TOWARDS AN ENHANCED AUTHENTICATION FRAMEWORK FOR e-GOVERNMENT SERVICES: THE GREEK CASE

Drogkaris Prokopios[1]*, Geneiatakis Dimitris*[1]*, Gritzalis Stefanos*[1]*,*
Lambrinoudakis Costas[1] *and Lilian Mitrou*[1]

Abstract: It is widely accepted that electronic Government environments have caused a complete transformation of the way individuals, businesses and governmental agencies interact with central government. However, the acceptance and success of e-Government services largely depend on the level of trust and confidence developed by the users to the provided services and the overall system security. Thus the employment of the appropriate authentication framework is a crucial factor. This paper focuses on the way to determine the appropriate trust level of an electronic service. Specifically, it provides guidelines according to the data required for a transaction, as well as to the available authentication and registration mechanisms. Moreover, a Single Sign-On architecture is proposed, supporting a uniform authentication procedure that depends on the level of trust required by the service. In the aforementioned research work specific requirements and limitations for Greece have been taken into account.

Keywords: e-Government, Security, Privacy, Authentication Framework

1. Introduction

Currently, governments all over the world have developed e-Government Interoperability Frameworks (e-GIFs) in order to achieve interoperability and information systems coherence across the "electronic" public sector, as well as in order to provide better services to the citizens. A vital part of the interoperability framework is the authentication sub-framework. Its main purpose is to provide an effective approach for determining the level of confidence, trust and assurance required by an electronic service as far as the authenticity of an individual's identity is concerned. However, the parameters of an authentication framework, do not involve solely security characteristics. Normative restrictions, identification techniques, ministerial departments' interaction and other social issues dominate the way such a framework is designed and implemented.

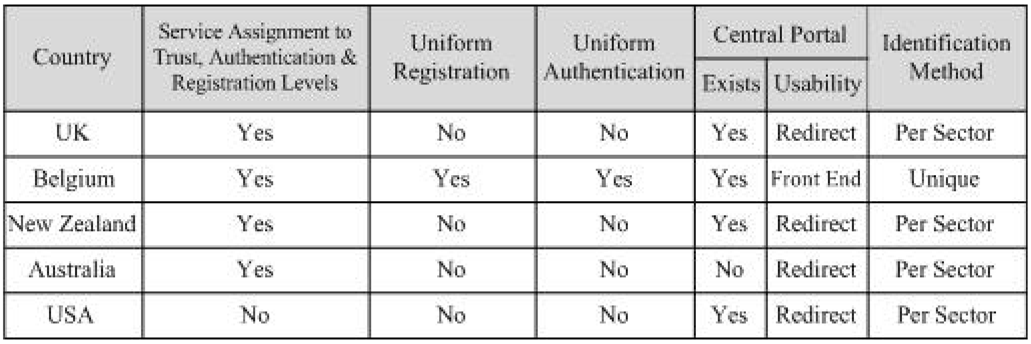
This paper presents an authentication framework that has been developed for the Greek Public Sector along with the corresponding guidelines for its adoption. Specifically: Section 2

[1] Information and Communication Systems Laboratory, Department of Informations and Communications Systems Engineering, GR-83200, Karlovasi Samos, {pdrogk,dgen,sgritz,clam,l.mitrou@aegean.gr}

provides an overview of well-known authentication frameworks all over the world. Section 3 deals with the electronic services already deployed by Greek ministerial departments as well as with corresponding legislation and central government decisions. Section 4 introduces the proposed authentication framework. Section 5 presents the guidelines structure for adopting the framework, while Section 6 introduces the corresponding Single Sign-On architecture. Finally, Section 7 concludes the article giving also some pointers for future work.

2. Worldwide Authentication Frameworks Practices – Related Work

The interoperability frameworks from United Kingdom [1], Belgium [2], New Zealand [3], United States of America [4] and Australia [5] have been widely accepted as best practises since they have gained the acceptance and trust of the users. The authentication sub-frameworks have been surveyed in order to identify the main common characteristics as well as the differences among them. Initially we investigate if the authentication frameworks provide rules or/and guidelines for assigning the electronic services to specific Trust, Authentication and Registration levels. Then we explore whether the registration and authentication procedures are uniform across the public sector. Furthermore, we review the identification methods employed for the provision of the electronic services, taking into account if the services are provided via a central portal or some other individua web site. Table 1 summarises those characteristics for the aforementioned authentication frameworks.



