Design Principles of Identity Management Architecture Development for Cross-Border eGovernment Services

Kamelia Stefanova[1], Dorina Kabakchieva[2] and Roumen Nikolov[2]
[1]University of National and World Economy, Sofia, Bulgaria
[2]Sofia University, St. Kl. Ohridski, Bulgaria
kamelia@fmi.uni-sofia.bg
dorina@fmi.uni-sofia.bg
roumen@fmi.uni-sofia.bg

Abstract: Identity Management is a very important research challenge within the framework of the EU eGovernment development. This paper presents the main aspects of research, analysis and design of the Open Identity Management Architecture for European eGovernment development (GUIDE), a project financed by the 6FP of the EC. An innovative interdisciplinary approach is used, aimed at covering the whole range of technical, process, policy, legal and social Identity Management issues, and seeking to overcome the existing fragmentation of Identity Management initiatives. The primary purpose of GUIDE is to develop a consistent approach to identity management across the EU that will enable Member States to agree on the identity of an entity (a citizen or a business) in order to enable sectoral applications to conduct cross-border transactions. The paper provides some important comments concerning the European aspects of Identity Management and presents the adopted Federation Identity Management model. The development of the Open Identity Management Architecture is driven by eight key political and functional axioms, regarding how these federations (Member State governments and commercial organisations) should be inter-linked and what criteria each constituent federation will need to satisfy in order to join the identity grid. The architecting approach is based on an enterprise model adopted as a framework for the EU eGovernment development since the research revealed that frameworks for eGovernment are in an early state of evolution. The architecture is developed as a Service Oriented Architecture (SOA), implemented through the Web Services model, thus satisfying the requirements for 'loosely-coupled' systems, independence of implementation and location, etc. The conceptual data model describes the key *data entities* that have to be supported for cross-border identity services - the citizen and the organisation. The logical service model presents the different types of identity management services that are relevant for the developed Open Identity Management Architecture. The interoperability issues, including the interoperability services and the Identity management interoperability infrastructure, are also considered.

Keywords: Identity management, European eGovernment, cross-border services

1. Introduction

EGovernment is one of the key areas of the EU's Information Society policy and a key factor for increasing the competitiveness of the European economy. Spending and investment in eGovernment in Europe is large and increasing, and has the potential for a high and positive impact on productivity gains within citizen services. The opportunity to transform relationships between citizens and business with all levels of government through electronic channels will be paramount to future economic growth and stability.

Identity Management is a very important research challenge within the framework of the EU eGovernment development. There is an urgent need for a consistent approach to identity interoperability across the EU that will enable Member States to agree on the identity of an entity (both individual and corporate, for example a citizen or a business) in order to enable government sectoral applications to conduct cross-border transactions with respect to that entity.

Recognising the needs of research and development in the area of Identity, Identity Management and Interoperability, the EC started the Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC) Work Program (2005-2009) (EC 2007). The Programme's main objective is the "provision of world class eGovernment services, underpinning the achievement of key European policy objectives like single market freedoms and enlargement, requiring interoperability between the IT systems of Europe's public administrations, as well as between their information holdings and administrative processes". These objectives will be achieved by taking the advantage of the opportunities offered by information and communication technologies: to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe; to improve efficiency and collaboration between European public administrations; and to contribute to making Europe an attractive place to live, work and invest.

Reference this paper as: Stefanova, K, Kabakchieva D and Nikolov, R. "Design Principles of Identity Management Architecture Development for Cross-Border eGovernment Services" *Electronic Journal of e-Government* Volume 8 Issue 2 2010, (pp189-202), available online at www.ejeg.com

The commission established the European Interoperability Framework (EIF) (EC 2004) as a reference document on interoperability for the IDABC Programme in order to support the pan-European delivery of electronic government services. The EIF is under perpetual development by following the progress and the emerging requirements of the pan-European infrastructures and services (Malotaux et al., 2007).

A number of research and development projects dealing with the issues of Identity Management (IdM) and Interoperability have been supported by the EC during the Fifth, Sixth and Seventh Framework Programmes, such as GUIDE, PRIME, FIDIS, CROSSROAD, IMPACT, SPACES, etc.

This paper focuses mostly on the research and development outcomes of a European project, whose overall goal was to create the main critical requirements and principles for Identity Management Open Architecture development that will support EU eGovernment services interrelations and interoperability, based on durable trans-national co-operation and consensus on a pan-European basis. The project brought together European industrial, financial and technical market leaders in eGovernment solutions, as well as leading academic institutes of the relevant scientific disciplines. An innovative interdisciplinary approach was used, aimed at covering the whole range of technical, process, policy, legal and social Identity Management issues, and seeking to overcome the existing fragmentation of Identity Management initiatives.

The paper initially provides some important comments concerning the European aspects of Identity Management and presents the adopted federation Identity Management model. In the next section the scope of the research activities is discussed. The applied methodology, including the architecture framework, the functional aspects of the architecture, the conceptual data model and the logical service model approach are then briefly described. The identity management interoperability issues are considered in the last paper section, including interoperability services and interoperability infrastructure.

2. The European dimensions of identity management

Identity management of citizens, organizations and other public institutions has been a central function of governments for ages. The issues involved in creating, using and changing an identity have different dimensions - technical, procedural, legal and policy. Many of these issues have risen anew in the information age. Current information management approaches provide tremendous leverage in accessing, processing, manipulating and stealing information. This raises questions of privacy, security and fair information practices on one hand, to be balanced against convenience of e-government service delivery, the need to protect and secure information, and the need to interoperate across governments and private systems on the other hand.

The primary purpose of the performed research work is to develop a consistent approach to identity management for EU that will enable member states to agree on the identity in order to enable sectoral applications to conduct cross-border transactions. The notion "*Interoperability*" is defined as "*the ability to join systems in a heterogeneous area so that they can operate efficiently together*" (GUIDE 2006). The basic underlying concept is the one of *Federated Network Identity Management*, in which the stakeholders (individuals, administrations and businesses) can engage in virtually any transaction without compromising the privacy and security of vital identity information. The usual approach to creating a trust relationship is to introduce a third component, an identity provider, where each of the two entities independently 'trust' the identity provider (Figure 1).

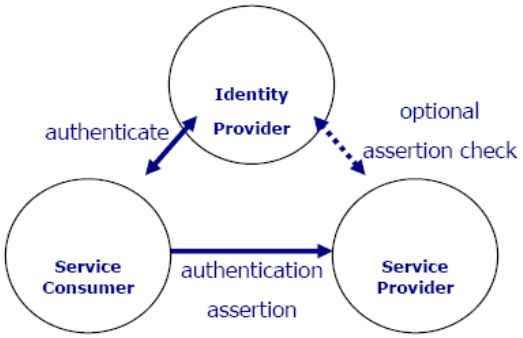

Figure 1: Initial identity federation model

This model requires the affiliation of stakeholders into circles of trust based on operational agreements that define trust relationships between them. In other words, a circle of trust is a federation of service providers and identity providers that have established formal relationships and operational agreements and with whom service consumers can transact in a secure and apparently seamless environment.

