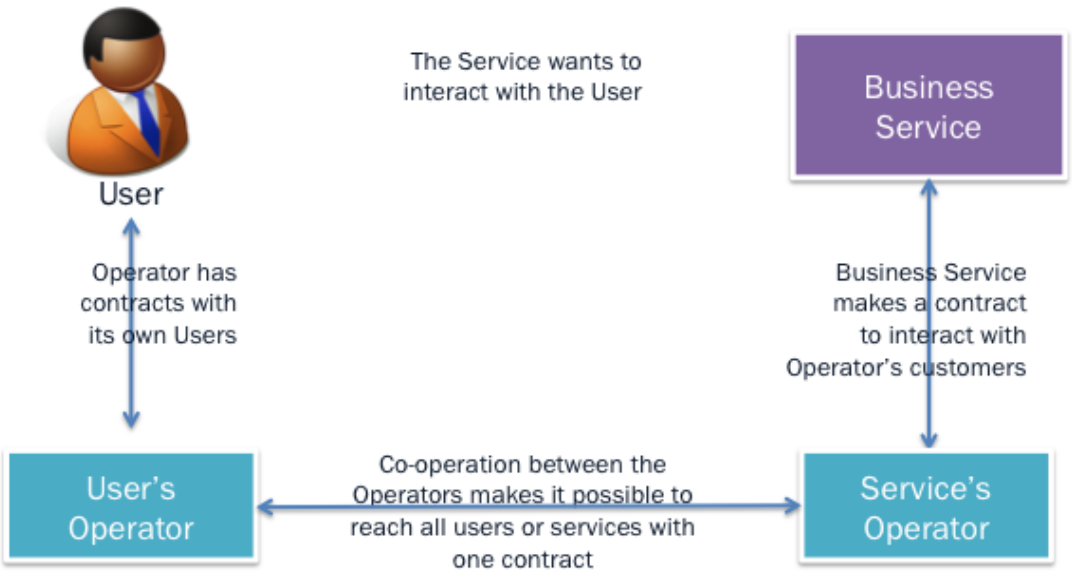


Figure 6 - Multi-operator Business Model

4.3.1.2.1 Benefits and Drawbacks

Multi-operator business models give rise to several benefits:

- It is much easier to create critical mass, when every new contract increasing the total number of users or services;
- If the users or services can reach the whole network with one contract, the competing operators are true alternatives, which fosters competition;
- If one contract is required to access the whole network, the administrative burden of service provider and users goes down.

Multi-operator business models also meet with challenges:

- Multi-operator markets will not emerge by themselves and it might be impossible to achieve a common understanding of the potential benefits between competing operators;
- Agreement between operators might be difficult to achieve, if the service is not standardised well – this allies to both business model and technical standards;
- Through lock-in of prices, transfer fees may seriously hamper competition;
- Finding a responsible operator may be difficult when something goes wrong in a multi-operator transaction;
- The absence of a geographical separation between operators, of the kind commonly found among telecom operators, may impede the adoption of a multi-operator model in online markets.

4.3.1.2.2 Possible Development Scenarios

The following characteristics are common in markets that are driven by two-sided market models:

- Active competition between operators as more or less all compete in the same market field;
- If the service is widely accepted, critical mass may be achieved at high speed;
- Customers are able to switch operator and thereby choose the one that is most suitable for their needs;
- Active standardisation work is pursued in support of simplified and improved co-operation among operators;
- Innovation by one operator often benefits the entire market.

4.3.1.3 Conclusions

There are several reasons why no international identity service market has evolved on its own. These include the presence of local factors in identity management, the low revenue potential of strong authentication services and the clumsy nature of security-driven implementation. The GINI project has concluded that such a market will not arise by itself in the future either. Rather, a series of actions are needed in order to enable the rise of several viable operators, each of which would specialise in complementary aspects of identity management, in compliance with INDI infrastructure and functionality.

For several reasons, a functional INDI framework must crucially be based on international infrastructure and multi-operator co-operation:

- Market experience has demonstrated the difficulty of achieving critical mass in identity services based on an operator-centric business model;
- Identity data is scattered and context-dependent. Exchanges in the market need to be based on smooth conditions for accessing the databases and services of multiple providers;
- The Internet and virtually any digital frameworks are now inherently international by nature. Any attractive applications need to extend beyond national borders. At the same time, international identity applications are hardly possible in the absence if effective conditions for operator co-operation.

A functional INDI framework needs to be based on an international multi-operator business model which is two-sided or even multi-sided. In order to promote competition, we favour an approach that abstains from reliance on transfer fees but favours open pricing in INDI implementation from the outset.

4.3.2 Contracts

This section reviews the operator model from a contractual viewpoint. In the scenarios to follow, it is assumed that operators interact with one another. The contracts and market scenarios differ depending on the nature of the contractual offerings made towards different customer groups. While operators are described in different domains, in the examples below we abstain from discussing the precise number of operators, or to what extent their different

functions are to be separated. The focus here is not on the separation of operator functions but on the different contractual roles assumed by the identity operators within the INDI framework.

4.3.2.1 Contracts with Users and Relying Parties

In this scenario, the operators offer services towards end users and service providers. The customers and their operators are divided into domains based on customer types (cf. Figure 7). The contractual models for both customer groups are rather light.

