GINI Global Identity Networking of Individuals - Support Action

GINI Position Paper

on Personalized, Privacy-enhancing

Identity Management

Updated on June 6th, 2012

This document serves as background note for the presentation of GINI concepts to stakeholders within the industrial, policymaking and civil society communities and the articulation of some key questions that need to be addressed by these constituencies..

The high-level objectives are to provide an overview of GINI-SA, describe the gaps towards the development of a Personalized Identity Management ecosystem we encountered thus far, and to receive feedback that can help guide the way forward towards the realization of such a framework.

Interested parties are invited to reflect on the contents of this position paper and offer their own views and thoughts on the issues, to comment or criticize the views and statements presented by GINI or otherwise contribute to the discourse.

GINI welcomes views on societal, business, legal, or technological aspects that need to be considered in developing a viable long-term solution to the challenges of identity management still outstanding in the digital world.

Please contact info@iked.org and visit www.gini-sa.eu

SEVENTH FRAMEWORK PROGRAMME

About GINI-SA

GINI-SA is a Support Action for the European Commission, which aims to analyse how a Personalized Identity Management (PIM) ecosystem in which individuals can manage their digital identities and control the exchange of their identity information. Under the GINI vision, individuals would manage their identities by means of an Individual Digital Identity ('INDI'). An INDI can be described as a self-generated and self-managed digital identity, which is verifiable against one or more authoritative data sources. Once created, users would have the ability to link their INDI with authoritative identity data maintained by both public- and private-sector entities. This data (or links thereto) could then be presented by the user towards relying parties. The user might wish to do this in order to meet transactional requirements (e.g., access control conditions set by a relying party) or underpin her trustworthiness towards others in various real life situations (e.g., verifying her education or presenting her skills when applying for a job).

The main objectives of GINI include:

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

GINI further examines the technological, legal, regulatory and privacy-related dimensions of the gap between the current state of the art and the vision for a functional INDI ecosystem beyond 2020. Detailed examinations of these gaps have been carried out in the individual work packages of the project. The following sections briefly introduce the major gaps identified thus far.

The INDI ecosystem

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 will 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 will be 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.

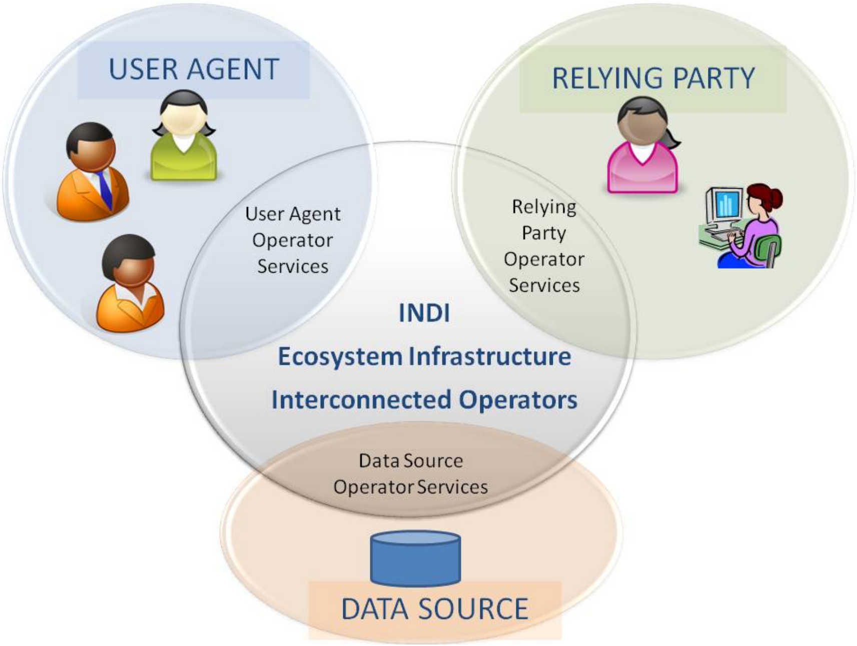
The INDI is a digital identity that is:

- 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 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:


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

A fourth type of interface must work out in order to achieve the required inter-Operator functionality, which is the basis for an infrastructure that allows for genuine interoperability. The inter-Operator interface needs to service requests from an actor that is connected to one Operator towards actors connected to other Operators.