Country	Service Assignment to Trust, Authentication & Registration Levels	Uniform Registration	Uniform Authentication	Central Portal		Identification Method
				Exists	Usability	
UK	Yes	No	No	Yes	Redirect	Per Sector
Belgium	Yes	Yes	Yes	Yes	Front End	Unique
New Zealand	Yes	No	No	Yes	Redirect	Per Sector
Australia	Yes	No	No	No	Redirect	Per Sector
USA	No	No	No	Yes	Redirect	Per Sector

Table 1: Wordwide Authentication Frameworks Characteristics

3. e-Government Services in Greece

Over the last decade, 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. Among those, it is worth mentioning: TAXISnet [7] for tax submission and payment; Social Insurance Institute (S.I.I.) [9] for insurance services; and Citizen Service Centres (CSC) [8] for certificates and public documents acquisition. However, the lack of a unified e-Government Interoperability Framework compels ministerial departments to develop different architectures and solutions. Thus, in most cases they cannot interact with each other in order to exchange all necessary information. For instance, citizens who would like to use the e-services provided by different public departments should follow a different registration procedure, based on the specific policy of each department. As a result, citizens not only have to register multiple times but they also have to manage different authentication tokens (credentials), thus turning the use of an e-government service to a complicated task. In the following subsections we raise two main issues that have significantly influenced the design choices of the proposed authentication framework.

3.1. Identification Issues

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.An alternative identification approach has already been adopted by several European Countries [10], which involves the utilization of a national unique identifier for each citizen. This identifier is issued once for every individual and cannot be changed afterwards. Such an identification scheme seems much more suitable for electronic services, since every user can be easily identified, irrespective of the requested service, and can also ease the exchange of information (interoperability) among different public departments. However, the Greek Constitution, which protects explicitly the dignity and the right to protection of personal data [13] sets a normative obstacle to the intentions of the Greek Government to deploy such a solution. Consequently, the identification method for the electronic services offered by Greek public departments should be based on the aforementioned "per-sector identifier" scheme.

3.2. Hermes Portal

Worldwide practises, as well as the domestic experience from Citizen Service Centers, clearly highlight the benefits deriving from the employment of a central portal for the provision of electronic services. Based on that experience, in conjunction with the attempt to implement a uniform e-Government architecture, the Greek government has decided to develop such a portal. This citizen portal, known as *Hermes,* will be 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*.

4. Authentication Framework Proposal

The authentication framework is a crucial sub-part of an e-Government Interoperability Framework, since the overall level of confidence established between an individual and the provided service (and vice versa) depends on it. Taking into account all the above parameters, as well as the restrictions imposed by the Greek law, we propose the Greek Authentication Framework (GAF). GAF acquaints with a unified architecture for providing the required level of security and trust for successfully accomplishing a specific transaction. It consists of a series of guidelines for establishing the appropriate level of trust, combining suitable registration and authentication procedures that are provided through a specific architecture employed as a one-stop shop.

4.1. Data Types

The main issue raised by the GAF is the identification of the data involved in a specific transaction. According to the Greek data protection law [12] and the European data protection framework directive [14] for the protection of individuals' "personal data", the data are classified to the following categories:

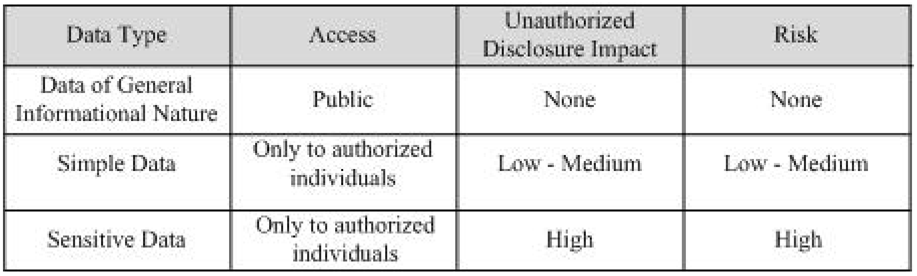
- *"Simple" - Personal Data*: It refers to data that relate directly to an individual (data subject), who is identifiable or can be identified and specified. Such data are – indicatively - First Name, Last Name, electronic address, per sector identifiers and any kind of financial data that don’t involve payments or are not protected by Greek Legislation.

- *Sensitive - Personal Data*: It refers to personal data that pertain to the racial or ethnic origin, political opinions, religious, and/or philosophical beliefs, membership of a trade union, health, social welfare and sexual life, criminal charges and convictions and membership of societies dealing with any of the aforementioned areas. Financial data that are protected by Greek Legislation or involve payments, although not included in the legislative definition of “sensitive data”, are considered –in our approach- as data, which deserves a higher level of trust.

