SWEB: An Advanced Mobile Residence Certificate Service

Spyridon Papastergiou, Despina Polemi, and Christos Douligeris

Department of Informatics, University of Piraeus, 80 Karaoli & Dimitriou Str,
185 34 Piraeus, Greece
{paps,dpolemi,cdoulig}@unipi.gr

Abstract. The design and development of an enhanced network infrastructure in combination with the adoption of new technologies, standards and architectural styles for the design, development and implementation of new platforms can give a significant push to the deployment of advanced mobile services in the area of public administration. In this context, we present an innovative m-government platform that provides an advanced mobile Residence Certificate service. The proposed platform is an interoperable, affordable, secure and scalable solution that addresses a set of crucial requirements such as security, user friendliness, interoperability, accessibility and scalability.

Keywords: m-government platform, mobile service, security.

1 Introduction

The entry in the ICT Society constitutes a basic strategic choice for all the members of European Union (EU), since it can be considered as the means to achieve economic growth and prosperity. However, the achievement of this objective presupposes two major conditions. The first is the creation of a suitable network infrastructure through the development, engineering, maintenance and operation of high-speed wired and wireless networks that enable the countries to strengthen their fundamental structure. Major initiatives [1], [2] have been launched and implemented in the EU member states towards this direction, creating the proper telecommunications infrastructure.

The second condition concerns the exploitation and adoption of new technologies, standards and architectural styles for the design, development and implementation of new platforms that are able to provide advanced services. These services aim to improve the relations among the involved stakeholders and to create significant revenue for them.

Especially in the area of public administration several activities have been initiated that define standards-based frameworks for the public sector bodies at the national [3], [4] and pan-European levels [5], [6]. The goal of these frameworks [7] is to empower a joined up and web-enabled government, and to improve its flexibility and efficiency. Typically, these frameworks focus on the precise definition of specific standards that should be applied and provides guidelines in the form of specifications that should be followed for the development of governmental platforms and services.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 421–430, 2010.

It should be also noted that most of the projects [8], [9], [10], [11] that are currently run or have been completed in the public sector either cover only the electronic dimension of the government or treat the mobile aspect in a superficial manner. Usually, the latter does not achieve to provide advanced mobile government (m-government) services due to the limitations of the existing mobile devices, thus failing to address several crucial requirements, such as security, in an effective way.

Although, in the past few years mobile phones have been continually improving and at the moment they present rather powerful computing and communication devices capable of executing complex applications. This factor can be considered as the starting point for the deployment of a number of m-government services.

In this context, this paper presents an innovative m-government platform, named SWEB [12], [13], [14], [15], [16] that is based on widely used Web Service-based technologies and Public Key Infrastructure (PKI) in order to address several security and interoperability aspects. SWEB is a secure, interoperable, open, affordable municipal platform upon which an advanced mobile Residence Certificate (mRCertificate) service has been built and offered for use and experimentation. The mRCertificate service enables the citizens of the municipality that hosts the platform to receive a document that proves the existence of a residence for a given citizen in the specific municipality.

The rest of the paper is structured as follows; Section 2 discusses the major requirements as imposed by the mRCertificate service. Section 3 presents the proposed m-government framework illustrating the main entities that it consists of and it describes the SWEB platform. Section 4 describes the main activities performed when a user (citizen) registered in the SWEB platform of his/her municipality uses this platform to request a mRCertificate document. Finally, Section 4 draws some conclusions and presents areas for further research.

2 Requirements of the mRCertificate Service

Residence certification is an important document that it is being issued by municipalities. The included business flow of this service can be considered as a time-consuming process due to the population movements within the same country or/and abroad. The main objective of the proposed mRCertificate service is to cover the needs of a citizen or civil servant to search for, request and receive a municipal mobile document certifying that a particular citizen is registered at the records of a municipality in an efficient and accurate manner. D

In order for the mRCertificate service to be widely accepted by the citizens and the municipalities that will host and operate the SWEB platform has to address a set of requirements. The major requirements that must be fulfilled are the following:

Security: The mRCertificate service has to be secure in all aspects (confidentiality, integrity, authenticity, non-repudiation), so that all users trust the service and feel confident in using it. The adoption of proper advanced security mechanisms such as XML encryption [17], XML Signatures [18] and Timestamping [19] that will undertake the responsibility to secure the exchanged documents and messages creating a trusted framework is considered crucial for the SWEB platform.

User Friendliness and Accessibility: The wireless environment needs to be easily accessible, with user-friendly interfaces. The mobile application of the mRCertificate service has to be designed and developed by properly taking into consideration the constraints that come from the size and the capabilities of the mobile devices. The application should offer a basic functionality while complex operations must be completely transparent to the user.

