Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy

Costas Lambrinoudakis a,*, Stefanos Gritzalis a, Fredj Dridi b, Günther Pernul b

a Department of Information and Communication Systems Engineering, University of the Aegean, Samos GR 832 00, Greece
b Department of Information Systems, University of Essen, Universitätstr. 9, 45141 Essen, Germany

Abstract

The concept of one-stop on-line government is not science fiction any more. On the contrary, the high reliability and performance of communication links, combined with architectural models that facilitate transparent access to distributed computational and storage resources, propel the development of integrated e-government platforms that support increased citizen mobility. The price we have to pay is the complexity introduced in the design of the security mechanisms required for protecting several heterogeneous information systems—each one supporting some of the services offered through the e-government integrated environment—and ensuring user privacy.

This paper demonstrates that the security services offered by Public Key Infrastructure (PKI) can be employed for fulfilling most of the identified security requirements for an integrated e-government platform. The list of security requirements has been compiled by adopting an organisational framework that facilitates the classification of e-government services according to the security requirements they exhibit.

The proposed approach has been applied, as a case study, to the e-government system ‘Webocrat’, identifying its security requirements and then designing a PKI-based security architecture for fulfilling them.

© 2003 Elsevier B.V. All rights reserved.

Keywords: e-Government; Security requirements; Public Key Infrastructure

1. Introduction

The advances in the Information and Communication Technologies (ICT) have raised new opportunities for the implementation of novel applications and the provision of high quality services over global networks. The aim is to utilise this ‘information society era’ for improving the quality of life for all citizens, disseminating knowledge, strengthening social cohesion, generating earnings and finally ensuring that organisations and public bodies remain competitive in the global electronic marketplace.

e-Government is the term reflecting the use of ICT in public administration in an attempt to ease access to governmental information and services for citizens, businesses, and government agencies. Furthermore it is always a target to improve the quality of the services and to provide greater opportunities for participating in democratic institutions and processes.

Such a rapid technological evolution could not be problem free. Concerns regarding the extent to which ‘information security’ and ‘user privacy’ can be ensured are raised. However, ‘growth’ of computerised facilities cannot be considered ‘progress’ until we are sure that the drawbacks do not outweigh the benefits. Information System Security is, therefore, an essential management responsibility for e-government, that has as a target to fulfil the fundamental security properties of: availability, confidentiality, integrity, accountability and information assurance [9]. A high level of confidence and trust among all users (citizens, businesses and government) will be the foundation of a successful e-government initiative [3].

In order to select and implement the necessary security measures it is necessary to identify and valuate the system assets, the associated threats and vulnerabilities, as well as to assess the consequences from a potential security incident. Risk analysis (RA) methodologies assist analysts to perform the above steps in a well structured way and thus
to select the countermeasures that will ensure a security level analogous to the level of risks. However, a precondition for performing an RA is to have precisely specified the boundaries—both in logical and physical terms—of the information system. This is clearly not a straightforward task for e-government systems that can normally be seen as an amalgam of heterogeneous information systems facilitating the exchange of information between citizens, businesses and several governmental agencies.

Thus, a new framework for identifying and organising the security requirements that are common to all information systems that have been utilised for the development of an integrated on-line e-government platform, is required. Such a framework can facilitate the development of a unified e-government security policy. This is because, security-wise, each information system is not considered any more as an isolated stand-alone system but as a component of the e-government platform, protected through countermeasures and security services that are applicable to the entire platform.

This paper demonstrates the feasibility of such an approach by utilising the ‘Organisational Framework for the Security Requirements of e-government services’ (e-GOV-OFSR) [6] for identifying the (common) security requirements for an integrated on-line e-government service platform that supports distance learning, electronic voting, electronic collaboration of governmental departments and several web-bases public services (Sections 2 and 3). In addition, Section 4 provides evidence that by utilising the security services offered by a Public Key Infrastructure (PKI), most of the consolidated e-government security requirements can be fulfilled. Finally, Section 5 presents, as a case study, the identification and classification of security requirements for the e-government system ‘Webocrat’, together with the PKI-based security architecture that has been implemented for its protection.