Within the EU landscape various such federations or circles of trust either already exist or are being developed in relation to different stakeholder groupings, both administrative and commercial. In particular, many Member States are engaged in developing such federations at the national level. However, in most cases these federations are being constructed in isolation from each other.

The main goal within the GUIDE project was to define an architecture that will enable the integration of these federations into a greater circle of trust, in order to facilitate an apparently seamless identity environment across the whole of the EU. This is a prerequisite before any identity can be safely exchanged between Member States. In this respect the research done is conceived as providing a pan-EU federation of identity federations, which can be achieved by connecting the existing identity providers to an identity network or grid (Figure 2).

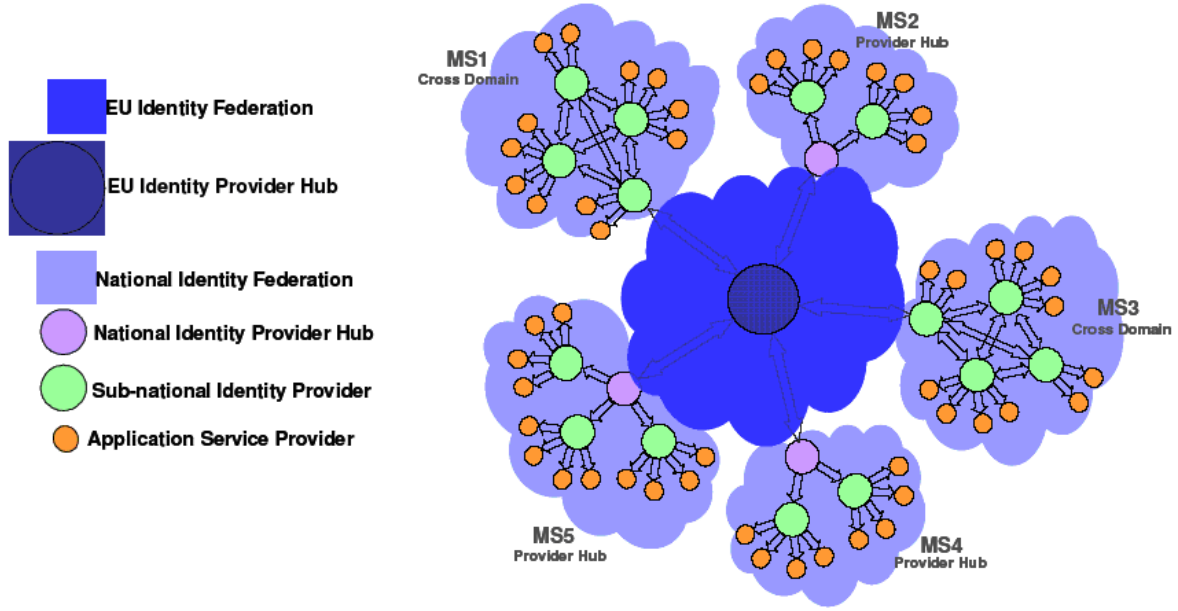

Figure 2: Architectural vision that integrates national and international (pan-European) identity management services to establish a conceptual 'Identity Grid' for Europe

The end-users (citizens and businesses) would interact with applications and/or application service providers (the orange circles) in any of the participating Member States. Their interaction with applications takes place outside of the scope of Guide's influence, which ends at the Gateways (purple) connected to the grid (blue cloud). One of the first things a citizen does when interacting with an application is authenticating himself, which can be done via a number of mechanisms. These range in strength from simple passwords via digital certificates up to biometrics.

3. Scope of the research activities

The main problem that GUIDE addresses is the definition of a logical, technical, institutional and policy/legal framework, supporting the development of identity management services, which integrates existing identity management systems while being consistent with the juridical and regulatory conditions prevailing in member states. The aim of GUIDE is neither to address national identity management issues as such, nor to enable nationally constructed applications. Its objective instead concerns interoperability across national systems and structures (processes, cooperation, interfaces) within broader transnational, policy, legislative, and socio-economic boundaries. The creation and operation of the GUIDE architecture involves public administration and industrial cooperation in order to develop interoperable processes, cooperation models and interfaces.

The central operating assumption of GUIDE is that eGovernment requires more than transforming paper-based forms of information exchange into digital ones. eGovernment involves significant transformations along institutional, policy, legislative, and technological lines. GUIDE's approach in this respect is 'integrative' in that it seeks to overcome the existing fragmentation of initiatives which inhibits the seamless and efficient operation of eGovernment services they are designed to facilitate. The re-design of existing structures and processes with the aim of improving collaboration between and across different government departments and the harmonization of eGovernment practices on a pan-European level are the main challenges GUIDE addresses.

There are a number of other eEurope initiatives that have complementary objectives to GUIDE, and with which GUIDE must be correctly positioned, as described on Figure 3. The intention is to complement rather than compete with these other initiatives.

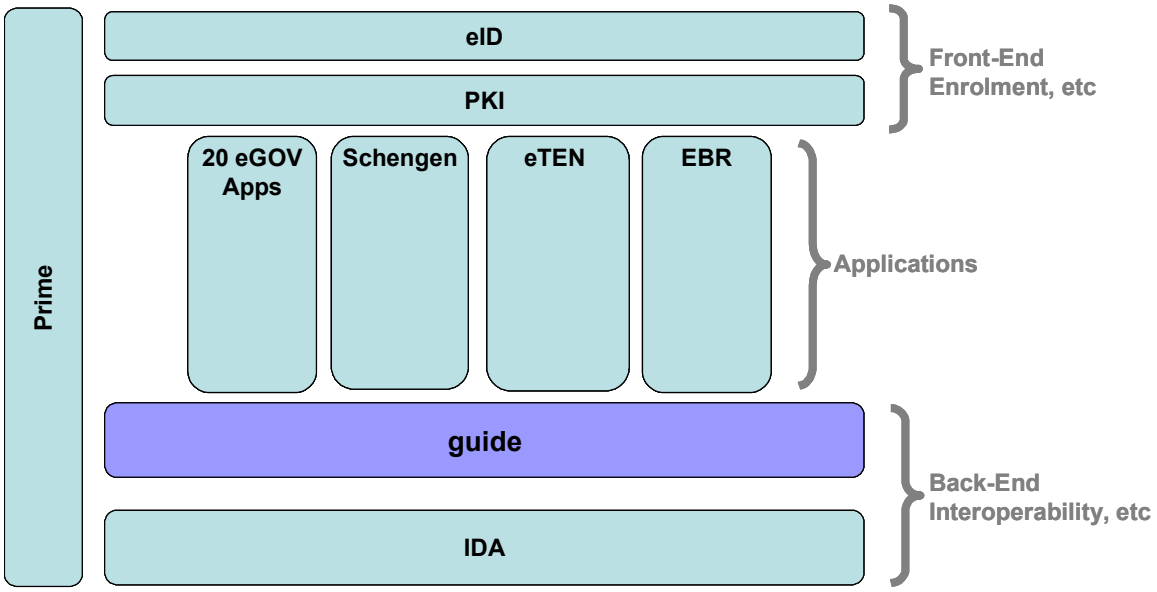

Figure 3: Scope within the eEurope Initiatives

Similarly, to a considerable extent, identity management specifications and standards are already available in the open market, e.g. the Liberty Alliance initiative. The challenge for GUIDE is to tie these together and create a manageable environment for end-to-end Identity Management in a pan-European eGovernment setting. Issues like trust models, liability and privacy are crucial to tackle during the project implementation.

