The e-Government digital credentials

Flavio Corradini, Eleonora Paganelli*
and Alberto Polzonetti

DMI University of Camerino,
Via Madonna delle Carceri 9, 62032 Camerino, Italy
E-mail: flavio.corradini@unicam.it
E-mail: eleonora.paganelli@unicam.it
E-mail: alberto.polzonetti@unicam.it
*Corresponding author

Abstract: Digital identities, profiles and their management enable online interactions and transactions among people, enterprises, service providers and government institutions. In this paper, after having examined the European identity management policies, we explain the differences between digital identity and digital citizenship and introduce digital credentials. We also discuss how an identity management framework, composed by shared and standardised services supporting authentication procedures, can change within the e-Government domain. The paper concludes by outlining future trends and the potentiality of the extended digital identity in both public and private sectors.

Keywords: digital identity; e-service; digital credentials; anonymity; pseudonymity; e-Government; identity management framework; data protection; authentication; authorisation.

Reference to this paper should be made as follows: Corradini, F., Paganelli, E. and Polzonetti, A. (xxxx) 'The e-Government digital credentials', *Int. J. Electronic Governance*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Flavio Corradini is Full Professor of Computer Science at the University of Camerino. His research interests are centred around design methods, formal and semi-formal specification and verification of complex software systems, e-Government and Information Society. He is the coordinator of 'UEG – UNICAM e-Government research group' and 'COSY – Complex Systems' research group. He collaborates with several IT companies and public administrations and coordinates research projects for the diffusion of digital identity through a national service card.

Eleonora Paganelli got a Master Degree in Computer Science at the University of Camerino. Her research interests are centred around e-Democracy and trust and identity management. She is a member of 'UEG – UNICAM e-Government research group' of the University of Camerino and project manager of 'e-Lios – e-Linking on-line systems' a company active in the area of IT innovation of public administrations and small and medium enterprises.

Alberto Polzonetti is Assistant Professor of Computer Science at the University of Camerino. His research interests are centred around computer networking, e-Government and Information Society. He is a member of

'UEG – UNICAM e-Government research group' and coordinates several projects regarding network infrastructures, broadband initiatives, AAA, peer-to-peer systems and web service technologies.

1 Introduction

Most people are registered in hundreds if not thousands databases scattered across disparate systems. In identity management jargon, individuals have multiple *network identities*: collections of information that relate to an individual, that are created and managed as single units in a network, and that are stored in electronic form. Advancements in networking technologies make it increasingly easy to collect and compare these network identities.

Of course, this crossdomain aggregation power by itself is not of much value to organisations, unless it is combined with the ability to determine which network identities correspond to the same individual. Traditionally, identifiers such as health insurance numbers and Social Security Numbers serve as keys to facilitate such crosslinking. The current efforts in the electronic world to enable crossdomain identity management and information sharing rely on their own unique crossdomain identifiers, such as biometric templates and digital certificates.

For businesses, an increase in crossdomain linking power ultimately translates into increased sales and cost reduction. For government organisations, the ability to share client information translates into more efficient interactions with citizens and an improved ability to detect and contain fraud.

This paper focuses on the concept of an extended digital identity in e-Government field. In the next section, we provide a brief overview of Digital Identity Management European trends. In the third section is underlined the need for a digital identity and how to pattern it by an Identity Management model. The fourth section analyses the extended digital identity in the perspective of an e-Government identity Management Framework. Finally, concluding remarks are given in Section 5.

2 eIDM at pan-European level

Before starting to analyse the problem of a Digital Identity Management from a technical point of view it could be useful to have a look at Privacy and Identity European Union (EU) policies.

In all EU members, the e-Europe 2005 action plan (European Commission, 2005) stresses that e-Government identity management in the EU should be advanced by addressing interoperability issues as well as future needs, without ignoring differences in legal and cultural practices and the EU framework for data protection.

In all EU Member States, several initiatives are underway to introduce electronic Identities (eID) for public services. While often used interchangeably, these notions are usually not defined clearly enough. For the purposes of this paper, 'identification' should be taken to indicate the process of using claimed or observed attributes of an entity to deduce who or what the entity is. 'Authentication' is the validation of the claimed identity of an entity and a set of its observed attributes. Thus, identification in general

refers to a process of deduction based on a set of information allowing to determine who a given person is (with different degrees of reliability); while authentication implies that a decision is made based on the actual corroboration of information, implying a larger degree of dependability.

A range of different approaches and solutions has been proposed to address shortcomings inherent to crossborder electronic Identity Management (eIDM) approaches (e.g., federated vs. centralised (Bhargav-Spantzel et al., 2006), driven by public or by private sector, different degrees of information assurance, different choices to trade-off between privacy and convenience).

While this diversity is an inevitable and often desirable outcome of the Member States' principal competence in this field, it also complicates matters for any entity (e.g., citizen, business or administration; collectively referred to as the 'user' of any given eIDM system) that desires to communicate with administrations outside the scope of its own local eIDM system. In such circumstances, there is a need to be able to connect the eIDM system from a local jurisdiction to a public service provided outside the scope for which the system has been designed. In short, there is a need for an interoperability framework to address eIDM requirements at an EU level.

In the e-Government action plan, adopted by the European Commission on 25 April 2006, the following commitment was made to this end (European Commission – IST, 2005):

> "The Commission, in cooperation with the Member States, will pursue policies to grant safe access to services EU wide. When citizens travel or when they move they want easy access to services. EU governments have agreed to facilitate this process by establishing secure systems for mutual recognition of national electronic identities for public administration websites and services. The Action Plan foresees a full implementation by 2010. The Commission will help make this happen by supporting wide-scale cross-border demonstrators, identifying common specifications for electronic ID management during 2007 and by reviewing the rules of electronic signatures in 2009."

Public services can be offered only within an environment where trust and confidence flourish. Such environment should always guarantee secure interaction and access for citizens and businesses.

Protection of personal data, authentication, and identity management are primary issues where no public service should ever fail. Public institutions should always ensure that digital transactions and communications are secure and that personal data will remain protected.

Citizens should always be able to control access to their personal data, and how these data have been stored, used and accessed. Failure to ensure this may, in addition to breaching the law, entail significant social and economic costs. Only data that are necessary for the fulfilment of the respective purpose may be collected (European Commission, 1995). To this end, the use of privacy-enhancing technologies should be favoured.

Privacy-enhancing technologies in e-Government should be promoted through the relevant EU programmes.

