ENABLING SECURE DATA MANAGEMENT IN E-GOVERNMENT ENVIRONMENTS: THE GREEK CASE

Drogkaris Prokopios\(^1\), Gritzalis Stefanos\(^1\) and Lambrinoudakis Costas\(^1\)

Abstract: Modern e-Government environments adopt technologies that can support interoperability across the entire “electronic” public sector and thus new improved electronic services. At the same time new requirements are raised from the users. This paper presents ongoing research on a secure user data management architecture for e-Government environments. More specifically the utilization of Privacy Preferences and Privacy Policies along with the introduction of two entities responsible for administrating user documents and data management is proposed. The research work presented has been based on the Greek Interoperability Framework and it's specific requirements and limitations.

Keywords: e-Government, Security, Privacy, Interoperability, Personal Data Management

1. Introduction

Over the last decade e-Government environments have undergone massive transformations towards information systems coherence and interoperability. Modern e-Government environments support a seamless flow of information across ministerial departments and users, while several new requirements have been raised in order to deliver integrated services. One of these requirements, already known to other similar to e-Government environments such as e-Commerce, is the concept of secure user data management. Up to now, the data involved in such management architectures were mainly personal data, such as first and last name, email address and date of birth. The prospective of enabling secure management over all data types (personal, sensitive, financial) and documents could significantly improve the seamless, citizen-cantered e-Government scenarios.

\(^1\) Information and Communication Systems Laboratory, Department of Informations and Communications Systems Engineering, GR-83200, Karlovasi Samos. {pdrogk,sgritz,clam}@aegean.gr
Let us consider a citizen who wishes to electronically apply for a job in the Greek public sector. In order to successfully complete the required registration and authentication procedures the user has to submit an electronic application form and the following documents: i) a birth certificate, ii) a marital status certificate, iii) a criminal record copy and iv) an army enlisted record copy if user’s gender is male. Consequently, the user has to invoke the appropriate services in order to obtain the aforementioned documents prior to electronically applying for the job. Similarly, in a conventional case, the user would have to request the documents from the appropriate offices and then submit them in person along with the application. The ideal case for the user would be to submit the application electronically and authorize the ministerial department to request the necessary documents on his/her behalf. However, due to the several data interconnection restrictions that are in place this is not feasible. An alternative case would be to allow e-Government users to store personal data and documents and enable their retrieval whenever an electronic service would require them. In this case, and assuming that the user has already obtained all necessary documents, she would not be obliged to request them again; instead she would provide them directly to the electronic service.

This paper presents the initial results of our ongoing research work on secure user data management architecture for e-Government environments. The proposed framework aims at enabling secure storage and privacy compliant management of user data and documents, based on the user’s privacy preferences and on the privacy policies of the corresponding Service Provider. The rest of the paper is organized as follows: Section 2 provides background information regarding other proposals for secure user data management. Section 3 presents the characteristics of the Greek e-Government Environment on which our proposal has been based. Section 4 introduces and analyzes the proposed architecture, while Section 5 presents the considerations that should be taken into account during further development of the scheme. Finally, Section 5 concludes the paper by providing some thoughts in regard with the deployment of the proposed architecture.

2. Related Work

The conception of secure management of personal data over the web is certainly not new. Carminati and Ferrari have proposed an architecture in [1] where an entity is responsible for encrypting and releasing personal data depending on user’s privacy preferences. The key component of their proposal was the introduction of a new entity, known as Trusted Privacy Manager (TPM), which is responsible for data encryption as well as for the generation and delivery of encryption keys. The privacy of the stored data is achieved by delivering the corresponding decryption keys to the data owner, thus appointing her responsible for any subsequent decryption process. Even though this approach appears to be efficient, password protection is not appropriate for environments managing the personal data of many users. An alternative approach proposed by Efraimidis, Drosatos, Nalbadis & Tasikou in [2], is an architecture for Personal Data Management over e-commerce environments. In this proposal each data owner has to participate into a privacy contract (consisting of privacy agreements) with the data collector, otherwise no transaction can be performed between the two parties. The challenge, though, in privacy contracts is how to ensure that the participants will not violate the pre-agreed terms.
3. An Overview of the Greek e-Government Framework

The proposed security architecture has been based on the characteristics of the Greek e-Government Interoperability Framework and the corresponding Authentication sub-Framework as presented in Error! Reference source not found.. A general overview of this framework is depicted in Figure 1, while its main characteristics / components are briefly presented next.

![Figure 1: Greek e-Government Environment Architecture](image)

- **Central Portal “Hermes”**: This citizen portal, known as Hermes, 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 “Hermes”. Registration and Authentication Authorities operate under the supervision of Hermes where: the Registration Authority (RA) is responsible for the registration procedure and for maintaining a record of the services that a user may access, while the Authentication Authority (AA) is responsible for authenticating users and allowing them to interact with the Service Providers.