One of the main aspects of the guidelines and recommendations that GUIDE will ultimately deliver in the physical perspective is a definition of the various standards that will be recommended by the architecture (see Figure 4). These must be inclusive of all other standards and initiatives relevant to identity management and interoperability. GUIDE will not attempt to "re-invent the wheel", but rather "fill the gaps" and supplement these other initiatives.

The development of the Open Identity Management Architecture is driven by eight key political and functional axioms to which further research is dedicated to add more knowledge and insight:

- Axiom 1: "A European Open Identity Architecture will be defined".
- Axiom 2: "The architecture will conform to an overall EU legal framework and governance".
- Axiom 3: "Each member state will have governance over Identity Management Services operating within their boundaries, and the identity data underpinning these Identity Management Services".
- Axiom 4: "Each functional element of identity data within the identity Grid will have clear data ownership and data obligations".

In accordance with Axiom 3 and the principle of subsidiarity, it is not the intention that the developed Open Identity Management Architecture should be prescriptive regarding how each constituent federation is constructed. This is deferred to the 'owners' of the federations, including Member State governments, and commercial organisations. Rather, the focus is on how these federations should be inter-linked.

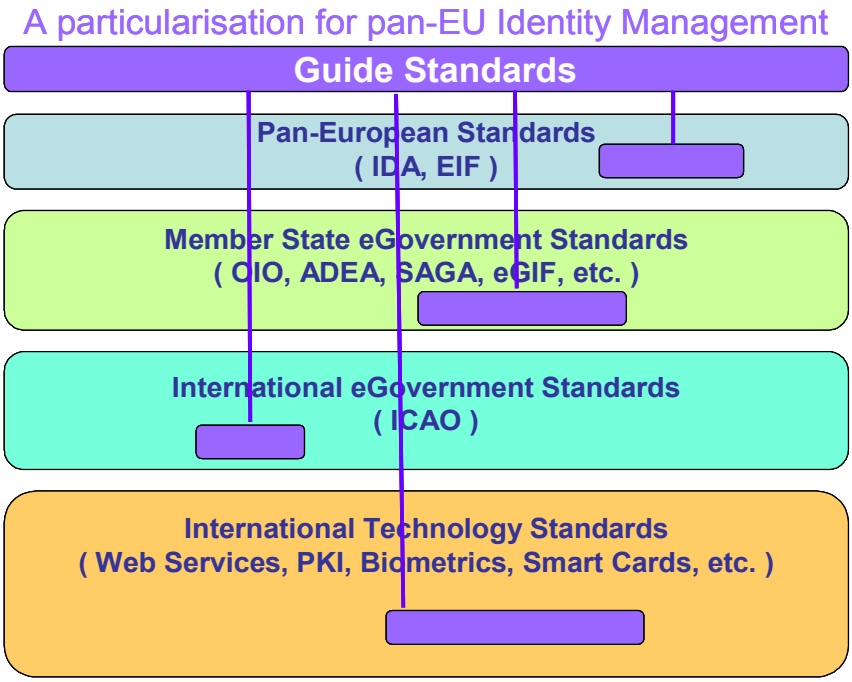

Figure 4: Standardization scope

There are certain criteria that each constituent federation will need to satisfy in order to join the identity grid. It is expected that there will be a process of Registration and Accreditation in accordance with Axiom 2 – EU Governance, to ensure that.

The functional axioms on which the Open Identity Management Architecture is based are:

- Axiom 5: "All identity data is produced and consumed through applications outside the Identity Grid".
- Axiom 6: "A significant amount of identity data will always stay outside the Grid"
- Axiom 7: "A significant amount of identity transactions will always be done outside the Grid"
- Axiom 8: Applications outside the Grid will interact with a set of "Identity Management Services" within the Grid.

4. Methodology

Every Identity Management solution to be implemented in the area of eGovernment faces the challenge to integrate smoothly with existing systems. The integration can be achieved through interoperability that can only be secured through the development of an open architecture.

4.1 The architecture framework

Frameworks for eGovernment are in an early state of evolution. In this situation a look at the state of development in the well developed domain of Enterprise Architectures allows adopting existing results and experiences in their development process. Enterprise Architecture is a disciplined approach to understand how components of an enterprise communicate, change, and function together as a whole.

An enterprise architecture is defined as a system of systems, being a collection of independently useful systems that have been integrated together to achieve additional properties not associated necessarily with any of the individual systems. The strong focus in these systems is on communication and cooperation, and therefore the idea of interoperability between systems is paramount.

In the course of the development of the field, architectures have become more encompassing in that they do not only cover computer hardware and software, but increasingly as well organizational and

business dimensions. They have as well become more sophisticated in their internal structure to respond to more demanding requirements especially for integration and flexibility.

GUIDE has assessed a number of industry approaches for architecture development such as Zachman and TOGAF8, which are implemented using Popkin System Architect and RUP SE tools. Finally, Zachman model is adopted in the project work as a general industry standard framework for describing the conceptual architecture. However, the project research was not confined only to the Zachman approach. Other complementary approaches such as BPEL and UML have also been used and adapted to incorporate other models according to the requirements and suitability.

The Zachman Enterprise Architecture Framework in shown on Figure 5. Each cell represents the intersection of a particular focus and a perspective. Each focus (the question what, how, where, who, when, and why) is depicted in a column and each perspective (point of view) - in a row. The perspectives define the point of view or the level of abstraction for the information contained in the cells. The information and models within a single row represent a complete description of the architecture from that perspective. Each column captures all of the architecture knowledge for the particular question being asked, i.e., the focus. The total architecture knowledge for each focus is obtained by isolating each focus and defining the artefacts for each perspective within it.