2. The e-government platform

As suggested in Ref. [16], the architecture of an integrated on-line e-Government service platform is depicted in Fig. 1.

Users (who can either be citizens or employees of public authorities) can utilise the supported e-government services through a global entrance point: the governmental portal. The portal can be either accessed through the local network or remotely through the Internet or even through other type of wireless devices like mobile phones.

Normally, the ‘e-government services’ are supported through several collaborating (in terms of information exchange) client–server information systems. This conventional client–server architecture assumes to know where computing and storage power is located. However, the continuously increasing user requirements, in conjunction with the huge number of potential users, impose the need for evolved computational models that can transparently access distributed computational and storage resources.

Nowadays such architectures can be supported, an example being the GRID technology which forms the next logical step in computing infrastructure following a path from standalone systems to tightly linked clusters, enterprise-wide clusters and geographically dispersed computing environments. The Open Grid Services Architecture (OGSA) [15] is supporting the creation, maintenance and application of services through a common representation for computational and storage resources, networks, programs, databases and the like. The advantage of such a service oriented view is that most of the interoperability issues are limited (a) to the definition of service interfaces and (b) to the specification of the protocols that can invoke a specific interface [4].

3. Security issues

Although state-of-the-art technology eases the development of on-line ‘one-stop government’ platforms, it is, at the same time, a major contributor to some of the problems associated with the design and implementation of a secure environment [1], especially when combined with the continuously increasing citizen mobility. By allowing users to access services from virtually anywhere, the universe of ineligible people who may attempt to harm the system is dramatically expanded.

Moreover, existing methodologies for determining risk factors and identifying security requirements for the assets (hardware, software and data) of an information system with well-defined boundaries, are not necessarily applicable or/and cost effective for new architectures like GRID. GRID security requirements, including authentication, communication protection and authorisation, should provide for interoperability among different domains, adoption of different security rules and policies and take into consideration the definition of globally unique identities for each involved entity (user, resource, service), the provision to each entity of a mean to prove that it possesses a specific identity and the adoption of rights delegation mechanisms to other entities.

3.1. Identifying security requirements

In Ref. [6] an Organisational Framework for the Security Requirements of e-Government services has been proposed; namely the ‘e-GOV-OFSR’. Its aim is to alleviate the inefficiencies of conventional RA methodologies by increasing the granularity of the analysis and by interrelating, in multiple ways, the risk assessment results. Specifically, a distinct risk level value is calculated for each supported system service, or even service process (phase), and this is done independently for each actor type (user group). Depending on the RA methodology, it may be necessary to
repeat the RA study several times or simply to extract and process, in an appropriate way, intermediate results.

The adoption of such a framework for identifying security requirements facilitates:

- The classification of e-government services according to the similarity of the security requirements that they exhibit.
- The protection of all services (or service phases) of the same class in a uniform way, through the appropriate security measures.
- The identification of security requirements associated with each type of user.
- The development of a common, but also flexible and extensible (in terms of supporting additional services or employing new underlying architectures like GRID), e-government security policy.

The succeeding sections list the security requirements that have been derived through several independent RA studies for the following e-government services:

1. Provision of on-line courses for distance learning (e-University)
2. Supporting the participation of citizens to various election processes through internet (e-voting)
3. Electronic collaboration of various governmental departments through email, video conference, use of shared documents, etc.
4. Supporting transactions between citizens and governmental departments (like ordering birth certificates, submitting tax forms, conducting electronic payments, etc.)

It is emphasised that the RA results have been formulated in accordance with the e-GOV-OFSR framework described above and that the security requirements have been organised in terms of service phases, and actor type. It is clarified that neither the above mentioned services cover the entire spectrum of e-government services, nor the entire lists of security requirements, as resulted from the respective RA studies, have been utilised here—only the most significant ones were exploited.

3.1.1. e-University

The term ‘e-University’ represents a suite of services supporting open distance learning activities. In addition to the development, management and offering of on-line courses, the system supports administrative tasks like registration, payments, certification, etc.