- **Assignment of the offered services to different Trust Levels**: All electronic services offered through the Hermes Portal have been assigned to pre-determined levels of trust; these levels are understood as “The level of confidence at an 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.
4. The Proposed Security Framework

The proposed framework enables secure storage and privacy compliant management of user data and documents, based on her privacy preferences and the privacy policies of the corresponding Service Provider. The innovative feature of the proposed framework lays in its ability to utilize different user privacy preferences for each different piece of information. This segregation supports an improved and much more detailed comparison between Privacy Preferences and Privacy Policies, thus allowing a better data management. The main entities of the proposed architecture are the Data Management Authority and the Privacy Policies Authority. As demonstrated in Figure 2 below, these two entities are under the supervision of Central Portal “Hermes” in order to preserve the One-Stop Shop character of the Greek e-Government Environment, ensure their acceptance from ministerial departments and their uneventful collaboration with electronic services.

![Proposed Framework Overview](image)

5.1 Privacy Policies and Preferences

Since the proposed framework aims towards data and documents management without user’s interaction, it adopts the notion of Privacy Policies and Privacy Preferences. Privacy Policies are used for each electronic service that is provided through the “Hermes” portal. The Privacy Policy of an electronic service clearly states:

- **What type of data and documents** are required for the successful completion of the service,
- **What is the purpose** of requesting these data and documents,
- **How these data and documents** will be processed.

The validity of Privacy Policies is attained through the Digital Signature of the Service Provider that accompanies it. These policies will be expressed through the Privacy Preferences (P3P) [5] platform that provides a standard way for encoding privacy policies in XML format. However, as described in [7], several additions to the P3P privacy statements syntax are necessary in order to fully support the required context.
Apart from Privacy Policies, the notion of Privacy Preferences is adopted in order to support the expression and storage of user preferences regarding the data and documents privacy. For each user, every document or data that has been submitted is related to a specific Privacy Preference statement. Through this statement, she is able to express her preferences regarding:

- **The type of data or documents** that have been submitted,
- **For what purpose these data or documents** can be forwarded to an electronic service,
- **How these data or documents can be processed** by an electronic service.

Similarly to Privacy Policies, the validity of user Privacy Preferences is attained through the user’s digital signature. For the expression of these preferences, APPEL (A P3P Preference Exchange Language) [4] standard language has been selected as it is based on XML syntax and can be easily matched with the P3P Privacy Policies. Again, some syntax extensions are necessary due to APPEL’s weaknesses as described in [8] & [9].

### 5.2 Data Management and Privacy Policies Authorities

The Data Management Authority is responsible for storing data and documents that are submitted by users wishing to utilize the proposed data management functionality. Furthermore, it is responsible to release data or documents regarding a specific user whenever it is instructed to do so by a Privacy Policy Authority.

### 5.3 Data Management in Use

An overview of the proposed architecture’s data management procedures is provided in Figure 3 below. The description is divided into three discrete phases. The first phase is the “**Service Provider Privacy Policy Submission**”. As described in Error! Reference source not found, each Service Provider who wishes to offer electronic services through the Hermes Portal, must report to “Hermes” about the “per-sector identifier” that utilizes, the Trust Level that the electronic service must be assigned to and finally the documents that users are required to submit during their registration with the specific service. The additional step required by our architecture is that each Service Provider must also submit its Privacy Policy (1.2) which is forwarded and stored to the Privacy Policies Authority (1.3).
The second phase is “User Data submission to Hermes Portal” which includes the procedures that the users should follow in order to store their documents and data. It is assumed that User A has registered with an electronic service offered through the Hermes Portal and that she has acquired an electronic document that was previously requested from this electronic service. This document is digitally signed by the Service Provider who issued it. In step (2.1), the user authenticates herself to the Hermes Portal, assuming a new session is being initiated, and requests to store the document she acquired earlier. In step (2.2) the user submits the document along with her privacy preferences about that document. The Registration Authority forwards the document to the Data Management Authority for storage (2.3) and validates the digital signature attached to it. Moreover, user’s A Privacy Preferences that relate to that document are forwarded and stored to the Policies Authority (2.4). The last phase is “Data Management”. User A requests Service B, through the Hermes Portal (3.1). For the successful completion of this service, the document that the user previously stored in the Data Management Authority is required. Service Provider B requests this document from the Data Management Authority (3.2), which forwards Service Provider’s A request to the Policies Authority (3.3). The Policies Authority restores Service Provider’s A Privacy Policy and User’s Data Privacy Preferences for the specific document and compares them (3.4). If they match, Policies Authority instructs the Data Management Authority (3.5) to dispatch the data to Service B Server (3.6).
5. Conclusions and Future Work

Irrespective of how promising the prospective of secure user data management in e-Government environments may be, the nature of the data processed imposes the need to preserve their confidentiality and integrity by preventing unauthorized disclosure and misuse. Currently, we are conducting a risk analysis of the proposed architecture in order to identify the necessary security mechanisms that it should feature and compare them against those already adopted in the Greek e-Government environment. These security measures should not only safeguard the storage and access of data but also preserve the existing security characteristics of the overall framework. Another vital aspect of our ongoing research is the compliance with the existing Greek and European legal framework, regarding personal data processing. Greek Data Protection 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, user’s consent is required. Finally, in an attempt to contribute towards electronic services coherence, there is on-going work towards the standardization of the contents of Privacy Policies and Preferences that are exploited by the proposed framework.

References

[4] A P3P Preference Exchange Language 1.0 (APPEL1.0), http://www.w3.org/TR/P3P-preferences/


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