On Possible Secure Cross-Border M-Government Model

Prof. Dr Milan Marković  
Banca Intesa ad Beograd  
milan.markovic@bancaintesabeograd.com  

Goran Đorđević  
Institute for Manufacturing banknotes and coins NBS,  
djg_goran@mail.com

MeTTTeG 2011, June 30 – July 1, 2011, Camerino, Italy
M-Government – Outline

- Introduction
- Security in Mobile Communication
- Possible M-Government architecture
- Possible m-Residence certificate service scenario
- JAVA Mobile Client Application
- Cross-border m-Residence certificate service scenario
- Conclusion
Introduction

- In this presentation, we describe a possible model for secure cross-border M-Government system based on secure JAVA mobile application and a SOA-Based M-Government platform.
- The model additionally consists of external entities, such as: PKI, XKMS, STS, UDDI and Time Stamping servers.
Introduction

- One example of possible mobile government online services is particularly emphasized: sending m-residence certificate request and obtaining the m-residence electronic document (m-residence certificate) as a governmental organization’s (e.g. municipality) response in the cross-border case.

- In this paper, the cross-border means either scenarios between two municipalities in the same country or between governmental organizations in different countries.
Security in Mobile Communication

- User authentication
- User identity
- Federation Identity
- User authorization to the proposed platform
- Authenticity, Integrity and Non-repudiation of transactions
- Confidentiality
- Electronic signature verification on the user’s side
- Long-term validity of transactions
Possible M-Government architecture

- STS Server
- PKI
- TSA
- UDDI
- e/m Government Platform
- Citizen / Company

SWEB e/m Government Framework
Local m-Residence Certificate Scenario

1: Citizen sends request() to SWEB Platform.
2: SWEB Platform sends notification() to Citizen.
3: SWEB Platform sends request() to Legacy System.
4: Legacy System approves request() and sends mRCertificate() to Civil Servant.
5: Legacy System sends request() to Civil Servant.
6: Legacy System creates mRCertificate().
7: Legacy System sends mRCertificate() to Civil Servant.
8: Civil Servant approves mRCertificate().
9: Civil Servant sends mRCertificate() to SWEB Platform.
10: SWEB Platform sends notification() to Citizen.
11: Citizen retrieves mRCertificate().
12: Citizen sends mRCertificate() to SWEB Platform.
Secure JAVA Mobile Application Architecture
Secure JAVA Mobile Application

- JAVA Mobile application comprises of following functionalities:
  - Graphical User Interface (GUI) for presenting business functionalities to the end user
  - Business (core) functionalities of the application – m-government functionality, e.g. m-residence certificate
  - Security functionalities
  - Communication
Secure JAVA Mobile Application

- The Security object of the considered JAVA mobile application is responsible for overall application-level security functionalities
- It consists of the following modules:
  - Authentication module to the JAVA application
  - XKMS module
  - SAML module
  - XML security module
  - WS-Security module
  - Time-Stamping module
Secure JAVA Mobile Application

- The solution is based on PKI digital certificates for endusers/citizens, digital signature and encryption and is also based on cross-certified PKI systems of platform (SWEB)-enabled municipalities in different countries.
Secure JAVA Mobile Application

- This JAVA application works with a corresponding SOAP-based Web Service Module on the M-Government side which is a part of the SWEB JAVA platform that needs to be installed in the SWEB-enabled municipality.

- The Secure JAVA application, as well as the SWEB platform itself, supports a cross-border M-document requests which means that a citizen in one municipality in one country could securely requests M-document from the original municipality in another country.
Security aspects

- Security aspects in communication between the client and M-Government platform:
  - XML signature
  - Time Stamping
  - SAML token
  - WS-Security (WS-Encryption and/or WS-Signature)
Security aspects

- User authentication and authorization
  - Username/password to access the client application and asymmetric private key
  - User’s digital certificate to be authenticated by the STS server
  - SAML token issued to the user for authentication to the particular service
  - User profile (digital certificate) for user authorization to the platform
Security aspects

- Secure communication between two SWEB enabled M-Government platforms
  - Digital certificate for platform’s authentication to the STS server
  - SAML token for platform’s authentication to the service
  - User’s profile (digital certificate) for platform’s authorization
Security aspects

- Identities of users
  - Digital certificates
  - PKI hierarchy
  - XKMS for certificate locating (LocateRequest) and validating (ValidateRequest)
SWEB Architecture Overview
SWEB Architecture Overview

**IntegrationTier** provides interface to the Legacy System

**Mobile Client Tier** holds components necessary for the user to access the system from mobile devices.

**EnterpriseTier II** orchestrates components in business services.

**External Services:**
- Secure Token Services (STS) server for issuing SAML (Security Assertion Markup Language) tokens
- TimeStamping server (TSA) for time stamping official documents
- PKI services for certificate issue and validation
- UDDI repository to store URLs of SWEB components

**InteractionTier** provides the interface to the other tiers and holds components providing communication with the platform and implementing security features.
The Residence Certification Service Cross-Border request scenario
The Residence Certification Service Cross-Border request scenario
Main contributions

- Proposal of a possible secure cross-border m-government model based on JAVA mobile/desktop application and SOA-based m-government platform.
- Usage of secure JAVA mobile application in which all modern security techniques are implemented (XML-security, WS-Security, SAML, Time Stamping, PKI, XKMS) which are used in optimum way in order to cope with majority of security issues of the mobile Web Service communication.
- Usage of SOA-based request-response m-government platform (Web Services) which is far more suitable in the mobile communication systems instead of session-based Web application platform.
- Usage of XKMS service which is more suitable for mobile PKI system since it outsources complex operations such as PKI validation services to the external entity – the XKMS server, compared to usages of other techniques [4].
Future research directions

- Full implementation of JAVA mobile application into the JAVA CDC 1.1 enabled mobile devices
- Development of similar application for other mobile platforms (iPhone, BlackBerry, Android, Windows Mobile)
- Full implementation of advanced electronic signature formats (e.g. XAdES, PAdES)
- Integration of PKI SIM technology in the Mobile Client application
- Using SWEB-like system for other PKI based e/m-governmental services (strong user authentication to other e-gov web portals, signing documents prepared through some other communication channels, qualified signatures, etc.)
Thank you for your attention

Thank You