Data protection, network and information security, the fight against cyber crime and dependability are prerequisites for a properly-functioning information society, and consequently core policy issues within the EU. The Commission together with the Member States has launched a comprehensive strategy for these issues.

A range of R&D projects, supported by the EU Sixth Framework Information Society Technologies (IST) programme and the Sixth Framework programme address these issues (FP6/IST, 2006).

For network and information security the rapid adoption of the European Network and Information Security Agency, now on the table of Council and European Parliament, will be an important step forward. The new EU Seventh Framework Programme (FP7/IST, 2007) reserves a particular topic on Identity Management within the "ICT Challenge 1: Pervasive and Trusted Network and Service Infrastructures, management and privacy-enhancing tools". The result of these EU policies should be the empowering of the ICT users to handle their digital identity and personal data and to protect their privacy.

Identity management in the EU should be also advanced by addressing interoperability issues as well as future needs while taking into account differences in legal and cultural practices and the EU framework for data protection. Council conclusions on e-Government, invite the Commission and the Member States to comply to the following action guideline:

> "By 2010 there will be seamless online access to major public services for citizens and business across Europe with the help of interoperable electronic identification and authentication." (CEN, 2000)

This is a significant assertion that attests the EU will to improve digital identity management policies.

3 Digital identity

There is currently no general agreement on a definition of the term 'digital identity'. We will first of all discuss digital identity in a narrow sense that reflects the concept that is implemented in most of today's information systems (Camp, 2004). In this sense, a digital identity is commonly considered as the machine-readable representation of a human identity. It is used in electronic systems for interactions with local or remote machines or people. The purpose of a digital identity is to tie a particular transaction or a set of data in an information system to an identifiable individual. With the help of a digital identity, a user can be identified and authorised to use a given resource or service.

Before a digital identity can be used, it must be established between a user and an organisation. In today's applications (e.g., free e-mail services), this is commonly done by a registration process that creates a digital identity for the user. This implies that the same user can have several digital identities for different digital services.

3.1 The need for digital identity

When the need for digital identity is arisen? The growing mismatch between the security needs of crossdomain identity management and traditional security tools and practices is not all that surprising. The currently prevailing authentication techniques (password only, biometrics, Kerberos and PKI) were all invented more than two decades ago, when open networks were hardly existent, let alone organisations seeking to securely share identity-related information over such networks. At that time, privacy legislation was virtually non-existent. The only privacy protection that the designers of the traditional

security techniques had in mind was protection against unauthorised outsiders (e.g., wire tapping). In the new frontier of crossdomain access and identity management, however, the biggest threats to privacy do not come from outsiders, but from insiders (Goth, 2005).

To better understand the shortcomings of PKI and other authentication mechanisms that were not designed with crossdomain identity management requirements in mind, it is important to understand the relation between (information) security and privacy (Housley et al., 1999). *Security* is generally defined as "the extent to which information can be stored and transmitted in such a manner that data access is limited to authorised parties". *Privacy* is generally defined as "the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others". In accordance with the Fair Information Principles of the OECD (2006) (which form the basis of most of today's data protection legislation around the world), 'security safeguards' is only one of the eight principles necessary to achieve privacy. In contrast to security, which is aimed at preventing access by unauthorised outsiders, the other basic privacy principles are primarily aimed at unauthorised use by insiders. As such, security safeguards are necessary to achieve information privacy, but not sufficient. Ironically, traditional authentication technologies have a highly adverse impact on two of the most important privacy principles: collection and use limitation. They are, in fact, privacy-invasive technologies.

The purpose of a digital identity is to enable access control functionality and to tie a particular transaction or a set of data in an information system to an identifiable individual. With the help of a digital identity, a user can be identified, authenticated and authorised to access a given resource or service.

The concept of digital identity emerged with the general availability and adoption of the internet technologies that paved the way for new methods of conducting transactions (Camp, 2004). In electronic business (e-business) and electronic commerce (e-commerce) as a part thereof, the internet was leveraged to conduct business in general or marketing and sales, respectively. In electronic government (e-Government), the new technologies can be used in the public sector for the interaction between authorities and citizens, businesses or other authorities (Clemens and Maibaum, 2001).

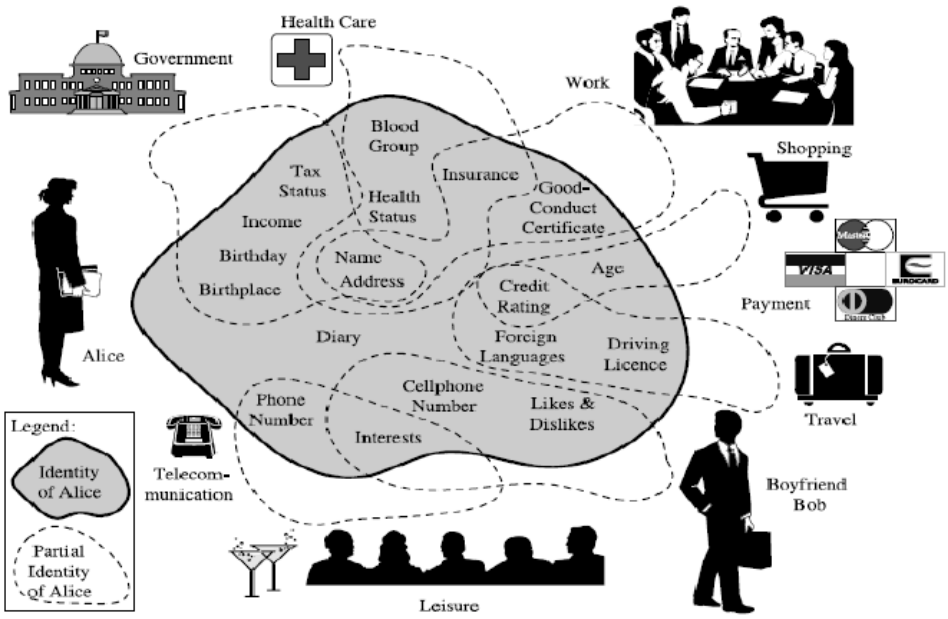
When services are delivered over the internet through e-business, e-commerce and e-Government, the concept of digital identity is needed in the following contexts:

- *Restricted access*. In many cases, access to services or transactions is restricted to certain individuals. A digital identity is thus needed to identify a user and then determine if access can be granted or must be denied.
- *Accountability*. If the accountability of the participants is to be ensured in a transaction, it is necessary to establish a user's identity.
- *Personalisation*. A very powerful aspect of e-business, e-Government, and particularly e-commerce is an improved Customer Relationship Management (CRM). In an internet environment, an organisation can easily tailor its services and offers to the customer's preferences. If organisations know the profiles of their customers, they can adopt one-to-one marketing practices.
- *Reputation*. In some applications (e.g., online marketplaces and auctions), users want to establish a reputation for themselves. This is only possible if an individual can be recognised by others in a later transaction.