- **User Domain** describes the users and their operators who are utilizers of the infrastructure, i.e., those who use the Service's operator to access the offerings provided by the Services. Typically, users are individuals accessing identity services in order to access Services.
- **Service Domain** consists of the Services who are offered to users with the help of identity services and the operators of such services.
- The Operators in between offer interoperability and data integrity.

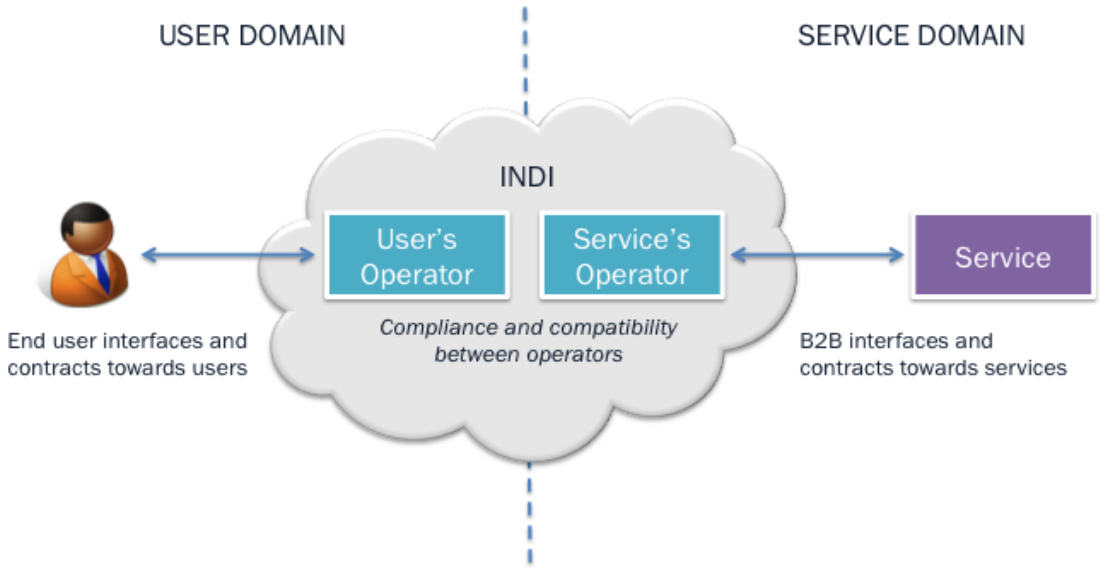


Figure 7 - Contracts with Users and Relying Parties

4.3.2.1.1 User Contracts

Operators will devise their services to users independently of other operators unless some regulation or agreement requires something else. This means that operators exercise a lot of freedom in defining their services, which is important for innovation and competition between alternative solutions. However, some aspects are generically important and thus likely to be found in most services offered by operators to users:

- Definition of end user services:
  - It is probable that users enter in a contractual arrangement as a prerequisite for accessing a service which includes many subservices or products from the operator or third parties;

- Use of an operator's service will require some kind of registration or enrollment. The rules for such registration will be defined in the user contract;
- Fees and billing – as operators have a commercial interest in offering INDI services, they will want to charge:
    - Typical methods of payment are operator bills, credit cards or pre-paid accounts;
    - In some cases, the operator might charge on behalf of a third party – this then needs to be reflected in the user contract;
- It is reasonable to require that users use only their own valid data and do not on purpose take advantage of possible errors in INDI infrastructure;
- Management and ownership of users' data. If operators are in the position to define the terms, they will probably require full freedom to use the data. In the INDI framework, however, use of the data will typically be regulated somehow. The user contract will refer to such regulation;
- Storage of data and messages:
    - The operator offers a service which entails that users can maintain and store their own data – which in turn may be the result of input provided by users themselves and/or which has been provided and verified by some trusted data source;
    - An important aspect will be the opportunity for the user to store other users' data. This might include signed documents or some certificates, which the user has validated with the help of the operator.

A critical feature of the user contract has to do with the level of user centricity. Currently, the major problem with user data is that service providers ask users to provide information for one purpose but then use it freely for other purposes, such as profiling and marketing. This means that the current management of user data is service centric.

In INDI, user centricity is improved through the introduction of strong user consent in regard to use of the data. This means that the operator will be contractually obliged to ensure that user data is not used for "other" purposes unknown to the user. In practise, the might require that the revenue of identity services must be based on user fees and not on marketing. A compromise solution might arise according to which users allow the operator to use their data for purposes such as marketing in exchange for a discount in the user fees.

4.3.2.1.2 Relying Party Contracts

Similar to the users, the operators will define their services relying parties independently of other operators, unless some regulation or agreement requires something else.

The following aspects are likely to be represented in most of the contractual agreements settled between operators and the relying parties:

- Services to the relying parties are B-to-B, which means they are described very differently than the user services. However, the object of the service can be users or data on the users;
- Use of operator services will require some kind of registration or enrollment. This process works differently for the relying parties compared to the users;

- Fees and billing – as both operators and relying parties have a commercial interest in contracting INDI services, they will negotiate these services on business terms:
  - In b-to-b-services, billing is typically made through invoices or by credit card;
- Management and ownership of users' data:
  - It is probable that the relying parties will acquire only the right to use the users' data, not the data themselves;
  - It is stipulated that the relying parties must respect users' data and use them only for the fulfillment of the defined service, which they offer, and not for other purposes;
- Support services:
  - Support for the relying parties is different from support of users;
  - A support contract may include some kind of SLA, Service Level Agreement.

