Serdica J. Computing **2** (2008), 73–88

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

INTEROPERABILITY OF CROSS-BORDER EUROPEAN EGOVERNMENT SERVICES: SOME DESIGN ISSUES

Kamelia Stefanova, Roumen Nikolov

Abstract. The authors analyse some of the research outcomes achieved during the implementation of the EC GUIDE research project "*Creating an European Identity Management Architecture for eGovernment*", as well as their personal experience. The project goals and achievements are however considered in a broader context. The key role of Identity in the Information Society was emphasised, that the research and development in this field is in its initial phase. The scope of research related to *Identity*, including the one related to *Identity Management* and *Interoperability of Identity Management Systems*, is expected to be further extended. The authors analyse the abovementioned issues in the context established by the EC *European Interoperability Framework* (EIF) as a reference document on interoperability for the *Interoperable Delivery of European eGovernment Services to Public Administrations, Business and Citizens* (IDABC) Work Programme. This programme aims at supporting the pan-European delivery of electronic government services.

ACM Computing Classification System (1998): J.1.

Key words: Administrative data processing; Government, Business; Distributed databases; Security, integrity, and protection; Transaction processing; User/Machine systems; Human information processing.

1. Introduction. The role of Identity in the Information Society is rising dramatically but the research and development in this field are in their initial phase. The scope of research related to Identity will be further extended, e.g., the "*identity of persons in different roles (e.g., citizen; costumer; individual) in different places (home; work; mobile) and in different modes (offline; online; mixed modes) are equally relevant. Likewise, explorations of identity in different contexts are significant, as they range from the individual through the organisational, the national, international and the global*" [6]. In addition, there already exist "*concepts of physical, digital, virtual, partial and cyber identity*" that require some systematic research about "*how they are used, how they might be used and abused, the nature of the impact that they will have on shaping the e-Society as well as its supporting technologies, and how they ought to be defined in order to respect the fundamental rights of the citizen*". Other very important areas of research, as Halpein states, are "*Identity in the context of supporting and emerging technologies*", "*Identity in relation to risk and regulation*", "*Identity Management*" and "*Interoperability of Identity Management Systems*".

The EC also recognises 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 Programme (2005–2009) [8]. 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, requires 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 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;
- to contribute to making Europe an attractive place to live, work and invest.

The commission established the European Interoperability Framework (EIF) as a reference document on interoperability for the IDABC programme in order to support the pan-European delivery of electronic government services [7]. The document represents the highest-ranking module of a comprehensive methodological tool kit for implementing pan-European eGovernment services. The EIF is under perpetual development by following the progress and the emerging requirements

of the pan-European infrastructures and services [11].

The EC defines *Interoperability* as "*the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge*". *Interoperability framework* is defined as "*a set of standards and guidelines that describes the way in which organisations have agreed, or should agree, to interact with each other. An interoperability framework is, therefore, not a static document and may have to be adapted over time as technologies, standards and administrative requirements change*" [7]. Interoperability is "*like a chain that allows information and computer systems to be joined up both within organisations and then across organisational boundaries with other organisations, administrations, enterprises or citizens*" [1]. It has three main aspects:

- *Technical interoperability*, which is concerned with the technical issues of linking up computer systems, the definition of open interfaces, data formats and protocols, including telecommunications;
- *Semantic interoperability*, which is concerned with ensuring that the precise meaning of exchanged information is understandable by any other application not initially developed for this purpose; and
- *Organisational interoperability*, which is concerned with modelling business processes, aligning information architectures with organisational goals and helping business processes to co-operate.

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 and Sixth Framework Programmes, such as GUIDE [4], PRIME [14], FIDIS [2], etc. The paper focuses mostly on the research and development outcomes of the GUIDE project, which are mainly related to the technical interoperability issues. However, the paper considers these issues in the context of the dynamics of research and development in the area.

2. The GUIDE Project. The primary purpose of the research within the FP6 GUIDE Project "*Creating an European Identity Management Architecture for eGovernment*" 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*" [5]. 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).