The INDI allows the individual to act in various roles, for instance as citizen, employee, or customer. GINI assumes an operator model, i.e. the actor's "User", "Data Source", and "Relying Party" are served by operators. It may be possible for these three different roles to be managed through a single INDI operator, or to utilize multiple ones for different interactions. The user chooses which roles to act in and what information to reveal in the different roles. As such, an INDI operator may serve to represent the user in many different kinds of context. Still the user is able to manage a set of partial identities, similarly to the situation in the physical world, by providing the information that is relevant for each situation, including those cases where anonymity, pseudonymity, and limited attribute provision are desired and acceptable.

Business Aspects of the INDI ecosystem

As INDI is a new infrastructure, with no INDI market or operators existing as of today, there is a need of determining what prerequisites must be put in place, in order to enable private organizations to assume the tasks of INDI operators.

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

- Independent Trust Anchors are needed to enable trust within the INDI environment and provide added value beyond users' self-asserted claims;
- From a risk management and privacy point of view, it is important to avoid centralised single points of failure which also present threats for privacy-compromising data aggregation and/or profiling. INDI management and data should be de-centralised and decoupled from each other;
- The INDI Operator concept and the business models it enables make it easier to create a truly global and competitive market for INDI services;
- Users have difficulty managing trust decisions on their own, without appropriate supporting services. If they would have to understand and evaluate a large number of trusted third parties, the situation gets unmanageable. Users want entities which they can trust and which can "represent" the "whole infrastructure". Users must, however, be able to enjoy sufficient technical assurances and legal warranties, if they are to be able to undertake well-founded "trust decisions";
- The Operator Network model can be standardised and regulated easier than a model that is based on strongly heterogeneous, uneven entities.

A variety of business models for Operators will emerge once the technical aspects of the INDI ecosystem's infrastructure are implementable and a set of governance procedures are in place. Some key assumptions about business models can serve as starting point in this respect:

- An Operator can choose to deploy one or more interfaces according to its business scope. When multiple interfaces towards more than one actor category are in place, additional privacy safeguards are warranted. The GINI project will explore these privacy constraints and requirements;
- Entities which are already active at either end of the INDI ecosystem (e.g., existing service providers, banks, telcos, social networks and large relying parties) may opt to deploy INDI interfaces and inter-Operator interfaces, thereby becoming Operators themselves;

- In any and all business models, certain requirements should be met in order to enable trusted relationships with Users:
    - The INDI Operator should act a trust anchor, which helps verify the User's identity data in the INDI ecosystem – the whole ecosystem has a trust relationship with the user through the INDI Operator;
    - The INDI ecosystem is global, which means that the INDI Operator and the User need not be from the same country or identity domain;
    - The relationship has a contractual and legal dimension and not just a technical side;
    - The User should be able to have a relationship with several INDI operators at the same time and in parallel, and also be able to switch from one to another, much as can happen with mobile telcos.

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

For the GINI project, any business models should be examined with a view to finding the best possible solution for the user, while creating a competitive open market and avoiding vendor and technology lock-in. Operator business models should allow competition whilst promoting synergies in order to avoid "gated communities", "islands" or "silos".

Technological Gaps and Issues

Establishing Trust Relationships: The technical framework of GINI is based on the combination of different services all influencing the lifecycle of a user's digital identity. Building trust relationships is complex and can be achieved at either the technical or organizational level. Every interaction involving more than one entity requires a stable trust relationship.

Cloud Computing: Currently, cloud computing represents one of the most important emerging new frameworks set to shape the IT sector. An effective implementation requires, however, that the electronic identification issues are resolved. Technology gaps arise when moving existing identity systems to the cloud or when designing an Identity as a Service Model.

Interoperability: Having a look at the world-wide eID landscape, various eID solutions are already in place. However, they usually differ at the technological, legal and/or organizational levels. These differences stemming from different domains lead to technical challenges, e.g., due to conflicting domain requirements.

User centricity: One of the main aims of GINI is to allow for the evolution of an effective user-centric ecosystem for identity management, so as to enable the user always to have control what data are being transferred or processed. Since decentralisation often hinders direct user control, however, further research is required what technologies can manage such trade-offs the best.

„The Eraser“ issue: Any user has the right to demand deletion or correction of her data. Today, many providers do not oblige and users tend to have weak or no control in this respect. Although users have the legal right, technical and business models realizations to effectuate deletion are virtually lacking.

Digital Exhibitionism: Many users are not aware on the sensitivity of personal data and may unconsidered over-share personal information. E.g., they might be willing to disclose personal information to attain economic advantage. On this basis, there is a need of increasing user awareness of privacy issues.

Compliance: When processing or storing sensitive data this may have to occur in accordance with legal regulations or policies, e.g., in some cases data must only be stored in specific countries. It is still not clear what technical means are best suited to accommodate jurisdictional discrepancies.

Privacy by Design: When designing software, at the moment privacy aspects are usually covered by non-functional requirements only. However, future software developments should follow approaches where privacy-enhancing functions are considered and built-in throughout the design process.

Digital Evidence Chains: Traditional means for gathering digital evidence and compiling evidence chains are highly challenged by todays heavily distributed, possibly federated, and partially encrypted operating environments. The seamless compilation of digital evidence chains that reflect the complete end-to-end workflow are almost impossible to produce, which results in scattered audit events.

Trusted Platform Design: Although a variety of trusted platforms are available to user nowadays, their particular implementation is often misguided. Instead of empowering the user of such devices, the commonly available trusted platforms are actually restricting the end user, while enabling the service and platform provider to take a significant level of control over the user. Consequently, the term “trusted platform” is often used as a synonym for digital rights managements (of the service provider).

Invention, Innovation, and Research Cycles: In today's world, the period in which inventions and research are implemented into real-world software and international standards is significantly shortened. Traditionally, the "best-before" time of international best practices of approximately ten years was considered to be adequate. In the current reality, even "new" approaches and implementation processes are frequently subjected to deprecation and disqualification (e.g., incidents that have been seen among certification authorities, flawed security protocols, or progress on breaking fundamental building blocks such as cryptographic services).

Legal and Governance Gaps and Issues

eID mutual recognition: Where qualified eID exists (national eID, sectoral credentials), the recognition beyond their initial domain of application (e.g., outside the country, between public and private sector) is typically not ensured. Which policy initiatives may be adopted to stimulate further mutual recognition?

Levels of Assurance: How will oversight and enforcement of Levels of Assurance requirements will be organized within the INDI environment? How will liability be allocated in case of a breach? What enforcement regimes should be put in place (accreditation, supervision, compliance-declaration)?

Appropriate regulatory and governance framework for Operator-driven INDI ecosystems: Pros and cons of self-regulated, government regulated, or co-regulated approaches must be evaluated. Which arguments support regulatory intervention, what is the drawback?

Roles and responsibilities of the actors: Is the current classification of actors under Directive 95/46/EC ('controller' / 'processor' / 'data subject') still adequate in today's (and tomorrow's information society)?

Data portability: To what extent may sector-specific legislation be needed in order to address the barriers concerning the re-use of public-sector information, even when the user has consent-ed?

Governance of the PIM ecosystem: Who sets the "rules" for the INDI environment (e.g., interoperability standards, audit requirements)? Should there be any internal oversight or "policing" of the ecosystem (e.g., accreditation/revocation of participants)?

Data minimization: Which measures could EU policymakers undertake in order to stimulate the adoption of privacy enhancing technologies (PETs) such as anonymous credentials?

Are we re-inventing wheels? Are existing approaches to eID systems fit for purpose? Can e.g. the current E-Signature framework be transposed to the eID domain? Are there other examples that may be applied?

Diverging Speed of Domains: Traditionally, new technology and applications are advancing much quicker that the respective regulatory frameworks. However, due to a significantly accelerated development and swift derivation of formerly unavailable services within the technology domain, the legal domain is merely responding with "quick fixes" and specific addressing of details instead of bringing forward an "umbrella" under which new applications and technology may be implemented and operated.

Privacy Gaps and Issues

Data anonymization: Recent research has demonstrated that seemingly anonymized data can often be processed in such a way that it is possible to "re-identify" or "de-anonymize" individuals with significant accuracy. Given the theoretical limits of anonymization techniques, scientists look for more holistic approaches, such as differential privacy. How these new approaches can be integrated into user-centric identity management systems, and what kind of new challenges emerge from them, is still to be investigated.

Digital Exhibitionism: Many users are not aware on the sensitivity of personal data and are willing to over-share personal information. In general, they are willing to disclose personal information to attain economic advantage. Thus one further objective in research must be increasing user awareness on privacy.

Data minimization: Technological advancements, such as attribute-based credentials, enable us to better address fundamental privacy principles such as data avoidance and minimization. In practice, data controllers very often obtain consent to collect information beyond that which is necessary for the fulfilment of the core contract that constitutes their service. Future research should investigate how the use of privacy-enhancing technologies might be stimulated in practice, including incentive-driven models where data collectors receive additional benefits for adoption of PETs.

