Employing privacy policies and preferences in modern e-government environments

Prokopios Drogkaris* and Stefanos Gritzalis

Laboratory of Information and Communication Systems Security,
Department of Information and Communication Systems Engineering,
University of the Aegean,
Samos GR-832 00, Greece
E-mail: pdrogk@aegean.gr
E-mail: sgritz@aegean.gr
*Corresponding author

Costas Lambrinoudakis

Department of Digital Systems,
University of Piraeus,
Piraeus GR-185 34, Greece
E-mail: clam@unipi.gr

Abstract: The evolvement of e-government has raised users' concerns on personal data disclosure and privacy threats as more and more information is released to various governmental service providers. This paper addresses the consideration of users who would wish to retain control over their personal information while using advanced governmental electronic services. Additionally, it proposes a simple, yet effective, architecture which promotes the employment of Privacy Policies and Preferences in modern e-government environments. The aim is to simplify the provision of electronic services while preserving users' personal data and information privacy.

Keywords: e-government; security; privacy policy; privacy preferences; XML schemas.

Reference to this paper should be made as follows: Drogkaris, P., Gritzalis, S. and Lambrinoudakis, C. (xxxx) 'Employing privacy policies and preferences in modern e-government environments', *Int. J. Electronic Governance*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Prokopios Drogkaris is a Research Assistant at Laboratory of Information & Communication Systems Security, Department of Information and Communications Systems Engineering, University of the Aegean, Greece. He is an author of nine scientific publications, an editorial board member in two international journals and has served as a member on programme and organising committees at several scientific conferences. His main research interests include Privacy Enhancing Technologies (PET) in e-government environments, electronic Identity Management (eIdM) and Cloud Computing privacy and ethical issues.

Stefanos Gritzalis is the Head of the Department of Information and Communication Systems Engineering, University of the Aegean, Greece and the Director of the Laboratory of Information and Communication Systems

Security. His research work includes 30 books or book chapters, 100 journals and more than 130 international refereed conference papers. The focus of these publications is on Information and Communications Security and Privacy. He has served on more than 330 PC of international conferences and workshops and is an Editor or Editorial Board member for 20 journals. He acts as President-elect of the Hellenic Association for Information Systems.

Costas Lambrinoudakis is an Assistant Professor at the Department of Digital Systems, University of Piraeus, Greece. His current research interests are in the areas of Information and Communication Systems Security and of Privacy Enhancing Technologies. He is an author of more than 85 scientific publications in refereed international journals, books and conferences, most of them on ICT security and privacy protection issues. He has served as programme committee chair of two international scientific conferences and as a member on the programme and organising committees of many others.

1 Introduction

The provision of e-government services by Central Government has evolved rapidly from services based on static information to more mature services supporting transactional and interoperable operations. A continuously increasing amount of data are collected by several Governmental Service Providers without the users being aware to whom, for what purpose and for how long their personal data are released to. This evolvement has raised the concerns regarding data privacy, data disclosure and emerging privacy threats, especially since trust is recognised as a prerequisite for their acceptance and usage (Vrakas et al., 2010).

This paper addresses the consideration of users who would wish to retain control over their personal information while using advanced governmental electronic services. An architecture that promotes the employment of Privacy Policies and Privacy Preferences in modern e-government environments is being proposed. The aim is to simplify the provision of electronic services and, at the same time, to allow users to monitor the way their personal data are accessed and processed.

The rest of the paper is structured as follows. Section 2 presents Privacy Policies and Preferences whereas Section 3 discusses the e-government privacy protection requirements. Section 4 presents the proposed architecture and its evaluation while Section 5 introduces a use case that provides evidence about its usability and functionality. Section 6 discusses the evolution of privacy policies and preferences in e-commerce environments while Section 7 concludes the paper providing directions for future work.

2 Privacy policies and privacy preferences

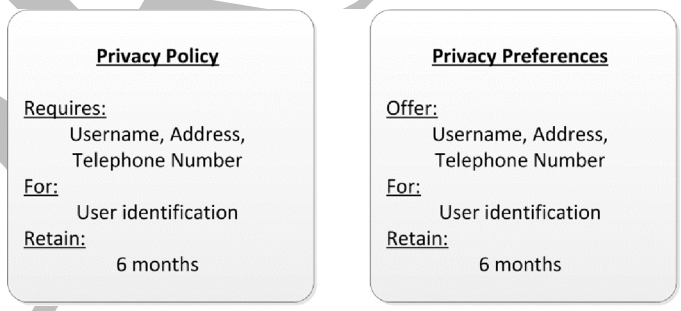
According to Gritzalis (2004) and Li et al. (2006), the notion of privacy can be defined as the right of individuals to determine by themselves when, how and to what extent information about themselves will be communicated to others. Unsurprisingly, a growing concern for ensuring and safeguarding the desired characteristics of communication, processing and storage derives, is developing. The growth of ICT and the transition

towards electronic services has only strengthened this concern; users not only expect high levels of online privacy (Chellappa and Pavlou, 2002), but they have also developed privacy awareness. When asked, they mention lack of trust or lack of knowledge of how their information will be used, as the main reasons for not requesting a service electronically (Grabner-Kräuter and Kaluscha, 2003; Teltzrow and Kobsa, 2004). Equivalently, from the provider's perspective, the need to protect consumer privacy and to comply with privacy legislation is also a growing concern. If efficient privacy practices are not followed, users may digress and/or legal consequences may arise. As a result, the formalisation of providers' commitments regarding privacy practices and privacy requirements is an indispensable task since users will be able to review these requirements and practices and preserve their privacy (McDonald et al., 2009).