In order to better satisfy the needs for a digital identity made up of a multitude of facets, we must abandon the narrow definition previously introduced.

A broader definition of digital identity (Kohntopp and Pfitzmann, 2001) subsumes all personal data of an individual under this term (Figure 1). The subsets of these data represent partial identities of an individual. Some of these partial identities (such as credit card numbers) uniquely identify a person, whereas others (such as an individual's citizenship) do not. Users present these partial identities depending on their situation or context. Individuals may for example show a different partial identity to their employer than to the tax authorities. The tax authorities will be entitled to know about a citizen's financial situation, whereas the employer will not. By disclosing only partial identities to organisations, users can define how much information is available to whom.

Figure 1 Partial identities of an individual



3.2 A concept for an extended digital identity

Numerous European countries are engaged in projects for digital citizen cards. Today's generation of digital citizen represents information related to the identity of the holder mostly with X.509 certificates. Chapter two has introduced some of these citizen card projects. All current cards contain two key pairs, one for the identification of a citizen and another one for issuing digital signatures. The goal of a strong identification is at the heart of this approach. In their nature, most of these cards are static and do not allow the addition and management of further information to model a citizen's identity.

Once these two certificates are stored on the card, the digital identity of the citizen is fixed. The current approach is thus static in nature.

The current cards that are to be used in public and private sector services pose the danger that a cardholder's transactions can be easily linked and that transactions will increasingly necessitate an identification of the cardholder.

An extended digital identity in e-Government domain needs the introduction of new elements to the digital identity of the citizen and thus provides scope for new applications of citizen cards. The major enhancement is that the concept comprises privacy-enhancing technologies. Pseudonymous credentials are introduced as part of the citizen's digital identity. Cards that comprise credentials can be used to deliver e-services anonymously or pseudonymously (Camenisch et al., 2006). From a data-driven perspective, the concept includes new data elements to model the citizen's digital identity. From a functional perspective, it proposes new functionality for digital citizen cards. Concerning the infrastructure for smart card-based solutions, this approach requires additional system components.

In this approach, the citizen's digital identity comprises the following elements:

- authentication certificate
- signature certificate
- attribute certificates
- privacy Preferences Profile document (P3P profile)
- pseudonymous credentials
- digital documents.

Most importantly, anonymous credentials are added to the digital identity as an anonymous element (Camenisch et al., 2006). Credentials enable the citizen to demonstrate attributes in an anonymous manner and to access services without disclosing their identity. By use of credential technology it also becomes possible to split identity-related information into a set of smaller statements that may be shown independently of each other. The inclusion of credentials as an anonymous element in the digital identity constitutes a form of Privacy-Enhancing Technologies (PET) on the citizen card. There are currently no citizen cards that integrate privacy-enhancing technologies. Introducing new elements to the citizen's identity also necessitates the introduction of new functionality to address the management of these elements.

We propose the following set of functionality for a device that manages the digital identity:

- authentication, encryption and signature capability
- storage of P3P profiles
- storage of digital documents
- credential management functionality
- identify information management functionality.

Authentication, encryption and digital signature capability are standard features of today's digital citizen cards. The approach thus introduces three new management functionalities to citizen cards. The card serves as a bearer for P3P profiles that may be used in conjunction with any P3P-enabled web browser. The card also manages the citizen's anonymous credentials (Camenisch et al., 2006). As third innovative element, the approach incorporates identity information management functionality on the card.

3.3 Digital credentials

Similarly to the Digital Identity, the digital credentials are signed statements concerning attributes of a subject. A digital credential serves the purpose of communicating a statement made by a third party about a subject in a trustworthy manner.

As such, credentials constitute a form of digital identity and can be used in distributed settings to establish trust.

According to the definition by Herzberg and Mass (2001), a digital credential is a statement by an issuer on some properties of the subject of a credential, that is digitally signed by the issuer and that is presented by the subject to relying parties. In a digital setting, the party that issues a credential is called the credential issuer. The party that accepts a credential is called the relying party (or verifier). A great variety of credential types exists in the digital world. Examples for digital credentials include:

- *Public-key certificates*. Public-key certificates bind a public key to a subject. They make the public key of an entity available to other parties in a trustworthy manner. Public-key certificates contain (in the least) a public key, the name of a subject, a serial number and the signature by an issuer over that data. A well-accepted standard for the format of public-key certificates is the ITU-T X.509 standard.
- *Attribute certificates*. Attribute certificates bind arbitrary attributes to a subject. Attribute certificates contain (in the least) attributes, a reference to a subject and a signature by the issuer over that data. The reference to a subject is established by including the serial number of the subject's public-key certificate. Attribute certificates are intended to communicate information other than public keys in a trustworthy manner. The X.509 standard also addresses the format of attribute certificates.
- *Digital documents*. Digitally signed or otherwise authenticated documents can be used to express statements about an individual. Examples for such documents are a digital vaccination card or a digital driver's license. Individuals can be authorised to access e-services on the basis of such digital documents. Often, database records are represented by XML and are digitally signed in order to provide trustworthy information about an individual.
- *Anonymous and pseudonymous credentials*. An anonymous or pseudonymous credential serves the purpose of conveying attributes related to a subject without disclosing an identity. A pseudonymous credential binds attributes to a pseudonymous identity while an anonymous credential conveys attributes only. Credentials can contain arbitrary attributes and constitute an anonymous form of digital identity.