	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*	
Objective/ Scope *Contextual* *Role: Planner*	List of Things Important in the Business	List of Core Business Processes	List of Business Locations	List of Important Organizations	List of Events	List of Business Goals/Strategies	**Objective/ Scope** *Contextual* *Role: Planner*
Enterprise Model *Conceptual* *Role: Owner*	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan	**Enterprise Model** *Conceptual* *Role: Owner*
System Model *Logical* *Role: Designer*	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Role Model	**System Model** *Logical* *Role: Designer*
Technology Model *Physical* *Role: Builder*	Physical Data/ Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design	**Technology Model** *Physical* *Role: Builder*
Detailed Representations *Out of Context* *Role: Programmer*	Data Definitions	Program	Network Architecture	Security Architecture	Timing Definition	Rule Specification	**Detailed Representations** *Out of Context* *Role: Programmer*
Functioning Enterprise *Role: User*	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy	**Functioning Enterprise** *Role: User*

Zachman Institue for Framework Advancement - (810) 231-0531 Copyright - John A. Zachman, Zachman International

Figure 5: The Zachman Enterprize architecture framework

Service Oriented Architectures (SOAs) are state of the art in enterprise architectures. Conceptually, SOA represent a model of loosely-coupled applications working together by exposing services to each other. Business wise, services are expressing data- and function-services that one party can offer other parties to use. Technologically, SOA consists of a group of emerging standards that defines protocols and creates a loosely-coupled framework for programmed communication between different systems. Web services are a specific implementation of a SOA, i.e., a method which enables an application to be invoked by other applications by receiving and sending data in standardized XML (OIO, 2003).

Taking into consideration the above mentioned, the essence of the GUIDE architecture is foreseen as a Service Oriented Architecture (SOA), given the obvious requirements for 'loosely-coupled' systems, independence of implementation and location, etc. Furthermore, the only real candidate implementation of SOA currently is the Web Services model, and this is envisaged as the most likely physical perspective candidate for the GUIDE architecture. Given that there will be a need for a highly secure approach, it is envisaged that the Service Oriented Security Model (SOSA) as currently

delivered by the emerging Web Services Security Model (WSSM), will be overlaid onto the basic WS architecture.

4.2 Functional aspects of the architecture

Identity management pertains to at least three major architectural aspects: data, functionality, and data protection.

- Identity data is any data that can either directly or indirectly identify an entity (be it an individual or an organization);
- Functionality in IT systems always refers to some form of data transformation. Given certain assumptions on input data and the transformer's environment (in particular, the user of the transformer), input data is used to produce output. We assume all data to be encapsulated by some form of access functionality. Functionality can be more or less related to identity management in itself. For instance, preparing a letter and printing it is some form of functionality that pertains to the core of an application rather than to ID management. Authentication, on the other hand, is tied to IdM in a stronger sense;
- Data protection embodies policy, legal, social and ethical requirements that relate to identity data. These are elicited in GUIDE and must be rendered operational in the sense that essentially, data protection means to integrate technical and governance constraints into the above data transformers.

In this context, the GUIDE architecture identifies structures of identity data, technical, policy, legal, and sociological constraints that relate to its usage, and transformers that work on the identity data while respecting, in particular, data protection constraints. The functionality that is needed to enable the provision of eGovernment services is considered from three different perspectives: processes, services, and software components as illustrated on Figure 6. As mentioned above, functionality embodies both application cores (printing a letter) and functionality that more strictly pertains to identity management.

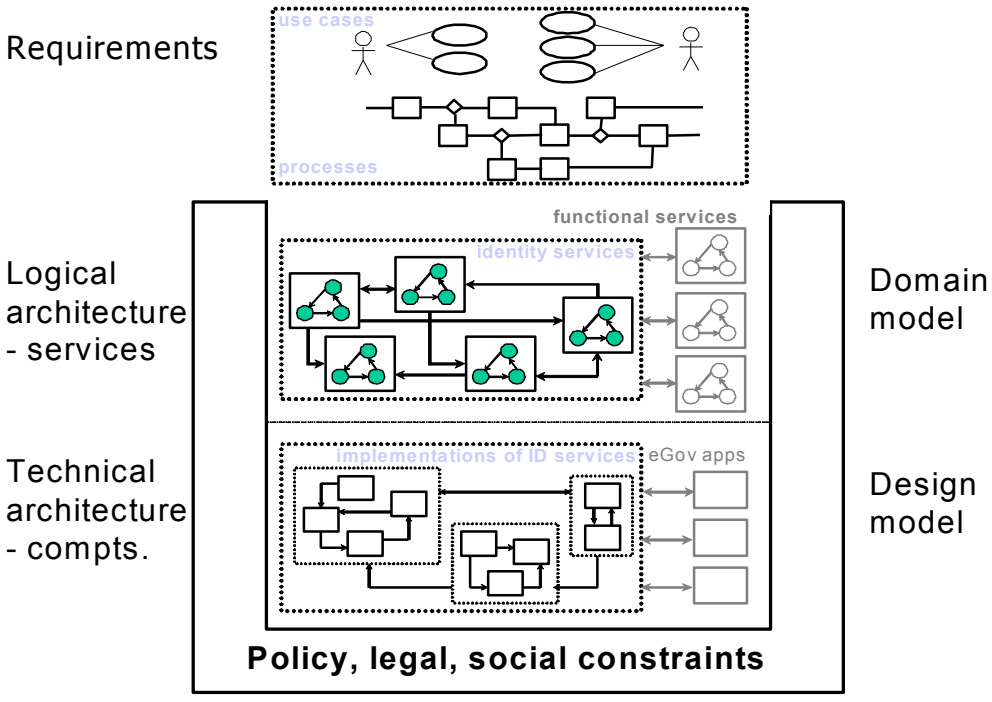

Figure 6: Functional view of the architecture

The distinction between processes, services, and components describes identity management at (a) the level of users, (b) logical units necessary to carry out respective tasks, and (c) technical units that implement the logical ones. The rationale for this layered structure is that an analysis at the user's level is needed to elicit technical, functional, and non-functional requirements for the management of identity data at a Europe level. These requirements are then mapped to logical entities, or aggregations of entities, that, in sum, are needed to fulfill the requirements. They form the 'domain

model': at an abstract level they specify how identity-related eGovernment transactions can be performed. Different providers, or different member states, will implement eGovernment systems that are possible on the basis of the logical entities, and which must conform to the regulatory, legislative, and social rules imposed on these entities.

From a stakeholder perspective, processes are the sequences of actions that are necessary to perform some well-defined and explicitly documented objectives. Processes are reflected in user requirements that are both functional and non-functional, at both the conceptual and technical levels. Processes and requirements drive the architecture, but are not part of it.

When translated to the level of processes, these processes make use of instances of specific services. Services can be application services and identity management services. The description of identity management services, constraints on their usage and aggregation, forms the logical GUIDE architecture. This is the domain model. As such, it defines and analyzes the building blocks that are necessary to perform identity-related transactions in eGovernment. Depending on applications, policy and legal constraints related to specific member states, different profiles defined by different possible interconnections of services, can be developed taking account of the heterogeneity of the EU.

