Transforming the Greek e-Government Environment towards the e-Gov 2.0 Era

Prokopios Drogkaris[1], Stefanos Gritzalis[1], and Costas Lambrinoudakis[2]

[1] Laboratory of Information and Communication Systems Security,
Department of Information and Communication Systems Engineering,
University of the Aegean Samos, GR-83200, Greece
{pdrogk,sgritz}@aegean.gr
[2] Deptartment of Digital Systems,
University of Piraeus, GR-185 34, Greece
clam@unipi.gr

Abstract. Modern e-Government environments across the public sector have achieved significant interoperability and coherence but are now in front of the next leap forward, which is the adaptation of Web 2.0 technologies. This transition towards e-Government 2.0 will not only improve participation, transparency and integration but it will also speed up the pace of innovation through collaboration and consultation. This paper presents an enhanced Greek e-Government Framework that fully incorporates Web 2.0 technologies along with an identification mechanism that retains compliance with existing authentication sub-framework taking into account the specific needs and requirements of the Greek Governmental Agencies.

Keywords: e-Government 2.0, Web 2.0, Security, Privacy, Identification.

1 Introduction

During the last decade e-Government environments have undergone considerable transformations in an attempt to satisfy the incessant demand of improved interoperability, acceptance and systems coherence. Currently, they are called to make the next leap forward by embodying technologies and methodologies that will not only improve participation, transparency and integration but also speed up the pace of innovation. The second incarnation of Web named "Web 2.0" or "Social Web" can facilitate towards this direction through public interaction, collaboration and consultation.

The term "Web 2.0" was first introduced in 2003 by Oreily Media and referred to a second generation of the World Wide Web which would provide the platform for Web-based services and communities of social interaction. A formal definition of Web 2.0, given by Hoegg in [3], is "the philosophy of mutually maximizing collective intelligence and added values for each participant by formalized and dynamic information sharing and creation". The tools of Web 2.0 include blogs, wikis, social

K.N. Andersen et al. (Eds.): EGOVIS 2010, LNCS 6267, pp. 142–149, 2010.

networking platforms, syndication, discussion groups, machine automated content and topic analysis based on open standards and technologies. Terms such as "e-Government 2.0", "Government 2.0" and "eGov. 2.0" are used to describe the incorporation of Web 2.0 fundamentals in e-Government environments. These fundamentals include public participation, deliberation, and engagement to government consultation along with transparency.

In this paper we propose an enhanced Greek e-Government Framework which fully incorporates Web 2.0 technologies along with an identification mechanism that retains compliance with existing authentication sub-framework and identity assurance levels. The rest of the paper is structured as follow. Section 2 provides an insight in worldwide endeavors relating to government interaction attempts with Social Web. Section 3 discusses the identification issues emerging in e-Government 2.0 environments. Section 4 presents the current state of Greek e-Government environment, which constitutes the basis for our proposal, while Section 5 presents the proposed model and identification mechanism for Greek e-Government 2.0 environment. Finally, Section 6 concludes the paper providing thoughts on future work.

2 Related Work

One of the first governmental initiatives towards e-Government 2.0 was by the German government in 2005 [9] as part of a universal strategy for the modernization of federal administration. The scope of this initiative was to identify the objectives for further expansion of electronic services, improve cooperation between citizens and public administration, introduce an electronic identification mechanism (e-ID) and finally provide a secure communications infrastructure. In 2006, European Union issued the EU *i*2010 – *Information Society and the media working towards growth and jobs initiative* [10] and the *eGovernment action plan* [11] which provided guidelines and goals for member states towards ameliorating public services and administration transparency, effectiveness and efficiency. President Obama in 2009 signed a memorandum for "*Transparency and Open Government*" [12] which actuated implementations of social media technologies to improve central governance engagement with public. In 2009, as well, Australia has issued a report [13] regarding the engagement of Australian Government with Government 2.0. This report derived from the results of nineteen different projects that were designed to "provide insight into key Government 2.0 issues" [13]. An alternative representation of the transition being conducted and the effort towards e-Government 2.0 is provided by a wiki titled "*Government 2.0 - Best Practices Wiki*"[1], which catalogs official and unofficial worldwide initiatives that involve social media and central government. Currently, this list consists of six countries and it is continuously updated, enriched and improved by user contributions. Table 1, below, summarizes the approximate number of official Web 2.0 tools that are currently available, through ministerial departments and government organizations, in each country.