A privacy policy can be regarded as a statement or document describing what information is collected by an electronic service and how this information will be used (Salas and Krishnan, 2008). Most commonly, a privacy policy explicitly states what personal information (such as e-mail addresses and users' names) is collected, whether shared or sold to third parties and for how long it will be retained. On the other side, users should also be able to formally express acceptable privacy practices and requirements. Such formal statements comprise the so-called privacy preferences. Usually they affirm which personal information can be collected, for what purpose, whether they can be transmitted to third parties and for how long they can be retained. Figure 1 presents an example of Privacy Policy and Privacy Preferences documents.

Different types of languages have been proposed to represent human readable policies in more precise and computer compatible formats. Some of them were designed to help Service Providers express their privacy policies in ways that are more amenable to policy enforcement while some others were designed to help users state their privacy preferences. Every language has its own syntax and mechanisms for implementation. In general, they are expected to be fairly simple and short and have been designed as light-weight XML mark-up languages (McDonald et al., 2009).

Figure 1 Privacy policy and privacy preferences example



3 E-government privacy protection requirements

The provision of governmental electronic services is necessary to comply with specific principles and obligations regarding protection of personal data. Normally these principles and obligations are imposed by the existing legal and regulatory framework and are based on the principles of purpose specification, fairness, minimality, accuracy,

privacy and anonymity. A thorough description of these principles is provided by Siougle and Zorkadis (2002) and Vrakas et al. (2010), where it is also remarked that data controllers must comply with the privacy protection requirements and implement privacy protection based on them. Correspondingly, governmental Service Providers, and consequently the electronic services they offer, have explicit obligations regarding the processing of personal data submitted during services' provision. Personal data and information must be gathered by fair and lawful means and only after user's consent. The required data should be limited only to those that are absolutely necessary for successful service provision and should be collected for explicitly specified and legitimate purposes that have been communicated to the data subject prior to their collection. Finally, data subjects must be aware of any personal information that is maintained by the service provider along with the corresponding justification.

The notion of interoperability and the deployment of e-Government Interoperability Frameworks (e-GIF), to enable the seamless flow of information across service providers and governmental departments, constitute a cornerstone policy for modern e-government environments. However, when examined from the prospective of multi-entry electronic services, where the provision of an electronic service involves the transmission or request of user data across multiple service providers, data subjects must be aware and give their consent for the supplementary data processing purposes and procedures.

4 Privacy policies and preferences in e-government environments

This paper introduces an architecture which promotes the employment of Privacy Policies and Privacy Preferences in modern e-government environments. The aim is to enjoy advanced electronic services and, at the same time, ensure users' privacy. The user consents to the use of his personal data by specifying, through fine-grained privacy preferences, how these data items can be used. This is done for each data item or group of personal data items. This approach has the advantage of coping with situations where the data subject decides to revoke the right that has previously granted to the data collector.

In a typical privacy policy model, the data collector defines its privacy policy and makes it available online, through the website that provides the service. Alternatively, the data collector requires from the user (data subject) to review and agree to its policy prior to the provision of the electronic service. In any case, the user reviews the policy; most of the times this is done through third party software that is being installed locally at the browser, comparing it against predefined privacy preferences. If the policy is compatible with the user's privacy preferences, the user will continue with the service, else he will be informed of the incompatibilities and will be prevented from using the service.

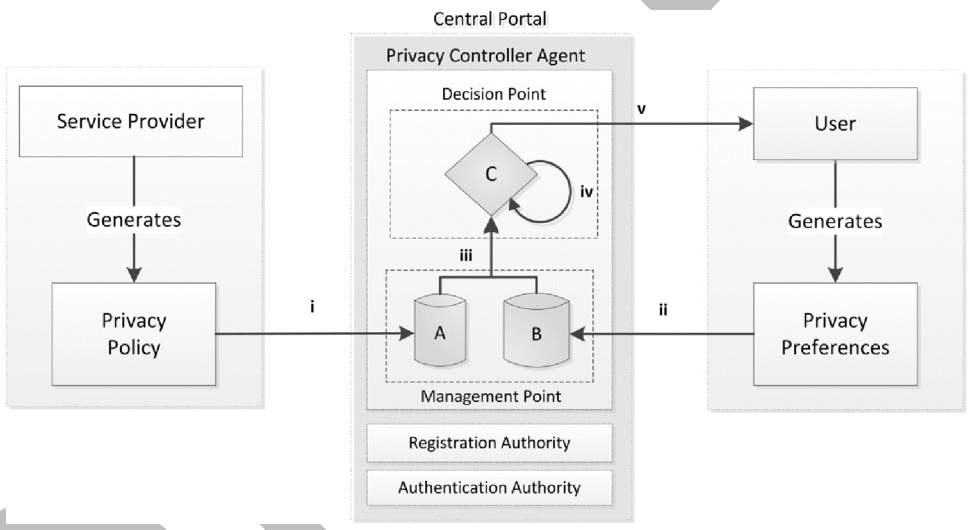
Irrespective of how functional this approach has proved for existing e-environments, mostly e-commerce, it has two major deficiencies when applied to e-government environments; personal data protection and privacy preferences portability. Privacy preferences cannot be administered by third party software or be created by the user on the fly. In the first case, as described by Silic et al. (2010), malicious applications could be loaded and executed by the web browser, affecting its security and consequently the confidentiality, integrity and availability of the data it has access to. Secondly, storing users' privacy preferences confines their portability and prevents electronic service delivery from different locations and devices. Surely, the privacy preferences can be update by the user at every device or workstation most commonly utilised or even

create them on the fly, prior to the employment of the electronic service; however, the security risk is increased.

4.1 Proposed architecture

To overcome the aforementioned impediments, the architecture of modern e-government environments and more specifically the existence of a central portal, is being exploited. It most commonly operates as a one-stop shop being the front end for all service providers (Tambouris and Wimmer, 2005; Votis et al., 2008; Gotoh, 2008; Zhang and Wang, 2008; Sedek et al., 2011). Typically this portal implements the authentication and registration procedures, or it incorporates the federated identity management infrastructure for every service provider. Alongside these authorities, a new entity named Privacy Controller Agent (PCA) is being proposed. PCA will be responsible for storing and comparing service providers' privacy policies and user privacy preferences. An overview of the agents' architecture can be seen in Figure 2.

