Identity Management Systems (IMS): Identification and Comparison Study

Independent Centre for Privacy Protection (ICPP) / Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein

and

Studio Notarile Genghini (SNG)

2003-09-07

Contract N°19960-2002-10 F1ED SEV DE.

EXECUTIVE SUMMARY

Identity management is one of the most far-reaching and promising topics for modern society, but barely analysed so far. Administering and controlling identities will presumably become a task which requires technological support. Identity Management Systems (IMS) will provide such technological assistance for managing identities. A holistic all-purpose tool for identity management is still a mere vision. In the current discussion of industry and academia, specific solutions of Identity Management Systems are elaborated which deal with the following **core facets**:

- Everybody in information society possesses many accounts (so-called digital identities) where authentication data such as passwords or PINs have to be memorised. As a unique and universal ID concept is far from being implemented – not only because of privacy obstacles – the amount of **digital identities** per person will even increase in the next years. Users need convenient support for managing these identities and the corresponding authentication methods.

- Users also need convenient support for situations where they are addressed by other people or even machines. **Reachability** management could put users in a better position to handle their contacts by providing an intelligent filter mechanism, e.g., to prevent spam e-mail or unsolicited phone calls.

- Today's digital networks do not ensure **authenticity** and render an **identity theft** rather easily. Systems which support methods for authentication, integrity and non-repudiation such as digital signatures can prevent unnoticed unauthorised usage of digital identities.

- Users leave data trails by using digital networks – mostly without their knowledge and without any possibility to prevent those trails. Instead each user should be empowered to control which parties can link different occurrences of one's personal data in order to estimate how much they know about oneself. This demand can be derived from the right to informational self-determination. Methods to support users in asserting this right are being developed, e.g., for providing **anonymity** or **pseudonymity**.

- **Organisations manage personal data** of their employees and are in need of quick methods for creating, modifying and deleting work accounts. Additionally to this internal management of members, organisations strive for administration of their client data, using e.g., profiling techniques.

Regarding these aspects, this study focuses on the **user-controlled management of own identities** rather than describing systems, which only do user profiling without offering the individual a possibility to manage those data. These types of self-called "Identity Management Systems" are found quite often in today's business, but in contrast to the user-controlled Identity Management Systems they concentrate on business processes rather than comprising the user's point of view. With our notion of IMS, putting the user in the centre, but nevertheless discussing possible implications also for organisations of different kinds, we take into account, that IMS in fact create a new paradigm in the sociological, legal and technological realm.

The study "Identity Management Systems (IMS): Identification and Comparison" is built on **four pillars:**

1. **Basis** of and **requirements** for Identity Management Systems, which are elaborated from sources of academic literature and business information;

2. **Usage scenarios**, which show the practical relevance and additional requirements of IMS in various contexts;

3. Analysis of presently available **Identity Management Applications**;

4. **Survey** on expectations on Identity Management Systems, which was conducted among experts world-wide.

It is important to point out that technologically supported identity management affects the whole social evolution. In order to correlate the evaluation of applications and the reflection on social impacts of IMS, we made the important distinction between "**Identity Management System**" (IMS) and "**Identity Management Application**" (IMA): We define the term "Identity Management System" as an infrastructure, in which "Identity Management Applications" as components are co-ordinated. Identity Management Applications are tools for individuals to manage their socially relevant communications, which can be installed, configured and operated at the user's and/or a server's side.

1st Pillar: How to construct identity

The "identity" of an individual in the form of a person can be described as mostly socially formed. Henceforth, it becomes necessary in order to understand the complexity of identities to distinguish the **social contexts** in which persons navigate and in which some of their partial identities, bundles of attributes of their complete identity, become relevant. From the standpoint of sociology, the main types of social systems need to be discussed as specialised forms which are operating along the difference of "I" and "Me" and the difference of "role making" and "role taking". Identity management then means recognition of situations and their valuation as "applicable to one self" (role taking) or forming them (role making). IMS should assist users to correctly identify social situations and their relevant addressing options. The perspective of future information society is: No communication without the assistance of an IMA.