[1] Government 2.0 - Best Practices Wiki:
http://government20bestpractices.pbworks.com

Table 1. Official e-Government 2.0 Initiatives Worldwide

	Blogs	*Disc. Groups*	*RSS*	*Wikis*
AUSTRALIA	●●	●●	●	●
CANADA	●	●●●	●●●	●●●
NETHERLANDS		●		
NEW ZEALAND	●●●	●		●●
U. K.		●		
UNITED STATES	●●●●	●	●●	●
Legend	● *1-5*	●● *6-10*	●●● *11 -15*	●●●● *16 - 20*

3 Identity Assurance in e-Government 2.0

The security risks emerging in e-Government 2.0 environments do not significantly vary from those identified in traditional e-Government environments. Unauthorized access, modification, loss, destruction or disclosure of data that are transmitted, processed and stored, are the risks that have to be confronted through the deployment of appropriate measures and procedures. This is also supported by a report from the secure enterprise 2.0 forum [17], published in 2009, which identifies Web 2.0 security threats and vulnerabilities along with known incidents and possible exploit scenarios. However, issues related to user identification do have a significant diversion.

For the provision of traditional electronic services, a certain level of assurance for user's identity is required. For informational services almost no identity assurance is required while for transactional services there is need for high assurance level for the identity of the user. The required level of assurance is accomplished through the employment of the appropriate registration and authentication procedures which are specified in the corresponding authentication sub-frameworks. For Web 2.0 services, though, almost no assurance for user's identity is required, since no transaction or two way data exchange is taking place. In existing commercial Web 2.0 services and applications, user identification and authentication is performed through the utilization of username/password authentication mechanisms. These credentials are issued through web registration procedures where only user's email address can be verified. For the purposes of these commercial applications, such a level of user's identity assurance may be adequate but this is not the case for governmental applications. For instance, how can central governance take into account public opinion if she cannot distinguish between opinions that do represent public feelings and those aiming to misdirect the conclusions and findings? It is therefore clear that depending on the significance and impact of the service and its results, central governance should be either able to weight different opinions or, alternatively, predefine the levels of identity assurance that are necessary for the establishment of the required level of confidence. No matter what the selection will be, the necessity for guidelines and policies that will be used to determine the required level of assurance, prior to the implementation of the services, is evident.

4 e-Government in Greece: Current Status

4.1 Greek e-Government Environment

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 through a comprehensive e-Government framework [4]. 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, namely "Ermis"[2], that operates as a *one-stop shop* providing to Greek citizens a common interface for all electronic services offered by the public sector. Framework's main characteristics are briefly described next;

- *Uniform Registration and Authentication Procedures*: The registration and authentication procedures required for accessing the offered electronic services are provided through Ermis Portal.
- *Classification of electronic services to Levels of Trust*: All electronic services offered through the Ermis Portal have been classified to pre-determined trust levels; these trust levels are understood as "The level of confidence of an end-user's electronic identity along with the assurance achieved by the security measures and procedures employed for safeguarding the access, processing and transmission of data" [4].
- *Per Sector Identifiers*: The identification of the users wishing to utilize one of electronic services is accomplished through sectorial identifiers. These identifiers are given to each citizen the first time she requests to use a service (through the registration process) of a particular sector, identifying her uniquely within that specific sector. The bonding of these identifiers, for the provision of user-centric *Single Sign-On* is accomplished through identifier's encryption in a predefined sequence, along with an identifier assigned by Ermis itself.

5 Greek e-Government 2.0: Proposed Model

In this paper we propose an enhanced Greek e-Government Framework which fully incorporates Web 2.0 technologies along with an identification mechanism that retains compliance with the existing authentication sub-framework. Our proposal is based on the existing Greek e-Government Framework, as described in Section 4, in an attempt to ensure backwards compatibility with implemented services, procedures and normative regulations through the exploitation of framework's open architecture while taking into account the specific needs and requirements of the Greek Governmental Agencies. In order to keep the Ermis portal as the interface between users and ministerial departments and thus maintaining the One Stop Shop characteristics, Web 2.0 services will be provided through the existing central portal, as demonstrated in Figure 1. Each Web 2.0 Service will be offered through a specific Service Provider that will be responsible for specifying the required level of assurance on users' identity, the data required for the registration process as well as the data utilized during