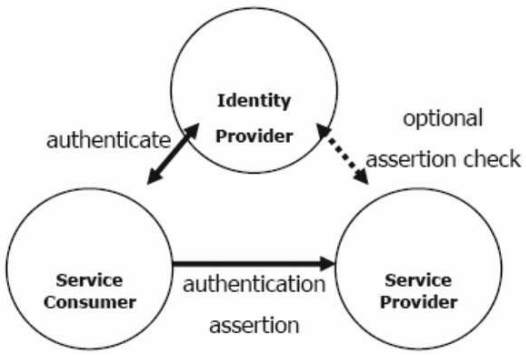

Fig. 1. Basic Identity Federation Model

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 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 a national level. However, in most cases these federations are being constructed in isolation from each other. It is the objective of the research to define an architecture that will enable to join together these federations into a greater circle of trust, in order to facilitate an apparently seamless identity environment across the whole EU. In this respect the project is conceived as providing a pan-European federation of identity federations, which can also be described as an *identity grid* or *identity network*.

The GUIDE interoperability approach envisages that each member state could situate a GUIDE 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 [3]. These adaptations are made on both sides, so the number of possible end to end mappings will be reduced (see Fig. 2). 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 local security system used should be capable to operate in 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.

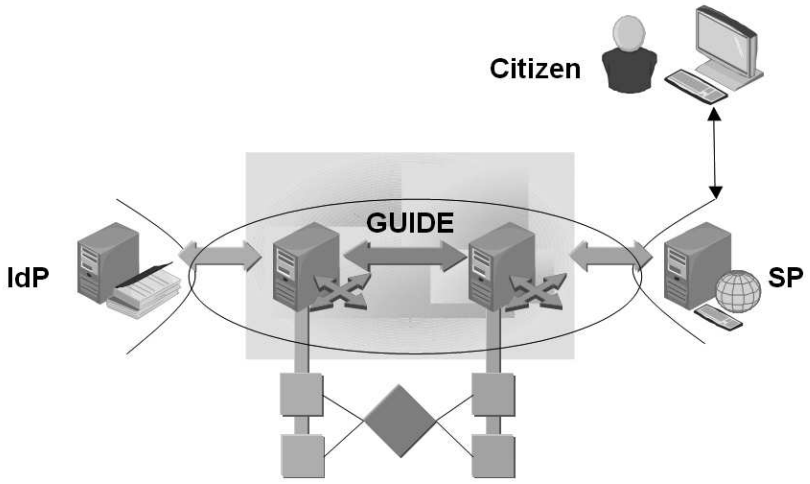

Fig. 2. GUIDE adaptation to existing systems

3. GUIDE Services and Scenarios. In order to establish a "*Pan-European Government Services* (PEGS)" system, some additional layers and services must 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 GUIDE 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 GUIDE infrastructure as an additional layer over the existing identity and application service providers. This infrastructure interacts with the existing systems on the basis on state-of-the-art industry standards. The enhancements proposed by the GUIDE 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 GUIDE 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 user's 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 Fig. 3), 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 GUIDE 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 was 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 Bindings*. This aspect covers the transport mechanism of a single interaction.