4.3.2.2 Contracts and Data Verification

In this section, we analyse contractual aspects based on considerations of data verification functionality. Customers may be individual users, organisations or technical services (cf. Figure 8).

- Users in the **Presenter Domain** hold/own/are related to certain information that they wish to share with users/relying parties in the Verifier Domain.
- Users in the **Verifier Domain** require certain verified information presented by users/relying parties in the Presenter Domain.
- The operators in between offer the interoperability and data integrity.

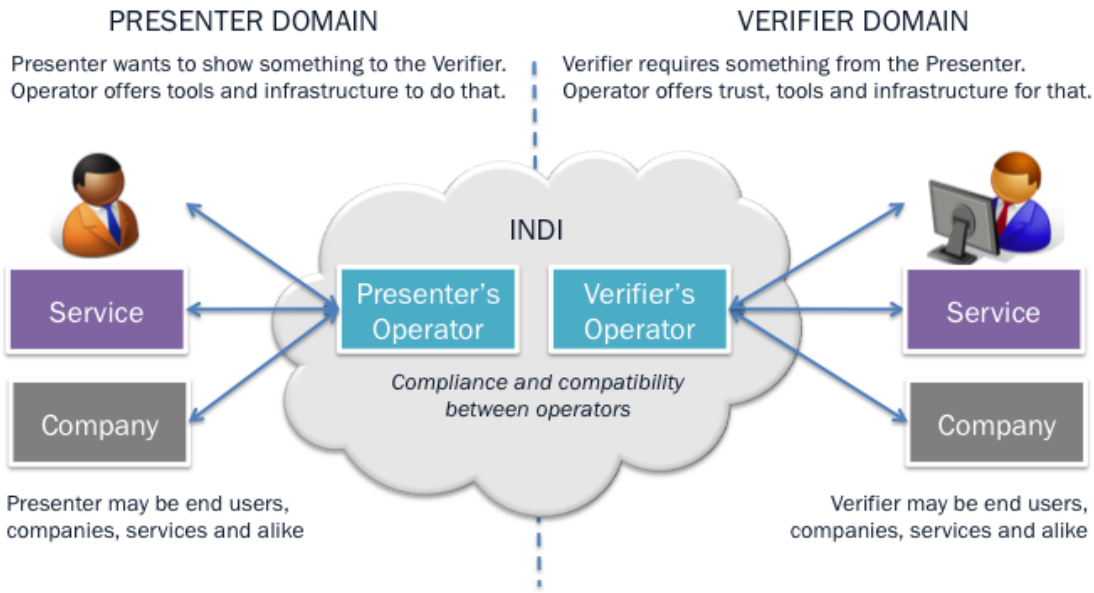


Figure 8 - Contracts and Data Verification

4.3.2.2.1 Contracts for Data Presenters

Users or organisations may have a need to prove various assertions about themselves:

- The counterpart may require a user or a company to prove something as a condition for fulfilling a transaction - typically, such verification requirements are related to risk management;
- Regulation may stipulate that some data is verified – often, this requires accessing physical documentation, which has a particular historical administrative background;
- A user or a company may want to present something voluntarily in order to improve trust and credibility – this often applies to consumers and small companies which are not known well. This kind of need is also on the increase in exchanges at global level, as it is difficult to obtain information about actors that originate from, and primarily reside in, a foreign environment.

Data presentation has some impact to the contract between the operator and the user or organisation. At least the following aspects need to be considered:

- The contract must define the method through which the user is enrolled and verified:
  - Often, checks are required of physical documentation;
  - An Increasing number of online methods has emerged, often drawing on knowledge that the user is in the sole possession of;
  - A third party may be requested to verify the user and or the validity of data for the operator;
  - The user may be verified with the help of some existing business processes, e.g., with reference to a customer relationship or a credit card;
  - Contact networks may be used to verify the user –social networks are rapidly attaining a more important role in risk management processes;
- The contract needs to define the service and its scope:
  - The operator will probably take responsibility of the presentation of the data within the INDI domain or when INDI APIs are used;
- Operator liability has to be defined. Today operators meet with limited liability unless particular regulation explicitly requires something else;
- Users need to assume responsibility for not presenting false information on purpose. Tricky issues may arise, e.g., since some data may have been verified from registers which are no longer up to date.

4.3.2.2.2 Contracts for Data Verifiers

Operator contracts will need to include data verification aspects. This is particularly relevant when users within the INDI framework user view information about other users.

The following contractual aspects need to be considered in regard to data verification:

- In INDI, users need to take some responsibility for the accuracy of data emanating from them;
- Operator liability should be defined. Again, today operator liability is generally limited;
- Use of data subsequent to verification needs to be defined.

4.3.2.3 Data Source Contracts

Data sources connecting to the INDI network can be divided into two categories (cf. Figure 9):

- **Authoritative data sources**, for instance population centers, business registers and many other public sector registers, fill an important function in maintaining some of the most important personal data. Also, some private sector data sources, such as credit rating institutes, may in practice have the same status as public sector registers.
- **Organisation data sources** have an interest in maintaining data for their employees, members or even customers. Typically, inclusion of data in the organisation's register requires some kind of contractual or membership based relationship between the user and the organisation.

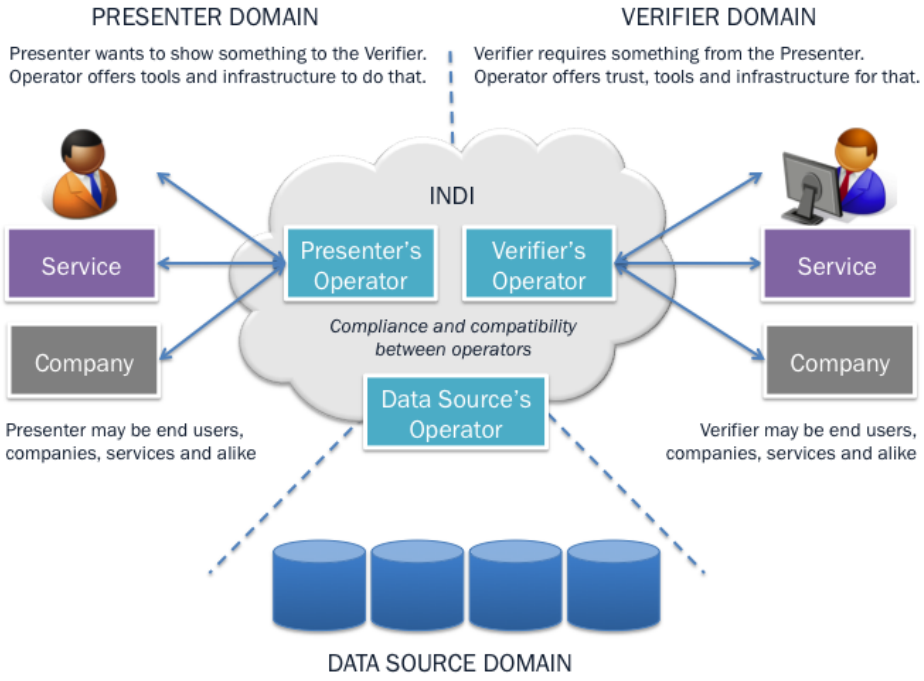


Figure 9 - Data Source Contracts

4.3.2.3.1 Authoritative Data Sources

The following aspects need to be considered in contracts between operators and authoritative data sources:

- Data sources typically charge fees for data queries – price and any aspects related to resale of the transaction need to be agreed (meaning that the operator will charge the fee from some user or service provider);
- Right to give the data to the service providers, who are not indirect contact with the operator;
- Data source and operator liabilities – typically, the public sector registers have quite fixed rules and liabilities for their data;
- Principles of matching persons to the personal data – e.g., based on name, birth date and some additional information, when needed.

4.3.2.3.2 Organisation Data Sources

The following aspects need to be considered in contracts between operators and organisation data sources:

- The organisation has a need of providing data as a service for its employees, members or customers, meaning that the organisation's data source is ready to pay for the services;
- Data source liabilities – it is plausible that many organisations will fail to maintain data properly, or even commit fraud – the data source liabilities must be defined clearly;
- Operator liability typically is about guaranteeing that data integrity is kept inside the INDI network;
- Principles for matching persons with personal data, e.g., based on name, birth date and additional information, as needed.

4.3.2.4 Contracts between Operators

The INDI model presupposes that operators agree to co-operate between each other. Such agreement covers:

- Definition of roles in the INDI network;
- Service interoperability;
- Agreement of the division of responsibilities between the operators.

The agreement may reflect rules or recommendations for contracts between INDI operators and external entities.

The basis for co-operation between the operators could be set with the help of European regulation, where authorities define and certify INDI operators. However, this model would be Europe-centric and it is difficult to see how INDI could expand outside the EU on that basis.

If co-operation between operators is arranged with the help of a co-operation contract, there is a better chance for putting in place a supportive global infrastructure. Pioneering initial contracts among European operators may, however, be warranted for several reasons:

- Rules for person data management and privacy are stricter in Europe than most other parts of the world and a contract with European origin would probably protect users better than if it was created outside Europe;
- By adopting INDI functionality before others, Europe and European companies could first utilise the benefits of an international identity management framework and thereby spur competitive advantages for European industry in global competition;
- By demonstrating the benefits of INDI, Europe could help pave the way for an orderly framework for identity management worldwide.

4.3.2.5 Conclusions

Our contractual review of the multi-operator business model has concluded on the following:

- Multi-operator co-operation requires some sort of basis for far-reaching contractual relations between INDI operators, as well as between the operators, users, relying parties and data sources;
- INDI operators need to have a lot of freedom in how to shape their contractual interfaces – which will be conducive to innovation and competition;
- The following responsibilities are reasonable and should be accepted by the different relevant parties:
    - Users should carry responsibility for acting honestly in the provision and use of valid personal data;
    - Relying parties should respect user data and use it in a fair way, which is limited to the fulfillment of the service they offer;
    - Data sources should take responsibility for the maintenance and accuracy of personal data;
    - Operators should guarantee the integrity and security of the INDI network – they also need to carry responsibility for the accurate authentication of users and associated services.

Main Gaps to be addressed:

- How can future identity management systems help increase productivity or decrease administration costs and efforts?
- Can the deployment of more secure and privacy-friendly identity management systems increase user satisfaction?
- In terms of business value, how can compliance with legal regulations or policies be improved?
- How can users be induced to articulate demands for identity management on their own terms?
- Will the market accept a multi-operator model for identity management?

5 Timelines

This Roadmap outlines actions required for realising the INDI framework, divided into short-, mid-, and long-term. We derive the respective timelines directly from the recommendations that have been developed throughout the project.

5.1 Research Timeline

In this section, we indicate a timeline for further research and development notably at European level, although much of this agenda is relevant at the global level as well. Particular attention in the European context is given to the transition from FP7 projects to Horizon2020.

Recommendations that have been developed in the project and the corresponding suggestions on their timeline are:

1. *Further research is needed on the architecture and protocols for inter-operator and multi-operator communication. It must be investigated whether SAML might be sufficient for an INDI ecosystem, as it was developed for the corporate paradigm of identity and access management. Further research work is required on other new protocols such as OpenID, OAuth, or the e-operating model*[25] *if they could satisfy the requirements of a multi-operator model.*

   This recommendation should be addressed in the short term. The technology work of GINI-SA has demonstrated that the basic technologies required for supporting the INDI vision already exist. Advances in understanding of the required GINI architecture can help pull innovations, however. Questions raised also relate to scrutinising technology for user control.

2. *Further research is required on increasing the scalability and usability of privacy enhancing technologies (PETs), such as of anonymous credential systems. In addition, research is needed to investigate whether PETs are able to evolve to support a multi-operator model.*

   This is a short-term action as PETs might play a major role within a fully-fledged GINI ecosystem. Furthermore, increased practicability of PETs could help in achieving mainstream adoption at service providers. Increased adoption of PETs might also solve parts of the privacy paradox.

3. *Further R&D work is needed on trust meta-models through interdisciplinary approaches involving more than technology but also social sciences, with a strong dimension for international cooperation.*

   We consider this recommendation a mid-term action. While involvement of other disciplines like social science should start early, inter-disciplinary research tends to take time to be successful, as common understanding in each discipline is needed.

4. *Further R&D work is needed on the process of technology-linked innovation, particularly as driven by behavioural motivation, e.g., what is required for raising user awareness of identity management and privacy issues, and what associated market*

[25] http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=400

demand may arise from such awareness under different circumstances? International cooperation should be pursued in this area to account for cultural differences.

This research is assigned a mid-term to long-term agenda. With new services new privacy impacts evolve which leads to continuous research needs.

5. *Further research is needed on non-intermediation of entities, being able to interact directly between participating entities without any intermediary involved.*

   We consider this research recommendation as long-term action. Within the GINI ecosystem, GINI proposes operators to act as intermediaries between entities such as users, business services, or data sources. However, fundamental research is required to allow interaction between those entities without intermediaries (e.g. direct person-to-person interactions), as the question on non-intermediation is not fully investigated yet.

Given these recommendations and their respective indicative duration, the following figure puts the actions and timelines into perspective. Note, that the grey block "Horizon 2020" is an existing initiative. It is not influenced by GINI-SA but nevertheless incorporated as an important programme that can potentially provide strong support for the INDI vision.

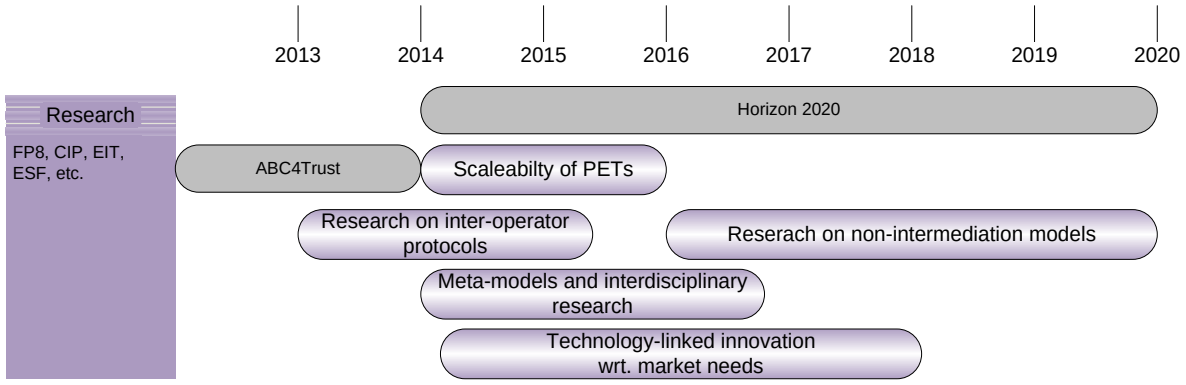


Figure 10 – Research Action Roadmap

5.2 Institutional and Governmental Timeline

The recommendations directed towards policy makers are listed below. To derive a roadmap, we provide indicative timelines.

1. *Data handling principles and decisions by governments will be pivotal for the emergence of an INDI-like ecosystem:*

   a) *Governments should allow citizens to own their identity data, which resides in public registries. They should further award 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 of identity data. 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 in the public domain. It will increase public sector productivity by reducing bureaucracy, minimise regulatory complexity and turn*

regulatory requirements into an enabler rather than an obstacle to cross-border interoperability, by reducing identity-related errors at the same time.

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.*

This is a mid-term to long-term recommendation. Government action is driven by legislation that also needs to fit administrative culture. Where such user controlled scenarios are not yet implemented, change of laws and processes take time.

2. *Governments should put pressure on business to be transparent in the enrolment and transfer processes of identity data.*

   Transparency in processes related to personal data is a basis for proper data protection. We thus assume this a short-term action that can be implemented quickly.

3. *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.*

   A balance needs to be worked out between regulation, co-regulation and no regulation. The process needs to be settled with relevant stakeholders, implying this recommendation applies mid-term.

4. *Governments should foster innovation and experimentation in the development of new business models while taking action to support interoperability among Operators (see Recommendations for Industry above).*

   This is a short-term recommendation. Support for innovation can be initiated via both national, European and multilateral innovation activities and piloting schemes.

5. *Governments should ensure that digital evidence protects the user, in contrast to today's situation where users are forced to rely on the evidence produced and owned by service providers, thus preventing them from pursuing potential violations of their privacy. Creating awareness of privacy issues can enable users to make better informed choices. This is especially important since users seem willing to disclose personal information to gain an economic advantage.*

   Similar to recommendation 1 on general policy actions, enforcing changed conditions for service provision requires the adoption of policy measures which, thus, is a long-term recommendation. As with recommendation 3, a balance needs to be worked out between regulation, co-regulation, and self-regulation.

6. *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.

Adapting existing research and innovation programmes is a short-term measure, creating new ones ad mid-term. Thus, the action is a short-term to mid-term aspect.

7. *The European Commission's Data Protection Regulation and the eID and eSignature Regulation need to be further analysed in case of gaps relating to the GINI ecosystem.*

   We see this action as mid-term action as both regulations are currently still under discussion and finalisation can be expected app. around 2014 (eID and Trust Services Regulation) and 2015 (Data Protection Regulation).

8. *Governments should foster the adoption of standards to support existing policies and regulations. Standardisation mandates should be created involving a broad group of interested parties, such as customers, industry, civil society, etc.*

   The formulation of standardisation mandates is viewed primarily as long-term action since they have to be preceded by some advances in technology and innovations.

The figure below provides the Roadmap setting for the noted recommendations and their timing. Major on-going initiatives include the revision of the Data Protection Directive and also that of the Signature Directive to a comprehensive eID and Trust Services Regulation. Again, these are indicated as grey boxes (including assumptions for their completion).

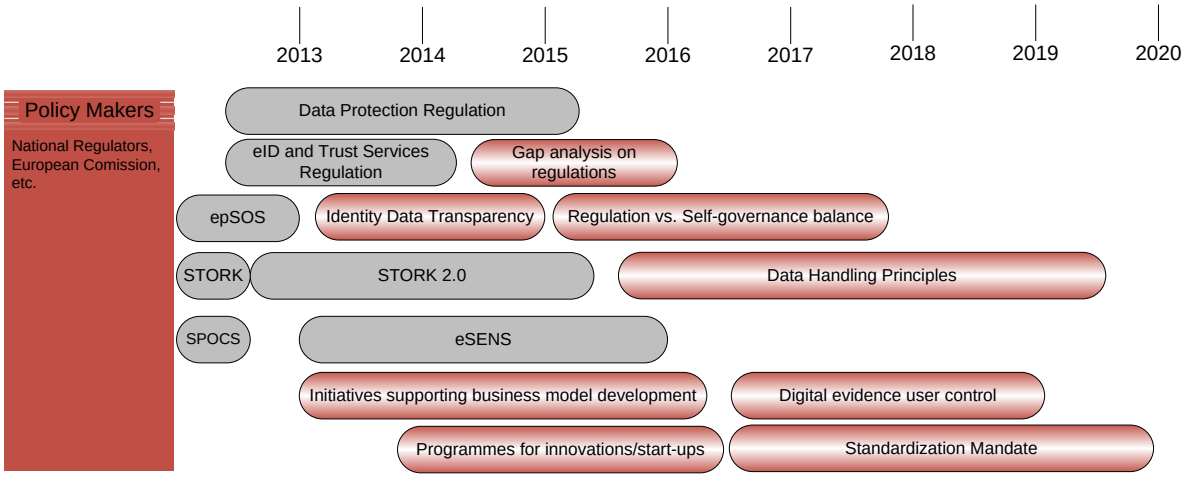


Figure 11 – Policy Action Roadmap

5.3 Industry/Market Timelines

GINI-SA has developed the following recommendations related to industry. For each we provide an indicative timeline.

1. *Concerted collaboration (e.g. interest groups, forums) 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 limiting 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.*

We assume that such collaboration can be started swiftly as pilots between players already operating in the market. These should be devised so as to contribute to innovation and competition between competing solutions. We consider this a short-term to mid-term recommendation.

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.*

   For being successful, standardisation requires some implementation and experience with the technologies. The action thus is a mid-term recommendation following the collaboration recommendation above.

3. *Agreements on the GINI inter-operator architecture should be achieved, addressing:*

   a) *Interface specifications between interacting entities such as between operators and users, business services, or data sources;*

   b) *The inter-operator communication protocols and message must be defined;*

   c) *Interoperability must be achieved between operators to guarantee a fully-fledged INDI ecosystem across domains, sectors, or borders.*

   In order to progress towards a viable INDI ecosystem, working agreements need to be established for individual parts of the inter-operator architecture and how they relate. Given the scope for such agreement, this action is mid-term.

4. *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 standardized inter-operator interfaces (see point 2 above).*

This is considered a mid-term to long-term recommendation. As for the standardisation aspect, some experience with INDI services need to be gained before developing proper governance frameworks.

5. *A thoroughly defined trust framework should be created, fostering the adoption and provision of an interoperable INDI ecosystem based on a widely accepted trust framework and certification mechanisms.*

   The creation of a well-defined trust framework and certification mechanisms require the involvement and agreement of several interest groups, including enterprises, governments, consumer groups and civil society. There is also a need of legal and institutional advances. We anticipate such a framework to be the result of various collaboration activities and hence as mid-term to long-term action.

6. *Contracts between operators and their customers (users, businesses, data sources) should be carried out for allowing appropriate service provisioning.*

   We see this as a final step for the evolvement of an INDI ecosystem and thus as long-term action. Contracts and market scenarios differ depending on the customer group; hence different contractual offerings might be the result.

7. *GINI-enabled services should be designed and developed for penetrating the electronic identity market.*

   The design and the development of GINI-enabled services, either setting-up new services or adopting GINI functionality to existing services, will be the result of the preceding and parallel actions. The development of INDI services and thus the evolvement of an INDI ecosystem will be long-term action.

These recommendations are illustrated as a roadmap below.

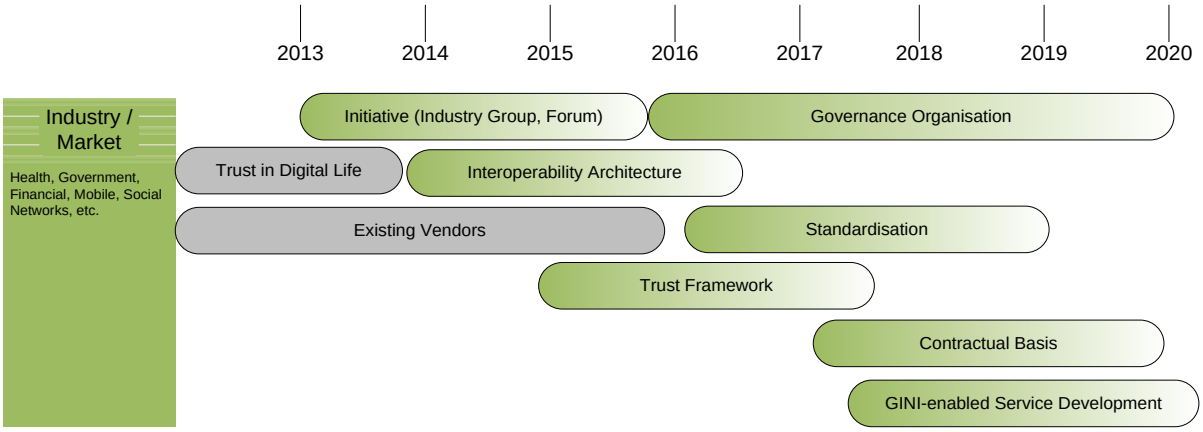


Figure 12 – Industry Action Roadmap

6 Conclusions

The main aim of the GINI-SA project has been the elaboration of what is required for putting in place a fully functional user-centric identity management system. For that purpose, the project examined legal, technical, privacy, and business aspects. While main findings and issues in these domains have been presented in a number of background reports, this Roadmap has reviewed some of the main gaps identified between current state-of-the-art and the envisaged GINI ecosystem.

In order to address and overcome these gaps, we present a number of recommendations for specific future actions. These have been structured as part of the Roadmap described in this document. The analysis and the conclusions have drawn on extensive consultations with stakeholders, such as research communities, policy makers, industry and market players. Apart from representing different social spheres, consultations have been carried out within Europe as well as with international organisations and in other parts of the world. Lastly, the actions proposed by GINI have been aligned with existing initiatives and been directed so as to match with the agendas of the prime stakeholder communities.

Summarizing, we propose the following main actions to be taken up by relevant actors to make the GINI vision of a user-centric identity management system become reality:

Research:

- Research should be undertaken on the architecture and protocols required for the advance of orderly inter-operator collaboration and interface. Research on security and privacy-reserving technologies should help foster broad-based adoption and the applicability of GINI multi-operator architectures.

Governmental/Institutional:

- Governments should embrace the GINI vision and allow citizens to own their identity data residing with public registries. They should further award individuals right and facilities required to control, under conditions that satisfy the public interest, the whole life cycle of identity data, including insertion, access, modification, re-use, or erasure of identity data. While Europe is well placed to take the lead, it should combine a pioneering effort with an inclusive approach, demonstrating the wider benefits and working with multilateral organisations as well as other regions so as to facilitate the establishment of a functional global INDI framework.