Alongside the abovementioned categories, we should also include *Data of General Informational Nature* which refer to public available data or information that not relate, by any means, to any individual. Such data are ministerial department’s announcements and forms. All in all, it is clear that the more crucial the data are for the data subject, the more robust the security measures should be for protecting them.

4.2. Trust in e-Government

In order to determine the appropriate security measures for an electronic service, taking into account the “sensitivity” of the data involved, we have followed the approach of other frameworks, which is to define distinct “Levels of Trust” and the security mechanisms that must be employed per level. Under the view of GAF, a Level of Trust is understood as “*The level of confidence in 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”*. This means that different levels of trust are used to sort out the security characteristics and the required protection levels. Particularly, in order to define these levels we have assessed the risk associated with each specific transaction. This risk assessment was based on the impact that may arise for the organisation from the loss of confidentiality or / and integrity of the data involved. In other words, we have assessed the financial loss that could endure, the defamation of the data subject and finally any other harmful consequences from unauthorised data disclosure. Table 2 illustrates the relationship between the different data types and the potential risks.



Data Type	Access	Unauthorized Disclosure Impact	Risk
Data of General Informational Nature	Public	None	None
Simple Data	Only to authorized individuals	Low - Medium	Low - Medium
Sensitive Data	Only to authorized individuals	High	High

Table 2: Data Types Processed by Greek electronic services

More specifically, no risk was identified for Data of General Informational Nature and low to medium risk for simple data. It is clear from their definition that “simple data” include a large variety of data, hence two degrees of risk were assigned. For example, information such as First Name is not exposed to the same level of risk as identifiers. Finally, for sensitive data the risk was set to high, based on the consequences from their unauthorized release.

Coming back to the security prospective: the higher the risk that data are exposed to, the higher the security characteristics should be. Consequently, based on the identified risk levels, we propose the following Levels of Trust:

- *Trust Level 0*: In this level no identity assurance or data protection is required. It will be adopted by services that make use of publicly available information and do not require any personal or sensitive data. The security requirements that could be optionally satisfied are the integrity of the data transferred and the authenticity of the service provider.
- *Trust Level 1*: In this level low identity assurance and data protection is required. It will be adopted by services that require the exchange of simple data such as First Name, Last Name, Postal Address and Email Address, etc. The security requirements that must be satisfied are the confidentiality of the submitted data, the integrity of the data transferred and the authenticity of the service provider.
- *Trust Level 2*: In this level, a relatively high level of confidence in end's-users identity is required in order to preserve the correctness of the submitted data and prevent unauthorized access. The security requirements that should mandatorily be satisfied are the confidentiality of the data submitted, the integrity of the data transferred, the non-repudiation of submitting and receiving data and the authenticity of the service provider.
- *Trust Level 3*: A high level of confidence in end-users' identity is needed in order to preserve the correctness of the data submitted and prevent unauthorized access to them. Clearly, it includes services, which require the exchange of sensitive or financial data which are considered as sensitive from Greek Legislation [11]. The security requirements that should mandatory be satisfied are the confidentiality of the data submitted, the integrity of the data transferred, the non-repudiation of submitting and receiving data and the authenticity of the service provider.

4.3. Authentication

In accordance to the Level of Trust that an electronic service belongs to, the appropriate security mechanisms and procedures must be in place in order to establish the required level of confidence to the end-user's identity. Informal or lower risk transactions require lower levels of confidence in contrast to higher risk or legally significant transactions, which require a higher one. In practice, confidence in user's identity is strongly linked to the authentication process that is being deployed. Hence, the higher the level of trust, the more robust the authentication mechanism - process should be. Having that in mind, along with the robustness of existing authentication systems (passwords, one time passwords, soft tokens, hard tokens) we introduce the following authentication levels:

- Authentication Level 0: No identity assurance is pursued.
- Authentication Level 1: The identity assurance pursued is low and can be satisfied by employing a username/password authentication mechanism.
- Authentication Level 2: The identity assurance pursued is medium and can be satisfied by employing a combination of username / password / one-time password authentication mechanisms.
- Authentication Level 3: The identity assurance pursued is high and can be satisfied through digital certificates or smart card – based authentication mechanisms.

4.4. Registration

In order to establish the appropriate level of security, it is necessary not only to define the appropriate level of trust and deploy the corresponding authentication mechanisms, but also to determine the procedures that end-users should follow to register to a specific service and obtain an authentication token that corresponds to service's specific level of trust. It should be stressed that registration procedures are very important to achieve the required level of trust and security, as a lot of impersonation frauds are realized in the registration phase. For instance, consider the case where a malicious user sends a registration request on behalf of a legitimate user. If the agency does not follow the appropriate procedures, the malicious user may register as a legitimate user and, thus, use the provided service on behalf of the latter. For example, in the Greek tax electronic service, an individual is able to impersonate a legal user by only knowing her unique identity number, which is actually public. Thus, registration should be considered as a critical task in order to avoid such incidents and obtain an acceptable level of security.