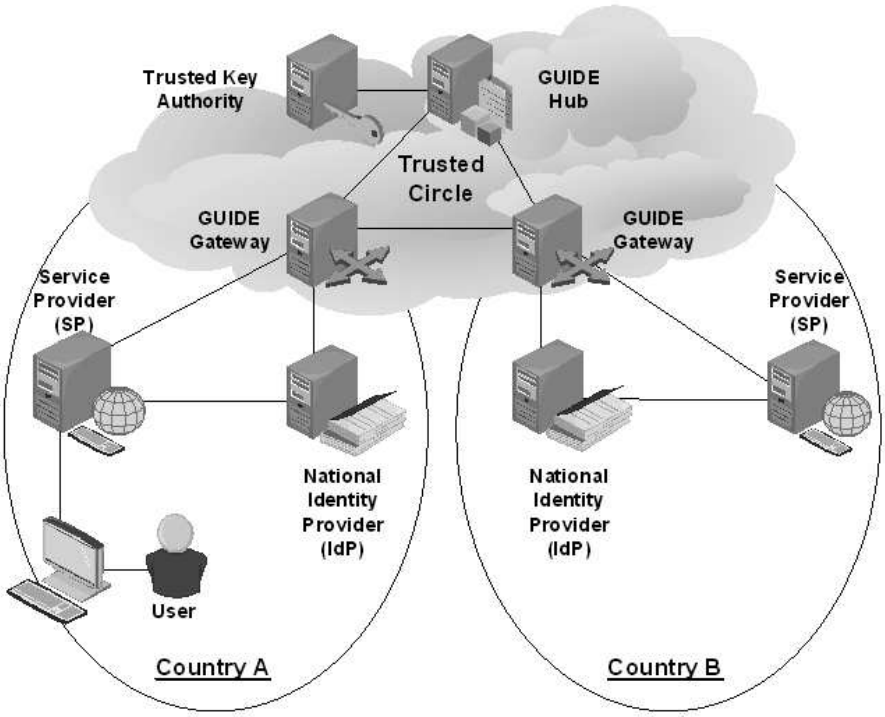

Fig. 3. Overall Context for Services

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 GUIDE infrastructure solution is developed. For the description of the services, required for the GUIDE 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 who 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 Citizen's 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 who 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.

The abovementioned services are employed in a trial for users who temporarity work in a member state other than their original one. They continue to receive their salary from their country of residence, but they have to pay their social insurance contributions to the member state that they are working in. The scenario is based on using "*E-forms*" in order to speed up the process of claiming social security benefits when one is moving between European Economic Area (EEA) countries. These forms are standardised throughout the EEA and can be obtained from any social security institutions in these countries.

The e-form *Request Initialisation Process* within the country of origin could be described as follows:

a. The employer fills in an e-form application for one of his migrant workers. A civil servant from the original Member State Administration (MSA1) accepts it.

b. The identity of the employee will be checked and all essential data (identity and attribute data) will be retained at the database of the MSA1.

c. An e-form form is issued and provided to the employee and the employer.

d. The e-form is provided to the social security web site of the country of origin.

The process within the destination state could be described as follows:

a. The e-form is made available to the MSA2 in order to announce an entitlement to social benefits. The civil servant accepts and initiates a cross-border authentication process. Since MSA2 wants to maintain data of the migrant worker on its part, it requires some identity data (or attribute data) from MSA1. In this case the authentication method applied in the destination state is used.

b. An authentication request is created and delivered to the MSA1. Before conveying the request through the secure interoperable GUIDE grid, a transformation process takes place.

c. Within the GUIDE grid the transformed authentication request is transported to the GUIDE gateway associated to the home state. The authentication service is provided by credential processes in the GUIDE grid.

d. After a re-transformation of the authentication request, it is conveyed to the associated MSA1. The credentials are sent. Within the MSA1 the provided credentials are checked and an authentication response is created to specify the effected authentication process.

e. The authentication response is sent back to the MSA2. Before transporting it through the GUIDE grid, the authentication response is transformed into a GUIDE specific format. The response message includes all information required by the MSA2 in order to allow access to the secured resource.

f. Within the GUIDE grid the authentication response is delivered to the GUIDE gateway related to the state of destination.

g. A retransformation of the authentication response is processed and the MSA2 obtains the authentication response including the authentication status and possibly some identity data (and/or attribute data).

h. The MSA2 sends a list of the requested attributes and attribute values to the MSA1.

i. The obtained identity and attribute data are registered at the database of the country of destination and made available at the social security web site.

j. The identity of the employee and some attribute data are now available for the MSA2.

4. GUIDE Infrastructure. As described earlier, the GUIDE infrastructure is positioned between the IdPs and the SPs. The adapters are responsible for interacting with the different systems, for transforming any request from the source format to an internal format, and for putting it to the target adapter where the request will be transformed to the target format (see Fig. 4).