Interoperability: The mRCertificate service should be interoperable enabling the interconnection with many different infrastructures (e.g. existing legacy systems) of the municipality. For this reason, new technologies that promote the interoperability (i.e. Web Services [20]) and light protocols in the messaging exchange have to be adopted.

Reduced organizational and technical complexity: The mRCertificate service should add a small amount of organizational and technical complexity, concerning financial and temporal parameters. This is achieved by introducing standard solutions, applicable in different municipal organizations that are quick to be adopted and easily customizable to the organization's requirements, trying to diminish the need for maintenance during operation.

Scalability and extensibility: The mRCertificate service has to be simple, open, reconfigurable, scalable and easily extensible. It should be capable to serve a large number of citizens with acceptable levels of quality of service.

3 Proposed m-Government Framework

This section presents the proposed m-government framework illustrating the main entities that participate in it and describing the m-SWEB platform.

3.1 Involved Entities

In this section, a description of the five major entities that constitute the m-Residence Certificate process is provided. A high level representation of the framework is presented in figure 1, highlighting these entities. The Mobile User and the Home-Municipality are the two main entities of the framework that initiate the process and handle the request correspondingly.

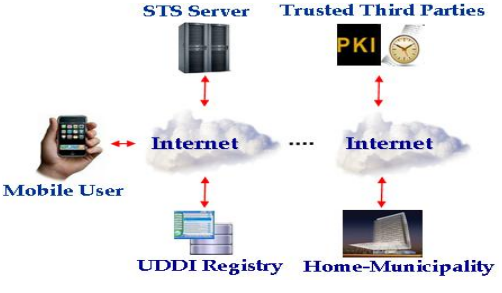

Fig. 1. Entities and Actors

The involved actors are described in the following:

Home-Municipality
This is the municipality that hosts the proposed m-SWEB platform and thus it is able to offer the mRCertificate service to its citizens. It takes the appropriate steps to develop and make available the mobile application required to access the provided service.

Mobile User
The mobile users are citizens that have their residence in the region being under the control of a municipality that has adopted and operates the m-SWEB platform. It should be noted that the user himself may be either a citizen requesting its own residence certificate or a delegate who is allowed to undertake such a request.

Secure Token Service (STS) Server
This entity authenticates users that want to access the provided m-RCertificate service issuing the needed authorization token. Based on this token the "Home-Municipality" is able to grand or deny access to their service.

Trusted Third Party (TTP)
The required TTPs are at a minimum a Certification Authority (CA) and a Registration Authority (RA) offering the PKI services of registration and certification, as well as a Time Stamping Authority (TSA) offering standard based time stamping services.

UDDI Registry
This operator hosts a public UDDI directory where the offered mRCertificate services of the "home-municipalities" are published in order to become publicly available.

3.2 m-SWEB Platform Overview

A major objective of the SWEB platform is to exploit the functionality of the existing legacy systems (e.g. back-office systems, independent applications, databases) of the municipality in order to provide advanced mobile services such as the Residence Certificate service. The basic achievement of the SWEB platform is that is able to overcome the internal obstacles of the legacy systems.

Most of these systems are typically developed based on a centralized model. Therefore, they are usually large and monolithic since their functionality is not well divided into smaller and more manageable modules/procedures. In this context, the legacy systems are not able to provide well-formed standardized interfaces that can be used by remote users in order to access all the available services and provided functionalities.

The innovative design of the SWEB platform architecture aims to hide the complex processes of theses services by providing interoperable and easy-to-use services and to achieve expandability of their functionality and high level of quality by means of system security. This is accomplished by using advanced XML-based technologies, PKI and design methodologies, resulting in an elaborate platform that fulfils several critical requirements and offers a trusted environment to their citizens.