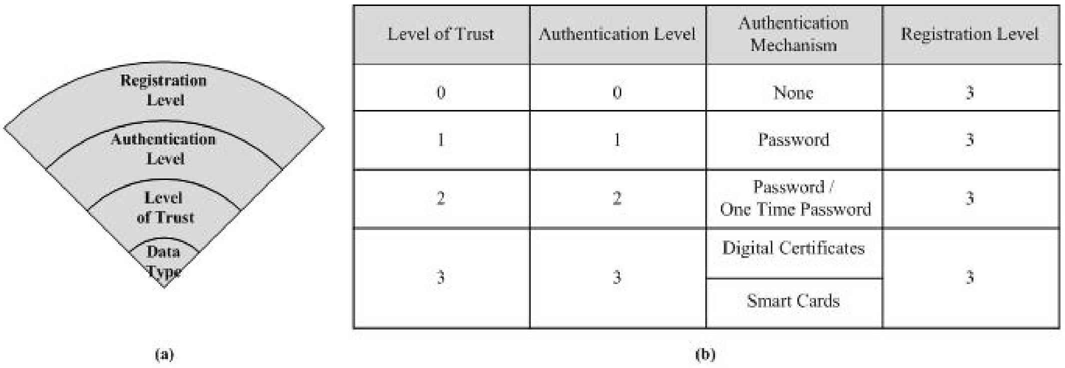
As a result, in the GAF the registration procedure varies according to the required level of trust. The common characteristic is that users have to submit an electronic registration form to start the procedure. After that and depending on the required trust level, different courses of action are proposed to establish the desired level of assurance for user's identity. The GAF's registration levels are the following:

- *Registration Level 1*, for services requiring low identity assurance. After the registration form has been submitted, user will receive the authentication token (e.g password) that has been issued through her registered postal address.
- *Registration Level 2,* for services requiring medium identity assurance. After the registration process has been successfully completed, the user will be informed to collect her authentication token (e.g. "one time password") from the appropriate office, after proving her identity through the appropriate public certificates.
- *Registration Level 3,* for services requiring high identity assurance. After the registration process has been successfully completed, the user will be informed to collect her authentication token (e.g. digital certificate or smartcard) from the appropriate office, after proving her identity through the appropriate public certificates and will receive the PIN of the issued token through her registered postal address.

5. Guidelines for Adopting the Proposed Framework

Equally important is the way and the extent to which service providers (SP) adopt the GAF for implementing and offering the electronic services. There is almost no point in designing an authentication framework if strict guidelines for its adoption do not come along with it. To this direction, we introduce a number of rules, divided in two distinct sets, which every SP should follow in order to be compatible with GAF. The first set includes the mandatory rules (MR) that must be satisfied by all SPs, while the second set includes the optional ones (OR) which are not obligatory but are simply suggested. Figure 1a, briefly illustrates the procedure that a SP should follow in order to apply the GAF. Specifically, every time that a SP decides to offer a service electronically, it is necessary to specify the data required for the registration process as well as the data utilized during the execution of the electronic service itself. The next step is to identify the correct Level of Trust for the specific electronic service, according to the provided rules. From the GAF's point of view these two steps are considered as the most important ones during the implementation of an electronic service. Once a Level of

Trust has been assigned to the electronic service, the SP should refer to Figure 1b in order to identify the appropriate Authentication and Registration Levels.



Level of Trust	Authentication Level	Authentication Mechanism	Registration Level
0	0	None	3
1	1	Password	3
2	2	Password / One Time Password	3
3	3	Digital Certificates	3
		Smart Cards	

Figure 1: Framework Adaptation Procedur3 & Levels Relation

For Levels of Trust 0, 1 & 2, the Authentication and Registration Levels that should be followed are pretty straight forward since they are related with a one to one relationship. On the other hand, for an electronic service that has been assigned to Trust Level 3, the SP should adopt Authentication and Registration Level 3 but he has the freedom to choose between two authentication mechanisms. Even though both mechanisms utilize digital certificates, only for one of them the use of smart cards for the storage of the certificate is considered compulsory. The fact is that smartcards allow for a higher level of security compared to digital certificates but they also impose a higher implementation cost.