During the ‘Setting up the System’ phase the system administrators are expected to ensure that the system will be set up in a way that can support the desired functionality and the maximum number of students, without any non-availability or deterioration in performance problems (for example protection against denial of service attacks and viral software). Furthermore
they must specify the access privileges for all types of users.

During the ‘Authentication’ phase the appropriate mechanisms are employed for authenticating the credentials of all registered users (students, tutors, etc.).

During the ‘Setting up the Service’ phase the educational material is authored by the trainers and in collaboration with the tutors it is structured in a way that conforms to the characteristics of the potential students, their knowledge and requirements profiles, etc. With the exception of the required procedures for ensuring the suitability and correctness of the educational material, no other significant risks were identified.

During the ‘Offering the Service’ phase the integrity (i.e. non-modification) and confidentiality (i.e. non-disclosure) of the material provided to and submitted by the students, as well as of the information generated through network discussions and communication among students, must be ensured. Furthermore, the proof of origin, submission, delivery and receipt, whenever transactions between students and trainers–tutors occur, must be maintained. In addition to that, time stamping and partial logging must be employed for handling possible disputes.

Finally, during the ‘After Service Tasks’ phase (implying that the on-line courses are not offered any more), information like student marks and other personal data collected during the registration of the students, should be protected from non-authorised access. Furthermore, a logging mechanism should be employed (Table 1).

### Table 1  
Risk levels and security requirements for the e-University services

<table>
<thead>
<tr>
<th>Suite of services</th>
<th>Service phase</th>
<th>Actor type</th>
<th>Risk level</th>
<th>Security requirements</th>
</tr>
</thead>
</table>
| e-University      | Setting up the System (setting up the hardware and software infrastructure required for the operation of the designed services) | System administrators | Medium | • System availability  
• Performance  
• Management of privileges |
| Authentication     | Service customers<sup>a</sup> | Service operators<sup>a</sup> | Medium | • Authentication |
| Setting up the Service (course organisation and material preparation) | Service operators<sup>a</sup> | Service operators<sup>a</sup> | High | • Integrity  
• Logging |
| Offering the Service (offering on-line courses and other supporting—educational—tasks to students) | Service customers<sup>b</sup> | Service customers<sup>b</sup> | Low | • Confidentiality  
• Integrity  
• Non-repudiation  
• Logging |
| After Service Tasks (maintaining progress—issuing certificates, etc.) | Service operators<sup>a</sup> | Service operators<sup>a</sup> | Medium | • Secure storage  
• Logging |

<sup>a</sup> Tutors, trainers, authors.  
<sup>b</sup> Students.

3.1.2. e-Voting

This suite of services supports the conduction of several types of election procedures, like polls, internal elections, decision-making, etc. through the Internet. All eligible voters can thus participate in the election irrespective of their geographical location.

The role of system administrators during the Setting up the System phase is identical to that described for the e-University suite of services. Furthermore, the authentication of voter and election organiser credentials (Authentication phase) is a prerequisite prior to any kind of interaction of the user with the system.

During the Setting up the Service phase, the election organisers, normally state officials, set up all necessary system parameters (i.e. election districts, parties, candidates, lists of eligible voters, etc.). Although state officials, will normally be trusted, they must be authenticated before accessing the system and all their actions must be logged.

During the Offering the Service Phase, which is probably the most important system process, an eligible voter can select a ballot and cast her/his vote. There are numerous important security requirements during this phase [8], many of them imposed by the respective legal and legislative
framework [12]. Some indicative ones are anonymity, confidentiality, integrity, no one can vote twice, etc.

The last system phase After Service Tasks, mainly refers to the storage of the ballots cast and the calculation of the election tally. Specifically the tallying process should be available only after the election process has ended and its aim is to validate votes and determine the total number of votes each candidate has received. During tallying the integrity is ensured through the participation and active involvement of party representatives, while logging of all actions is necessary. After the tallying process the votes and other relevant evidence must be stored in a secure way (Table 2).

### 3.1.3. Electronic collaboration of governmental departments

Several services, like email, video conference, discussion forums, use of shared documents, etc. are supported for assisting the efficient and productive collaboration of remote governmental departments. Since the functionality of the provided services is well known, no detailed description of each service phase is provided (Table 3).