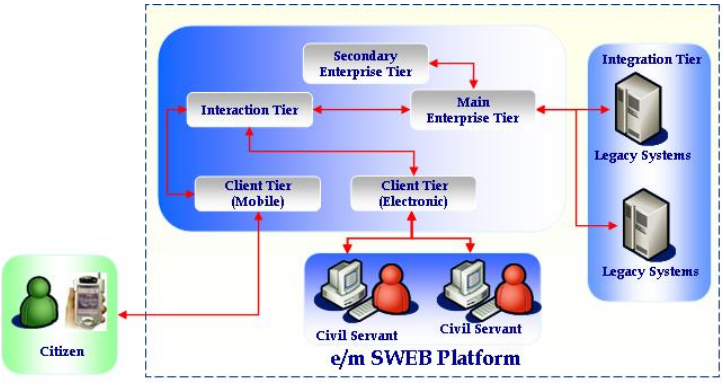

Fig. 2. m-SWEB Platform

In more detail, the architectural overview of the SWEB platform, as depicted in Figure 2, consists of five concrete tiers, which are listed below:

- ✓ The *Interaction Tier* includes all the components that are directly used to communicate with the platform. It includes all the required interfaces for the establishment of the appropriate communication channels with every electronic and mobile entity (e.g. citizens, organizations and civil servants) that want to access the provided m/e-services.
- ✓ The *Main Enterprise Tier* where all basic services and the platform core are deployed. These basic services provide the basic functions that are used by the architecture as a whole to perform primitive tasks. In the SWEB platform the basic services include:
  - o *Security services*, responsible for implementing the needed security mechanism such as the creation and the validation of simple XML digital signatures.
  - o *Transformation services*, which actually handle all the data transformation mechanisms from one form to another.
  - o *Integration services*, responsible for the communication with the legacy infrastructures of the municipality (Integration Tier).
- ✓ The *Secondary Enterprise Tier*, which undertakes the responsibility to manage the choreography of the main platform services (mRCertificate service), and to implement their business logic.
- ✓ The *Integration Tier*, which consists of the required adaptation components that sit "on-top" of the existing/ legacy systems of the municipality.
- ✓ The *Client Tier*, which integrates all the necessary components for accessing the SWEB platform and requesting the m-government services. The client tier differentiates in two concrete nodes:
  - o The *electronic node*, which enables the civil servants to access the pending Residence Certificates via the use of browsers in order to review, approve and sign them.

- The *mobile node*, which consist of a stand alone mobile application that should be downloaded and installed by the mobile users on their mobile devices in order to access the mRCertificate service.

Each one of these tiers contains independent components which communicate with each other through clearly defined operation channels.

4 Mobile Residence Certificate Processes

This Section describes the activities performed by a user (citizen) who communicates with a municipality that hosts the SWEB platform using a mobile device in order to request a Residence Certificate document for a person having its residence in the region being under control of the specific municipality.

The mRCertificate processes are divided into four phases, namely *registration/installation*, m-*Residence Certificate Request submission*, *Request processing/issuance of Residence Certificate* and *Retrieval of Residence Certificate*, comprising the following processes:

Fig. 3. Registration/Installation Phase actions

registration/installation
The steps (Figure 3) that take place in this phase include the following:

a. the mobile user's communication with the TTP for the acquisition of the appropriate security credentials. The required credentials are a private key and the corresponding X.509 certificate which are stored locally on the mobile device.
b. The user's communication with the SWEB platform that operates in his/her "home-municipality" to be registered as a valid user.
c. The access to the municipality site in order retrieve and install the mobile application on his/her mobile device.

This is a preparatory phase which contains actions that should be performed before the initiation of the actual mRCertificate service.

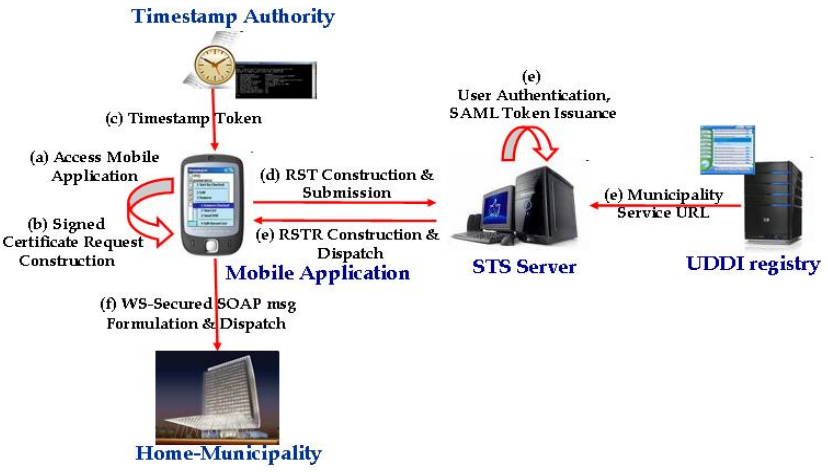

Fig. 4. Residence Certificate Request submission Phase actions

Residence Certificate Request submission

In this phase the mobile user creates a request for a Residence Certificate and submits it to the "home-municipality". The basic actions (Figure 4) that are included in this phase are the following:

- ✓ The User initiates the Mobile Application (MA) and accesses the RCertificate form. The mobile User Interface enables the user to create a RCertificate request supplying the necessary data. This data input is automatically checked for prevention of errors.
- ✓ The MA, following a completely transparent process gathers the form data and formulates the RCertificate request. The signature of the request is formulated based on the cryptographic primitives in the mobile phone, the user's certificate and the RCertificate request data.
- ✓ A timestamp token that corresponds to the signed request is requested from the Time Stamping Authority and the obtained timestamp data is embedded on the generated signature.
- ✓ The MA communicates with the STS server submitting a Request Security Token (RST) [21]. The RST consists of the name of "home-municipality", the requested service (residence certificate) and the user authentication credential (X.509v3 certificate).
- ✓ The STS server, initially, authenticates the user based on the included RST credential and issues an authorization token (SAML token [22]). This token is a short lived credential which contains the role that is assigned to the user by the corresponding "home-municipality". Afterwards, the STS server communicates with the UDDI Registry in order to obtain the URL of the municipality service which, along with the issued SAML token, is packaged in a RST response (RSTR) that is returned to the MA.
- ✓ The MA receives the RSTR and extracts the included information (SAML token and municipality service url). Automatically, a SOAP message is formulated that contains the signed RCertificate request and the SAML token and

the appropriate WS Security extensions are applied to it, so that it becomes encrypted with the municipality's public key, and digitally signed with the user private key. Finally the protected SOAP message is dispatched to the "home-municipality".

Request processing/issuance of Residence Certificate

The reception of the RCertificate request, at the "home-municipality", is a fully automated process that requires no human intervention. The SOAP message containing the request is received and decrypted with the municipality's private key and the validity of its WS Security extensions digital signature is verified, so that the point of origin is validated.

Then the embedded SAML token is extracted and the mobile user's authentication and authorization processes are initiated. According to these processes the signature of the SAML token is validated and the included role is retrieved. Based on this role, the SWEB platform is able to grand or deny access to the requested mRCertificate service. When, these processes have been completed, the platform constructs and sends a reply WS-Secured SOAP message to the Mobile Application with the result of the authentication and the authorization. The Mobile Application receives the SOAP message, decrypts and verifies the applied WS-Security mechanisms and informs the Mobile User.

If the authentication and/or the authorization processes fail the access to the service can not be accomplished and the whole workflow is terminated. Otherwise, the SWEB platform proceeds to the included mRCertificate request processing. The request itself is extracted from the SOAP message and the verification of the applied signature and the validation of the embedded timestamp are performed. Then, the request is sent to the municipality's Legacy System which processes it according to its internal procedures.

The Legacy System takes the decision to approve the received request and issues the corresponding Residence Certificate document. A unique identifier, a "Residence Certificate id", is assigned to the document which finally is stored in the SWEB platform in a list of pending for approval documents.

A Civil Servant of the "home-municipality", who is authorized to access the Residence Certificate pending list, proceeds with the approval process. Initially, the civil servant using a municipal electronic application is authenticated towards the SWEB platform in order to be able to retrieve the pending mRCertficate documents. As soon as, he/she accesses the list, he/she selects each document and verifies, edits (if required) and signs it.

The approved signed mRCertificate document is stored locally in the platform in an approved document list along with the unique identifier. Automatically, an SMS message is created and sent by the platform to the mobile user in order to inform him/her that the submitted request has been handled successfully and the issued mRCertificate document with a specific "Residence Certificate id" is ready for retrieval.

The above functional description illustrates that the most active actors are the complementary primitive services that compose the SWEB platform and handle all the underlying complexity of the request processing, enabling the service' semi-automation. Complete automation cannot be achieved due to the restrictions posed by the service itself that requires the issued mRCertificate document to be monitored by the civil servants responsible for the validity of their content.

Retrieval of Residence Certificate
In this phase the Mobile User receives the SMS notification which informs him/her that the processing of the request has been finished and the resulting document is ready for retrieval. Additionally, the SMS message contains the "Residence Certificate id" which is the unique identifier with which the user is able to request his/her document.

The actual process that the user has to perform in order to retrieve the mRCertificate is similar with the process of the Residence Certificate Request submission phase. The user has to access the RCertificate form and insert the received "Residence Certificate id". The Mobile Application constructs the corresponding request and signs it using the user's credential. Then, the user is authenticated towards the STS server retrieving the required authorization token (SAML Assertion) that is embedded in a SOAP message along with the formulated request.