6. GAF Architecture

Since Hermes (central portal; see section 3.2) will be the front-end interface for all available electronic services, there is no point in authenticating separately for each service, neither for issuing different authentication tokens. Our proposal is that Hermes should support Single Sign-On (SSO) functionality. This will allow users to authenticate themselves only once (to Hermes) and then being able to use all electronic services with which they have been registered, provided that the authentication credentials that were utilised satisfy the authentication requirements (Authentication Level) of the services. Figure 2 below illustrates a scenario where a user has authenticated successfully using a “one time password” and has registered to electronic services A, B, D and E. Based on the authentication tokens required by the services, user is allowed to use services A and E without the need to authenticate him to each service separately. However, the current Hermes infrastructure does not support the proposed SSO functionality. Consequently, Hermes architecture should include Authentication and Registration authorities for the corresponding tasks. These two authorities will operate under the supervision of Greek Government so as to ensure their global acceptance from ministerial departments and their uneventful collaboration with electronic services. The Registration Authority (RA) will be responsible for the registration process and for maintaining a record of the services that a user may access, while the Authentication Authority will be responsible for authenticating users and allowing them to interact with SP’s. Their interconnection with the Hermes Portal is also presented in Figure 2.

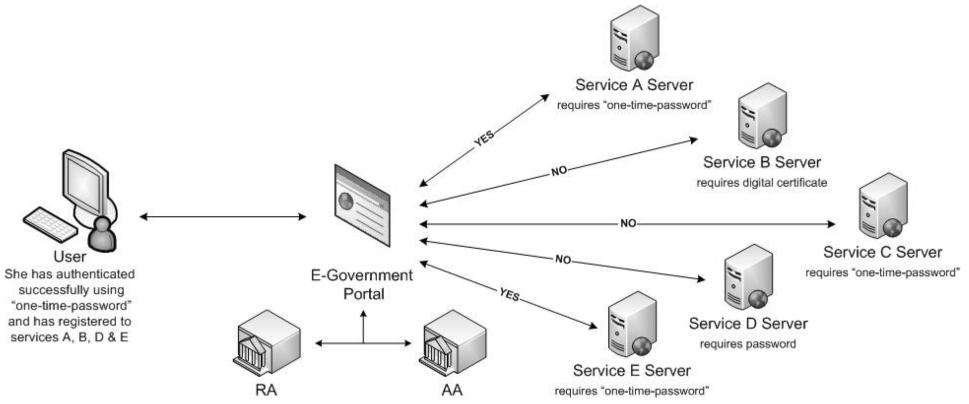

Service A Server
requires "one-time-password"
YES
NO
Service B Server
requires digital certificate
NO
Service C Server
requires "one-time-password"
User
She has authenticated successfully using "one-time-password" and has registered to services A, B, D & E
E-Government Portal
NO
YES
Service D Server
requires password
Service E Server
requires "one-time-password"
RA
AA

Figure 2: Hermes with SSO Functionality and RA - AA communication

7. Conclusions

The authentication process in the e-Government domain is certainly more than a technical issue. Particularly, governmental agencies and in general the entire public sector, must implement all the necessary procedures in order to offer the appropriate level of identity assurance and trust in the provided e-Government services. In this paper we have presented an authentication framework which takes into account the specific needs and requirements of the Greek governmental Agencies, consisting of the guidelines that should be followed by both the citizens and the public departments, in order to establish the appropriate level of trust and consequently the appropriate registration and authentication procedures, while trying to preserve a high level of user's data protection and confidentiality .

References

[1] UK government : Directgov, www. www.direct.gov.uk, visited 22.1.2008

[2] Federal Portal, www.belgium.be, visited 22.1.2008

[3] E-government in New Zealand, www.e.govt.nz, visited 22.1.2008

[4] Michael Caloyannides, Dennis R. Copeland, George H. Datesman Jr., David S. Weitzel, "US E-Government Authentication Framework and Programs," IT Professional, vol. 5, no. 3, pp. 16-21, May/Jun, 2003

[5] Australian Government - e-Authentication Framework for Business, December 2005, http://www.agimo.gov.au/infrastructure/authentication, visited 22.1.2008

[6] Observatory for the Greek Information Society, http://www.observatory.gr/files/meletes/Dlv3_BestPractices.pdf, visited 20-1-2008

[7] TAXISnet, www.taxisnet.gr, visited 24.1.2008

[8] Citizen Service Centres, www.kep.gov.gr, visited 24.1.2008

[9] National Insurance Institution, www.ika.gr, visited 24.1.2008

[10] Amir Hayat, Herbert Leitold, Christian Rechberger, Thomas Rössler, Survey on EU's Electronic-ID Solutions', Vienna, 2004

[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.g

[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.)