### 3.1.4. Web-based public services

Another typical use of a governmental portal is to provide information to the citizens and to support several types of citizen–government transactions (e.g. issuing birth certificates, submitting tax forms, conducting electronic payments, etc.). The description of each service is evident and is thus not provided here (Table 4).

### 3.2. A consolidated view of the security requirements for an e-Government platform

Fig. 2 presents the consolidated security requirements for an e-Government platform. Their compilation has been based on the security requirements derived for each independent service suite, while they are again organised in terms of the identified ‘service phases’ and ‘actor types’.

The conclusions drawn from such a classification can be summarised to the following:

- **Actors per Service Phase.** It is demonstrated that the role of each actor type is confined to specific service phases; system administrators are only active during the Setting up the System phase, while service operators during the Authentication, Setting up the Service and After Service Tasks phases. The service customers interact with the system during the Authentication and Offering the Service phases.

- **Risk Levels.** The average value of the calculated risk level for all service phases is Medium, as far as the system administrators and service operators are concerned. Of course there may be specialised applications

<table>
<thead>
<tr>
<th>Suite of services</th>
<th>Service phase</th>
<th>Actor type</th>
<th>Risk level</th>
<th>Security requirements</th>
</tr>
</thead>
</table>
| **e-Voting**      | Setting up the System (setting up the hardware and software infrastructure required for the operation of the designed services) | System administrators | Medium | • System availability  
|                   |               |            |           | • Performance  
|                   |               |            |           | • Management of privileges |
|                   | Authentication | Service operators<sup>a</sup> | High | • Authentication |
|                   |               | Service customers<sup>b</sup> | High | |
|                   | Setting up the Service (type of election, management of candidates, eligible voters, etc.) | Service operators<sup>a</sup> | Medium | • Logging |
|                   | Offering the Service (eligible voters after having authenticated themselves can cast their votes) | Service customers<sup>b</sup> | High | • Confidentiality  
|                   |               |            |           | • Integrity  
|                   |               |            |           | • Public trust  
|                   |               |            |           | • Anonymity  
|                   |               |            |           | • Untraceability |
|                   | After Service Tasks (maintaining cast votes and result tally) | Service operators<sup>a</sup> | High | • Secure storage  
|                   |               |            |           | • Public trust  
|                   |               |            |           | • Logging |

<sup>a</sup> Election organisers and other state officials.

<sup>b</sup> Voters.
Table 3
Risk levels and security requirements for the electronic collaboration services

<table>
<thead>
<tr>
<th>Suite of services</th>
<th>Service phase</th>
<th>Actor type</th>
<th>Risk level</th>
<th>Security requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic collaboration of governmental departments</td>
<td>Setting up the System (setting up the hardware and software infrastructure required for the operation of the designed services)</td>
<td>System administrators</td>
<td>Low</td>
<td>• System availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Performance</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Service operators</td>
<td>Low</td>
<td>• Management of privileges</td>
</tr>
<tr>
<td></td>
<td>Setting up the Service (manage user accounts and access privileges)</td>
<td>Service operators</td>
<td>Low</td>
<td>• Logging</td>
</tr>
<tr>
<td></td>
<td>Offering the Service (emails, video conference, etc.)</td>
<td>Service customersa</td>
<td>Low</td>
<td>• Confidentiality</td>
</tr>
<tr>
<td></td>
<td>After Service Tasks (storing emails, shared documents, etc.)</td>
<td>Service operators</td>
<td>Medium</td>
<td>• Integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Secure storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Logging</td>
</tr>
</tbody>
</table>

- Governmental employees.

(like e-Voting) where the risk level becomes High. On the contrary, for the service customers the calculated average value for the risk level is Medium to High.

- Security Requirements. There is a clear distinction of the security requirements per service phase (and thus per actor type). By adopting the security measures that can effectively satisfy the identified security requirements it is feasible to develop a uniform, but also generally applicable and easily expandable, security policy for e-Government platforms.