Different implementations of this logical architecture are provided by components (actual pieces of software) and their possible and actual compositions. Components and their relationship form the technical GUIDE architecture. Services and components are different views on the above data transformers.

On the basis of current research it is unlikely that there will be one single IdM GUIDE architecture. Instead, public administrations at different levels of political granularity will implement their own systems, and they are likely to make use of existing legacy systems.

The GUIDE architecture can help them to identify the necessary technological structures and policy, legal, and social conditions for their implementations, and it can also be used to show compliance with a set of general agreed-upon principles on composition and deployment of services, or the implementing technical components, that are stipulated in the GUIDE logical architecture.

The logical architecture leaves room for different implementations by (a) presenting different architectural variants in itself, and (b) by leaving the technical implementation completely open, up to a set of mandatory requirements that pertain to technology and data protection.

4.3 Conceptual data model

The key *data entities* required to be supported for cross-border identity services are the citizen and the organisation as these are the entities that are being identified within an eGovernment service. The architecture describes these entities, covering the attributes associated with the citizen and organisation entities required for cross border identity services. As such they are not a full representation of these entities, but instead focus on identity and identity related data only.

At the highest level, both organisations and citizens share a common conceptual data model. This model is shown on Figure 7 below.

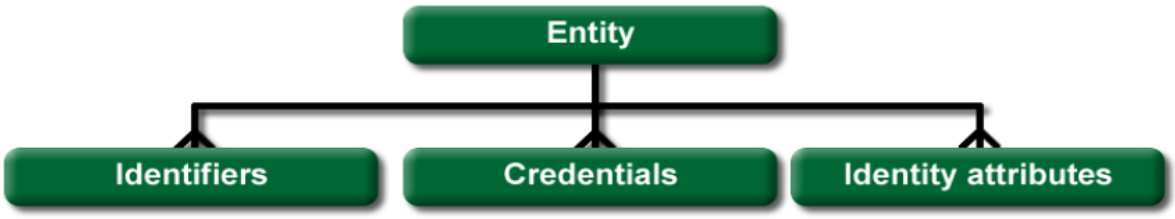

Figure 7: Architecture's conceptual entity data model

Identifiers are data elements that are unique to the entity and can be used to uniquely reference it. Examples of identifiers include social security numbers, driver numbers and company registration numbers. Often these identifiers will need to be accompanied by a data domain to ensure uniqueness (e.g. drivers' number in Germany). *Credentials* are data elements that are used to validate that the

entity is taking part in the transaction. Examples of credentials include passwords, biometrics and digital signatures. *Identity attributes* are other pieces of information and data about the entity that are used in the identity service. Examples include date of birth, address and name.

This conceptual data model has been elaborated for citizens and organisations to develop logical data models. It would be possible to elaborate a similar logical data model for documents that are participating in eGovernment services. However, this work is outside the scope of the project.

4.4 Logical service model

This section provides an overview of the different types of identity management services that are relevant for the developed Open Identity Management Architecture. Two types of services are implemented (see Figure 8):

Support Services, providing mechanisms to navigate in the architecture and to interact with the architecture.

Identity Transaction Services, enabling the PEGS applications to utilise the developed architecture in such a way that the needs for cross-border identification and authentication can be met.

The implementation of Pan European Government Services (PEGS) requires applications to become aware of their “counterparts” in other Member States. This leads to two main services: cross-border authentication (citizen from country A wishes to interact directly with an application from country B, that application authenticates the citizen via an Identity Provider in country A); and Attribute Provisioning (applications can exchange information about authenticated users, such as name, address, etc.).

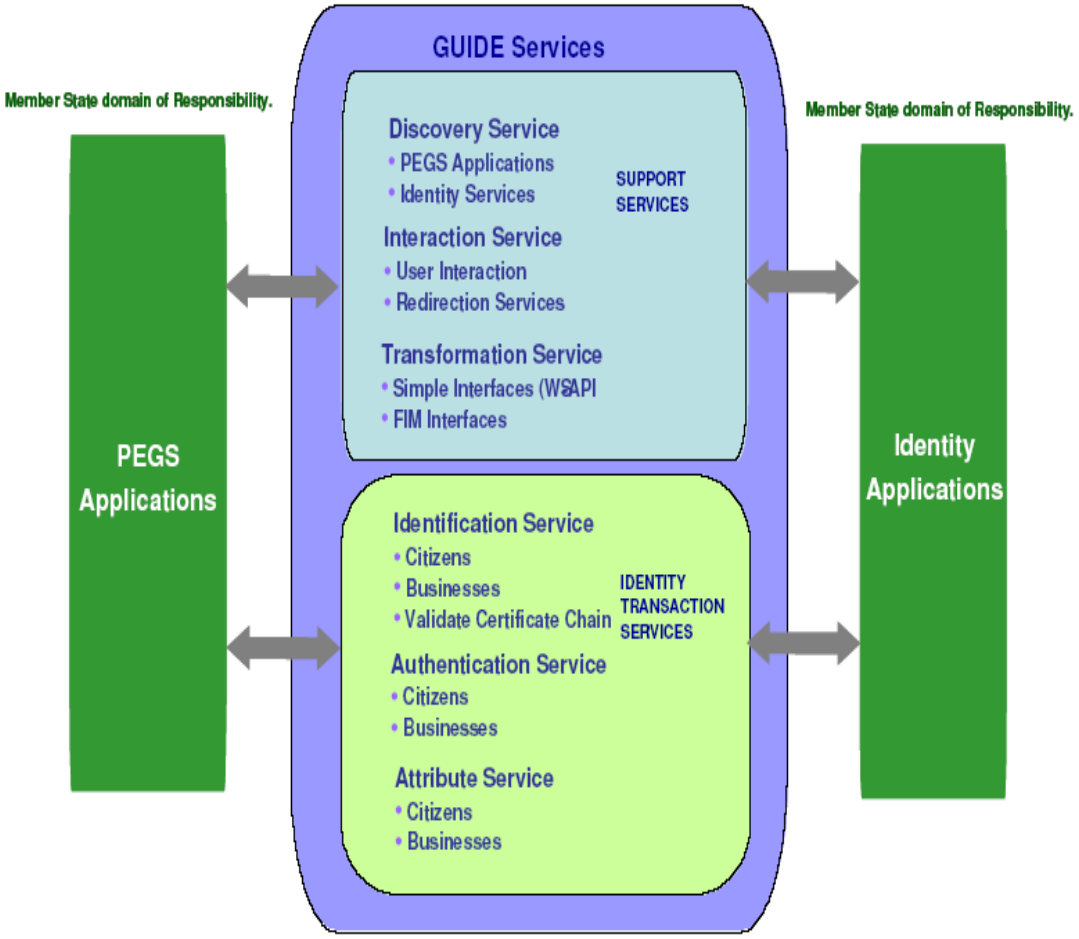

Figure 8: Overview of GUIDE services

In order for a PEGS (Pan-EU Government Service) to establish the identity of an unknown foreign Principal the following very simplified outline process must be followed:

- The PEGS must first engage a Discovery service to find a suitable IP (Identity Provider) that can identify the Principal.
- The IP essentially provides two services - an AS (Authenticator Service) and an APS (Attribute Provider Service). If the Principal is logging on, they can be called upon to assist with this via an Interaction service enabling them to choose an appropriate IP. The Principal can then be redirected via a Redirection service to the IP for authentication, and subsequent redirection back to the PEGS.
- The PEGS will then require an Identification service or Authentication service, depending on the given use case scenario described above, to verify the Principal's identity, but in this case GUIDE must provide the services necessary to allow the associated credentials to be delivered to the IP.
- The Assertion service is again used to provide the result to the PEGS.
- Once Identification or Authentication is achieved, by whatever means, the PEGS may optionally invoke an Attribute Provision service to either check or obtain identity attributes of the Principal. To enable these services, a Trusted Channel must also be provided, over which they can be carried, that includes an appropriate end–to–end Security service, and Assurance service that can indicate the veracity of the asserted Identification or Authentication.

5. Identity management interoperability

The interoperability approach envisages that each member state could situate an interoperable gateway which integrates an *adapter*. This term is widely used in the "*Enterprise Application Integration*" area and describes a component that transforms an external interface to an internal protocol. These adaptations are made on both sides, so the number of possible end to end mappings will be reduced (see Figure 9). The requirements that the existing federated Identity Management systems have to comply with when they are integrated within an open architecture, are:

- All participating entities should be classified either as a Service Provider (SP) or as an Identity Provider (IdP), or - as both;
- The used local security system should be capable to operate into a heterogeneous area;
- Each involved IdP should apply a web-based authentication mechanism (Login);
- The existing discovery service of the local security system should be able to identify the project-specific local discovery services in order to find foreign IdP's or SP's;
- If no discovery service is implemented, then the SP redirects the request to a project-specific local discovery service.

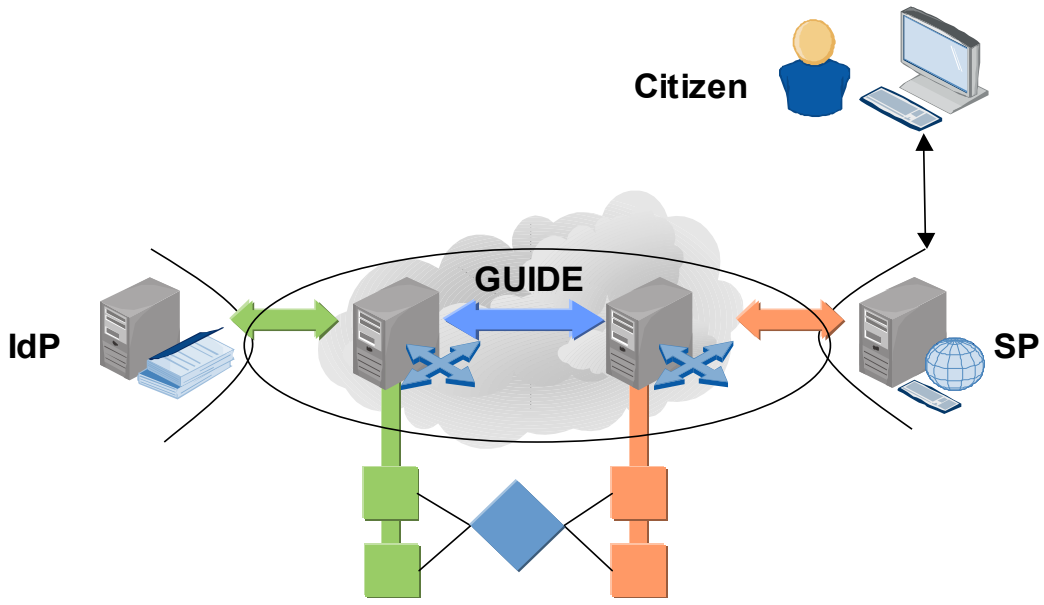

Figure 9: Interoperability architecture components

5.1 Interoperability services

In order to establish a "*Pan European Government Services* (PEGS)" system, some additional layers and services are necessary to be build. This new infrastructure has to interact with an existing mechanism in order to provide identity and application services. The interoperability should be guaranteed by implementation of additional interoperability services that cover all existing protocols or bindings. The architecture provides a set of necessary building blocks, such as the GUIDE gateway, with their services to implement the concrete adaptation. The basic architecture includes the interoperable infrastructure as an additional layer over the existing identity and application service providers. This infrastructure interacts with the existing systems on the basis of some state-of-the-art industry standards. The enhancements proposed by the architecture are transparent for the involved systems. GUIDE itself builds a trusted circle for a secure data exchange between the connected systems and bridges the existing identity providers to an identity network or grid. In this grid every user is able to use his identity to get access to any service with user authentication that uses this grid. Every national identity hub is a single access point for the interoperability services. Any country or organisation should have its own part of the identity management services that provides opportunities:

- To add, modify or remove an user;
- To define the users authentication characteristics;
- To store or create additional information about a user;

GUIDE, on its side, provides trusted circle services, such as:

- Global exchange of requests and responses between the national identity hubs and the SPs;
- Interoperability with existing systems.

A more complete overview of the concept is given below (see Figure 10), where all the important components necessary to get access to a PEGS system are shown. The national service and identity providers are connected together via the interoperability gateways in such a way that any user would be able to use all services. The interoperability enables end-to-end scenarios over multiple domains, systems or standards across national and system borders. The GUIDE gateways are able to interact with different national implementations. In order to implement this interoperability, the GUIDE gateway has to translate between these different protocols of the connected systems.

As it is mentioned above, GUIDE deals mostly with the technical interoperability, which has different aspects of interoperability, such as:

- *Interactions and Behaviours*. This aspect covers the involved components, the flow of messages between them and the possible sequences to handle a whole service scenario.
- *Messages and Message Content*. This aspect covers the single messages with their structure and content to handle a single step in the service scenario.
- *Protocols and Binding*s. This aspect covers the transport mechanism of a single interaction.