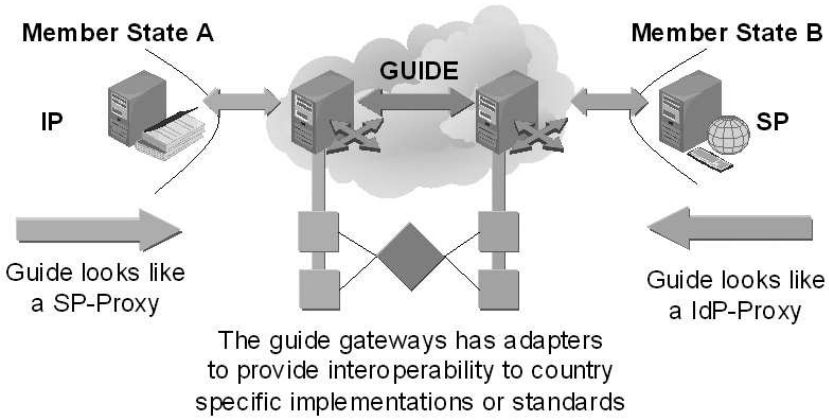

Fig. 4. GUIDE adapter architecture

A perfect GUIDE 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 also be 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 5. 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.

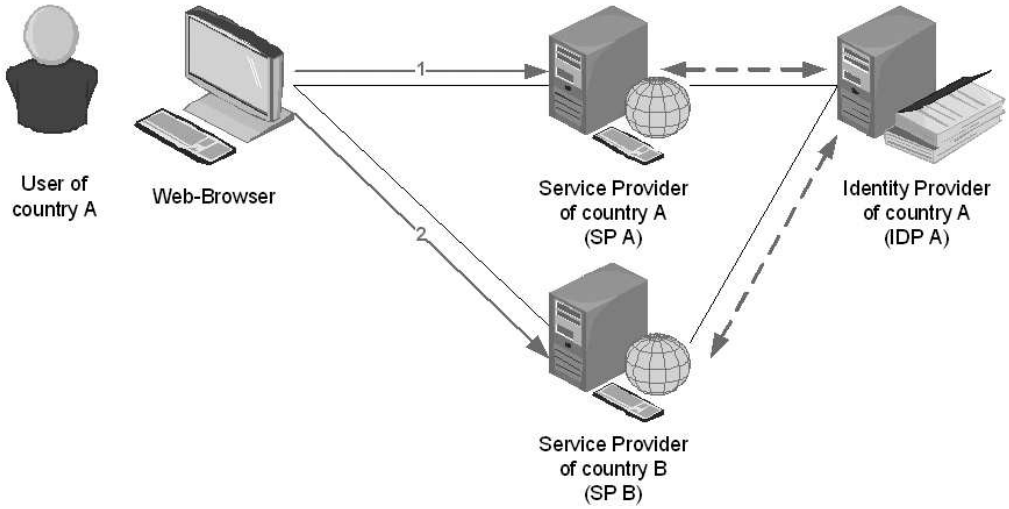

Fig. 5. Single Sign On (SSO)

Since most 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 GUIDE infrastructure between them. Such architecture would enable interoperability and single sign on service at a pan-European level.

5. Federated Identity Management Standards and Technologies Used. In order to achieve Federated Identity Management (FIM) through the GUIDE network common FIM standards are used. The FIM standards are SAML-based standards [13], such as Shibboleth [9], Liberty Alliance ID-FF [10] and SAML V2.0. SAML, developed by OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML is a flexible and extensible protocol designed to be used and customized, if necessary, by other standards. The Liberty Alliance and Internet2 Shibboleth project have adopted SAML as a technological underpinning. The SAML V2.0 specification was completed in January 2005 with the purpose to achieve full convergence for FIM standards, because it unifies Liberty ID-FF, Shibboleth and SAML V1.1. SAML V2.0 is actually a superset of these standard specifications

and therefore it is adopted by GUIDE for composing all profiles, protocols and bindings.