Table 4
Risk levels and security requirements for the Web-based public services

<table>
<thead>
<tr>
<th>Suite of services</th>
<th>Service phase</th>
<th>Actor type</th>
<th>Risk level</th>
<th>Security requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-based public services</td>
<td>Setting up the System (setting up the hardware and software infrastructure required for the operation of the designed services)</td>
<td>System administrators</td>
<td>Medium</td>
<td>• System availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Performance</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Service operators</td>
<td>Medium</td>
<td>• Management of privileges</td>
</tr>
<tr>
<td></td>
<td>Service customersb</td>
<td></td>
<td>High</td>
<td>• Logging</td>
</tr>
<tr>
<td></td>
<td>Setting up the Service (updating Web servers and maintaining supported services)</td>
<td>Service operatorsa</td>
<td>Medium</td>
<td>• Integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Secure storage</td>
</tr>
<tr>
<td></td>
<td>Offering the Service</td>
<td>Service customersb</td>
<td>Low</td>
<td>• Integrity</td>
</tr>
<tr>
<td></td>
<td>Search/retrieve information</td>
<td></td>
<td></td>
<td>• Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Request for birth certificate</td>
<td></td>
<td>Medium</td>
<td>• Integrity</td>
</tr>
<tr>
<td></td>
<td>Submission of tax forms</td>
<td></td>
<td>Medium</td>
<td>• Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Electronic payments</td>
<td></td>
<td>High</td>
<td>• Integrity</td>
</tr>
<tr>
<td></td>
<td>After Service Tasks (store submitted tax forms, electronic payment receipts, etc.)</td>
<td>Service operatorsa</td>
<td>Medium</td>
<td>• Confidentiality</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Non-repudiation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Secure storage</td>
</tr>
</tbody>
</table>

- Web Administrator.
- Citizens.
4. The Public Key Infrastructure

4.1. Services and functions

The user requirements, for several distinct application domains, that a PKI should fulfil have been widely recorded in the literature. However, most current attempts to specify the desirable set of PKI services have not been based on the user-security requirements [14]. In Refs. [10,11] it has been reported that the 'minimal set' of user requirements includes authentication of users, integrity of messages, privacy and confidentiality of messages, non-repudiation of message origin and destination, availability of services and ease of use. Furthermore, issues like anonymity, time-stamping, uniqueness of documents, interoperability between different elements, protection from abuse of any participant by another and several legal constraints have been identified as important. The PKI services that satisfy the above requirements [7,11] are listed in the first column of Table 5.

4.2. Adopting PKI for satisfying e-government security requirements

Table 5 demonstrates the fact that PKI could be adopted for building the appropriate level of security for a one-stop governmental portal. Specifically, the PKI services presented in Section 4.1 are listed together with the consolidated security requirements for an e-Government portal. For each security requirement there is a clear indication of the PKI service(s) that could be employed for fulfilling it.

It can be noticed that the majority of e-government security requirements can be fulfilled through the available PKI services. Still, there are requirements like availability, performance, uncoercibility, untraceability, anonymity (in the context of e-voting), etc. that cannot be fulfilled. Additional security measures are therefore necessary for handling requirements imposed by:

- The hardware and software infrastructure supporting the e-government portal. It is clear that there is no common way to handle the risks introduced by the inappropriateness of the hardware or software employed by the authorities for building the portal. Issues like, unreliable hardware, limited computing resources, poor communication infrastructure, unstable software, maintainability, etc. must be certainly examined on a case-by-case manner. Countermeasures like redundant servers, backup communication lines, service contracts, testing procedures, etc. can be adopted in accordance to the peculiarities and needs of the environment.
Security critical applications. In order to satisfy highly specialised, application specific, security requirements—like anonymity, uncoercibility, untraceability, verifiability, etc. that are applicable to the e-Voting suite of services—it is necessary to implement the required countermeasures as part of the application itself. For instance, the e-Voting security requirements are fulfilled through a specialised voting protocol that is being developed as part of the service.

5. A case-study: the e-government system Webocrat

The e-GOV-OFSR framework has been used for identifying and classifying the security requirements for the e-government system Webocrat, which is designed and implemented within the Webocracy Project. Capitalising on the results, the countermeasures (in terms of security services) that are necessary for ‘protecting’ the system were derived and they have been implemented through a PKI-based security architecture, called CSAP (Communication, Security, Authentication and Privacy). Currently, CSAP is almost fully implemented and integrated in the Webocrat system.