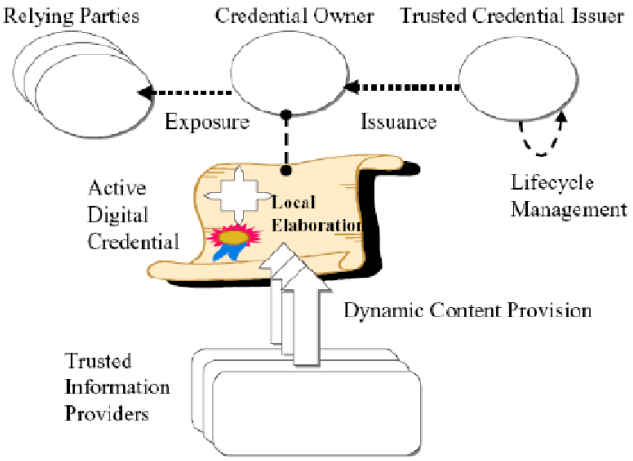
3.3.1 Active digital credentials

The concept of active digital credentials (Casassa Mont and Brown, 2002) has been investigated as a mechanism to extend traditional static digital credentials by providing means for dynamically updating their content along with the assessment of their trustworthiness.

The main goal is to provide enterprises and people with certified and up-to-date data, specifically identities and profiles information to boost trust during internet relationships and transactions, provide accurate data to be used for access control and decision-making purposes and simplify the overall life cycle management of digital credentials.

Figure 2 shows our high-level model of active digital credentials. In contrast with traditional digital certificates – which have static content and a predefined period of validity – active credentials embed certified mechanisms and algorithmic procedures to dynamically retrieve, calculate and update their content and check their current level of trustworthiness and validity. This includes dynamic evaluations of: values of credential attributes (including credit card numbers, credit limits, expiration dates, references, etc.); validity and trustworthiness of these attributes; validity and trustworthiness of the whole digital credential.

Figure 2 High-level active digital credentials model



This method is based on a late binding of values associated to credential attributes. A key aspect of active digital credentials is that not only they provide certified mechanisms to retrieve their up-to-date content, but they also contain mechanisms to perform local elaboration of this information. Credential issuers certify the trustworthiness of these mechanisms: the relying party uses them to obtain up-to-date information from trusted sources and evaluate their trustworthiness and validity (Herzberg and Mass, 2001). This contrasts with traditional approaches, in which the credential issuers only certify the trustworthiness of data. A local interpretation of active digital credentials (at the relying party site), by using an execution framework, ensures that specific security and privacy requirements are satisfied and that the interactions between the involved parties happen in a predefined and controlled way.

The work on active digital credential is ongoing. A prototype is under construction including mechanisms to represent credentials (including attributes and procedures), issue and evaluate them. Further research needs to be done to understand the complete set of requirements for the underlying infrastructure and the implications in term of life cycle management. We are planning for real-life experiments in order to judge the benefits brought by this approach and compare them to traditional PKI systems.

3.4 Basic requirements for the use of credentials in e-Government

This section discusses basic requirements that must be met in order to deploy anonymous and pseudonymous credentials as part of the citizen's digital identity. This list states requirements at a high level of abstraction and is not intended as a detailed requirements specification. We state the following basic requirements (Auerbach, 2003):

- *Storage of credentials in a device under the user's control*. Credentials should be stored on a device that the citizen can carry along rather than on a server that makes credentials accessible over the network.
- *Smart card as a tamper-proof storage*. The digital identity of the citizen should be stored on a tamper-proof device in order to minimise the risk of identity theft (Arnold, 2000) and comply with legal regulations for digital signatures. Also, a tamper-proof environment is the safest way to prevent the transfer and lending of credentials.
- *Citizen card as anonymous bearer of the digital identity*. If a card is to act as an access device for anonymous services, the card itself must not leave identifiable traces upon insertion into a card terminal.
- *Nontransferability of credentials*. Citizens should not be able to transfer or lend their credentials to other citizens. The property of nontransferability is best achieved by use of a tamper-proof storage device.
- *Support for anonymous and pseudonymous transactions*. Both anonymous and pseudonymous credentials should be supported. In some e-Government applications, it may be important to personalise services for citizens. Personalisation in anonymous settings is possible by use of pseudonyms.
- *Support for unlinkable multishow credentials and one-show credentials*. A credential system for e-Government should support both one-show and multishow credentials. Citizens should be able to show their credentials to many different service providers without transactions becoming linkable. Multishow credentials should also be constructed in a way so that citizens do not have to recertify them after every use. For some scenarios, one-show credentials are necessary. A one-show credential is used to model rights that can be used only once. For instance, a citizen on low income may have the right to one free consultation with a counsellor within 1 month. Such a right can be implemented with a one-show credential that is valid for 1 month. A citizen can then freely choose when to use the credential (within the 1-month period) but cannot use the credential (and thus the associated right) more than once.
- *Use of credentials over the network and in local settings*. Citizens should be able to use their credentials in internet-based transactions. Notwithstanding, credentials should also be available in local settings where a citizen demonstrates possession of a credential at the point of service provision (e.g., at the local library or a sports facility).
- *Traceable anonymous transactions*. In order to embrace a service provider's need for security, credentials should implement a revocable form of anonymous identity.

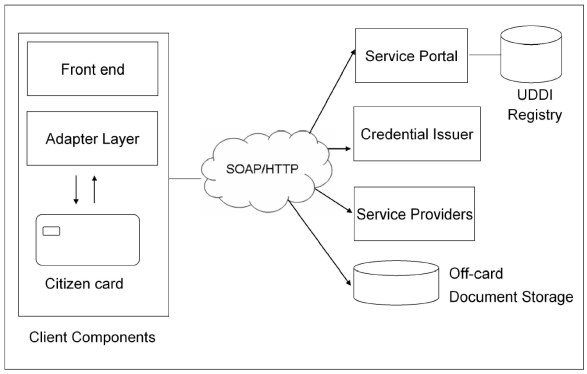
- *Anonymous communication infrastructure*. System components are interconnected by a middleware based on web services. The middleware must allow for anonymous communication channels in order to provide anonymity at the application level.
- *Offline storage to augment the citizen card's capacity*. Citizens may accumulate many credentials and digital documents over time. Documents that are infrequently used should be kept on a server accessible via internet. Similarly, credentials that have expired should be archived in a secure network-based storage space.
- *Audit trail for citizens*. Any access to an element of the digital identity should be logged by the card. The citizens should be able to inform themselves what information concerning the identity was provided in a transaction. This feature also helps to discover unauthorised access to identity elements.
- *High degree of usability*. Despite the use of a rather complex technology such as pseudonymous credentials, it is an important goal that credential-based services are nevertheless easy to use. If the handling is complicated, there is the danger that users bring themselves at a disadvantage through lack of understanding of the user interface. Also, lack of usability poses the danger that users will not embrace credentials.