Switching to the **legal perspective**, identity management is not explicated by legislation as such. Identity from a legal perspective has a dual function: identification of subjects and reference point for rights and obligations. Nonetheless legislation provides some (in most cases) constitutionally protected rights to individuals, that allow them to change some aspects of their identity, even if such changes are in conflict with uniqueness and identifiability of subjects. In this sense one could point to well-known, conventional rights like "right to a name", "right to change name", "right to have a pseudonym", "right to move and to change domicile", "right to dress and decide the personal outlook", "right to be left alone (privacy protection) and right to anonymity", "right to change gender" and "right of honour". The legal perspective also includes the liability of the user and giving evidence.

A **technically supported identity management** through Identity Management Applications respectively Identity Management Systems has to empower the user to realise the right to communicational self-determination. For this purpose it should recognise different kinds of social situations and assess them with regards to their relevance, functionality and their security and privacy risk in order to find an adequate role making and role taking. Pseudonyms and credentials, i.e., convertible authorisations, are the core mechanisms for the handling or the representation of identities. The IMA should provide functions for context detection and support the user in choosing the appropriate pseudonym. A log function for all transactions of the IMA should give valuable input to the context detection module and inform the user about past transactions.

The **analysis** of identity management in the socio-psychological, legal, and technological contexts demonstrates:

- Role management, which has been handled intuitively by people so far, will become explicit.

- The current regulatory framework in the EU offers many degrees of freedom in pseudonym handling without inevitably losing assurance in legally binding transactions.

- Although technological concepts of multi-purpose privacy-enhancing identity management are already about 20 years old, they have only been partially implemented, yet.

All these findings prepare the ground for an effective identity management in both the off-line and the on-line world.

2nd Pillar: Usage Scenarios

We have analysed 18 usage scenarios which demonstrate typical workflows in different social contexts and which are relevant to a big population group. These scenarios show the practical relevance of identity management and identify requirements for IMS/IMA. We started with some basic identity-related scenarios like identity theft and data trails to give some ideas on the general problems in today's digital networks. These lead to **general scenarios** of multi-purpose IMA as PDAs, the identity protector concept, and the task assignment scenario to prepare the ground for more specific scenarios. One main part of the study was the examination of more concrete scenarios like **e-Commerce** (e-Shopping, e-Auction, e-Banking), **e-Government** (tax declaration, inquiry), e-Court (civil action, on-line mediation, criminal proceedings), e-Voting, **e-Health**, and some miscellaneous scenarios like e-Science (review process), e-Notary (e-Witness), and Location Based Services.

In each scenario firstly the current workflow for handling the concerned task is described. Then the role of identity management is elaborated, giving the benefits and explaining a possible integration – considering necessary **modifications in the traditional workflow** – of identity management functionality. We derived requirements from each scenario, focusing on the specifics of each scenario where we explicitly concentrate on the demands for identity management functionality.

The analysis of the scenarios results in the following:

- Most typical applications consist of logically separated **pseudonym domains** where any linkability of the user's personal actions can be avoided in order to provide maximum privacy. This may be achieved by separating distinct transactions, e.g., by using different pseudonyms for usage, payment, and delivery of goods. The concept of pseudonym domains can be used in all kinds of scenarios as a structuring method which shows the possibilities for identity management support with respect to pseudonyms.

- When designing and implementing identity management support for a workflow, the appropriate **types of pseudonyms** have to be used. Typical pseudonym properties may be, e.g., addressability by other parties, possibility of re-use, e.g., in order to built a reputation, limitation of validity, transferability to other persons, or the possibility to reveal the identity of the pseudonym holder by other parties under specific circumstances.

- There are scenarios where identity management and the detachment of pseudonym domains are already practised today (e.g., review processes). For some scenarios identity management could make the workflow more effective and could help to avoid media conversions while raising the **privacy level** (like tax declaration, e-Court, e-Voting). The implementation of some of the scenarios (e.g., tax declaration, e-Court) would require the prior adaption of national regulations.

3rd Pillar: Evaluating Identity Management Applications

We have sighted the presently known products for identity management, compiled a **list of the main products and prototypes** (88 entries), and tested some of them. Selection criteria for test candidates were whether the products are popular or setting trends, whether they were mentioned by the experts in the survey or whether they cover the aspects of the introduced so-called "operational areas", i.e., access management, form filling, automatic choice of identity, pseudonym management, and reachability management.

The **evaluated products** comprise Mozilla 1.4 Navigator, Microsoft .NET Passport, Liberty Alliance Project, Novell Digitalme, Yodlee, Microsoft Outlook Express 6 SP1, and CookieCooker. Additionally some **trend setting** products or prototypes were shortly described: ATUS, DRIM, Sun One, Digital Identity, Open Privacy, IBM WS-Security, and American Express Private Payments.

These products demonstrate the bandwidth of what current technologically supported identity management could mean. We have evaluated the Identity Management Applications according to requirements that are analogously used for describing consumer requirements in relation to ICT standardisation. These requirements were substantiated in form of a **grid of attributes** which comprises functionality, usability, security, privacy, law enforcement, trustworthiness, affordability, and interoperability.

In general we can distinguish between **centralised** identity and **federated identity**: Centralised identities are provided by a central IMS provider which acts like a single gateway for the user's management of identities. Federated identities have multiple IMS providers. As there is no concentration of personal data outside the users' scope, users have more control over what personal data they share with whom. Federated identity management puts bigger responsibilities on the user and can mean more effort in user support. In contrast to that, centralised identity management is easier and cheaper to maintain, but the single point of control also means a single point of failure and an attractive target for attackers.

The evaluation of Identity Management Applications according to the grid of attributes results in the following:

- The available products and prototypes vary in **functionality range and maturity**. This indicates that the business models for IMA and the academic perception of this topic have not yet been solidified, but are still pliable.

- None of the evaluated products meets all elaborated criteria. There are especially significant **deficiencies** regarding privacy, security, and liability functionality. Applications which try to address such functionalities reveal usability problems.

- Many products rely on the centralised identity model which offers less control by the user, but is easier to implement and to maintain. It will be a **question of trust** whether users might agree to the involvement of central identity management providers or prefer to manage their identities on their own.

The building blocks for a multi-purpose Identity Management System, that will take security and privacy criteria into account, seem to exist at least on a conceptual level. Still there are some **open research questions** – not only in the technological, but also in the legal and socio-economic fields.

The overview of Identity Management Applications reveals an advantage of the US in the field of distributed products, whereas the European Union scores especially regarding innovative identity management concepts, fitting into the legal and cultural EU framework. The study highlights **EU capacity** to transform those concepts into marketable solutions. Privacy seals could help to tag those IMA which implement privacy-enhancing concepts and are compliant to law, e.g., the European Data Protection Directive.

4th Pillar: What do experts think on IMS?

During this study a survey on IMS was conducted. The developed questionnaire was answered by **89 experts world-wide** from research, business, administration, and data protection authorities. Most of the experts who answered came from a European background. Nearly half of the experts were researchers at universities or companies. In the perception of most of the

answering experts, Identity Management Systems are rather the subject of a predominantly technologically oriented research than already real products. IMS is still a research topic where concepts or visions are being discussed. However, a few of the experts understand a privacy-reflecting dealing with standard communication software as technology-based identity management. An extensively fixed paradigm of what makes and includes an IMS has obviously not yet gained general acceptance.

The main results of the survey on Identity Management Systems (in the meaning of "Applications") show:

- So far there is no generally accepted paradigm of IMS. Nevertheless, experts predict a good marketability of IMS after a period of **10 years'** time.

- As the main obstacle to proliferation of Identity Management Systems we have identified not pure technology factors like, e.g., insufficient security, but **socially related factors** such as insufficient usability and slow standardisation.

- Privacy protection, security, and usability consistently receive the highest scores from the experts as **essential functions** of IMS.

Conclusion

This study shows that a user-controllable IMS is plausible and probable from a sociological perspective, already possible as of today on a basis of Europe-wide regulations, and technically presumably copeable. Considering the use of IMS in fields of operation such as e-commerce and e-government by means of future scenarios, we conclude that many workflows would work more effectively based on IMS while integrating a better privacy level than up to now. The evaluation of currently available applications and studies of concepts respectively prototypes of identity management anticipates the path which technological development will pursue. Thereby experts expect complicated usability of Identity Management Applications, an inadequate level of computer security and privacy, and also lengthy standardisation processes as main bottlenecks for developing a society-wide Identity Management System.