5.1. The Webocracy project

Webocracy\(^1\) is an ongoing EU funded research project [2]. It aims to demonstrate innovative uses of state-of-the-art web technologies for supporting direct participation of citizens in democratic processes. Specifically, it capitalises on new technologies for providing citizens, businesses, and government agencies with more convenient access to governmental information and services, improving the quality of the services and for providing greater opportunities to participate in democratic institutions and processes.

The Webocrat system (Fig. 3) has been designed in a modular way implementing the following functionality: discussion management, publishing on the Web, opinion polling, reporting, intelligent retrieval of information, and knowledge management.

Although an application like the Webocrat system involves a large number of heterogeneous users, they can still be characterised in terms of the actor types defined in Section 3, namely: system administrators, service operator and service customers. System administrators are responsible for setting up the hardware and software infrastructure.

---

\(^1\) Acronym for ‘Democracy on the Web’; The project’s full name is ‘Web Technologies Supporting Direct Participation in Democratic Process’.

---

### Table 5
Use of PKI services for fulfilling e-government security requirements

<table>
<thead>
<tr>
<th>PKI services</th>
<th>Security requirements</th>
<th>Availability</th>
<th>Performance</th>
<th>Management of privileges</th>
<th>Authentication</th>
<th>Logging</th>
<th>Integrity</th>
<th>Confidentiality</th>
<th>Non-repudiation</th>
<th>Anonymity</th>
<th>Public trust</th>
<th>Untraceability</th>
<th>Secure storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital signatures</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time stamping</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-repudication</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information repository</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camouflaging communication</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorisation</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTP to TTP interoperability</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) Not in the context of e-voting.
required for the operation of the designed services and for
the security services implemented through the CSAP
module (see Section 5.3). The service operators (e.g.
government employees) are responsible for setting up
the Webocrat modules. The service customers (e.g. citizens,
politicians) are the primary external users, accessing the
system via well-specified ‘User Interfaces’. They can use
the ‘Citizens Information Helpdesk’ for searching or
retrieving information, and also for accessing published
documents.

The ‘Webocrat–Webspace’ is a part of the system
that can be accessed by the Service Customers through
the appropriate user interfaces. It is composed of three parts:
The ‘Publishing Space’ includes documents that are of
interest not only to the citizens but also to entrepreneurs,
professional associations, students, etc. Different types of
documents (i.e. laws, resolutions, budgets, reports on
activities carried out by local and regional government)
can be published there. The ‘Discussion Space’ is used
for supporting intelligent communication between citi-
zens, elected representatives and public servants in
several areas. Inputs and comments from citizens,
interest groups, professional associations, etc. on legal
documents that are under preparation (bills, resolutions,
etc.) can be published in the Discussion Space. The
‘Opinion Polling Space’ enables the electronic opinion
polling on several issues/questions of interest. Another
module of the system is that of ‘Knowledge Manage-
ment’ [13]. Its purpose is to specify the concepts and
relations that are useful for representing knowledge
(metadata) about a particular document in domain
specific terms; create contextual information attached to
the documents and thus facilitate searching and retrieval
of documents.

5.2. Security requirements and risk analysis

The large number of users, combined with the fact that
the Webocrat system processes documents that may contain
confidential or other sensitive information, substantiate the
importance of the security issues for the success of the
system. Three RA studies have been conducted, one for
each local authority participating in the project. The
calculated risk levels for the system assets as well as the
resulting security requirements have been organised in
accordance with e-GOV-OFSR framework (see Section
3.1). The consolidated results are presented in Table 6. Due
to space limitation only a subset of the Webocrat service
phases have been considered.

The description of the activities during the Setting up
the System and Authentication phases is skipped since it
coincides with that given for the e-University suite of
services (Section 3.1.1). During the Setting up the Service
phase the documents to be published in the Webocrat–
Webspace are authored by the service operators (government
employees). Furthermore, for each local authority that
uses the Webocrat system a knowledge model must be
defined and implemented. Another task of the service
operators is to implement the appropriate user profiles in
order to ensure that every registered user is presented with
a personal access page that grants personalised access to the
system.