In the high-level use cases (see for instance Fig. 5) two levels of communication mechanisms are involved, namely:

- *Front end communication.* It is achieved by *http redirection* which extends a simple click on a web address. It gives the possibility to handle more control information and to move the user from one location to another. The user at the web browser has to be guided to the right service location which is necessary for the next step in the workflow. For example, a user from a public web page with no encrypted connection could be moved to more secured pages, which are accessed with encrypted connection (SSL).
- *Back end communication.* The back end communication between servers using SAML based assertions is achieved by *web services* with XML formatted data. The distributed systems and functionality have to exchange information to complete the workflow.

The Authentication Service defines the interaction between a Web Service Consumer (WSC) and the Web Service Provider (WSP). If the WSP is willing and able to provide the service, an authentication exchange will take place. The authentication exchange is based on a SOAP protocol and can involve an arbitrary number of round trips, as is the case with a mechanism based on Simple Authentication and Security Layer (SASL) [12]. The WSC may have out-of-band knowledge of the server's supported SASL mechanisms, or it may send the server its own list of supported SASL mechanisms and allow the server to choose one among them. At the end of this exchange of messages, the WSC will either be authenticated or not. The nature of the authentication highly depends on the SASL mechanism that has been employed. WSP will also be authenticated depending on the SASL mechanism employed.

In order to successfully address interoperability, it is important to know what type of scenarios exist. Once they are created, it would be clear how the interaction between determined entities is taking place. Within a scenario all participating system entities and users, as well as the way of exchange of information between them, are determined.

6. The GUIDE Adaptor Structure. As was stated above, the main tasks of a GUIDE gateway are *adaptation*, *transformation* and *transportation* of interactions between the different parties of a pan-European government scenario. In order to support these tasks some additional services have to be employed. (See

Fig. 6 and Fig. 7, where only one direction of interaction is marked—the other direction is symmetric.) Such services are described bellow:

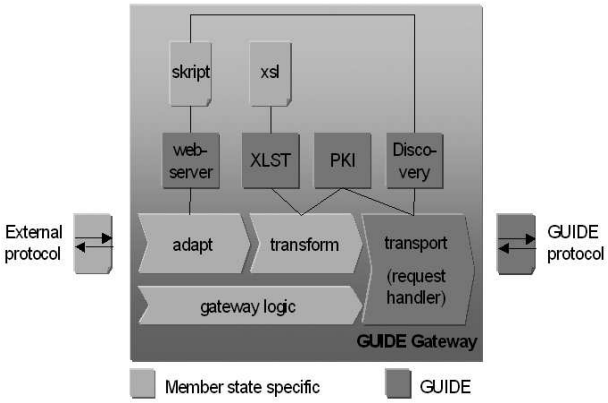

Fig. 6. Adapter Structure

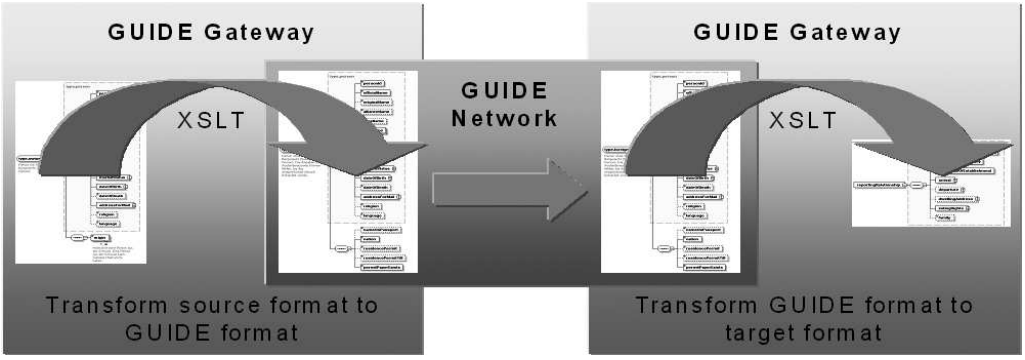

Fig. 7. Data transformations in GUIDE

- The web server has to be able to handle redirections that are often used in the citizen present scenario and standards like Shibboleth or Liberty Alliance. Additionally, it has to be able to provide some dynamic web pages to give the citizen the possibility to select the associated IdP in case of authentication. This selection process requires the discovery service to be able to get the essential information.
- The "*Extensible Stylesheet Language Transformations* (XSLT)" can be used to transform the data content from one structure to another, especially in the case of XML-based data. The transformation would be controlled by a

stylesheet.

- The PKI infrastructure is responsible for encrypting and decrypting the content between the different parties. The only way to enable a data transformation between the country specific data format and the GUIDE data format is to know the name of a single data element.
- The discovery service stores the routing information about the associated system entities, such as IdP, SP and the GUIDE Gateway.

7. Conclusions. Interoperability is the ability of systems to provide services to and to accept services from other systems. To facilitate mutually using services from other equipments a communication layer between them is needed. Since the involved systems use different set of instructions concerning semantic and syntactic aspects, they must be transformed, so that the opposite system can understand them. The abovedescribed interoperability solution deals mostly with its technical aspects. The GUIDE approach aims at building an eGovernment pan-European interoperability infrastructure based on SAML related FIM standards.

The new EIF v2.0 will provide a new set of recommendations both for doing research in the area of Identity Management and for real deployment of a pan-European infrastructure for eGovernment services [11]. Among the main issues to be addressed in the EIF v2.0 are:

- *Public Service Legislation.* It includes administrative law, identification and authentication, intellectual property rights, liability, privacy and data protection, public administration transparency relationships between public administrations, citizens, businesses and other IT actors and the re-use of public sector information in base registries.
- *Public Service Pricing* of basic and aggregate public services at a European level.
- *Accessibility* of aggregate public services, e.g., disabled and digitally agnostic persons should be able to experience the same service levels as other people.
- *User Identification and Authentication* in a multi-layered federation of the EU: states, businesses, and employees;
- *Transaction Certification* to provide signed, certified, encrypted and logged document exchange between administrations, businesses and citizens.

- *Aggregate Service Certification* to create trust though certification of intermediaries to provide aggregate services using basic public services.
- *Business Process and Semantic Standardization* – to align business processes and information exchange between constituencies as a prime condition for interoperability.
- *Technical Standardization* to provide technical interoperability between disparate systems of constituencies, including citizens using browsers as their primary access point.
- *Basic Public Service Authorization* to determine which public services may be disclosed to which constituency and/or intermediary.
- *Basic Public Data and Service Certification.* Intermediaries delivering aggregate services must be able to trust the basic services provided;
- *Cross-Certification.* It is needed for secure exchange of information (in documents and services) between constituencies in different Member States, each having their own (multiple) identification, authentication and certification infrastructures.

REFERENCES

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

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

[3] Gorton I., Thurman, D., Thomson, J. Next Generation Application Integration: Challenges and New Approaches, Proceedings of 27th Annual International Computer Software and Applications Conference COMPSAC, Dallas, November 3–6, 2003.

[4] GUIDE, Creating an European Identity Management Architecture for eGovernment, `http://www.guide-project.org/`.

[5] GUIDE, GUIDE Technical Implementation Interoperability guidelines: Core Services Interoperability Guidelines, Internal Document, October, 2006.

[6] Halperin R. Identity as an Emerging Field of Study, *Datenschutz und Datensicherheit* **9**, Wiesbaden (2006), 533–537.

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

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

[9] Inernet2, Shibboleth Introduction, `http://shibboleth.internet2.edu/shib-intro.html`.

[10] Liberty Alliance, The Liberty Alliance Project, `http://www.projectliberty.org/`.

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

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

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

[14] PRIME, *Privacy and Identity Management for Europe*, `http://www.prime-project.eu.org/`.

Centre of Information Society Technologies
Sofia University
125, Tsarigradsko Shose Blvd, Bl. 2
Sofia 1113, Bulgaria
e-mail: `kamelia@fmi.uni-sofia.bg`
`roumen@fmi.uni-sofia.bg`

Received January 11, 2008
Final Accepted February 11, 2008