eChallenges e-2009 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2009
ISBN: 978-1-905824-13-7

Introducing Federated Identities to One-Stop-Shop e-Government Environments: The Greek Case

Prokopios DROGKARIS, Costas LAMBRINOUDAKIS, Stefanos GRITZALIS
Lab. of Information and Communication Systems Security, Dept. of Information and Communication Systems Engineering, Greece
Tel: +30-2273-82275, Email: pdrogk@aegean.gr

Abstract: Even though e-Government environments have achieved a certain interoperability level and coherence across public sector, there are several approaches, technologies and mechanisms that could aid these environments towards delivering more user-centric electronic services. This paper focuses on the aspect of identity management. More specifically it presents a framework that incorporates the notion of federation and federated identities in order to overcome the impediment of per-sector identifiers. Moreover, it provides Single Sign-On access to electronic services through the utilization of a linking mechanism. This framework has been based on the Greek Interoperability Framework and its specific requirements and limitations.

1. Introduction

Modern e-Government environments strive to achieve interoperability across the entire "electronic" public sector, thus offering effective information sharing, simplified access to services while preserving data privacy and security. The effect of Identity Management (IdM) towards this direction is certainly of great importance since it is responsible of linking real world identities to digital ones [1]. A relatively new concept, that has been proposed as an extension of identity management, for granting user access to multiple resources offered by different providers, without imposing the need for separate authentication to each one, is that of Federation Identity Management (FIM) [2][4].
In this paper we propose a simple and practical mechanism for bonding together the different per-sector identifiers that are currently used for the identification of users within the Greek public sector. This mechanism utilizes the existing Public Key Infrastructure deployed in the Greek e-Government Environment and conforms fully to the existing legal framework. The rest of the paper is organized as follows: Section 2 provides the objectives of our research after presenting the current status of the Greek e-Government Environment on which our research was based on. Section 3 presents the methodology of our research along with a brief overview of recent successful FIM deployments in other e-Government environments, while Section 4 provides some background information regarding Federated Identities and FIM. Section 5 discusses the proposed mechanism and Section 6 presents how this mechanism was incorporated into the Greek e-Government Environment. Finally, Section 7 provides an overall analysis of our proposal while Section 8 concludes the paper.

2. Objectives (Greek e-gov)

Over the last decade, the Greek public sector has moved to the e-Government era, in an attempt to improve the quality of the provided services. Currently, several ministerial departments offer their services electronically and a complete e-Government framework has

been proposed as described in [9] and is currently being implemented. The main objective of this framework is the support of common authentication and registration mechanisms for accessing all available electronic services as well as the development of a Central Portal, named "Ermis" [10] , that operates as an *one-stop shop* that provides to citizens a common interface for all public sector electronic services. A general overview of this framework is depicted in Figure 1, while its main characteristics / components are briefly described next.

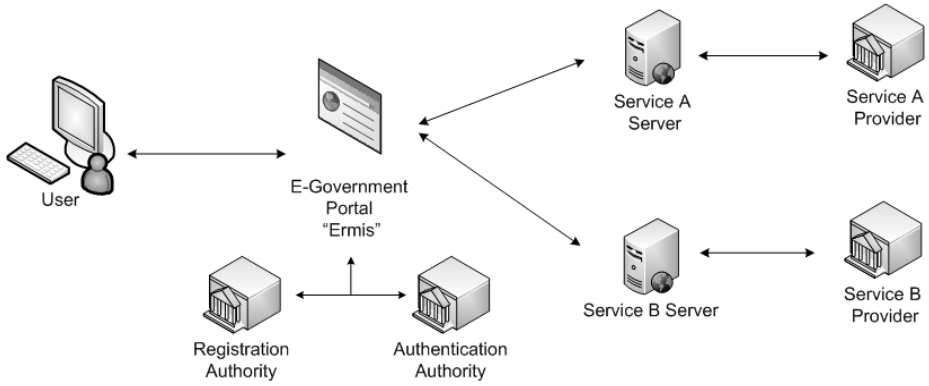

Figure 1: Greek e-Government Environment Overview

- *Central Portal "Ermis"*: This citizen portal, known as *Ermis,* is the interface between users and ministerial departments. Its main purpose is to bring electronic services together providing a common interface between citizens and public sector, operating as a *one-stop shop*.
- *Uniform Registration and Authentication Procedures*: The registration and authentication procedures required for accessing the offered electronic services are provided through the Central Portal.
- *Assignment of the offered services to different Trust Levels*: All electronic services offered through the Ermis Portal have been linked to pre-determined trust levels; these trust levels are understood as "The level of confidence that the organization offering the service has at the end-user's electronic identity along with the assurance that the security measures and procedures deployed to safeguard the access, the processing and the transmission of data are adequate".
- *Per Sector Identifiers*: The identification of the users wishing to utilize one of the Greek public sector services is accomplished through "per sector identifiers". These identifiers are given to each citizen the first time she requests to use a service (through the registration process) of a specific sector, identifying her uniquely within that specific sector.

