Universitatea Tehnică a Moldovei

DEZVOLTAREA INFRASTRUCTURII ȘI SETULUI DE WEB-SERVICII PENTRU PRESTATORUL SERVICIULUI DE SEMNĂTURĂ MOBILĂ

Student:
Anastasia Haritonov

Conducător:
conf.univ.dr. Pușneac Iurie

Chișinău - 2019

Ministerul Educației, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Programul de masterat „Securitatea informației în sisteme și rețele de comunicații"

Admis la susţinere

Şef departament: dr. P. Nicolaev

„ _ " _____ 2020

DEZVOLTAREA INFRASTRUCTURII ȘI SETULUI DE WEB-SERVICII PENTRU PRESTATORUL SERVICIULUI DE SEMNĂTURĂ MOBILĂ

Teză de master

Masterand: _____ **(Anastasia Haritonov)**

Conducător: _____ **(Pușneac Iurie)**

Consultant: _____ **(Tatiana Șestacova)**

Chișinău – 2019

REZUMAT

În proiectul de master a fost dezvoltată infrastructura prestatorul serviciului de semnătură mobila creat din programe ce generează servicii web, interfață client pentru accesarea serviciului și baza de date pentru stocarea temporara a semnăturii mobile.

A fost reprezentate rezultatul analizei teoretice pentru conceptul de securitatea cibernetica prin intermediul infrastructurii cu cheie publica - PKI, serviciului de semnătură digitală în special pentru semnătura mobilă. A fost prezentata structura, funcționalitatea, acestora cit și structura și tipurile serviciilor web care sunt la baza serviciului de semnătură mobila.

Au fost definite funcțiile de baza realizate a prestatorului serviciului de semnătura mobilă cit și scenariile posibile de utilizare.

A fost realizat setul de metode ce generează serviciile web, proiectă și elaborată baza de date MS SQL la fel și interfață web pentru demonstrarea funcționării serviciilor pentru aplicarea semnăturii mobile.

În urma realizării programului de generarea serviciului de semnătură mobilă și a interfeței client a fost prezentat și explicat procesul de funcționare utilizând un exemplu de cerere cu introducerea manuală a parametrilor de intrare și obținerea semnăturii în formatul xml.

A fost demonstrat ca soluția realizată a rezolvat probleme ca utilizarea neeficiente a timpului, utilizarea neeficienta a resurselor materiale predestinate pentru semnarea unor contracte, a necesității de securitate în lucrul cu documente.

Teza de master conține 42 file, 20 figuri, 7 tabele, 12 surse bibliografice și 18 anexe. Anexele contau din 31 file și conțin suplimentar 8 figuri și 4 tabele.

SUMMARY

In the master project, was created the infrastructure of the mobile signature service provider, the component parts for AP are programs that generate web services, the client interface for accessing the service and the database for the temporary storage of the mobile signature.

Was represented the result of the theoretical analysis for the concept of cyber security through the public key infrastructure - PKI, of digital signature service, especially concept of mobile signature. As well was represented the structure, functionality of all those concepts and the structure and types of web services for mobile signing process.

Was defined the basic functions of mobile signature service provider and implementation use-cases.

Was developed the set of web services, was designed the MS SQL database and the web interface for functionality demonstration on applying the mobile signature.

Was represented and explained functionality process of mobile signature provider using an example of request and response with the manual input of parameters.

It was shown that the solution solved problems such as the inefficient use of time, the inefficient use of material resources predestined for signing contracts, the need for security when working with documents.

The master project contains 42 pages, 20 figures, 7 tables, 12 bibliographic sources and 18 annexes. The annexes counted: 31 files and additionally contained 8 figures and 4 tables.

CUPRINS

INTRODUCERE **9**

1 ANALIZA CONCEPTULUI DE SECURITATE CIBERNETICĂ **10**

1.1 Analiza sistemului de securitate cibernetică bazat pe criptografia asimetrică 10

1.2 Familiaritatea cu noțiunea de semnătură digitală și tipurile ei 11

1.3 Studierea serviciului de semnătură mobilă 12

1.3.1 Structura 13

1.3.2 Structura web serviciilor, tipurile 15

1.4 Concluzie 19

2 DEZVOLTAREA PRESATORULUI DE SERVICIU PENTRU SEMNĂTURĂ MOBILĂ **20**

2.1 Structura prestatorului de servicii 20

2.2 Pășii de realizare 20

2.3 Dezvolatrea setului de web-servicii 21

2.3.1 Definirea funcțiilor necesare pentru servicii web 21

2.3.2 Realizarea serviciilor 22

2.4 Dezvoltarea interfeței pentru AP 28

2.4.1 Definirea modelelor de utilizare (use-cases) și a sarcinilor 29

2.4.2 Dezvoltarea arhitecturii 30

2.5 Crearea, instalarea bazei de date MS SQL 32

2.5.1 Configurarea bazei de date; 33

2.5.2 Realizarea conexiunii intre serviciul web și baza de date 34

2.6 Concluzie 34

3 DESCRIEREA PRESTATORULUI DE SERVICIU **35**

3.1 Descrierea serviciilor web 35

3.2 Descrierea interfeței de test 37

3.3 Concluzie 39

CONCLUZIE **40**

BIBLIOGRAFIE **42**

ANEXE **43**

INTRODUCERE

Omul contemporan în spațiul digital necesita utilizarea instrumentelor eficiente pentru sporirea calității și securității vieții. Sub noțiunea de "instrumente eficiente" se subînțelege utilizarea adecvata a resurselor, planificarea eficienta a timpului și colaborarea profitabila utilizând mecanisme de securitate înalta. Aceste concepte au putut a fi obținute prin introducerea a serviciilor web, dar asigurarea securității în spațiul cibernetic a fost atinsa introducând noțiunea de semnătura digitala.

În prezent, practic, toți oamenii dețin un dispozitiv care conține o cartelă inteligentă și care poate fi citita prin intermediul unui instrument de uz personal - telefon mobil. Telefonul mobil reprezintă alegerea naturală pentru implementarea unei soluții de autentificare sau semnare electronică.

Semnăturile electronice create prin intermediul telefonului mobil au devenit cunoscute sub numele de "semnătura mobila". În prezent, soluția dată este rar întâlnită în Republica Moldova, ceasta se datorează mai multor probleme cum ar fi standardizarea elementelor care sunt implicate în procesul de semnare, realizarea interconexiunii intre platforma de aplicare a semnăturii și a interfeței client utilizate.

Utilizarea serviciului de semnătură mobila oferă disponibilitatea posesiei semnăturii digitale nu doar pentru persoanele juridice dar și pentru persoanele fizice, accesibilitatea și simplitatea aplicării semnăturii indiferent de locul și timpul, fără mijloace suplimentare (prin utilizarea doar a telefonului mobil). În plus presatorul de serviciul va fi utilizat intern ca un instrument corporativ de semnare a documentelor cât pentru angajații atât și cu clienții companiei.

Scopul acestei lucrări este de a dezvolta infrastructura pentru sistemul corporativ a presatorul serviciului de semnătură mobila ce include: programa pentru generarea serviciilor web, interfață client și baza de date pentru stocarea temporara a semănaturilor mobile.

Realizarea scopului implică următoarele obiective:

1. Studierea standardelor cu privire la arhitectura și funcționalitatea semnăturii mobile, XaDes, SSL, SHA256, pentru servicii web SOAP, XML, WSDL;

2. Definirea sarcinilor, dezvoltarea logicii de implementare și funcționare a presatorului de serviciul de semnătură mobila;

3. Analiza cazurilor posibile de utilizare (use-case);

4. Dezvoltarea programului pentru generarea serviciilor web și realizarea sarcinilor de baza a prestatorului se semnătură mobila;

5. Proiectarea și implementarea a bazei de date MS SQL pentru stocarea temporara a semănaturilor;

6. Dezvoltarea interfeței client (aplicației web) pentru demonstrarea funcționalității setului de servicii web prin intermediul limbajelor: back-end: Pl-sql, C#;front-end: HTML, js, jQuery, CSS;

7. Testarea aplicației web de demonstrare;

BIBLIOGRAFIE

1. ETSI TS 102 204 V1.1.4 Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface (2003-08) - ;

2. ETSI TS 101 903 V1.1.1: "XML Advanced Electronic Signatures (XAdES)". Constituția RM, LEGE Nr. 264 din 15.07.2004 - privire la documentul electronic și semnătură digitala http://lex.justice.md/md/313061/.

3. Constituția RM , LEGE Nr.91 din 29.05.2014 - privind semnătură electronica și documentul electronic http://lex.justice.md/md/353612/.

4. RFC3161 Timestamping Protocol, https://www.ietf.org/rfc/rfc3161.txt.

5. IETF RFC 2630 - Cryptographic Message Syntax (CMS) - standard.

6. SOAP web services, https://www.itprotoday.com/web-application-management/calling-web-services-asynchronously.

7. ETSI TR 102 203 - Mobile Commerce (M-COMM); Mobile Signature; Business & Functional Requirements.

8. IETF RFC 3275: "(Extensible Markup Language) XML-Signature Syntax and Processing".

9. SOAP Version 1.2 Part 1: Messaging Framework", W3C Recommendation 24 June 2003, http://www.w3.org/TR/soap12-part1/ .

10. W3C Note 15 March 2001: "Web Services Description Language (WSDL) 1.1", http://www.w3.org/TR/wsdl .

11. W3C Recommendation 12 February 2002: "XML-Signature Core Syntax and Processing", http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.

12. RSA PKCS#7 Version 1.5: "Cryptographic Message Syntax Standard", RSA Laboratories.