These requirements have a direct impact on the architecture of a credential-based system. The next section presents the architecture components that support the concept of the extended digital identity.

3.5 Overview of the architecture

The concept for an extended digital identity introduces pseudonymous credentials as a privacy-enhancing technology on the citizen card. As compared to the infrastructure of current identity card projects, this approach to digital identity requires changes in the infrastructure for card-based services in order to support the use of pseudonymous credentials. The citizen card must be equipped with a credential manager that manages the life cycle of credentials. Both public and private sector organisations may act as issuers or as relying parties and thus need additional infrastructure components. This section provides an overview over the architecture for the use of credentials in e-Government. Figure 3 illustrates the architecture components.

Figure 3 Overview of architecture components



The architecture comprises the following components:

- *Identity manager on the smart card*. This component is installed identity. This includes the handling of pseudonymous credentials. This component also keeps track of how elements of the digital identity are used (identity information management). The card acts as representative for the citizen and as a manager of the life cycle of all pseudonymous credentials that the citizen owns. The card acts as an anonymous barrier for the identity of the citizen. The card must not contain a publicly readable card number or a publicly readable data set. The card is also used as an access key to the off-card storage facility.
- *Off-card storage for documents, credentials and audit data*. Smart cards have a very limited storage capacity. Today's smart cards feature about 64 KB of memory, which may not be enough to store all administrative documents and credentials that a citizen accumulates over time. A secure off-card storage extends the memory of the card and stores identity elements that have expired or that are rarely used (archival functionality). Similarly, the log files that track identity usage can be moved to the off-card storage periodically to free precious memory space on the card.
- *Credential issuers*. Both private and public sector organisations issue credentials to citizens. Issuers of credentials must therefore add infrastructure components to handle the issuing process and keep track of issued credentials. The issuer needs to maintain a high level of security, as unauthorised users should not be able to obtain credentials. A credential issuer publishes a list that details the type of credentials that an organisation issues. Credential issuers need to handle the registration and issuing process for credentials and administer credential revocation lists where necessary (Camenisch and Lysyanskaya, 2001). An organisation can both act as a credential issuer and offer credential-based services.
- *Service providers (relying parties)*. Both private and public sector organisations may offer services that can be accessed anonymously by use of credentials. The paradigm of credential-based service access necessitates additional software components. Service providers need to be able to establish trust based on credentials. They have to decide which credential issuers to trust and which credentials to accept. They also need to be able to establish the validity of credentials.
- *Middleware to interconnect components*. A middleware based on web services interconnects the components of the architecture. More specifically, the middleware supports all credential-related protocols (issuing and showing credentials) and the communication between citizen card and off-card storage. In order to preserve anonymity, anonymous service must be accessed through an anonymous communication channel.
- *Anonymous communication infrastructure*. Anonymity at the application level necessitates anonymous communication channels. Anonymity at the network level ensures that service providers cannot trace a communication back to a specific IP number of the user's machine. Such communication channels can be achieved, e.g., based on mix networks. Front end and adapter layer: on the client side, three components are deployed: the citizen card, an adapter layer and a front end. Citizens access services with the front end, which can be a proprietary client application or a web browser. An adapter layer serves as interface between client software and the citizen card. The adapter layer also provides integration with the middleware.

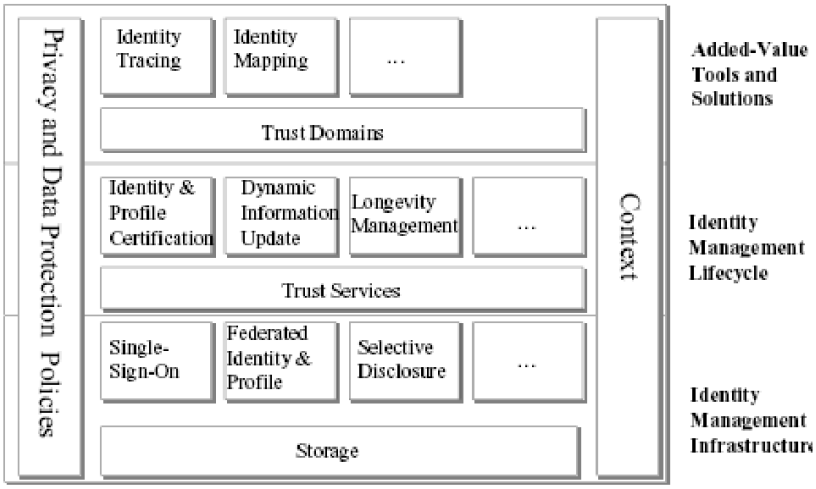
- *Service portal and service registry*. We presume that a service portal exists that serves as a single point of entry for e-Government services. The service portal helps citizens to discover services that are useful for them. The portal can be associated with a UDDI (Universal Description, Discovery and Integration) registry where descriptions of web services are published. This component serves the purpose of service discovery and is not specific to credential technology.

3.6 Identity management model

Identity management solutions must cope with this 'distributed' nature of identities and profiles and address the issues described in the previous section (Damiani et al., 2003). The emerging solutions are likely to be pervasive, in the sense that they are going to involve all the stakeholders: identity owners, identity providers, enterprises, relying parties, governments and other third parties.

In our vision identity management solutions are modular and composed of multiple service and system components, to address the new administrative and operational challenges. Components include infrastructure components, identity management life cycle components and added-value tools. Figure 4 shows our high-level model for identity management solutions, as an attempt to capture the relationships among relevant identity management components.

Figure 4 Identity management model



Infrastructure components underpin operational aspects of identity management. These components include mechanisms for authentication, authorisation and single-sign-on. Authentication and authorisation components are in charge of authenticating entities and granting rights depending on policies and involved risks. Those modules are critical as they check the validity of identities, their trustworthiness and allow entities to access resources and services accordingly. They have a direct effect on the perception that users have of the reliability and trustworthiness of providers of services.

The current trend towards federation of identities for distributed services, both on the internet and across enterprises and organisations, on one hand provides new business opportunities to users and service providers but on the other hand it introduces newt threats. Single-sign-on components, allow entities to authenticate once and access services supplied by multiple providers. Hackers or third parties can take advantage and misuse this process. These components have a direct impact on the liability that organisations have with their customers and other parties that rely on the supplied identity information. They need to be secure and compliant with privacy laws and data protection legislation.

In this context, it is important that identity management solutions provide mechanisms that allow identity owners (or trusted third parties acting on their behalf) to express their preferences and policies in term of privacy management. These mechanisms should allow a selective disclosure of identity information according to the policies expressed by their owners.