Industrial/Market:

- Agreement on the requirements of GINI multi-operator architecture needs to flow out of active collaboration among market players. Industry pilots need to be launched so as to generate learning, innovation and competition between competing solutions. Active engagement in standardisation work and collaborative ventures should at the same time support the establishment of a viable trust framework, certification mechanisms and governance. Market actors should be induced to realise GINI-enabled end-user services that can be deployed with high volume of transactions.

7 Abbreviations

Table 1 Abbreviations

ABA	American Bar Association
ABC4Trust	Attribute-based Credentials for Trust
CIP	Competitiveness and Innovation Framework Programme
COSME	Programme for the Competitiveness of enterprises and SMEs
DSL	Digital Subscriber Line
eID	Electronic Identity
EIP	Entrepreneurship and Innovation Programme
EIT	European Institute of Innovation and Technology
ESF	European Science Foundation
epSOS	European Patients Smart Open Services (CIP Large Scale Pilot)
FP	Framework Programme
G2G	Government-to-Government
GINI	Global Identity Network of Individuals
IAB	Internet Architecture Board
IAF	Identity Assurance Framework
ICF	Information Card Foundation
ICT	Information and Communication Technology
IdM	Identity Management
IEC	International Electrotechnical Commission
IEE	Intelligent Energy Europe programme
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
INDI	Individual Digital Identity

IRTF	Internet Research Task Force
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISOC	Internet Society
ITU	International Telecommunication Union
JTC	Joint Technical Committee
KIC	Knowledge and Innovation Communities
NGO	Non-Governmental Organisation
NSTIC	National Strategy for Trusted Identities in Cyberspace
OECD	Organisation for Economic Co-operation and Development
PET	Privacy Enhancing Technology
PICOS	Privacy and Identity Management for Community Services
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SC	Sub-Committee
SME	Small and medium-sized enterprise
SSO	Single Sign-On
SPOCS	Simple Procedures Online for Cross- Border Services
STORK (2.0)	Secure Identity Across Borders Linked (CIP Large Scale Pilot)
TAS3	Trusted Architecture for Securely Shared Services
TFMM	Trust Framework Meta Model
WG	Working Group
WSC	World Standards Cooperation
XACML	eXtensible Access Control Markup Language

8 List of Figures

9 References

Table 2 Table of References

[AWSC]	About WSC. http://worldstandardscooperation.org/about.html. Last accessed 2012-05-04.
[CaFiRa11]	Camenisch, J; Fischer-Hübner, S. Rannenberg, K. (Eds.), "Privacy and Identity Management for Life", Springer-Verlag, Heidelberg, 2011.
[ECa]	European Commission, "Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data"; COM(2012) 11 final
[ECb]	European Commission, "Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market"; COM(2012) 238/2.
[FB]	Facebook Developers, "Facebook for Websites", https://developers.facebook.com/docs/guides/web/
[IDABC]	IDABC, "Study on eID Interoperability for PEGS", http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521
[IDE]	The Identity Mixer. http://www.zurich.ibm.com/security/idemix/. Last accessed 2012-05-08.
[IPAS]	IdM Policy Audit System. http://www.isoc.org/projects/idm_policy_audit_system/. Last accessed 2012-05-03.
[IS12]	Internet Society (2012): Who We Are. http://www.internetsociety.org/who-we-are. Last accessed 2012-05-03.
[ISTO]	IEEE-ISTO: Member Programs. http://www.ieee-isto.org/member-programs. Last accessed 2012-05-07.
[ITU-T]	About ITU: History. http://www.itu.int/en/about/Pages/history.aspx. Last accessed 2012-05-07.
[JTC1]	ISO/IEC JTC 1 – Information Technology Standards. http://www.iso.org/iso/jtc1_home. Last accessed 2012-05-04.
[LIWSF]	Hodges, J. and Cahill, C. (Eds.): Liberty ID-WSF Discovery Service Specification. http://projectliberty.org/liberty/content/download/3450/22976/file/liberty-idwsf-disco-svc-v2.0-original.pdf. Last accessed 2012-05-04.
[Kantara]	The Kantara Initiative: About – FAQ|Testimonials. http://kantarainitiative.org/wordpress/about/. Last accessed 2012-05-07.
[Kro11]	Krontiris, I. (Ed.), "D2.1 Architecture for Attribute-based Credential Technologies - Version 1", ABC4Trust Deliverable D2.1, 2011.
[Modinis]	Modinis-IDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi

[NSTIC]	The White House, National Strategy for Trusted Identities in Cyberspace (NSTIC), http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[OASIS]	OASIS – About us. http://www.oasis-open.org/org. Last accessed 2012-05-04.
[SC27]	ISO/IEC JTC 1/SC27 – It Security techniques. http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306. Last accessed 2012-05-04.
[UPR]	The U-Prove SDK. http://www.credentica.com/uprove_sdk.html. Last accessed 2012-05-08.
[X.1252]	ITU (Eds): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY. Cyberspace security – Identity management: Baseline identity management terms and definitions. Recommendation ITU-T X.1252, 2010, http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1252-201004-I!!PDF-E&type=items. Last accessed 2012-05-07.

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 participate 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, August 17, 2013