The Mobile Application sends the SOAP message to the SWEB platform which performs the required authentication and authorization processes and returns to the user the requested Residence Certificate document. Once the final document has been dispatched, the platform removes it from the approved document list. Thus, there is not any critical information stored over time locally in the platform.

5 Conclusions and Future Work

The implementation and deployment of advanced m-government services is one of the priorities of the EU member states. It is expected that over the next years there will be a significant push to the deployment of these services having in mind the penetration rate and the performance improvements of the mobile devices.

Identifying this assumption, we have presented an innovative m-government platform that provides an advanced mRCertificate service. The main benefits of this service are that it achieves to simplify a multi-complex process improving the quality of life of its users (citizens), and enabling secure environment for dealing with public authorities from any place and at any time. Additionally, the proposed service can be used by the municipalities as a well-defined example for the design, development and implementation of new advanced composition services that will significantly increase the efficiency of their operations.

Our future research plan is to further investigate all the privacy issues that concern a m-government service taking into account several aspects such as anonymity, pseudonymity and adopting the required mechanisms that are able to address them.

Acknowledgments

This work has been supported by the GSRT (PENED) programme and the IST project SWEB (IST-2006-2.6.5). The authors would like to thank all the participants for valuable discussions and the European Union for funding the SWEB project.

References

1. European Telecommunications Standards Institute, `http://www.etsi.org/`
2. DG Information Society & Media, `http://ec.europa.eu/dgs/information_society/index_en.htm`

3. UK government's eGovernment Interoperability Framework (eGif), http://www.govtalk.gov.uk/interoperability/egif.asp
4. German Federal Ministry of Interior, SAGA - Standards and Architectures for e-government Applications, version 2.0 (2003)
5. Electronic interchange of data between administrations: IDA programme, http://europa.eu/scadplus/leg/en/lvb/l24147a.htm
6. Standardisation Action Plan in support of eEurope, http://ec.europa.eu/information_society/programmes/others/index_en.htm#Standard
7. Papastergiou, S., Polemi, D.: A testing process for Interoperability and Conformance of secure Web Services. Radio Communications, published by IN-TECH (to appear) ISBN 978-953-7619-X-X
8. Intelligent Cities (IntelCities), http://www.intelcitiesproject.com/wcm-site/jsps/index.jsp?type=page&cid=5026&cidName=HOME&isAnonymous=true
9. Impact of e-Government on Territorial Government Services (TERREGOV), http://www.terregov.eupm.net/my_spip/index.php
10. Usability-driven open platform for Mobile Government (USE-ME.GOV), http://www.usemegov.org/
11. E.C 6th Framework Programme, Electronic and secure municipal administration for European citizens – eMayor, IST-2004-507217, 2004 (2007), http://www.emayor.org
12. Karantjias, T., Papastergiou, S., Polemi, D.: Design Principles of Secure Federated e/m - Government Framework. International Journal of Electronic Governance/Special Issue on Users and uses of electronic governance (to appear)
13. Pentafronimos, G., Papastergiou, S., Polemi, N.: Interoperability Testing for e-Government Web Services. In: 2nd International Conference on Theory and Practice of Electtronic Governance (ICEGOV 2008), Cairo, Egypt, December 1-4 (2008)
14. Meneklis, V., Papastergiou, S., Douligeris, C., Polemi, D.: Towards advanced e/m-Government platforms. In: International Conference on Information Society (i-Society 2007), Merrillville, Indiana, USA, October 7-11 (2007)
15. Meneklis, V., Douligeris, C.: Extending a Distributed System Architecture with e-Government Modeling Concepts. In: Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), Workshop on Secure e/m Government Enhancing Cooperation with non-EU Regions, Athens, Greece, September 3-7 (2007)
16. Meneklis, V., Douligeris, C.: Enhancing the design of e-Government: Identifying structures and modelling concepts in contemporary platforms. In: 1st International Conference on Theory and Practice of Electronic Governance (ICEGOV 2007), Macao, China, December 10-13 (2007)
17. XML Encryption, http://www.w3.org/Encryption/2001/
18. XML Signature Recommendation – XML-DSIG, http://www.w3.org/TR/xmldsig-core/
19. Adams, C., Cain, P., Pinkas, D., Integris, R.: IETF RFC 3161 Time-Stamp Protocol (TSP), http://www.ietf.org/rfc/rfc3161.txt
20. Hartman, B., et al.: Mastering Web Services Security. Wiley Publishing, Chichester
21. OASIS Web Service Secure Exchange Technical Committee, OASIS WS-Trust 1.3, OASIS Standard (2007)
22. Cahill, C.P., et al.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf