The INDI Ecosystem of privacy-aware, user-centric Identity

Lefteris Leontaridis[1,2] · Thomas Andersson[2] · Herbert Leitold[3]
Bernd Zwattendorfer[3] · Shuzhe Yang[4] · Pasi Lindholm[5]

[1]Netsmart SA
lld@netsmart.gr

[2]IKED
{lefteris.leontaridis | thomas.andersson}@iked.org

[3]Technische Universität Graz
{herbert.leitold | bernd.zwattendorfer}@a-sit.at

[4]Goethe Universität Frankfurt
Shuzhe.Yang@m-chair.net

[5]NorthID Oy
pasi.lindholm@northid.com

Abstract

This paper presents a Roadmap to a Personalized Identity Management Ecosystem Infrastructure supporting Individualized Digital Identities (INDIs). The INDI ecosystem can enhance privacy by giving individual persons the ability to control with whom they share their identity data and under what conditions, while acting in a private, public or professional capacity themselves or through an authorized proxy. The role of intermediate Operators in a market for privacy-aware identity services offering individual choice is a key concept underpinning the INDI vision and is expected to contribute to the emergence of privacy-sensitive business models that differentiate from current data aggregation practices of commercial actors. The conceptualization and roadmapping was conducted by the GINI-SA project (2010-2012) that presented its outcomes and recommendations towards the main stakeholder communities: Industry, Government and Research. The material contained in the paper was extracted from the deliverables of the GINI-SA project as referenced. The GINI consortium is now engaged with the follow up stage devoted to implementation as its key partners continue to work together under a cooperation agreement aiming to continue promoting the GINI vision and lead to its implementation.

1 Introduction and Background

Information and communication technologies (ICT) exert a major societal and economic impact on virtually all countries and industries. They increasingly influence our daily lives and are in the process of transforming societies around the world. New applications and services are continuously becoming available online. Their maturity varies from simple informational services to sophisticated online transactions in e-Commerce, e-Government, e-Learning, e-Health, and so forth. With convergence, fixed and mobile networks are fusing whereas social networks are on the rise and others yet to evolve.

Despite the evidence of positive impacts, however, yet unresolved issues hinder a fulfillment of the potential benefits of ICT. This applies particularly to the fundamental task of achieving reliability, trust, integrity and accountability in connection with identity management and related services. Despite its importance, thus far there has been a lack of progress in putting in place a comprehensive framework for effective services development in this area. As a consequence, much digital communication is now plagued by a patchwork of half-hearted identity solutions, which is interrelated with the presence of other outstanding challenges such as accountability, security, traceability, interoperability, and lack of trust.

Against this backdrop, research undertaken by the GINI-SA project has identified the potential benefits at hand from putting in place orderly conditions for operator services meeting with the diverse needs of a multicorner model that comprise individual users, relying parties and data bases. The GINI Roadmap [GINI 5.1] has outlined timelines and milestones of a process for realising such an objective.

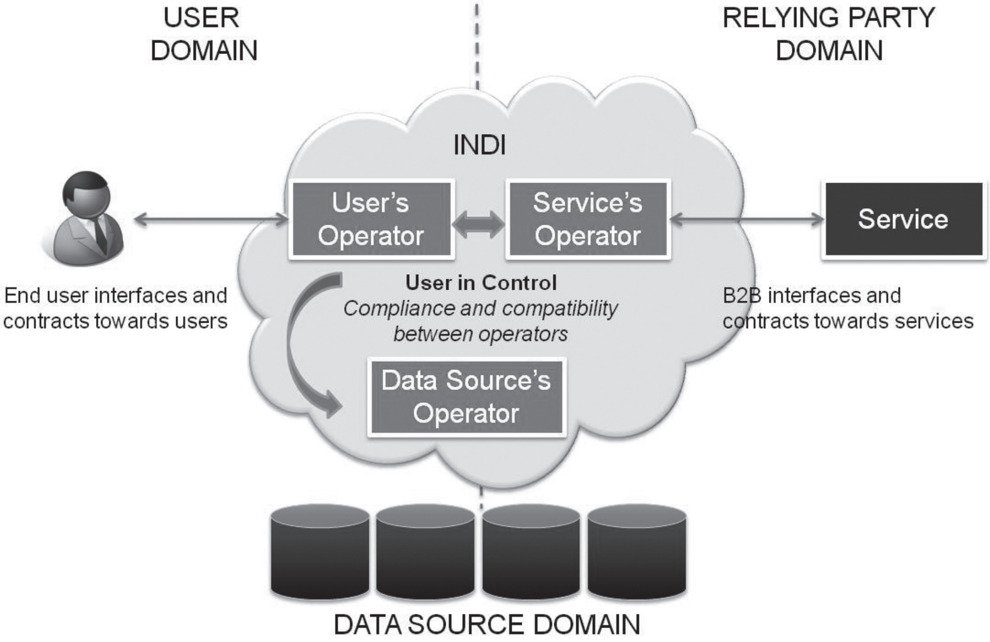
USER DOMAIN
RELYING PARTY DOMAIN
INDI
User's Operator
Service's Operator
Service
User in Control
Compliance and compatibility between operators
Data Source's Operator
End user interfaces and contracts towards users
B2B interfaces and contracts towards services
DATA SOURCE DOMAIN

Fig. 1: The multi-Operator model for an INDI ecosystem [GINI 5.1]

In practice citizens only have limited control and knowledge of how and where their identity data are collected, stored and processed digitally, resulting in severe problems with privacy, lack of trust, high transaction costs and economic inefficiency. No international market has yet evolved for user-centric identity services with viable business models that factor in the protection of privacy. A digital identity ecosystem needs to emerge, capable of enabling citizens to exercise control over their digital identities and to exploit the commercial potential of more effective utilization of user data.

Given the advance of cloud computing and interoperbility between systems and data bases, the potential benefits of the INDI ecosystem are becoming acute. Progress requires, however, determining the prerequisites for viable operator functions serving users, relying parties and databases in a secure and reliable manner. This in turn hinges on working out the architecture for inter-operator functions in the multi-corner model, outlined in Figure 1.

The GINI vision for an Individualized Digital Identity (INDI) ecosystem allows for a decentralised structure with flexibility and the capacity to handle changes in technology and government requirements, without being overly legalistic and without single points of failure. At the same time, there is need of over-archiching coordination and certification of the individual actors. This shall be integrated through a certificaton mechanism, issuing and administering User Certificates for individuals, organizations, Web-Servers, etc. Putting that in place will require transaction interfaces to users, organizations, companies, relaying parties and players on the eCommerce and ePayment scene.

2 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. A synthetic approach with a view to final recommendations and roadmapping was based on the linkages between the different dimensions and their combination for the realization of the INDI ecosystem.

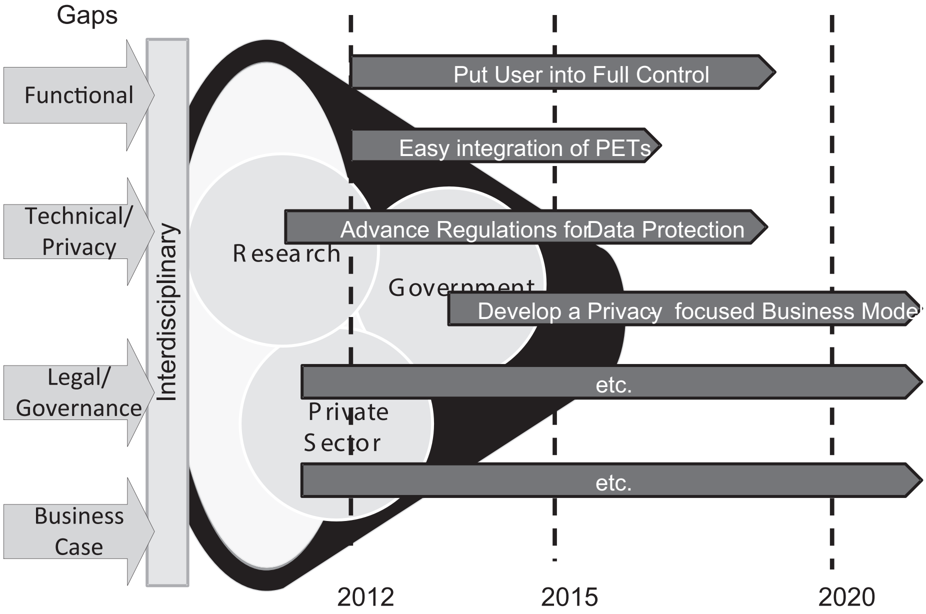

Fig. 2: Synthetic approach to GINI Roadmapping [GINI 5.1]

The GINI roadmapping methodology [GINI 5.1] started out with the gaps identified in the "technology gaps for longer-term research" document [GINI 2.2] and elsewhere in the GINI-SA project deliverables, ultimately compiled in the GINI roadmap [GINI 5.1]. An interdisciplinary approach is required to achieve synthesis of the drivers and expectations that flow from each of the main stakeholder groups – in Figure 2 depicted as Research, Government, and Industry – and lead on to future actions and developments associated with the key projected outcomes:

1. Putting users in control
2. Easy integration of Privacy Enhancing Technologies (PETs)
3. Advance regulation for Data Protection
4. Emergence of Privacy-focused Business Models
5. Vendor neutrality

3 GINI Vision - The INDI Ecosystem

As illustrated in [GINI 5.2], 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 and verifiable, partial digital identity to other individuals or entities that constitute the relying parties with which they wish to build trust relationships in order to perform transactions for personal, business or official purposes.

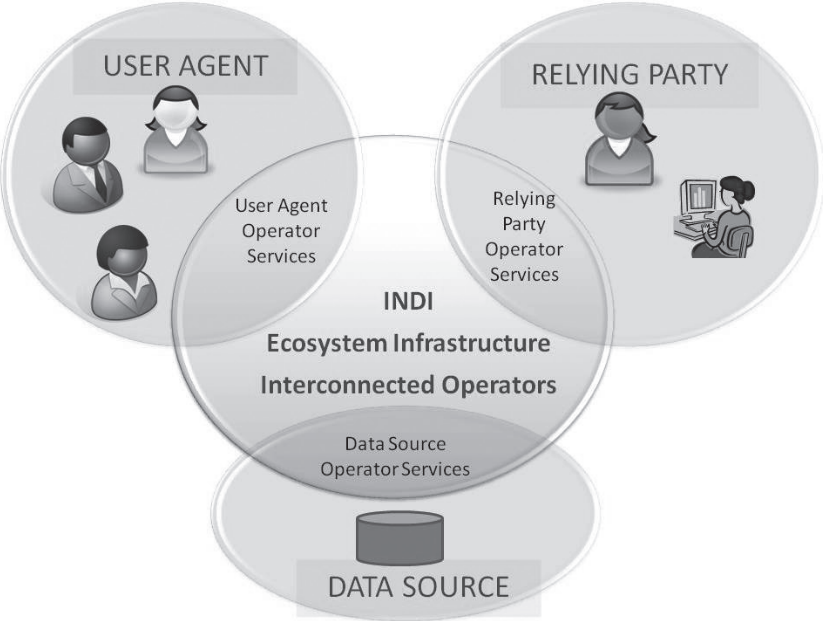
USER AGENT
RELYING PARTY
User Agent Operator Services
Relying Party Operator Services
INDI
Ecosystem Infrastructure
Interconnected Operators
Data Source Operator Services
DATA SOURCE

Fig. 3: INDI Ecosystem Infrastructure [GINI 5.2]

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 (Fig. 3), 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 Figure 4 below:

In a nutshell, the vision has been summarized in [GINI 5.2] as articulated below:

> *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.*

A critical aspect has to do with legal matters as 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.

Policymakers have fundamentally different views on the role of governments versus markets. Meanwhile, while the Internet is not bound by national borders, cybercrime along with various unethical behaviours originate in countries with particularly weak legislative tools.

4 A Multi-operator Market

Sometimes the 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. The model is often called "four-corner model", because in this model, the user and the service provider (or other user) may have contracts with different operators and they can still interact (Fig. 4).

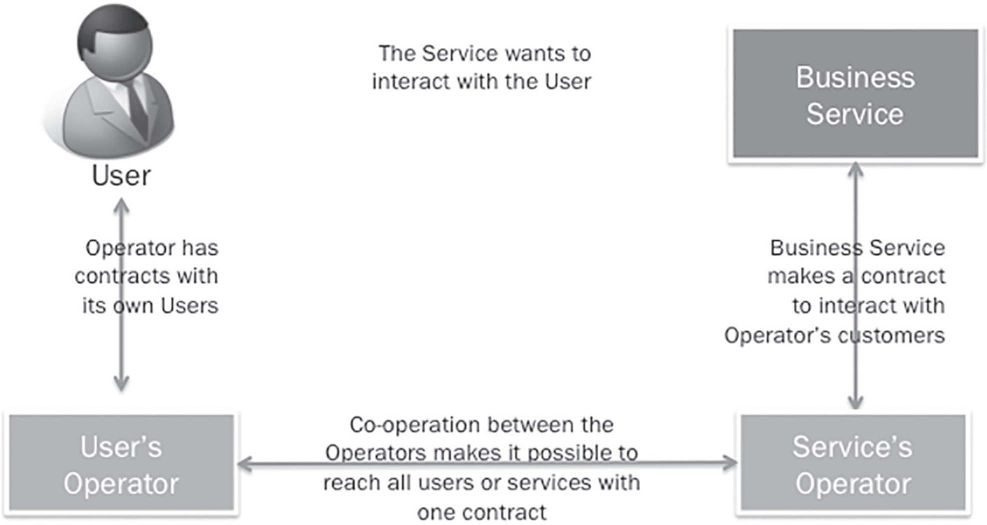
User
The Service wants to interact with the User
Business Service
Operator has contracts with its own Users
Business Service makes a contract to interact with Operator's customers
User's Operator
Co-operation between the Operators makes it possible to reach all users or services with one contract
Service's Operator

Fig. 4: Multi-operator Business Model [GINI 5.1]

A classic example of operator co-operators is the international telephone network, where the 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 business model for Internet connection service providers follows multi-operator business model, it is common in many specialised Internet services that the competing service operators do not interact.

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 four-corner model and money settling between the banks and created a global infrastructure, which can be accessed through a single contract.

Although the credit card payments are a great example, they have also revealed one of the challenges of the four-corner model. As the card payment fee is always charged from the merchant, the banks have created a transfer fee system, where also the card issuer bank gets part of the fee. Although there is fierce competition for the consumers and for the merchants, the transfer fee mechanism sets a fixed fee, which is always included in the transaction. In time, that fee has not changed much and the authorities have decided to force the credit card industry transfer fees down. Similar discussion seems to take place with the mobile operator roaming fees.

The solution to the transfer fee problem is open pricing, where there is no transfer fee related to the actual service fee. However, it is very clear that once transfer fee has been used for a while, it is very difficult to change to open pricing.

4.1 Benefits and Drawbacks

Multi-operator business model has several benefits:

- It is much easier to create critical mass, when every new contract adds 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.

The multi-operator business models also have some clear challenges:

- Multi-operator market will not emerge by its own and it might be impossible to achieve a common understanding of the market between the competing operators;
- Agreement between the operators might be difficult to achieve, if the service is not standardised well – this allies to both business model and technical standards;
- Transfer fees might lock the pricing in such a way that the competition is no more real;
- There might be difficulties to find responsible operator, when something goes wrong in a multi-operator transaction;
- There is no geographical separation of operators such it does exist for telecom operators. In online markets this is not the case, and may also be a significant hurdle towards the adoption of a multi-operator model.

4.2 Possible Development Scenarios

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

- Competition between the operators is active – all operators compete in the same market field;
- If the service is widely accepted, reaching critical mass may be very quick;
- Since customers may choose their operators from those available, customers tend to switch operator to one that is more suitable for the customer's needs;
- Standardisation work is active to achieve better and easier co-operation between the operators;
- Innovation of one operator often benefits the entire market field.

5 Roadmapping Timelines

The actions are divided into short, mid, and long-term actions and are illustrated via timelines. We derive the timelines directly from the recommendations that have been developed throughout the project.

5.1 Research Timeline

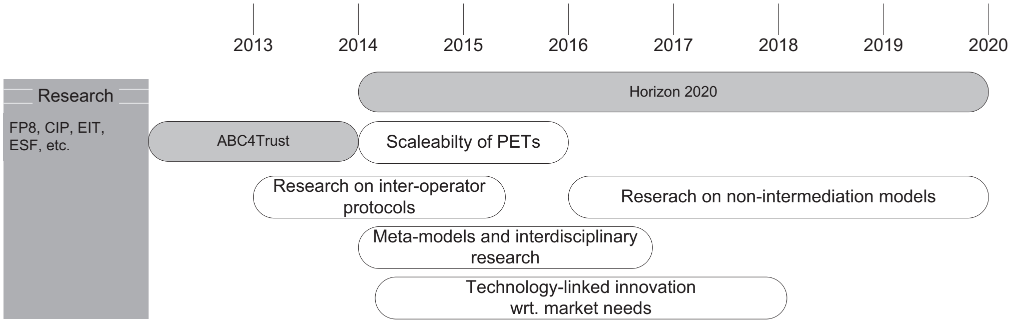
2013
2014
2015
2016
2017
2018
2019
2020
Research
FP8, CIP, EIT, ESF, etc.
Horizon 2020
ABC4Trust
Scaleabilty of PETs
Research on inter-operator protocols
Reserach on non-intermediation models
Meta-models and interdisciplinary research
Technology-linked innovation wrt. market needs

Fig. 5: Research action roadmap [GINI 5.1]

In this section a timeline of further research and development at a European level will be given. Particular attention will be given to the plans of the European Commission to go beyond the FP7 projects into Horizon2020.

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

1. Further research is needed on 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 protocols such as OpenID, OAuth, or the e-operating model [EPC] in order to assess if they could satisfy the requirements of a multi-operator model.
2. Further research is required on increasing the scalability and usability of Privacy Enhancing Technologies (PETs), such as the use of anonymous credentias. In addition, research is needed to investigate whether PETs are able to evolve to support a multi-operator model.
3. Further R&D work is needed on trust meta-models using innovative interdisciplinary approaches involving more than technology but also social sciences, with a strong dimension for international cooperation.
4. Further R&D work is needed on the encouragement and nurturing of technology-linked innovation, particularly on behavioural motivation drivers. Advances are needed on better understanding what is required for raising user awareness of identity management and privacy issues, and on exploring what associated market demand may arise from such awareness under different circumstances. International cooperation should be pursued in this area to account for cultural differences.
5. Further research is needed on non-intermediation ecosystems that would allow participating entities to interact directly between then without any intermediary involved.

Given these recommendations and indicative duration, Figure 5 [GINI 5.1] casts the actions across a timeline perspective. Note, that the grey block "Horizon 2020" is an existing initiative. It is not influenced by GINI-SA, but indicated as an important programme that can support the INDI vision.

5.2 Institutional and Governmental Timeline

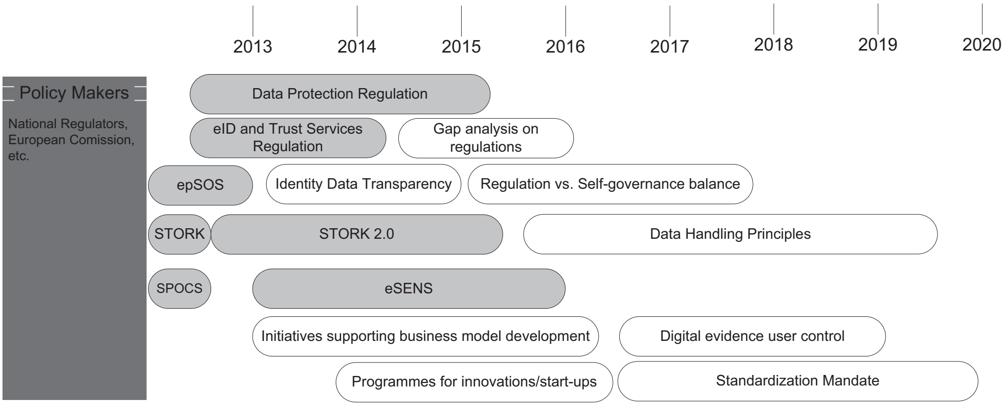
2013
2014
2015
2016
2017
2018
2019
2020
Policy Makers
National Regulators, European Comission, etc.
Data Protection Regulation
eID and Trust Services Regulation
Gap analysis on regulations
epSOS
Identity Data Transparency
Regulation vs. Self-governance balance
STORK
STORK 2.0
Data Handling Principles
SPOCS
eSENS
Initiatives supporting business model development
Digital evidence user control
Programmes for innovations/start-ups
Standardization Mandate

Fig.6: Policy action roadmap [GINI 5.1]

The recommendations given to policy makers are listed below. To derive a roadmap, we provide indicative timelines in Figure 6 above.

1. Data handling principles and decisions by governments will be pivotal for the emergence of an INDI-like ecosystem:
    a. Governments should allow their citizens to own their identity data, which resides in public registries, and should give those individuals the right and the facilities to control, under conditions that safeguard the public interest, the whole life cycle of identity data including enrolment, access, modification, re-use, or erasure. Apart from the obvious public good of respecting what can be considered as a basic human right, such moves by governments will actually facilitate the provision of eGovernment services by the public domain. Furthermore, they will increase the productivity of the public sector by reducing bureaucracy, minimise regulatory complexity and turn regulatory requirements into enablers rather than obstacles to cross-border interoperability, thereby reducing identity-related errors.
    b. 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 after obtaining the consent of the data owners.
    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.
2. Governments should put pressure on businesses to be transparent in the enrolment and transfer processes of identity data.
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.Different governance models involving cooperation between the public and private sectors should be explored.

4. Governments should support initiatives that foster innovation and experimentation in the development of new business models while taking action to support interoperability among Operators (see Recommendations for Industry in Section 5.3).
5. Governments should ensure that digital evidence protects individuals, in contrast with today's situation where they are forced to rely on evidence produced and owned by service providers, thus preventing them from pursuing potential violations of their privacy. Creating user awareness of privacy issues can enable them to make informed choices. This is especially important since users seem willing to disclose personal information to gain an economic advantage.
6. Governments should work out the best way to foster innovative start-ups motivated by developing new services and taking them to market exploringnew and potentially disruptivebusiness models. While existing EC-supported programmes could already be used or adapted to fill this purpose, they need to be complemented with new instruments. National government initiatives as well as schemes promoting cross-regional and global collaboration should be explored and synergies with EU-wide initiatives should be leveraged.
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.
8. Governments should foster the adoption of standards to support existing policies and regulations. Standardization mandates should be created involving a broad group of interested parties, such as customers, industry, etc.

The GINI-SA project has examined the role of different actors in implementing these actions. In particular, a Roadmap and timeplan for the steps ahead have been worked out [GINI 5.1]. A snapshot and further development of this plan is presented in the next section. Figure 6 at the beginning of this section gives a roadmap setting the recommendations into a time-relation. As major on-going initiatives that revision of the Data Protection Directive and the revision of the Signature Directive to a comprehensive eID and Trust Services Regulation is indicated as grey boxes (including assumptions for its completion).

5.3 Industry/Market Timelines

GINI-SA has developed the following recommendations on industry. For each of the recommendations we give an indicative timeline. The likely timelines for implementing these recommendations are illustrated as a roadmap in Figure 7

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 in the area of identity and attribute provision;
   b. Ways forward exploring to what extent 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.

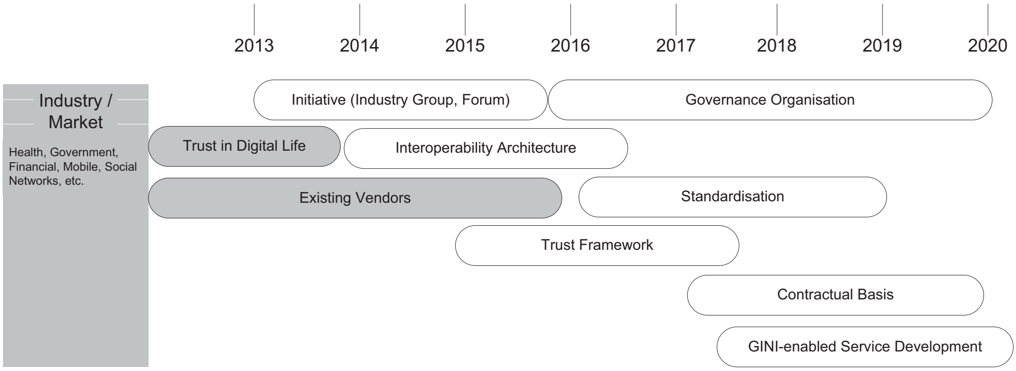

Fig. 7: Industry action roadmap [GINI 5.1]

2. Industry-wide standardisation initiatives should be undertaken, supported by major technology and service providers, in order to define various dimensions of inter-operator interfaces concerning:
   a. Interoperability and data handling processes ensuring privacy for users and confidentiality for relying parties;
   b. Portability specifications, aiming for compliance with upcoming EU regulation;
   c. Protocols, APIs, auditing and security for cross-operator relaying of claims and assertions.
3. Agreements on the GINI inter-operator architecture should be achieved, addressing funcamental aspects such as:
   a. Interface specifications between interacting entities such as 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.
4. A thoroughly defined trust framework should be created, fostering the adoption and provision of an interoperable INDI ecosystem based on an inter-operator interoperability architecture.
5. 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 points 1 and 4 above);
   b. Inter-operator agreements for the 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).
6. Contracts between operators and their customers (users, businesses, data sources) should be carried out for allowing appropriate service provisioning.
7. GINI-enabled services should be designed and developed for penetrating the electronic identity market.

6 Conclusions

It is far from trivial to establish the infrastructure required for INDI. A multi-operator infrastructure is naturally more complex than a solution which is based on a single service provider. However, INDI offers the benefits that follow from not having to confront users with the complexity of the infrastructure nor with the nitty-gritty of the inter-actor relations that denote the system, but to allow such matters to be shielded behind the operator user interface.

No international identity service market has evolved on its own because of the mostly given local nature of the identity management, low revenue potential of the strong authentication services and security-driven clumsy implementations. GINI project believes that the market will not evolve by its own in the future either. However, the market can be created with help of a coordinated effort of operators, which specialise in the identity management. These operators will create INDI market and infrastructure.

An INDI Operator Market can become an international infrastructure, which requires multi-operator co-operation for many reasons:

- Market experience has shown that it is difficult to create critical mass for identity services with an operator-centric business model;
- Identity data is scattered and context-dependent, hence it is not a preferable scenario that all identity data would be collected to the databases of one single service provider;
- Internet is international by nature and in order to create attractive applications, they need to be international – in practise creation of international identity application is not possible without operator co-operation.

INDI business models will be based on multi-operator business model, which is two-sided or even multi-sided. In order to promote competition, we suggest that transfer fees were not used from the beginning, but open pricing would be introduced from the beginning of INDI implementation.

Summarizing the main recommendations included in [GINI-D5.1] and [GINI D5.2] as well as in Chapter 6 earlier, 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 Community: Foster research on security and privacy-reserving technologies to allow for broader-adoption and applicability in GINI multi-operator architectures.
- Governmental/Institutional Community: Governments should follow the GINI vision and allow their citizens to own their identity data, which resides in public registries, and should give those individuals the right and the facilities to control, under conditions that satisfy the public interest, the whole life cycle of identity data including insertion, access, modification, re-use, or erasure of identity data.
- Industrial/Market Community: Agreements on the GINI multi-operator architecture should be achieved. Based on concerted collaborations between interest groups and GINI stakeholders topics such as standardization, the establishment of a trust framework, or governance organisation must be addressed. GINI-enabled end user services must be developed and deployed with high volumes of users and transactions.

Acknowledgements - Disclaimers

GINI-SA has been funded with support from the European Commission under the 7th Framework Programme Theme ICT 2009.7.3 ICT for Governance and Policy Modelling (contract no: 258630). Any opinions, results, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the European Commission.

References

[GINI 5.1] D5.1 - A longer-term research and implementation roadmap towards a fully user-centric INDI ecosystem, GINI-SA FP7 project 258630, 2012.

[GINI 5.2] D5.2 - White Paper on the establishment of an INDI Operator Market across the EU, GINI-SA FP7 project 258630, 2012.

[GINI 2.2] D2.2b: Technology Gaps for Longer-Term Research, GINI-SA FP7 project 258630, 2012.

[EPC] EPC e-Mandates e-Operating Model - High Level Definition, http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=400, 2010