Even if the deployment of unified registration and authentication procedures has transformed the provision of electronic services due to the lack of multiple authentication credentials, the utilization of per-sector identifiers confines the overall level of framework's flexibility, applicability and user friendliness as end user's are obliged to submit every time the corresponding identifier. Based on that remark, the objectives of our research are the following:

- Overcome the impediment of per-sector identifiers
- Provide improved Single-Sign-On access to electronic services
- Provide an identity management framework based on the use of a single identity
- Preserve data privacy
- Comply with Greek legal framework

3. Methodology

The methodology that was undertaken for our research was to examine identity management techniques that could provide cross domain digital identity linking and Single-Sign-On functionalities. The recent examples of e-Government Environments in United Kingdom [6] and New Zealand [8] that have incorporated the notion of Federated Identities are very promising indeed and demonstrate great potential. United Kingdom has created a Central Authentication Service that supports Single-Sign-On to government organizations that make use of a specific authentication protocol. In New Zealand two centralized services have been developed: Government Logon Service (GLS) for the authentication of users and the Identity Verification Service (IVS) for the delivery of user's identity attributes to SPs, supporting centralized registration and authentication procedures as well as provision of SSO access to users. Based on these successful cases and their positive contribution in the environments that they were applied, we examined the introduction of federated identities to the Greek e-Government environment.

4. Technology Description (FIM)

All Federated Identity Management (FIM) infrastructures rely on the establishment of trust relationships among the participating parties. After all participants mutually consent on legal agreements, they form a "*Circle of Trust*" and are then obliged to provide legitimate information about their users whenever some other trusted participant requests it. Two vital entities of the FIM infrastructure are the Identity Provider (IdP) and the Service Provider (SP). IdP is responsible for managing user identities, issuing and verifying authentication credentials and vouching for users' identity to SPs. SP, on the other hand, is responsible for validating users' identity information and granting access to services depending on the identity attributes. This interconnection of SPs, allows the Identity Management Systems (IdMS) of trusted parties to support Single-Sign-On (SSO) access by allowing users to access federation resources after a single authentication. SSO functionality is based on an "*account linking*" mechanism that is performed on user's distinct identity accounts in trusted parties' resources by introducing a Common Unique Identifier (CUID). This identifier is linked with all user's identity accounts and provides a common basis for user identification from every IdP to every SP.

The perspective of introducing Federated Identities to the Greek e-GIF Framework is very compelling. The Central Portal "Ermis" will not only be able to provide one-stop-shop services but also SSO access by incorporating the registration and authentication procedures and therefore acting as IdP. Ministerial departments will act as SP and together with Ermis they will form the requisite Circle of Trust. In order, though, to overcome the impediment of per-sector identifiers, an "account linking" mechanism must be applied. By performing this collation, Ministerial Departments and Ermis will be able to identify each user uniquely and exchange information regarding his/her identity and authentication status.

However, such a collation introduces security and legal issues that are not addressed by the current framework architecture. Since all ministerial departments are now able to identify each user uniquely through a CUID, they can also request and exchange data (data interconnection) about some specific user without previous notice and consent. Having studied the relevant Greek and European Legal Framework along with the Greek Constitution, the account linking functionality that is based on the introduction of Common Unique Identifiers cannot be deployed in the Greek e-Government Environment. Greek Law 2472/97, Greek Constitution (paragraph 9A) and article 12 of EU Data Protection Directive 95/46/EC clearly state that in order to exchange and process personal data, the user's consent is required. Moreover, the introduction of a unique identifier for the public

sector opposes to the Greek Constitution (article 2, paragraph 1) which refers to "Value of Individuals".

5. Developments

In this paper we propose a simple and practical mechanism for bonding together different per-sector identifiers that are currently used for the identification of users within the Greek public sector. This approach sets the corner-stone for introducing Federated Identities to the Greek e-Government Environment by providing a common user identification method for Ministerial Departments offering electronic services and Ermis. The proposed mechanism is based on Public Key Cryptography for preserving user's privacy and data security while overcoming the legal barriers imposed by the Greek and EU legal framework as described in Section 4. Greek e-Government Authentication framework embodies a PKI infrastructure for the support of digital signatures and for data encryption by ministerial departments and users. Our proposal is to utilize each department's encryption key pair for storing the corresponding per sector identifier to Ermis portal, in a predefined sequence, along with an identifier assigned by Ermis itself. Since the forwarded identifier is encrypted, only the ministerial department that performed the encryption can decrypt it and thus identify the user. Figure 2 below, depicts the sequence of encrypted identifiers for Users A and B that will be stored in the Central Portal.