In order to provide a secure interoperability of cross-border European eGovernment services, all of these aspects have to be taken into consideration when the mapping between a supported standard implementation and the architecture infrastructure solution is developed. For the description of the services, required for the sugested Interoperability Framework, an overall context had to be created. The overall context brings the different services in relation to each other and enables every one of them to recognize the interfaces that exist between these services. The interfaces describe the interoperability of the different services. The following minimal set of services have to be defined for an interoperability framework:

- Authentication. This service should confirm that any user is the one he or she pretends to be. Various methods will be available, ranging from the simple (e.g. personal data validation) through to the complex (e.g. biometrics). There will be also "graduated authentication" and "tiered authentication" where additional levels of authentication are required for certain access;
- Identity Attribute Provision. The service has to create, change or delete specific "fields" or "entries" within a Citizens, Business Identity record during the lifecycle of that Identity;
- Single Sign On (SSO). This service should provide the opportunity that for a user, who has authenticated oneself within a specific domain and moved to another, there would be no need for re-authentication. The new domain has to make sure that the initial authentication has indeed

taken place beforehand and therefore requests a confirmation of authentication from the original domain. The main purpose is to provide the user with a large virtual network of applications. These applications and services need to be able to recognise the user that wants to interact with them, but it is of utmost importance that the user maintains control over his or her data. This means that he or she can determine what happens with their personal data and what specifics pertaining to this data are distributed through the trusted network.

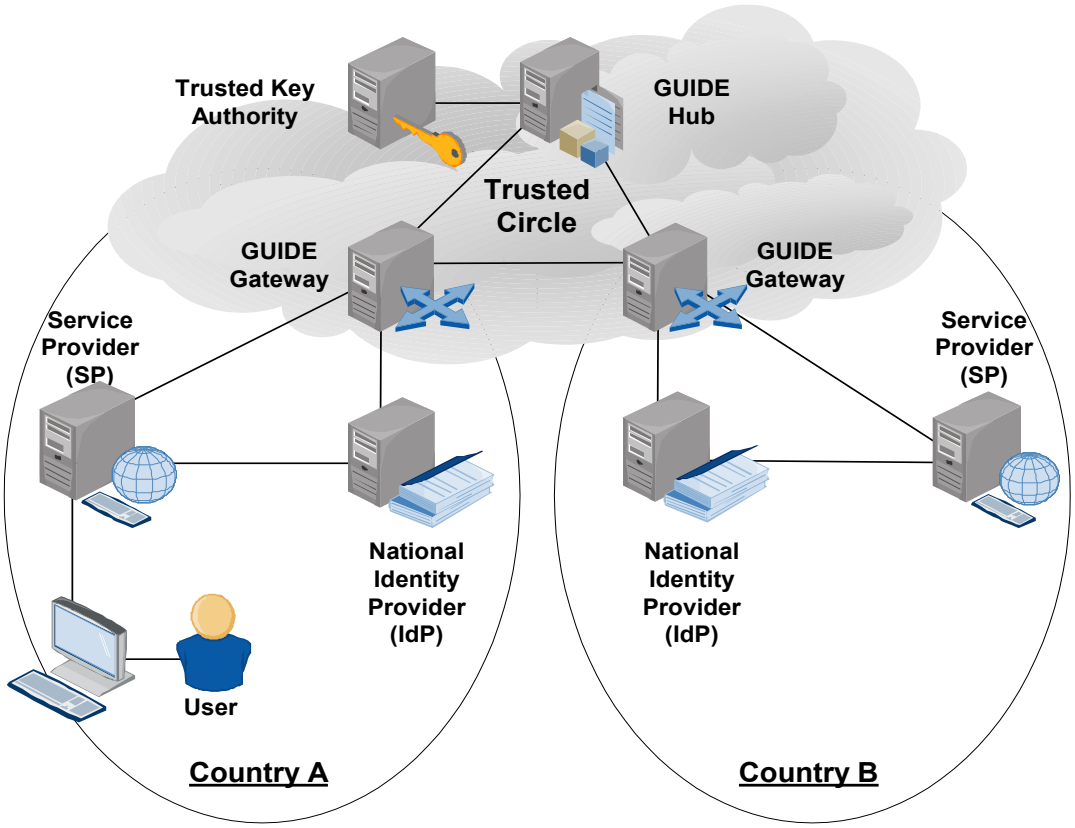

Figure 10: Overall context for services

5.2 Identity management interoperability infrastructure

As described earlier, the Identity Management interoperability infrastructure is positioned between the IdPs and the SPs. The adapters are responsible to interact with the different systems, to transform any request from the source format to an internal format, and to put it to the target adapter where the request will be transformed to the target format (see Figure 11).

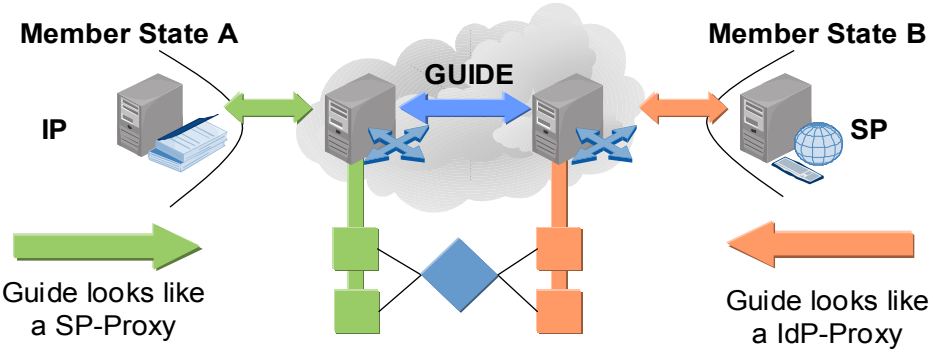

Figure 11: GUIDE adapter architecture

A perfect IdM interoperability infrastructure should be invisible for the external systems. The systems see any GUIDE gateway as a proxy of the opposite system. A GUIDE gateway consists of a set of adapters for every external system or standard in every proxy role this gateway takes. By using such architecture it would be also possible to interconnect two end points which implement different

standards. The main tasks of the gateway are *adaptation*, *transformation* and *transportation* of interaction between the different parties of a pan-European eGovernment services scenario:

- The *adaptation* covers the interaction with the external world including system entities, such as IdP's, SP's or citizens that exchange information.
- The *transformation* covers the handling of the content in order to put it in the data structure format defined by GUIDE.
- The *transportation* is responsible for exchange of information between the GUIDE gateways.

In order to better describe the processes and models of how a user can interact with a local or a pan-European government service, some high level use cases are used. For instance, the process of providing a single sign on capability is illustrated at Figure 12. If a user is once authenticated, he or she should be able to use any service of every country. His authentication will be taken from one service provider to the other.