[2] Greek Public Administration National Portal Ermis: `http://www.ermis.gov.gr`

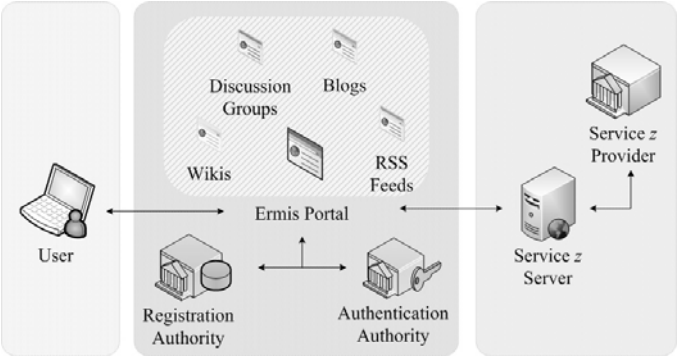

Fig. 1. Greek eGov 2.0 Proposed Architecture

the execution of the electronic service itself, based on the Greek Authentication Framework's guidelines [4]. In this way the desired level of security and trust are maintained.

5.1 Proposed Identification Mechanism

In order to maintain compatibility with identification and authentication procedures, we employ the notion of account linking along with the utilization of the underlying PKI infrastructure of the Greek Public Sector. In a way similar to the existing e-services, user identification in Web 2.0 services is based on identifiers. As described in Section 4, the Greek Public Sector does not utilize an all-embracing identifier (e-ID) due to legal impediments. On the contrary, each sector identifies users through sectorial identifiers. In Web 2.0 services, we propose the preservation of this mechanism in order to overcome Legal barriers imposed by the Greek Legal Framework [18][19] regarding data interconnection that would results from the introduction of a unique identifier. Our proposal is to utilize each department's encryption key pair for storing the corresponding Web 2.0 identifier to the Ermis portal, in a predefined sequence, as an extension of the mechanism described in Section 4 for the sectorial identifiers. Figure 2 below depicts the sequence of User's A encrypted identifiers for traditional e-Services and Web 2.0 services.

The first identifier "*User A Ermis Identifier*" is employed for the users' unique identification by the Ermis Portal, during the authentication procedure, and it serves as the linking mechanism to all per-sector and Web 2.0 identifiers of the specific user. The remaining blocks in the sequence consist solely by encrypted identifiers, each one of them corresponding to a specific service. Since each block is encrypted with the Public Key of a Service Provider, only the specific Service Provider can decrypt it and thus identify the user. Consequently, each encryption is performed by the Service Provider that is responsible for the provision of the corresponding service. The number of these blocks must be at least equal to the number of Service Providers that offer their services electronically and not greater than the available electronic and Web 2.0 services.

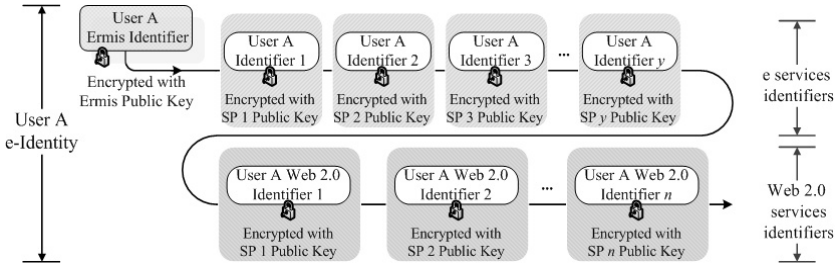

Fig. 2. User's Identifiers Bonding

5.2 Proposed Model of Operation

An overview of the operation of the proposed model and identification mechanism is provided in Figure 3 below. First, the user completes successfully the authentication procedure (*1*) and requests the Discussion Group *a* service (*2*). The authentication procedure depends on the Level of Trust that the specific service has been linked. After the Ermis portal has identified the user, through the aforementioned authentication procedure, it 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 (*3*). The encrypted identifier and user's service request are forwarded to the corresponding Service provider (*4*). The Service Provider decrypts the identifier using his private encryption key and is now able to identify the user who requested the service (*5*). After user identification, the Service Provider can grant user access to the requested service (*6*) and thus the user can start interacting with the requested service (*7*).

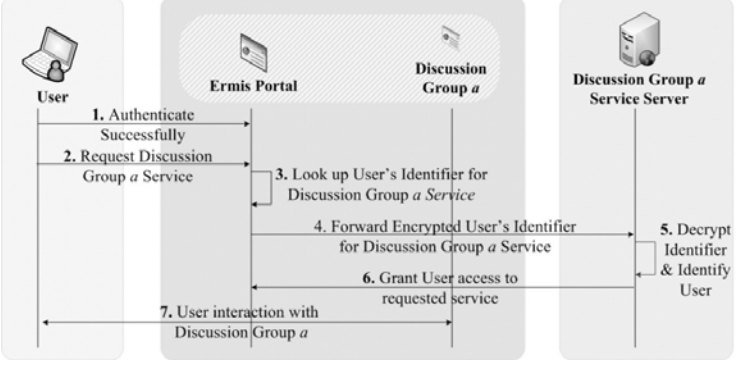

Fig. 3. User Identification in Proposed eGov 2.0 model

In cases where the user requests multiple services, the proposed model proves its efficiency and effectiveness. After a successful authentication the user can be identified by each Service Provider without the need to submit the corresponding identifier each time a new service is requested. Moreover, the authentication procedure is not