Purpose binding: Purpose binding so far has been dictated with legal means. Technological solutions that would prevent a business service (i.e., relying party) for using personal data outside the context of its original purpose are currently dependent on the success of DRM systems for which many challenges remain. Future solutions will have to be worked out at a socio-technical level, involving context, semantics and organizational developments.

Accountability: Under certain conditions, business services (i.e., relying parties) should be able to retrieve the identity of an anonymous user, who has misbehaved or misused the service. Technical advancements based on cryptographic techniques can allow for the inspection of anonymous credentials by trusted third parties. Further research is required, however, to make them fit for deployment in products.

Usability and responsibility: Usability is an important issue for a user-centric identity management system. Under the GINI vision, individuals would already be relieved of considerable burden of appropriately managing their partial identities due to the mediation by (or through) the INDI Operator(s). However, it still remains to be investigated to which extent individuals may reasonably be expected to micro-manage their own digital identities, and to what extent data collectors should be responsible for pro-actively limiting the burden incumbent on individual data subjects.

Integration, deployment and infrastructures: GINI focuses on user-centric identity management, where the flow of personal data is handled by the user agent. This way, individuals can supervise and limit personal data disclosure and exercise rights of access to their data held by third parties. However, its real deployment and its integration within surrounding systems in the enterprise environment may create interactions and additional data flows that are still unknown. Further research and experimentation focusing on integrations and deployment, through piloting deployments, will shed light in such interactions.

Data and Information Liberation: Many providers of digital services traditionally follow the “lock-in” principle concerning the user’s data and information. Such behaviour is rendering the proposed user-centric approach ad absurdum by preventing the user to easily take his business elsewhere whenever he simply wants to or when challenging the terms and conditions of the service provider.

User-Centric Digital Evidence: Traditionally, digital evidence in form of audit records and admission/access documentation was produced in and for the service provider domain. This pattern needs to be reconsidered when a user-centric operation environment is operated. The primary purpose of such digital evidence is relocated from protecting the consumer towards the user protection, since the “user” needs to be empowered in order to take informed decisions and enabled to pursue potential violations of his privacy policy without exclusively relying on the evidence as produced and owned by the service provider.

Consenting into new Applications: The electronic representation of consenting into a new, potentially complex service in today’s digital services is traditionally designed in a binary fashion: exclusive opt-in or total opt-out concerning the basic terms and conditions of the service provider. Furthermore, while the process of consenting is usually realised by a one-click solution, the terms in which one is consenting into are quite exhausting (60+ pages on a mobile screen) and through that rarely promoting an adequate “informed” consent.

Unavailability of Secure User Devices: A true user-centric operating environment is highly dependent on the availability of extraordinary mobile and highly versatile devices. However, in particular the currently available mobile devices have proven to be uncontrollable and assumed causes of privacy violations through manufacturer means, for example remote monitoring and localisation, remote device wiping, and the explicit prohibition of device software analysis (black box principle).

Some Key Questions to Stakeholder Constituencies:

1. *Which are the critical privacy challenges and solutions within the INDI ecosystem and what may be the privacy advantages? How can the application of “privacy by design/default” principles, enshrined in upcoming legislation, be supported within the INDI ecosystem and facilitated by its emergence? How can businesses and all types of organization be supported in their efforts to comply with current and emerging privacy requirements, given the problems of “big data aggregation” in new and legacy systems?*

2. *Can privacy enhancement be a driver for innovation that will become a viable and sustainable basis for new business models within the INDI ecosystem? If yes, what could be the impact on current business practices based on heavy profiling and unwarranted use of personal data?*

3. *Which operating and service provision models are likely to emerge, taking into account the current standing and discernible developments as well as views and interests of present and potential providers of IDM services such as telcos, banks, commercial cloud providers and niche start-ups? Can Identity as a Service be an answer to privacy challenges in the Cloud, or itself a Cloud service?*

4. *Which would be the end-user and consumer views on operating and service provision models within the INDI ecosystem and what is required for them to*

work out in practice? How could the emergence of viable business models be facilitated?

5. *What policy measures are most critical for moving us forward from the present unsatisfactory status, by enabling the rise of user-driven and user-operated identity services in an interoperable ecosystem of identity management supported by public administrations and private providers in the consumer market? What synergies with other initiatives should be developed?*

6. *Given the latest proposals for a revised EU Directive on Privacy, could implementers of Personalized Identity Management services from Industry and Government agree to start discussions around the interpretation of and compliance to new privacy regulation requirements such as data portability and privacy by default/design, which could promote interoperability among different providers and services under a common governance framework that sustains and expands the market whilst preserving and enhancing privacy rights for individuals?*