In general, infrastructure components rely on judgements and decisions made both at the time of the assessment and certification of identity information and during their overall life cycle management.

Identity management life cycle components are necessary to provide mechanisms for the assessment, creation, certification and evolution of identity information over short, medium and long periods of time. Specifically, certification components include processes to assess and certify identities, depending on their authenticity, nature, purpose and provenance.

Auditing tools need to be deployed to collect data about actions and decisions made during the execution of these processes and provide evidence about due diligence.

Life cycle management components also must deal with the dynamic evolution of information associated to identities and their trustworthiness. Identity providers (or certification authorities) are accountable and responsible for the identity information they provide to third parties: this information needs to be up-to-date and trustworthy.

Obsolete or compromised information might provoke financial and social losses and cause identity providers to be legally and financially responsible.

In the short term, specific life cycle-management components are in charge of retrieving up-to-date identity information from trusted sources, periodically evaluate their validity and trustworthiness (as dictated by policies) and revoke compromised data. In the medium and long term, those components are responsible for longevity maintenance of digital identities: this can be achieved by tracking the evolution of identities and associated profiles overtime. Evidence is created and collated each time identity information are modified or renewed. This information need to be stored in distributed and fault-tolerant systems to preserve its survivability and integrity over long periods of time.

In general, the overall management of identities is quite complex because of the fragmented and increasingly distributed nature of identity information.

Added-value identity management components are required to simplify the operational usage and management of identities and to make sense of laws and legislation.

Specifically, in our vision, organisations will use tools to cope with the administration of distributed and heterogeneous identities in increasingly more and more dynamic and boundaryless environments. These tools manage aggregations of multiple identities owned by the same entities, according to privacy and data protection policies (dictated by

identity owners, trusted third parties or organisations) and help administrators to visualise this information along with the associated policies. By better understanding identities, their interrelationships and the implications of their usage, organisations will have more visibility of the requirements and constraints they need to be compliant with and the effects that those requirements have on their businesses.

Along the same line, identity-tracing tools are added-value components that help organisations to administer and keep under control chains of disclosures of identity information that they manage on behalf of their owners.

This applies, for example, to identity providers or enterprises involved in B2B context, during single-sign-on processes or interorganisational interactions. Tracing tools help administrators to keep track of which information has been disclosed to whom and the compliance of those disclosures to privacy requirements and business policies. In case of a federated identity framework (Bhargav-Spantzel et al., 2006) these tools may rely on trusted platforms, messaging mechanisms for the notification of the requests to disclose identity information and the communication of authorisation decisions. Evidence collected during those interactions is used for auditing and forensic investigations, in case of identity thefts or frauds.

The understanding and monitoring of the compliance of identity management solutions to requirements, policies, privacy and data protection laws make organisations more accountable and trustworthy.

Some of the components described above (including identity mapping, tracing and mechanisms for selective disclosure of information) might be installed and run locally, within users', employees' or consumers' resources (PCs, PDA devices, next generation mobile phones, etc.) to help them to manage and monitor their identities (and profiles) and actively control their usage. Privacy, data protection and business policies must drive the behaviour of identity management components. As the accountability of the identity managers is dictated by the fulfilment of identity owners' requirements and the evaluation of involved risks and laws, these components need to adapt their behaviours accordingly, depending on the context where identities are used and the purpose by which they are used.

Policy-driven engines and rule-driven authorisation systems are mechanisms that can be used to enforce contextual privacy and data protection policies. They are at the very core of many of the components described above (Woerndl, 2004).

4 Identity management issues

The management of identities involves issues at the organisational, technical and legislative level (Claub and Marit, 2001). This section describes a few important related issues and introduces high-level requirements for identity management solutions. As a provisional example, we can consider the issue of managing authorities (MODINIS IDM-Consortium, 2006):

- From an organisational perspective, the system designer needs to decide which authorisations are required in the system, who may give and hold them, and what they mean.

- From a technical perspective, the system designer needs to decide how to model this into his system, e.g., by creating a central authorisations database, or through referrals to related trusted systems; as well as who may manage the authorisations (e.g., the technical aspects of issuing/revoking authorisations) or how their validity should be checked before an authorisation could be exercised.
- From a legal perspective, the system designer needs to be aware of the legal requirements for authorisation (does it require a written contract, signatures, acceptance of the receiver, etc.) as well as crossborder aspects (i.e., is the authorisation valid in the country where it is given, where it is received, where it is exercised, etc.).

It is important for identity management solutions to deal with the authenticity of identity and profile data. The provenance and credibility of these data has a direct impact on the overall perception of trust and the consequent willingness of people or enterprises to engage in business relationships and commercial transactions. This has strong implications on the mechanisms and solutions that are put in place to assess and certify identity and profile information.

The importance and impact of the authenticity of this information is directly proportional to the involved risks and the overall value of the transaction. In low-value e-commerce transactions the process of checking the authenticity of identity-related information, like credit card numbers, might be relaxed, because of other mechanisms underpinning the business model, for example, based on credit card insurances. In case of more important and valuable e-business transactions, obsolete or compromised identity information may have huge implications for a party engaged in these transactions, possible provoking financial and social losses. Trust and trust management play a key role in this space (Blaze et al., 1999). A common way to address authenticity and provenance issues is to rely on trusted third parties to assess, certify, verify and potentially revoke identity and profile information. Trusted third parties commonly include entities such as certification authorities, consumer organisations, business associations, etc. For example, Identrus (Identrus, 2002) has been created in the banking environment to provide a B2B and e-commerce trust framework, which includes mechanisms based on PKI to deal with authentication, confidentiality, nonrepudiation and integrity of identity information (Housley et al., 1999). The current trend is towards the provision on the internet of trust services, which deal with various aspects of trust and are accountable for the services they provide. Those services provide not only certification and management of identity information but also their verification, recommendation, credit rating, notarisation, trusted auditing and trusted storage.