directly related with the services, thus supporting Single Sign-On functionality. The compilation of user's e-identity, as proposed in Section 5.1, is performed every time the user completes successfully a registration procedure submitting, at the same time, the corresponding identifier.

6 Conclusions

Motivated by the belief that the employment of new governance models which utilize Web 2.0 capabilities will promote user participation and increase the overall effectiveness of the public sector, we have proposed an enhanced Greek e-Government 2.0 model. The expected results of this transition will be the improvement of quality and responsiveness of the Greek government policy making and service delivery.

However, the success of such a model does not solely lie on implementing and redesigning processes. A cultural change is necessary so that users will realize the extent of the participation they are allowed to, along with the responsibilities and obligations that come along with such involvement. As stated in an unofficial Australian Google group[3] "Government 2.0 is not specifically about social networking or technology … It represents a fundamental shift in the implementation of government — towards an open, collaborative, cooperative arrangement where there is (wherever possible) open consultation, open data, shared knowledge, mutual acknowledgment of expertise, mutual respect for shared values and an understanding of how to agree to disagree. Technology and social tools are an important part of this change but are essentially [just] an enabler in this process."

References

1. Osimo, D.: Benchmarking eGovernment in the Web 2.0 era: what to measure, and how. European Journal of ePractice 4 (2008) ISSN: 1988-625X
2. Osimo, D.: Web 2.0 in government: why and how? Technical Report. JRC, EUR 23358, EC JRC (2008)
3. Hoegg, R., Martignoni, R., Meckel, M., Stanoevska-Slabeva, K.: Overview of business models for Web 2.0 communities. In: Dresden (ed.) Proceedings of GeNeMe, pp. 23–37 (2006)
4. Drogkaris, P., Geneiatakis, D., Gritzalis, S., Lambrinoudakis, C., Mitrou, L.: Towards an Enhanced Authentication Framework for eGovernment Services: The Greek case. In: Ferro, E., Scholl, J., Wimmer, M. (eds.) EGOV 2008 7th International Conference on Electronic Government, pp. 189–196. Trauner Verlag (2008)
5. Ostergaard, D., Hvass, M.: eGovernment 2.0 – How can Government benefit from web 2.0? (2009)
6. German Federal Ministry of the Interior, eGovernment 2.0 The Programme of the Federal Government (2006)
7. Lundy, K.: Public Sphere 2: Government 2.0 Briefing Paper (2009)
8. Government 2.0 Best Practices Wiki, `http://government20bestpractices.pbworks.com`

[3] Australia Government 2.0 Google Group: `http://groups.google.com.au/group/gov20canberra`

9. Germany's Federal Ministry of the Interior in, titled eGovernment 2.0 – The programme of the Federal Government (2005)
10. EU i2010 – Information Society and the media working towards growth and jobs initiative (2006)
11. EU i2010 eGovernment Action Plan - Accelerating eGovernment in Europe for the Benefit of All (2006)
12. Obama, B.: Memorandum for the Heads of Executive Departments and Agencies Transparency and Open Government (2009)
13. Australian Government Information Management Office, Engage Getting on with Government 2.0 - Report of the Government 2.0 Taskforce (2009)
14. Seifert, J.: Reauthorization of the E-Government Act: A Brief Overview. CRS Report RL34492 (2008)
15. Baumgarten, J., Chui, M.: E-Government 2.0, Public Sector Practice (2009)
16. Eched, Y., Billiaert, E., Veyret, E.: e-Government 2.0 Identification, Security and Trust. Exploring European Avenues (2007)
17. Ofer, S.: Top Web 2.0 Security Threats, Secure Enterprise 2.0 Forum (2009)
18. Articles 8 & 2b of the Greek Data Protection Law (Law 2472/97), `http://www.dpa.gr`
19. Greek Constitution Articles 2 § 1 (human dignity) and 9 A (right to protection of personal data)
20. Suriadi, S., Foo, E., Jøsang, A.: A User-centric Federated Single Sign-on System. In: IFIP International Conference on Network and Parallel Computing – Workshops (2007)