Figure 2 Privacy Controller Agent (PCA)



The PCA is divided into two main units: the Management Point and the Decision Point. The Management Point consists of two storage repositories which are in charge of retaining the privacy policy of each service (A) and the privacy preferences of each user (B). When a Service Provider (SP) enrols an electronic service to the Central Portal (CP), apart from the remaining information required, it is necessary to submit the corresponding Privacy Policy. Since a Service Provider will most commonly offer numerous different electronic services, a separate privacy policy must be submitted for each service. The policy will explicitly state the data required for the provision of the service, the purpose for which the data are required, how they will be processed, if they will be stored, for how long they will be retained and if they will be communicated to another service provider. After its submission (action i), the PCA validates the origin of the policy and stores it at a Policy Repository (A).

Similarly, when a user registers to the CP it is necessary to submit his privacy preferences. The privacy preferences, set by the user, apply to the entire set of his personal data irrespective of the specific service that utilises them. Therefore, the user needs to submit only one document (privacy preferences) that applies to all electronic services. Apart from the categorisation of data types (personal data and personal identifiers) and the scope of their usage and processing, it is being proposed the users to name the service providers that can manipulate their data. Thus, the user will have to specify what type of data will be included in the privacy preferences document, for what purpose these data can be used and by which service provider. After submission, the PCA validates preference's origin and stores them at the Preferences Repository (action ii). Ideally, after both submissions have been completed, neither of the participating parties should request a revocation or modification. However, it is anticipated that services' requirements could change or, most likely, user will revise his preferences at some point. The revision option dissuades user from considering the submitted document as permanent and adds up to proposal's acceptance.

After the successful submission of both documents and the successful authentication, the user requests an electronic service. The CP passes the request to the PCA. The agent then retrieves the preferences and the corresponding policy and forwards them to the Decision Point (action iii). At this point the comparison procedure is invoked and the policy is checked against user's preferences. If preferences assent on the usage of data through the operations and for the purpose described in the policy, the agent informs the user, through the portal, of the concurrence and forwards service's request to the applicable Service Provider. Through this comparison and notification process, the user is now confident that his personal data will be accessed, processed and transmitted according to his preferences. In the case where these preferences do not match the policy of the service provider, the PCA informs the user, again through CP, of the conflict and its details. In a typical privacy policy model, the controller agent would initiate a negotiation between the user and the SP, in an attempt to overcome the conflict. However, due to the legal basis of all governmental services (electronic or not), the requisite pretences are not likely to change and only the user is prompted to review her preferences.

4.2 Evaluating the deployment of the PCA

The deployment of the proposed architecture promotes user's privacy and supports the provision of personalised electronic services. Through the Privacy Policy document, each Service Provider delivers a formal and public engagement of the information required, the purpose of the request as well as how the information will be used and to whom it will be disclosed. However, trivial this may seem, as each provider's requisites are known, it is necessary to keep in mind the occurrences of service's which initiate the provision of additional electronic services from different service providers. Privacy policy documents do not contain any confidential information regarding the Service Provider thus the preservation of their integrity can be ensured by Central Portals' underlying Public Key Infrastructure through digital signatures. Secondly, users can now retain and administer their preferences on a structured and formalised document. Through this document they can compare and verify provider's policy compliance with their preferences. Even if this document does not contain personal or sensitive user data, it does contain predilections on this data and should thus not be available to unauthorised

parties. Why should Mallory have access to Alice's preferences where it is stated that her personal identifiers can only be processed as confidential information? Therefore, the Central Portal apart from the integrity of the Privacy Preferences document should also preserve its confidentiality through the underlying Public Key Infrastructure.

An important issue that must be addressed during deployment of the proposed approach is the XML Schema to be utilised as well as the creation and administration of the XML documents that will support the hierarchy scheme. Selecting the appropriate XML schema can be a complicated task. Existing schemas have not been designed having in minded the needs and requirements of e-government environments. Thus, several aspects have been left uncovered or modifications may be necessary. The proposal of a new XML schema specialised to e-government environments seems to be a promising path. Yet, the deployment of newly proposed schemas introduces the challenges of compatibility, up keeping, evaluating and updating procedures. Finally, the additional workload added to Users and Service Providers for creating, maintaining and updating their documents should be also considered. Towards this direction, specific utilities and resources have been proposed that allow easier creation and management of existing XML Policy and Preferences schemas (Reeder et al., 2008).

5 Case study

To demonstrate the applicability of the proposed architecture in modern e-government environments, a case study where the PCA is incorporated to a Greek e-government environment is presented. Greek e-Government Interoperability Framework (Greek e-GIF) was first designed in 2007 (Charalabidis et al., 2008; Drogkaris et al., 2008) based on worldwide best practices along with the specific needs and restrictions set by the underlying legal and regulatory framework. The main objective of this framework is the support of common authentication and registration mechanisms for accessing all the electronic services offered. This is realised through a Central Portal, named 'Ermis', which operates as a one-stop shop that provides to Greek citizens a common interface for all electronic services offered by SPs of the public sector. The framework's main characteristics are uniform registration and authentication procedures for every service provider, implemented by the Ermis Portal, and classification of services to Levels of Trust depending on the required level of identity assurance and data protection.

For registering to the Payment Authority a user is required to obtain a taxation awareness certificate from Ministerial Department of Finance, a national insurance awareness certificate from Ministerial Department of Insurance and submit them along with her International Bank Account Number (IBAN). This service was introduced in 2010 by the General Secretary of Information Systems (GSIS) as an attempt to provide a centralised system for all public sector payrolls. The corresponding electronic service also requires the submission of the aforementioned documents and information, but the user is not expected to request all services. User can only request the registration to the Payment Authority and authorise the Service Provider to obtain the necessary certificates on her behalf.