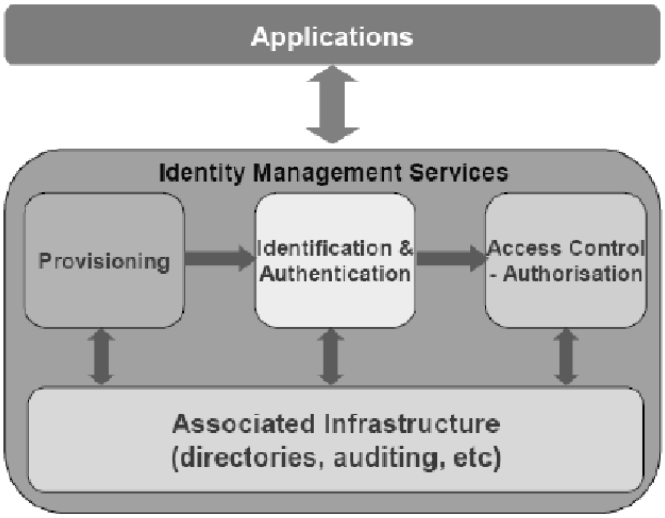
4.1 The e-Government identity management framework

If we would schematise the concept of an Identity Management Model we can introduce a possible Identity Management Framework. The framework collects a set of generic Identity Management services grouped by different categories hereunder described (see Figure 5) (PRIME, 2006).

The first category is the provisioning. With this term we mean the authority that releases the digital citizenship and it is composed by several services (Lenk and Traunmuller, 2000; Claub and Marit, 2001):

- Identity creation service; e.g., Registration Authorities able to verify and validate identity information in order to issue new digital identities. There may well be different registration 'levels'. The creation of an identity will normally involve the subsequent issuing of credential(s) to the requesting entity, for future authentication.

Figure 5 Identity management framework



These services may allow for Pseudonymity (Chaum, 1990):

- Identity Attribute input service; providing a level of verification for applications providing identity data
- Enrolment service; providing entities with the authorisation levels needed to use particular e-Government services
- Dissemination service; enabling the automated dissemination of new or changed identity data to all legitimate holders of such data.

The second category includes all the authorities that operate as authenticators and it provides the following services (Belanger and Hiller, 2006):

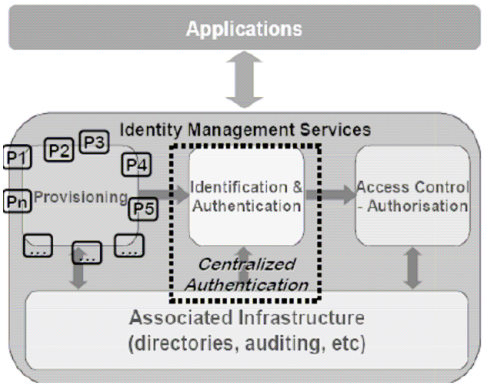
- Authentication service; e.g., password authentication service, PKI-based services and various biometric authentication services.
- Many authentication mechanisms are developed such as Identification (or Knowledge-Based Authentication) involving knowledge of one or more identity attributes, not necessarily secret; Credential-Based Authentication (or Shared Secret), typically involving username/password or certificate/PIN pairs or shared secrets; Token-Based Authentication – a special case involving a hardware token (smart card or SecureID) containing any of the above identity data (Auerbach, 2003).
- Single Sign On; that is, the services required to enable a principal, having authenticated in one system/application to use another system/application, without having to reauthenticate.

- Identity Attribute provision services; that is the services required to enable applications to retrieve identity attributes about a principal, once authenticated or identified.

The Access Control category is that which provides Authorisation services that is, Commonly Role-Based Access Control within applications, it is a subset of the set of total accessible services.

Within an e-Government's domain it is possible to enforce the Identity Management framework in a more specific way. The three category previously seen can be translated in the following manner (see Figure 6) (Belanger and Hiller, 2006).

Figure 6 e-Government identity management framework



The provisioning category becomes a set of provisioning authority because the digital citizenship is distributed by several local entities, whereas the Identification and Authentication authority should be unique, a Centralised Authentication. Only a point of identification that authorises all the people holding a digital citizenship; in this way all the public administrations connect themselves on a central server in order to promote an applicative cooperation between the PA. The Centralised Authentication provides the same authentication mechanism of the previous identity management framework in order to guarantee several Assurance levels (Claub and Marit, 2001). It is common practice, in Government Interoperability Frameworks, to specify different levels of assurance of authentication required in relation to different e-Government application contexts and we define them as (Siddiqi et al., 2006):

- *Level 1*: Minimal assurance (e.g., National Identity Number, passport number, etc.)
- *Level 2*: Low Assurance (e.g., username/password, certificate/PIN pairs, etc.)
- *Level 3*: Substantial Assurance (e.g., biometric identification)
- *Level 4*: High Assurance (e.g., smart card or SecureID).

The third category of the e-Government Identity Management Framework, that is the Access Control, keeps unchanged because it is realised by the application itself.

In particular, it has been defined as a logical framework for e-Government digital identity management.

5 Conclusions and future trends

At the moment, there is no availability on the market of interoperable, flexible, policy-driven management solutions that fully integrate the management of identity with security, trust and privacy aspects at different levels of abstraction and that can scale across multiple contexts to enforce policies, correlate events, quickly identify problems (such as misuses of identity information, attacks and policy violations) and react. This landscape is going to change. An emerging priority of commercial organisations, enterprises and government agencies is to deal with changes that affect their businesses in a flexible, fast and simple way. These changes can be dictated by market needs, dynamic workforces, new security threats, changing legislations and by people that are more aware of their rights.

Identity management products and solutions need to evolve towards higher levels of interoperability, flexibility and capability to react to changes: their functionalities need to be orchestrated with other management aspects, including trust, privacy and security management.

Identity management is about the management of digital identity and profile information. It encompasses operational aspects such as certification and issuance of identity information, authentication and single-sign-on, aggregation of fragmented identity information across organisations and authorisation. Its importance spans across the consumer, e-commerce, enterprise and government worlds.

On one hand, trusted, secure and accountable identity management solutions are key e-business enablers. On the other hand identity management introduces social dilemmas and issues due to the implications on privacy and fears to lose freedom.

We discussed current and foreseeable trends for identity management along with an analysis of important issues and requirements. We introduced a model of an identity management framework and discussed some of our past and current research activities in this area.

More work and research needs to be done in this space, especially for open and dynamic contexts. While closed environment (including stand alone enterprises, private internet business communities, etc.) can define strict criteria to deal with identity management issues and leverage their heavy and centralised control, the real challenge is for open and dynamic environments based on cooperation and collaboration of heterogeneous parties, ranging from people to organisations. Trends suggest that this is the directions towards which people, organisations, enterprises and governments are moving: being able to understand these new issues and provide solutions that address them is going to be strategic to enable new commercial and social opportunities.

We argue that this new generation is about *adaptive identity management* (HP, 2003), i.e., open, flexible, policy driven, context-aware identity management that scales across multiple contexts and level of abstraction and is integrated with other management aspects including security, privacy and trust.

These adaptive systems will be configurable and manageable (at the platform, application and service levels) via high-level policies dictating constraints and conditions on multiple aspects (IBM, 2003). These policies will involve identity management aspects such as authentication, authorisation, provisioning and data consolidation along with related trust, security and privacy aspects.

References

Arnold, T. (2000) *Internet Identity Theft: A Tragedy for Victims*, White Paper – SIIA.

Auerbach, N. (2003) 'Smart card support for anonymous citizen services', in Isaias, P. (Ed.): *Proceedings of e-Society*, IADIS Press, Lisbon, Vol. 1, No. 2, pp.33–46.

Belanger, F. and Hiller, J.S. (2006) 'A framework for e-government: privacy implications', *Business Process Management Journal*, Vol. 12, No. 1, pp.48–60.

Bhargav-Spantzel, A., Squicciarini, A.C. and Bertino, E. (2006) 'Establishing and protecting digital identity in federation systems', *Journal of Computer Security*, Vol. 14, No. 3, pp.269–300.

Blaze, M., Feigenbaum, J. and Keromyzis, J. (1999) 'The role of trust management in distributed systems security', in Vitek, J. and Jensen, C.D. (Eds.): *Secure Internet Programming*, Springer, Berlin, Vol. 1603 of Lecture Notes in Computer Science, pp.185–210.

Camenisch, J. and Lysyanskaya, A. (2001) 'An efficient system for non-transferable anonymous credentials with optional anonymity revocation', *Eurocrypt 2001*, LNCS 2045, Springer-Verlag, Berlin, pp.93–117.

Camenisch, J., Gross, T. and Sommer, D. (2006) 'Enhancing privacy of federated identity management protocols – anonymous credentials in Ws-Security', *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, Alexandria, Virginia, USA, pp.67–72.

Camp, L.J. (2004) 'Digital identity', *IEEE Technology and Society*, Vol. 23, No. 3, pp.34–41.

Casassa Mont, M. and Brown, R. (2002) *Active Digital Credentials: Provision and Up-to-Date Identity and Profile Information*, HPL-2002-59, Hewlett Packard Laboratories, Bristol, UK.

CEN – European Committee for Standardization (2000) *Smart Card Systems: Interoperable Citizen Services*, http://www.cenorm.be/isss.

Chaum, D. (1990) 'Showing credentials without identification: transferring signatures between unconditionally unlinkable pseudonyms', *Proceedings of AUSCRYPT'90, Advances in Cryptology*, LNCS 453, Springer-Verlag, Sydney, Australia, pp.246–264.

Claub, S. and Marit, K. (2001) 'Identity management and its support of multilateral security', *Computer Networks, Special Issue on Electronic Business Systems*, Elsevier, North-Holland, Vol. 37, pp.205–219.

Clemens, H.C. and Maibaum, N. (2001) 'Digital identity and its implications for electronic government', *Proceedings of the 1st IFIP Conference on E-Commerce, E-Business, E-Government (I3E 2001)*, Kluwer Academic Publishers, Boston, pp.803–816.

Damiani, E., de Capitani di Vimercati, S. and Samarati, P. (2003) 'Managing multiple and dependable identities', *IEEE Internet Computing*, Vol. 7, No. 6, pp.29–37.

European Commission – IST (2005) *i2010 eGovernment Action Plan*, http://europa.eu/scadplus/leg/en/lvb/l24226j.htm.

European Commission (1995) 'Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', *Official Journal of the European Communities*, 23 November, No. L. 281, p.31.

European Commission (2005) *eEurope 2005 Action Plan*, http://ec.europa.eu/information_society/eeurope/2005/all_about/action_plan/index_en.htm.

FP6/IST (2006) *Information Society Technology*, http://cordis.europa.eu/fp6.

FP7/IST (2007) *Information Society Technology*, http://cordis.europa.eu/fp7.

Goth, G. (2005) 'Identity management, access specs are rolling along', *IEEE Internet Computing*, Vol. 9, No. 1, pp.9–11.

Herzberg, A. and Mass, Y. (2001) 'Relying party credentials framework', in Naccache, D. (Ed.): *Topics in Cryptology – CT-RSA*, *Lecture Notes in Computer Science*, Springer, Berlin, Vol. 2020, pp.328–343.

Housley, R., Ford, W., Polk, W. and Solo, D. (1999) 'RFC2459: Internet X.509 public key infrastructure certificate and CRL profile', *IETF Network Working Group*, Request for Comments 2459 (Category: Standards Track), http://www.ietf.org/rfc/rfc2459.txt.

HP (2003) *Adaptive Enterprise Solutions*, http://www.hp.com/large/globalsolutions/ae/white papers.html.

IBM (2003) *On-Demand Business*, http://www 3.ibm.com/ebusiness/index.html.

Identrus (2002) *Identrus Case Studies*, http://www.identrus.com/.

Kohntopp, M. and Pfitzmann, A. (2001) 'Identity management and its support of multilateral security', *Computer Networks*, Vol. 37, pp.205–219.

Lenk, K. and Traunmuller, R. (2000) 'A framework for electronic government', *Proceedings Eleventh Int. Workshop on Databases and Expert Systems Applications*, London, pp.4–8.

MODINIS IDM-Consortium (2006) *Modinis Study on Identity Management in E-Government*, Identity Management Issue Interim Report II1, https://www.cosic.esat.kuleuven.be/ modinis-idm/twiki/bin/view.cgi.

Organisation for Economic Cooperation and Development (OECD) (2006) www.oecd.org/.

Privacy and Identity Management for Europe (PRIME) (2006) http://www.prime-project.eu.org.

Siddiqi, J., Akhgar, B., Naderi, M., Orth, W., Meyer, N., Tuisku, M., Pipan, G., Gallego, M.L., Garcia, J.A., Cecchi, M. and Colin, J. (2006) 'Secure ICT services for mobile and wireless communications: a federated global identity management framework', *Proceedings of Third International Conference on Information Technology, ITNG*, pp.351–357.

Woerndl, W. (2004) 'Authorization of user profile access in identity management', *Proceedings of IADIS International Conference*, WWW/Internet 2004, Lisbon, Portugal.