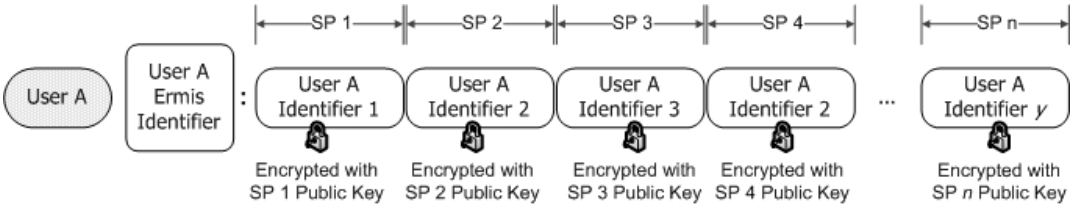

Figure 2: Per-Sector Identifiers Bonding Proposal

The first identifier "*User A Ermis Identifier*" is introduced in order for Ermis to be able to identify each user uniquely. Furthermore, it serves as the linking mechanism to all per-sector identifiers of each user. The next blocks of the sequence consist solely of encrypted identifiers. The number of these blocks must obligatory be equal to the number of Service Providers that offer their services electronically. Each Service Provider is assigned to a specific block where its identifier is stored. Since it is not rare for two different Service Providers to utilize the same per-sector identifier (for example SP 2 and SP4), this identifier must be encrypted twice, once with Service Provider's 2 public key and once more with Service Provider's 4 public key and each time stored in the appropriate blocks.

6. Results

The deployment of the proposed mechanism to the Greek e-Government Interoperability Framework drastically ameliorates the way end users interact with central portal Ermis and as a consequence with provided electronic services. As presented in Figure 3 below, after User A successfully completes the required authentication procedures, she can request the desired electronic services without having to submit the corresponding identifier to Service Provider. Each time she requests an electronic service, Ermis looks up which Service Provider is responsible for the provision of the requested service and knowing the sequence that the identifiers are stored, retrieves the appropriate encrypted identifier and forwards it to the Service Provider along with user's service request. Service Provider decrypts using his private encryption key and is now able of identifying the user who requested the service. Without the addition of the proposed bonding mechanism, end users are obliged to

authenticate to Ermis and submit the appropriate per-sector identifier for every electronic service request they make.

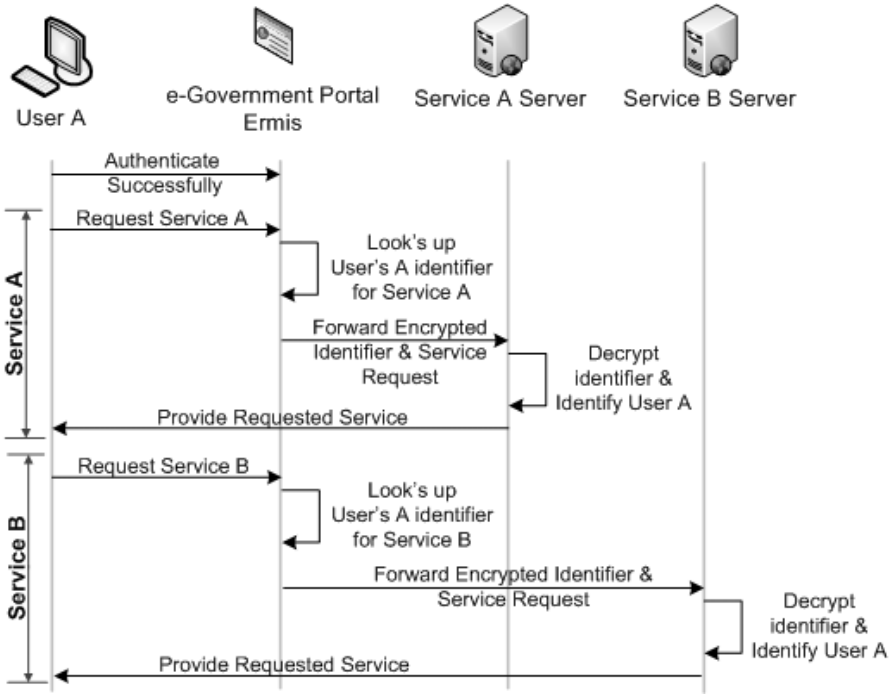

Figure 3: Greek e-Government Framework Operation with Federated Identities

7. Business Benefits

The expected benefit from deploying the proposed mechanism to the Greek e-Government Environment is the provision of user-centric Single Sign-On access across multiple Service Providers while embracing the use of different authentication mechanisms. Such access to electronic services will contribute towards better interoperability of the public sector as well as the ease of the overall's framework's acceptance, while preventing data interconnection and preserving data privacy. Of course, all these improvements come with a cost.

Since Ermis will be assigned to administrate all users' identifiers, one could argue that it constitutes a Single Point of Failure (SPOF) for the provision of electronic services. Even if the confidentiality of data is ensured due to the utilization of PKI, the integrity and availability of the data must also be preserved. In addition to that, even if the architecture of the Greek e-Government's environment is not drastically altered, minor changes would be required to communication protocols, standards and Service Provider's internal procedures in order to fully adopt and utilize FIM capabilities at their full extent. The existence of ratified open standards [7][16][19] aids towards this direction as they allow for full integration with existing standards and methodologies. Surely, for this transformation to be successful, e-acceptance metrics should be taken into consideration in order to satisfy the fundamental requirement of providing user-friendly electronic services.

8. Conclusions

In this paper we have presented a framework that incorporates the notion of federation and federated identities in order to overcome the impediment of per-sector identifiers as described in Section 2. The adoption of Federated Identities from the Greek e-Government environment will certainly contribute to its transformation to 'Joined-Up Government" (the integration of processes and services necessary to achieve a seamless, citizen-centered government)' that allows Single-Sign-On access to all available electronic services, through

a secure interoperability framework. However, the desired interoperability can be divided to many levels: Legal, Organizational, Semantic & Technical. Our proposal covers all these aspects as it ensures compliance with legal framework and provides the appropriate technical base through mechanisms and procedures apart from Organizational. From this point, Public Administration should take over by forming a strategic plan that will set the targets and the objectives of the transformation while ensuring the desired cooperation.

References

[1] Marco Casassa Mont, Pete Bramhall, Mickey Gittler, Joe Pato, Owen Rees, "Identity Management: a Key e-Business Enabler", Trusted E-Services Laboratory HP Laboratories Bristol, 2002

[2] Casassa Mont, M., P. Bramhall, J. Pato, On Adaptive Identity Management: The next generation of Identity Management Technologies, HP Labs Technical Report, HPL-2003-149,2003

[3] Dongwan Shin, Gail-Joon Ahn, Prasad Shenoy, Ensuring information assurance in federated identity management, 2004, IEEE International Conference on 2004

[4] Axel Buecker, Paul Ashley, Neil Readshaw, Federated Identity and Trust Management, IBM Redbooks, 2008

[5] Federation in eGovernment - Denmark Case Study, http://www.projectliberty.org/liberty/content/download/451/2916/file/Federation_eGov_Denmark.pdf

[6] The UK Leverages Open Federation and Interoperability to Serve Citizens, http://www.projectliberty.org/liberty/content/download/2460/15865/file/UK-CaseStudy.pdf

[7] Security Assertion Markup Language (SAML) V2.0, Oasis,2007, http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf

[8] New Zealand Sets the Pace for SAML 2.0 Deployments, http://www.projectliberty.org/liberty/content/download/4058/27272/file/Liberty%20New%20Zealand%20Case%20study.pdf

[9] P. Drogkaris, D. Geneiatakis, S. Gritzalis, C. Lambrinoudakis, L. Mitrou, "Towards an Enhanced Authentication Framework for eGovernment Services: The Greek case", EGOV'08 7th International Conference on Electronic Government, E. Ferro, J. Scholl, M. Wimmer (Eds.), pp. 189-196, September 2008, Torino, Italy, Trauner Verlag

[10] Ermis: Greek Public Administration National Portal, www.ermis.gov.gr,

[11] Article 8 of the Greek Data Protection Law (Law 2472/97) accessible www.dpa.gr

[12] Article 2b of the Greek Data Protection Law (Law 2472/97) accessible www.dpa.gr

[13] Greek Constitution Articles 2 § 1 (human dignity) and 9 A (right to protection of personal data)

[14] EU Data Protection Directive 95/46/EC (Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31ff.)

[15] Abhilasha Bhargav-Spantzel, Anna C. Squicciarini, Elisa Bertino, Establishing and protecting digital identity in federation systems, Workshop On Digital Identity Management, 2005

[16] W3C. "Web Services Description Language (WSDL) 1.1". W3C Note, March 2001. http://www.w3.org/TR/wsdl

[17] Liberty alliance project, www.projectliberty.org

[18] Internet2. Shibboleth, http://shibboleth.internet2.edu

[19] WS-Federation, Web Services Federation, http://www.ibm.com/developerworks/library/specification/ws-fed , 2007