According to our proposal the SP will have to submit its privacy policy during the enrolment with the Central Portal as described in Drogkaris et al. (2008). Figure 3 presents the basic parts of the policy.

Figure 3 Registration at Payment Authority Privacy Policy

```
A.1  <Privacy_Policy>
A.2  <Policy_ID="1033">
A.3       <Service_Provider> General Secretary of Information Systems (GSIS) </Service_Provider>
A.4       <Electronic_Service> Registration at Uniform Payment Authority </Electronic_Service>
A.5       <Description> Privacy Policy for Registration at Payment Authority Electronic Service </Description>
A.6  </Policy_ID>
A.7
A.8  <Data>
A.9       <Personal_Identifiers>
A.10           <Identifier_ID="1">National Identity Card Number (IdN)
A.11                <Processed="Confidential">Identification</Proccessed>
A.12                <Storage="Yes" Conserve="90">Payment Order</Storage>
A.13                <Transmitted="Yes">Taxation Awareness Certificate Aquicition
A.14                     <Policy_ID="2058"> </Policy_ID>
A.15                </Transmitted>
A.16                <Transmitted="Yes">National Insurance Awareness Certificate Aquicition
A.17                     <Policy_ID="3153"> </Policy_ID>
A.18                </Transmitted>
A.19           </Identifier_ID>
A.20
A.21           <Identifier_ID="13">Social Security Number (AMKA)
A.22                <Processed="Confidential">Identification</Proccessed>
A.23                <Storage="No"> </Storage>
A.24                <Transmitted="Yes">National Insurance Awareness Certificate Aquicition</Transmitted>
A.25                     <Policy_ID="3153"> </Policy_ID>
A.26           </Identifier_ID>
A.27
A.28           <Identifier_ID="26">National Taxation Identifier (AFM)
A.29                <Processed="Confidential">Identification</Proccessed>
A.30                <Storage="Yes" Conserve="90">Payment Order</Storage>
A.31                <Transmitted="Yes">Taxation Awareness Certificate Aquicition</Transmitted>
A.32                     <Policy_ID="2058"> </Policy_ID>
A.33           </Identifier_ID>
A.34      </Personal_Identifiers>
A.35
A.36      <Personal_Data>
A.37           <Data_ID="321"> IBAN
A.38                <Processed="Confidential">Payment Order</Processed>
A.39                <Storage="Yes" Conserve="90">Payment Order</Storage>
A.40           <Transmitted="No"><Transmitted>
A.41           </Data_ID>
A.42
A.43           <Data_ID="32"> First and Last Name
A.44                <Processed="Confidential">Payment Order</Processed>
A.45                <Storage="Yes" Conserve="90">Payment Order</Storage>
A.46                <Transmitted="Yes">Taxation Awareness Certificate Aquicition
A.47                     <Policy_ID="2058"> </Policy_ID>
A.48                </Transmitted>
A.49                <Transmitted="Yes">National Insurance Awareness Certificate Aquicition
A.50                     <Policy_ID="3153"> </Policy_ID>
A.51                </Transmitted>
A.52           </Data_ID>
A.53      </Personal_Data>
A.54 </Data>
A.55 </Privacy_Policy>
```

5.1 Service providers' privacy policies

For the purposes of this case study the necessary privacy policies and user's privacy preferences documents have been prepared in a simple XML schema. This schema consists of simple elements along with some attributes, in an attempt to describe a strict privacy policy in a structured yet easy way. Apart from the root elements *Privacy_Policy* and *Privacy_Preferences*, the leading elements *Service_Provider*, *Electron-ic_Service* and *Description* provide a general overview of the electronic service. The remaining part of the document regards user's data and is divided into two categories: *Personal_Identifiers* and *Personal_Data*. For each data type included in the

document, elements regarding processing, storage and transmission are utilised. Figure 3 presents the Privacy Policy for the Registration process of a user to the Payment Authority.

The first part of the privacy policy consists of XML elements that contain information about the Service Provider (*line A.3*), the electronic service it applies to (*line A.4*) and a short description of the electronic service (*line A.5*). To facilitate references among privacy policy documents, it is assumed that a unique identification number is assigned to each electronic service when enrolled by the Service Provider to the Central Portal (*line A.2*). This identifier refers to a specific electronic service and not to each privacy policy; regardless of the updates that the Service Provider performs on the document, the identifier remains unchanged. The data specified in this policy consist of three Personal Identifiers (PII):

- National Identity Card Number (IdN) (*line A.10*)
- Social Security Number (AMKA) (*line A.21*)
- National Taxation Identifier (AFM) (*line A.28*)

and two personal data:

- the IBAN number (*line A.37*)
- the data subject's full name (*line A.43*).

The *Identifier_ID* element is used for every personal identifier and includes an attribute based on a unique number that has been assigned to each identifier. This is common practice for e-government environments as it expedites referencing to personal identifiers amongst governmental departments and improves interoperability.

For the IdN identifier, the privacy policy document indicates that it will be processed as confidential information; it will be used for user identification (*line A.11*) and will be be stored for 90 calendar days to issue the payment order (*line A.12*). Additionally, it will be transmitted to the National Insurance Awareness Certificate Acquisition electronic service, with *policy_ID* 2058 and to National Insurance Awareness Certificate Acquisition electronic service with *poli-cy_ID* 3153. For these two services the policy does not describe IdN identifier since this is subject to their privacy policy. Inclusion of such information could introduce outdated or inconsistent information in case they are updated at a later point. To obtain this information for the comparison against user preferences, the Central Portal will have to retrieve these two policies as well. Figure 5 presents the corresponding privacy policies from Taxation Awareness Certificate and National Insurance Awareness Certificate Acquisition electronic services.

Regarding the Social Security Number (AMKA) privacy policy document indicates that it will be processed as confidential information and will be used for user identification (*line A.22*). It will not be stored (*line A.23*) and will be also transmitted to National Insurance Awareness Certificate Acquisition electronic service, with *policy_ID* 2058 (line A.31). Finally, the AFM will be processed as confidential information; it will be used for user identification (*line A.29*) and will also be stored for 90 calendar days to issue the payment order (*line A.30*) and it will not be transmitted.

The later part of the document regards personal data. It specifies that the IBAN number (*line A.37*) will be processed as confidential information and will be used to issue the payment order (*line A.38*), will also be stored for 90 calendar days and will not be

transmitted. Lastly, data subject's full name (*line A.43*) will again be processed as confidential information and will be used to issue the payment order (*line A.44*). It will be stored for 90 calendar days and it will be also transmitted to National Insurance Awareness Certificate Acquisition electronic service, with *policy_ID* 2058 (*line A.47*) and to National Insurance Awareness Certificate Acquisition electronic service with *policy_ID* 3153 (*line A.50*). Figure 4 presents the privacy policies for Taxation & National Insurance Awareness Certificates electronic services.

Figure 4 Taxation & National Insurance Awareness Certificates privacy policies

```
B.1  <Privacy_Policy>
B.2  <Policy_ID="2058">
B.3       <Service_Provider> Ministerial Department of Finance </Service_Provider>
B.4       <Electronic_Service> Taxation Awareness Certificate Aquicition </Electronic_Service>
B.5       <Description> Privacy Policy for Taxation Awareness Certificate Aquicition Electronic Service </Description>
B.6  </Policy_ID>
B.7
B.8  <Data>
B.9       <Personal_Identifiers>
B.10          <Identifier_ID="1">National Identity Card Number (IdN)
B.11              <Processed="Confidential">Identification</Proccessed>
B.12              <Storage="Yes" Conserve="120">Taxation Awareness Certificate</Storage>
B.13              <Transmitted="No">   </Transmitted>
B.14          </Identifier_ID>
B.15
B.16          <Identifier_ID="26">National Taxation Identifier (AFM)
B.17               <Processed="Confidential">Identification</Proccessed>
B.18               <Storage="Yes" Conserve="120">Taxation Awareness Certificate</Storage>
B.19               <Transmitted="No">   </Transmitted>
B.20          </Identifier_ID>
B.21      </Personal_Identifiers>
B.22
B.23      <Personal_Data>
B.24          <Data_ID="32"> First and Last Name
B.25               <Processed="Confidential">Taxation Awareness Certificate</Processed>
B.26               <Storage="Yes" Conserve="120"Taxation Awareness Certificate</Storage>
B.27               <Transmitted="No">  <Transmitted>
B.28          </Data_ID>
B.29      </Personal_Data>
B.30  </Data>
B.31  </Privacy_Policy>
```

```
C.1  <Privacy_Policy>
C.2  <Policy_ID="3153">
C.3       <Service_Provider> Ministerial Department of National Insurance </Service_Provider>
C.4       <Electronic_Service> National Insurance Awareness Certificate Acquisition </Electronic_Service>
C.5       <Description> Privacy Policy for National Insurance Awareness Certificate Acquisition Electronic Service </Description>
C.6  </Policy_ID>
C.7
C.8  <Data>
C.9       <Personal_Identifiers>
C.10          <Identifier_ID="1">National Identity Card Number (IdN)
C.11              <Processed="Confidential">Identification</Proccessed>
C.12              <Storage="Yes" Conserve="30">National Insurance Awareness Certificate</Storage>
C.13              <Transmitted="No">   </Transmitted>
C.14          </Identifier_ID>
C.15
C.16          <Identifier_ID="23">Social Security Number (AMKA)
C.17               <Processed="Confidential">Identification</Proccessed>
C.18               <Storage=""Yes" Conserve="30">National Insurance Awareness Certificate</Storage>
C.19               <Transmitted="No">   </Transmitted>
C.20          </Identifier_ID>
C.21      </Personal_Identifiers>
C.22
C.23      <Personal_Data>
C.24          <Data_ID="32"> First and Last Name
C.25               <Processed="Confidential">National Insurance Awareness Certificate</Processed>
C.26               <Storage=""Yes" Conserve="30">National Insurance Awareness Certificate</Storage>
C.27               <Transmitted="No"> <Transmitted>
C.28          </Data_ID>
C.29      </Personal_Data>
C.30  </Data>
C.31  </Privacy_Policy>
```

Similarly to the Registration process at Payment Authority Privacy Policy, the headers of each privacy policy document consist of information regarding the Service Provider that issued each document (*lines B.3 and C.3*), the electronic service it relates to (*lines B.4 and C.4*) and a short description (*lines B.5 and C.5*). The identification number assigned by Central Portal (*lines B.2 and C.2*) is also included through the corresponding element. Their difference lies in the data that each policy specifies. Privacy Policy B, for Taxation Awareness Certificate acquisition, indicates that the IdN, the AFM and data subject's full name are required (*lines B.10*, *B.16 and B.24*) and that they will be processed as confidential information for identification purposes (*lines B.11*, *B.17 and B.25*); they will be stored for 120 calendar days to issue the Taxation Awareness Certificate (*lines B.12*, *B.17 and B.26*) and will not be transmitted. Finally, Privacy Policy C, for National Insurance Awareness Certificate acquisition, indicates that the IdN, the Social Security Number (AMKA) and data subject's full name are required (*lines C.10*, *C.16 and C.24*) and that they will be processed as confidential information for identification purposes (*lines C.11*, *C.17 and C.25*); They will be stored for 30 calendar days to issue the Taxation Awareness Certificate (*lines C.12*, *C.17 and C.26*) and will not be transmitted to any other Service Provider (*lines C.13*, *C.18 and C.27*).

5.2 User's privacy preferences

On the basis of the proposal of Section 4.1, the user will also have to submit a Privacy Preferences document. Figure 5 presents the submitted user's Privacy Preferences. The first part of user's privacy preferences consists of an element, *Preferences_ID*, which is assigned by the Central Portal (CP) to every single document. Each user can maintain only one document and, depending on her pretentions, review it and update it at any given time. Consequently, each CP user can be assigned and associated to only one *Preferences_ID* identifier. As Privacy Preference's documents relate directly to user's personal data manipulation, they do not enclose any other information on user's real-world identity. Thus, a direct association with user's real-world identity is prevented and his privacy is preserved. The remaining document regards user's Personal Identifier (PII) and personal data. For each one of them, two elements and one attribute can be specified. The elements are titled processed and storage and the attribute concern the way this data or information can be manipulated by every SP. In these two elements the user can specify the Service Providers or the electronic services that can process or/and store his personal data.

Since a detailed description of each electronic service would be difficult for a user to administer and an inclusion of solely SPs could not imprint actual user's preferences, the establishment of sets and supersets is being proposed. Each Service Provider will constitute a superset that will contain all the electronic services that he offers; when a user allows his data to be processed or stored by this SP then this admission is transferred to each service. On the contrary an acceptance of a specific service does not imply approval of all SP's services. In addition to this principle, the lack of a SP or an electronic service shall be interpreted as a denial of data provision. Consequently, the simplest privacy preferences' documents may contain only a *Preferences_ID*, and based on the principle of denial, no SP or electronic service can process or store user's data. On the basis of the previous proposal of sets and supersets, the inclusion of attributes into specific supersets is also proposed. For instance, the Public attribute will also contain the

confidential one. Once more, this inclusion will reduce the administration burden on user's documents.

Through his Privacy Preferences document presented in Figure 5, user affirms that his IdN can be publicly processed and stored for 60 calendar days by GSIS, Ministerial Department of Finance and Ministerial Department of National Insurance (*lines P.7–P.13*). The same statements apply to his full name, however, they can be preserved for 360 calendar days by the same departments (*lines P.32–P.38*). Regarding AFM user affirms that it can be publicly processed and stored for 60 calendar days by GSIS and Ministerial Department of Finance (lines *P.16–P.20*). User's Social Security Number (AMKA) can be processed confidentially and stored for 60 calendar days by GSIS and Ministerial Department of National Insurance (lines P.23–P.27). Finally, IBAN can be processed confidentially and stored for 60 calendar days only by GSIS (*lines P.40–P.42*).

Figure 5 User's privacy preferences

```
P.1  <Privacy_Preferences>
P.2   <Preferences_ID="10451426">   </Preferences_ID>
P.3
P.4  <Data>
P.5
P.6     <Personal_Identifiers>
P.7          <Identifier_ID="1">National Identity Card Number (IdN)
P.8               <Processed="Public">General Secretary of Information Systems (GSIS)</Proccessed>
P.9                    <Storage="Yes" Conserve="60">General Secretary of Information Systems (GSIS)</Storage>
P.10              <Processed="Public">Ministerial Department of Finance</Proccessed>
P.11                   <Storage="Yes" Conserve="60">Ministerial Department of Finance</Storage>
P.12              <Processed="Public">Ministerial Department of National Insurance</Proccessed>
P.13                   <Storage="Yes" Conserve="60">Ministerial Department of National Insurance</Storage>
P.14         </Identifier_ID>
P.15
P.16         <Identifier_ID="26">National Taxation Identifier (AFM)
P.17              <Processed="Public">General Secretary of Information Systems (GSIS)</Processed>
P.18                   <Storage="Yes" Conserve="60">General Secretary of Information Systems (GSIS)</Storage>
P.19              <Processed="Public">Ministerial Department of Finance</Processed>
P.20                   <Storage="Yes" Conserve="60">Ministerial Department of Finance</Storage>
P.21         </Identifier_ID>
P.22
P.23         <Identifier_ID="13">Social Security Number (AMKA)
P.24              <Processed="Confidential">General Secretary of Information Systems (GSIS)</Processed>
P.25                   <Storage="Yes" Conserve="60">General Secretary of Information Systems (GSIS)</Storage>
P.26              <Processed="Confidential">Ministerial Department of National Insurance</Processed>
P.27                   <Storage="Yes" Conserve="60">Ministerial Department of National Insurance</Storage>
P.28         </Identifier_ID>
P.29    </Personal_Identifiers>
P.30
P.31    <Personal_Data>
P.32         <Data_ID="32"> First and Last Name
P.33              <Processed="Public">General Secretary of Information Systems (GSIS)</Proccessed>
P.34                   <Storage="Yes" Conserve="360">General Secretary of Information Systems (GSIS)</Storage>
P.35              <Processed="Public">Ministerial Department of Finance</Proccessed>
P.36                   <Storage="Yes" Conserve="360">Ministerial Department of Finance</Preserve>
P.37              <Processed="Public">Ministerial Department of National Insurance</Proccessed>
P.38                   <Storage="Yes" Conserve="360">Ministerial Department of National Insurance</Storage>
P.39         </Data_ID>
P.40         <Data_ID="321"> IBAN
P.41              <Processed="Confidential">General Secretary of Information Systems (GSIS)</Proccessed>
P.42                   <Storage="Yes" Conserve="360">General Secretary of Information Systems (GSIS)</Storage>
P.43         </Data_ID>
P.44     </Personal_Data>
P.45 </Data>
P.46 </Privacy_Preferences>
```

5.3 Electronic service provision

Assuming that the Privacy Policies presented in Section 5.1 and the Privacy Preferences presented in Section 5.2 have been successfully submitted to the Central Portal, the user can now request the provision of Registration at Payment Authority electronic service. On the basis of the architecture presented in Section 4.1, the Central Portal passes the request to the PCA. He then retrieves user's preferences along with service's privacy policy and forwards them to the Decision Point. At this point the comparison procedure is invoked and the policy is checked against user's preferences. Table 1 presents the comparison of these two documents.

Table 1 Comparison of user's privacy preferences and privacy policy

	User's preferences				*Privacy Policy A*			
	Process	*Storage*	*Conserve*	*Transmit*	*Process*	*Storage*	*Conserve*	*Transmit*
IdN	Public	Yes	*60*	Yes	Conf.	Yes	*90*	Yes
AMKA	Conf.	Yes	60	Yes	Conf.	No	–	Yes
AFM	Public	Yes	*60*	Yes	Conf	Yes	*90*	Yes
IBAN	Pubic	Yes	360	Yes	Conf.	Yes	90	No
Name	Public	Yes	360	Yes	Conf.	Yes	90	No

An inconsistency in the allowed and required retention periods between user's preferences and Service Provider's Policy emerges, thus the requested service cannot be provided. Through the Central Portal, the PCA informs the user of the inconsistency and exhorts user to review the retention period of her National Identifier (IdN) and her AFM. In case this inconsistency does not occur or is overcome, the Decision Point will have to compare Privacy Policy B and C against user's privacy preferences as well, since service A transmits user data at them. Only after compliance to all Privacy Policies the user is allowed to proceed with his request.

6 Related work

In an attempt to improve data and process interoperability, XML schemas have been widely adopted by e-government environments and their corresponding interoperability frameworks (e-GIF's) (Lee et al., 2009; Guijarro, 2007; Fung et al., 2010). New Zealand (E-GIF|Government ICT Directions and Priorities, 2012), Australia (Australian Government Information Interoperability Framework, 2012) and UK (eGIF policy document, 2012), amongst others, have issued directions, guidelines and technical standards regarding data modelling through XML schemas. All of them identify data modelling as a key issue in exchanging information and offering electronic services. Towards this direction, semantic model ontologies using the OWL Web Service Standard have been also proposed to expedite conformation, representation, searching and matching, of electronic services and facilitate their integration and interoperability (Apostolou et al., 2005; Klischewski and Ukena, 2007; Salhofer et al., 2009; Alvarez Sabucedo et al., 2010; Dombeu and Huisman, 2011). However, to the best of our knowledge, XML schemas for Privacy Policies or Privacy Preferences

representation have not been yet deployed or proposed for e-government environments. Nevertheless, for e-commerce environments they are not new.

Various Privacy-Enhancing Technologies (PETs) have been proposed and are currently available, including the platform for privacy preferences project P3P (Platform for Privacy Preferences (P3P) Project, 2012) and human-readable privacy policies. As acknowledged by relevant published works (Beatty et al., 2007; Said et al., 2012; Yingxin and Jutla, 2006; Yin et al., 2007) privacy policy plays a significant role in preventing unauthorised access to the user's private information in e-commerce environments. At some cases the posting of privacy policies on commercial websites has been a key component of online privacy protection. Privacy policies serve to increase transparency about data practices and support the 'notice' or 'openness' fair information practice principle.

7 Conclusions

The deployment of privacy aware e-government environments that allow for the provision of interoperable user-centric electronic services, while empowering users to retain control over their personal data, is undisputedly a challenge. In this paper a simple yet effective architecture which promotes the employment of Privacy Policies and Privacy Preferences in modern e-government environments has been proposed. This approach advances and simplifies the provision of electronic services, while it allows users to preserve, control and modify their personal data privacy characteristics based on their inclinations and needs. Furthermore, they are aware to whom and for what purpose their data are released. On the basis of this architecture e-government environments could expand their capabilities towards implementing services that meet citizen needs, promote further exploitation of electronic services to different user groups and finally (re)establish confidence in applications of e-government involving sensitive personal information.

References

Alvarez Sabucedo, L.M., Anido Rifón, L.E., Corradini, F., Polzonetti, A. and Re, B. (2010) 'Knowledge-based platform for eGovernment agents: a web-based solution using semantic technologies', *Expert Systems with Applications: An International Journal*, Vol. 37, No. 5, pp.3647–3656.

Apostolou, D., Stojanovic, L., Lobo, T., Miró, J. and Papadakis, A. (2005) 'Configuring e-government services using ontologies', *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government*, IFIP International Federation for Information Processing, Springer, USA, pp.141–155.

Australian Government Information Interoperability Framework (2012) http://www.finance.gov.au/e-government/service-improvement-and-delivery/australian-government-information-interoperability-framework.html (Accessed 10 October, 2012).

Beatty, P., Reay, I., Dick, S. and Miller, J. (2007) 'P3P adoption on e-commerce web sites: a survey and analysis', *Internet Computing, IEEE Internet Communication Journal*, Vol. 11, No. 2, pp.65–71.

Charalabidis, Y., Lampathaki, F., Sarantis, D., Sourouni, A-M., Mouzakitis, S., Gionis, G., Koussouris, S., Ntanos, C., Tsiakaliaris, C., Tountopoulos, V. and Askounis, D. (2008) 'The Greek electronic government interoperability framework: standards and infra-structures for one-stop service provision', *Panhellenic Conference on Informatics (PCI '08)*, pp.66–70.

Chellappa, R.K. and Pavlou, P.A. (2002) 'Perceived information security, financial liability and consumer trust in electronic commerce transactions', *Logistics Information Management*, Vol. 15, Nos. 5–6, pp.358–368.

Dombeu, J.V. and Huisman, M. (2011) 'Semantic-driven e-government: a case study of formal representation of government domain ontology', *IST-Africa 2011, IST-Africa Conference Proceedings*, pp.1–9.

Drogkaris, P., Geneiatakis, P., Gritzalis, S., Lambrinoudakis, C. and Mitrou, L. (2008) 'Towards an enhanced authentication framework for eGovernment services: the Greek case', *EGOV'08 7th International Conference on Electronic Government*, Trauner Verlag, pp.189–196.

eGIF policy document (2012) http://www.cabinetoffice.gov.uk/govtalk/policydocuments/e-gif/e-gif_policy_documents.aspx (Accessed 6 October, 2012).

E-GIF|Government ICT Directions and Priorities (2012) http://ict.govt.nz/guidance-and-resources/standards-compliance/e-gif (Accessed 10 October, 2012).

Fung, B.C.M., Wang, K., Chen, R. and Yu, P.S. (2010) 'Privacy-preserving data publishing: a survey of recent developments', *ACM Computing Surv*., Vol. 42, pp.1–53.

Gotoh, R. (2008) 'Assessing performance of e-government services for business users', *4th International Conference on e-Government (ICEG 2008), Academic Conferences*, pp.161–170.

Grabner-Kräuter, S. and Kaluscha, E.A. (2003) 'Empirical research in on-line trust: a review and critical assessment', *International Journal of Human-Computer Studies*, Vol. 58, pp.783–812.

Gritzalis, S. (2004) 'Enhancing Web privacy and anonymity in the digital era', *Information Management & Computer Security*, Vol. 12, No. 3, pp.255–287.

Guijarro, L. (2007) 'Interoperability frameworks and enterprise architectures in e-government initiatives in Europe and the United States', *Government Information Quarterly Journal*, Elsevier, Vol. 24, No. 1, pp.89–101.

Klischewski, R. and Ukena, S. (2007) 'An activity-based approach towards development and use of e-government service ontologies', *41st Annual Hawaii International Conference on System Sciences (HICSS 2007)*, IEEE, pp.215–215.

Lee, T., Hon, C.T. and Cheung, D. (2009) 'XML schema design and management for e-Government data interoperability', *Electronic Journal of e-Government*, Vol. 7, No. 4, pp.381–390.

Li, Y.H., Paik, H-Y. and Benatallah, B. (2006) 'Formal consistency verification between BPEL process and privacy policy', *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, ACM, pp.1–10.

McDonald, A.M., Reeder, R.W., Kelley, P.G. and Cranor, L.F. (2009) 'A comparative study of online privacy policies and formats', *9th International Symposium on Privacy Enhancing Technologies*, Springer-Verlag, pp.37–55.

Platform for Privacy Preferences (P3P) Project (2012) http://www.w3.org/P3P/ (Accessed 30 November, 2012).

Reeder, R.W., Kelley, P.G., McDonald, A.M. and Cranor, L.F. (2008) 'A user study of the expandable grid applied to P3P privacy policy visualization', *7th ACM Workshop on Privacy in the Electronic Society*, ACM, pp.45–54.

Said, A.A., Hussin, A.R.C., Dahlan, H.M. and Hossein Pour, M.M. (2012) 'Privacy policy preference (P3P) in e-commerce: key for improvement', *International Conference on Information Retrieval & Knowledge Management (CAMP)*, IEEE, pp.177–181.

Salas, P.P. and Krishnan, P. (2008) 'Testing privacy policies using models. Software engineering and formal methods', *SEFM '08. Sixth IEEE International Conference on Software Engineering and Formal Methods*, SEFM Publications, pp.117–126.

Salhofer, P., Stadlhofer, B. and Tretter, G. (2009) 'Ontology driven e-government', *Fourth International Conference on Software Engineering Advances (ICSEA '09)*, IEEE, pp.378–383.

Sedek, K.A., Sulaiman, S. and Omar, M.A. (2011) 'A systematic literature review of interoperable architecture for e-government portals', *(MySEC), 5th Malaysian Conference in Software Engineering*, IEEE, pp.82–87.

Silic, M., Krolo, J. and Delac, G. (2010) 'Security vulnerabilities in modern web browser architecture', *MIPRO, Proceedings of the 33rd International Convention*, IEEE, pp.1240–1245.

Siougle, E.S. and Zorkadis, V.C. (2002) 'A model enabling law compliant privacy protection through the selection and evaluation of appropriate security controls', *Proceedings of the International Conference on Infrastructure Security*, Springer-Verlag, pp.104–114.

Tambouris, E. and Wimmer, M. (2005) 'Online one-stop government: a single point of access to public services', in Huang, W., Siau, K. and Wei, K. (Eds.): *Electronic Government Strategies and Implementation*, Idea Group Publishing, Hershey, PA, pp.115–144, doi:10.4018/978-1-59140-348-7.ch006.

Teltzrow, M. and Kobsa, A. (2004) 'Impacts of user privacy preferences on personalized systems: a comparative study', in Karat, J., Vanderdonekt, J., Karat, C-M. and Blom, J.O. (Eds.): *Designing Personalized User Experiences in eCommerce*, Kluwer Academic Publishers, pp.315–332.

Votis, K., Alexakos, C., Vassiliadis, B. and Likothanassis, S. (2008) 'An ontologically principled service-oriented architecture for managing distributed e-government nodes', *Journal of Network and Computer Applications*, Vol. 31, No. 2, pp.131–148.

Vrakas, N., Kalloniatis, C., Tsohou, A. and Lambrinoudakis, C. (2010) 'Privacy requirements engineering for trustworthy e-government services', *3rd International Conference on Trust and Trustworthy Computing*, Springer-Verlag, pp.298–307.

Yin, C., Jianshi, L. and Ruxia, S. (2007) 'A modified model for private data security facing e-commerce', *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, IEEE, pp.762–765.

Yingxin, H. and Jutla, D.N. (2006) 'Contextual e-Negotiation for the handling of private data in e-Commerce on a Semantic Web', *39th Annual Hawaii International Conference on System Sciences (HICSS '06)*, IEEE, p.62a.

Zhang, W. and Wang, Y. (2008) 'Towards building a semantic grid for e-government applications', *WSEAS Transactions on Computer Research Journal*, Vol. 3, No. 4, pp.273–282.