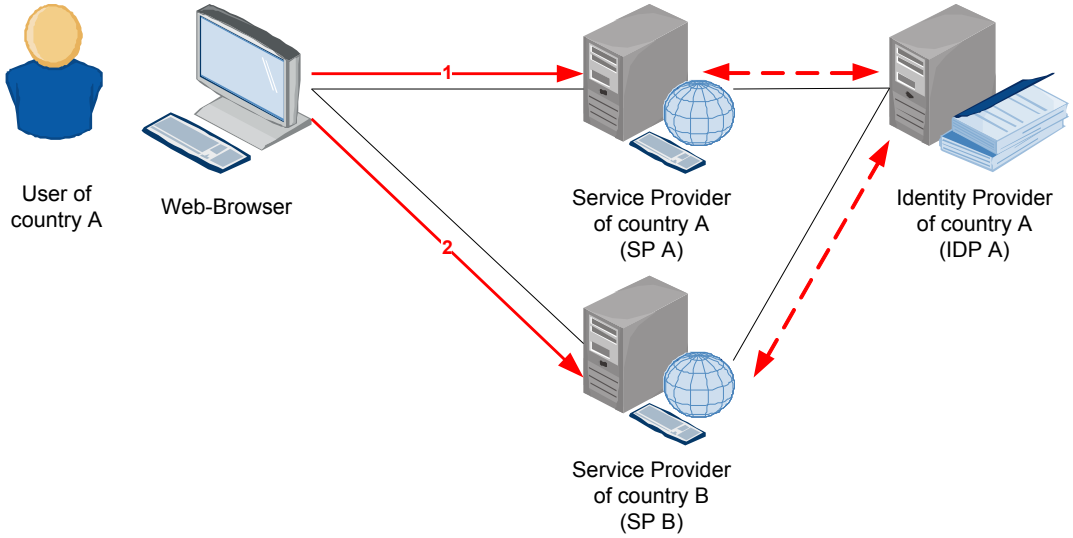

Figure 12: Single Sign On (SSO)

Since most of the EU countries have their own identity management solutions, for the evolution from local solution to a federated solution with single sign on capabilities, it would be necessary to split the existing systems and to move the IdM Interoperability infrastructure between them. Such architecture would enable interoperability and single sign on service at a pan-European level.

6. Conclusions

The ability of Governments in the EU to deliver services electronically has the potential to fundamentally change the way citizens and businesses relate to their public bodies. However, this change in service delivery does not change the fundamental values of the EU. As such it is important that the design and delivery of eGovernment services supports the principles of the EU as well as the best practice of eService delivery. A key factor in preserving the right of free movement of labour in an eGovernment age will be the availability of cross-border identity services to give citizens and businesses equal access to eGovernment services across the EU.

The research done has delivered a number of artefacts that provide an important contribution towards delivering cross-border identity services. These include a comprehensive analysis of the social, organisational, legal and technical context for identity services in the EU, a database of requirements for cross-border identity management services, an architecture for cross-border identity services, trials demonstrating the technical aspects of the open IdM architecture and providing feedback into the requirements database, an organisational architecture to support cross-border identity management services, and a set of policy recommendations to allow the development, deployment and management of cross-border identity services. The Architecture fully supports the principle of subsidiarity in general and does not insist upon a central EU-wide identity repository or a standardised solution across all Member States. Instead, it allows Member States to manage identity within their borders in the most effective way for them.

However, the research project is only considered to be a start in enabling cross-border identity interoperability. If cross-border identity services are to become a reality, the outlined policy recommendations should be implemented, the cross-border identity services work and the wider work on identity and eGovernment services within the EU should be integrated, and the architecture and standards should be further developed to include other aspects (e.g. support models, bilateral data exchange, certification and conformance models).

References

Bernus, P., L. Nemes, et al. (1996). Architectures for Enterprise Integration. London, Chapman & Hall.

CGEY (2004). Online availability of public services: how is Europe progressing? Cap Gemini Ernst & Young.

EC, Linking up Europe: the Importance of Interoperability for *e*Government Services, Commission Staff Working Paper, European eGovernment Conference, 2003

e-Envoy (2003). e-Government Interoperability Framework 5.0, Office of the e-Envoy.

Evernden, R. (1996). "The Information FrameWork." IBM Systems Journal 35(1): 37-68.

FIDIS, Future of IDentity in the Information Society, http://www.fidis.net/

GOL-IN (2004). Interoperability Frameworks. 2004.

GUIDE Project Deliverables, including Policy "White Paper" on Identity Management, GUIDE Architecture Summary, GUIDE Trial Evaluation reports, etc., 2007.

GUIDE, GUIDE Technical Implementation Interoperability guidelines: Core Services Interoperability Guidelines, Internal Document, October, 2006

GUIDE Consortium (2004) GUIDE Open Identity Management Architecture Overview, GUIDE Architectural Snapshot Vol.1.

GUIDE Consortium (2004) GUIDE Open Identity Management Architecture Overview, GUIDE Architectural Snapshot Vol.2.

GUIDE Consortium (2004) GUIDE Government Engagement Strategy, Ver.1.

GUIDE Consortium (2004) GUIDE Generic Co-operation Model Interim Synthesis, Ver.0.7.

Halperin, R., Identity as an Emerging Field of Study, *Datenschutz und Datensicherheit* 9/2006, pp. 533-537, Wiesbaden 2006.

Helbig, J. (2002). Fundamentals of Software Development, McKinsey & Co.

ICCP (2003). Identity Management Systems (IMS): Identification and Comparison Study, Independent Centre for Privacy Protection (ICPP).

IDA (2002). Architecture Guidelines V6.1. Brussels, Interchange of Data between Administrations.

IDABC, IDABC Work Programme Fourth revision (2007), European Communities, 2007.

IDABC, European Interoperability Framework for Pan-European eGovernment Services, Version 1.0, ISBN 92-894-8389-X, European Communities, 2004.

Inernet2, Shibboleth Introduction, http://shibboleth.internet2.edu/shib-intro.html

Liberty Alliance, The Liberty Alliance Project, http://www.projectliberty.org/

Malotaux, M., van der Harst, G., Achtsivassilis, J., Hahndiek. F., Preparation for Update European Interoperability Framework 2.0 - FINAL REPORT, Gardner Inc, 2007.

Myers, J., Simple Authentication and Security Layer (SASL), Network Working Group, October 1997, http://www.ietf.org/rfc/rfc2222.txt

OESIS, Security Assertion Markup Language (SAML) V2.0 Technical Overview Working Draft 10, October 2006

OIO (2003). White Paper on Enterprise Architecture. Copenhagen, Ministry of Science, Technology and Innovation.

Skip Slone & The Open Group Identity Management Work Area (2004) Identity Management, The National Electronic Commerce Coordinating Council (2002), Identity Management, Presented at the NECCC Annual Conference, New York, USA.

SSC (2003). E-government Interoperability Framework, E-government Unit State Services Commission.

Windley, P. (2004). Enterprise Computing Weblog. 2004.

Zachman, J. A. (1987). "A framework for information systems architecture." IBM Systems Journal 26(3): 276-292.