During the Offering the Service phase the service
customers access the Webocrat–Webspace. The integrity
and confidentiality of the published documents must be
ensured. Furthermore, the proof of origin, submission,
delivery and receipt of discussion items and polls must be
maintained. Finally, during the After Service Tasks phase
discussion summaries and evaluations of the finished
opinion polls must be securely archived. Furthermore, a logging mechanism should be employed.

5.3. CSAP security architecture

CSAP (Fig. 4) has been designed as an integral part of the Webocrat system, utilising PKI security services in order to minimise the consequences in case of a security incident. The main security requirements that CSAP fulfils are the ones listed in Table 6. Two main classes of security services are considered:

- Communication security. The services of this class are primarily aiming to handle the security requirements of integrity, confidentiality and non-repudiation for information communicated over the network.
- System security. This class of services can be divided into the following sub-classes: Identification and authentication that mainly supports the verification of the user credentials trying to access the Webocrat system. CSAP authentication mechanisms can range from simple username/password to more sophisticated models based on signed certificates.

Table 6
Risk levels and security requirements for the Webocrat system

<table>
<thead>
<tr>
<th>Suite of services</th>
<th>Service phase</th>
<th>Actor type</th>
<th>Risk level</th>
<th>Security requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webocrat</td>
<td>Setting up the System (setting up the hardware and software infrastructure required for the operation of the designed services, granting access rights)</td>
<td>System administrators</td>
<td>Medium</td>
<td>System availability</td>
</tr>
<tr>
<td></td>
<td>Authentication (user registration)</td>
<td>Service operators</td>
<td>Medium</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Setting up the Service (building a knowledge model, publish documents, open discussions, preparing opinion polls)</td>
<td>Service operators</td>
<td>Medium</td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Offering the Service</td>
<td>Search/retrieve information, accessing published documents</td>
<td>Service customers</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Discussion</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Opinion polling</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Personalization</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>After Service Tasks (closing and summarising discussion, evaluation of opinion polling, statistical data retrieval)</td>
<td>Service operators</td>
<td>Medium</td>
<td>Secure storage</td>
</tr>
</tbody>
</table>

Fig. 4. CSAP architecture and PKI security services.
Access control and authorisation that facilitates the management of privileges for eligible system users. Auditing that facilitates the logging of all security relevant actions in order to make users accountable for their transactions. Audit trails are used to find patterns of abnormal use as an indication of compromise or attempted compromise.

Secure storage that concerns the protection of the information (documents, statistical data, evaluation of opinion polls, summaries of discussions, etc.) maintained by the system from non-authorised access.

Fig. 4, in conjunction with Table 5 that associates PKI security services with e-government security requirements, demonstrates that PKI can be employed for implementing the required CSAP functionality.

6. Conclusions

This paper has highlighted that the design and implementation of the security mechanisms for an integrated on-line e-government platform is not a straightforward task. Existing RA methodologies can only be applied to information systems with well-defined boundaries and are thus not appropriate for studying an e-government environment as a single entity. Instead, each information system must be studied independently, in accordance with the guidelines of the chosen RA methodology, identifying the security requirements associated with it. Having repeated that for all information systems composing the e-government environment, the consolidated list of requirements can be processed in accordance with the organisational framework that has been proposed for assisting their classification in terms of the identified service phases and actor types. Indeed, the use of the e-GOV-OFSSR has allowed us to compile a list of security requirements, for each service phase or/and actor type, that are applicable to the entire e-government platform. By selecting the security measures that can effectively satisfy the identified security requirements it is feasible to develop a uniform e-government security policy.

Finally it has been demonstrated that most of the e-government security requirements can be fulfilled through the PKI security services. The requirements imposing the need for additional security measures are either related to the hardware/software infrastructure of the e-government platform (e.g. performance, availability, etc.), or to highly specialised-security critical applications (e.g. e-voting, anonymity, uncoercibility, etc.).

References