

Ministerul Educației al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Inginerie și Management în Electronică și Telecomunicații
Catedra Sisteme și Rețele de Comunicații Optoelectronice

Admis la susținere
șef de catedră:
conf.univ.dr. Nistiriuc Pavel

”_” _____ 2016

**Proiectarea rețelei DDOS de comunicații
pentru prestarea serviciului identificării
electronice pe platforma națională
M-Medicine din cadrul e-Guvernare**

Teză de master

Student: _____ (Colun V.)
Conducător: _____ (Țurcanu T.)

Chișinău 2016

REZUMAT

Lucrarea dată are ca scop identificarea soluțiilor și implementarea acestora pentru proiectarea unei rețele naționale, ce ar permite utilizatorilor accesul sigur și autorizat atât la serviciile electronice guvernamentale, cât și cele nonguvernamentale.

Lucrarea este compusă din 3 capitole, în care este descris detaliat conceptul de rețea eID și modul de proiectare a unei astfel de rețele, în baza cercetărilor și analizelor tehnologiilor și rețelelor existente la nivel național, astfel ca impactul economic asupra guvernului și utilizatorului să fie minim.

La efectuarea lucrării, în primul capitol a fost descris conceptul de infrastructură a cheilor publice (PKI), componentele și modul de utilizare a acestei infrastructuri. Este arătată relația instituțiilor de stat cu cetățenii prin prisma conceptului de e-guvernare și serviciile electronice disponibile.

În al doilea capitol sunt descrise tehnologiile existente mobile, locale și la distanță pentru accesarea serviciilor electronice, precum și dezavantajele acestor tehnologii.

De asemenea, în acest capitol sunt descrise metodele de integrare a infrastructurii PKI și dezvoltarea unei noi infrastructuri, numită Wireless PKI, ce permite stocarea materialului criptografic atât de partea utilizatorului, cât și din partea unui server distant amplasat la o autoritate de certificare.

În capitolul trei este proiectată o rețea eID în baza analizelor și cercetărilor din capitolele precedente. Acest capitol conține o serie de structuri de rețele proiectate, modurile de integrare a diferitor noduri și platforme.

De asemenea este arătat modul de gestiune a nodurilor rețelei prin interfața grafică și linia de comandă. Au fost elaborate scheme ce arată cum funcționează rețeaua nouă proiectată. Tot în acest capitol, sunt arătate configurările și comenzile pentru integrarea și definirea unor noi entități în rețea.

La efectuarea lucrării date, pentru a asigura indicatorii de performanță a rețelei la un nivel înalt, s-a analizat și implementat tehnologii ce asigură securitate înaltă pe părțile vulnerabile rețelei la atacuri de securitate.

SUMMARY

The main purpose of this thesis is identification for new solutions and implementation of these solutions in order to design a new national network, that would allow, for users secure and authorized access to, both governmental and non-governmental electronic services.

This thesis is composed of three chapters, where is described the concept of eID network and the methods of design of such networks, based on researches and analysis of existing technologies and networks on national level, and ensure the economical impact on users and government minimal.

In first chapter was described the concept of public key infrastructure, its components and methods of using this infrastructure. It is shown the relationship between public institutions and citizens through the concept of e-government and available electronic services.

In the second chapter are described existing, local and remote mobile technologies for accessing electronic services and also are shown the main disadvantages of these technologies.

Also, in this chapter are described the main methods for integration of PKI infrastructure and developing a new one, called Wireless PKI, which allows storing of cryptographic material on the user side, as well as on a remote server located at a certification authority.

In third chapter, a new eID network is designed based on analysis and research from the previous chapters. This chapter contains a number of structures of designed networks and methods for integration of different nodes and platforms.

It is also shown the method of administration of network nodes through graphic user interface and command line. Were created schemes that shows how new designed network works. Also, here are described main configurations and commands for integration and definition new network entities.

In this work, to ensure a high level of networks performance indicators, was analyzed and implemented security technologies which maintain a high level of security.

C U P R I N S

INTRODUCERE.....	9
1.1 IDENTIFICAREA ELECTRONICĂ. TEHNOLOGIA E-ID ÎN SISTEMUL MEDICAL M-MEDICINE.....	10
1.1.1 Introducere în Legea cu privire la documentul electronic și semnătura digitală Nr.264-XV din 15.07.2004.....	10
1.1.2. Importanța Legii cu privire la documentul electronic și semnătura digitală Nr.264-XV din 15.07.2004 electronice.....	11
1.1.3. Articolele legii cu privire la documentul electronic și semnătura digitală nr.264-XV din 15.07.2004 electronică.....	11
1.1.4 Dispoziții generale.Obiectivele implementării.Istoricul implementării.....	12
1.1.4.1 Definiții pentru documentul electronic și semnătura digitală.....	12
1.1.4.2 Regimul juridic al documentului electronic.....	13
1.1.4.3 Circulația electronică a documentelor.....	15
1.1.4.4 Regimul juridic al semnăturii digitale.....	20
1.1.4.5 Certificarea cheilor publice.....	21
1.1.4.6 Controlul de stat.....	27
1.1.4.7 Răspunderea.....	28
1.1.4.8 Dispoziții finale.Analiza implementării legii.....	29
1.1.5 Articolele cu privire la circulația electronică și impactul acestora.....	29
1.1.5.1 Definirea problematicii.Cadrul factologic existent.....	29
1.1.5.2 Circumstanțele și justificarea proiectului.....	33
1.1.5.3 Opțiunile posibile.....	39
1.1.5.4 Costul serviciilor de certificare a cheilor publice pentru semnături electronice și evoluția acestuia în dependență de numărul certificatelor eliberate.....	41
1.1.5.5 Implementarea la nivelul 2 a semnăturii electronice.....	41
1.1.5.6 Strategia de consultanță.....	42
1.1.5.7 Recomandări.....	43
1.2 IDENTIFICAREA ELECTRONICĂ ÎN REPUBLICA MOLDOVA.....	44
1.2.1 Noțiunea de Guvernare electronică.....	44
1.2.2 Serviciile electronice în Republica Moldova.....	45
1.2.3 Identitatea electronic.....	46

1.2.3.1	Conceptul identicatorului electronic.....	46
1.2.3.2	Conceptul PKI.....	48
1.2.3.3	Autoritatea de certificare.....	48
1.2.3.4	Autoritatea de înregistrare, repertoriul și arhiva.....	50
1.2.3.5	Modulul PKI bazat pe cartela SIM.....	50
1.2.4	Semnătură digitală.Ce este ea?.....	52
1.2.4.1	Algoritmul semnăturii digitale (DSA).....	52
1.2.4.2	Algoritmul semnăturii digitale RSA (RSA).....	53
1.2.4.3	Algoritmul semnăturii electronice în curbă eliptică (ECDSA).....	53
1.2.4.4	Semnătura digitală.Cum funcționează?.....	54
1.2.4.5	Beneficiile utilizării semnăturii digitale.....	56
1.2.4.6	Riscurile care se asociază cu utilizarea semnăturii digitale.....	56
1.2.5	Cardul de indentificare electronic.....	57
1.2.5.1	Care tip de informație stochează cardul de indentificare electronic?.....	58
1.2.5.2	Avantajele cardului de indentificare electronic?.....	58
1.2.6	Avantajele identității electronice.....	58
1.2.7	Interacțiunea dintre biometrie și identitatea electronică.....	59
1.2.8	Cardurile de indentificare electronic e-ID sunt o amenințare pentru viața privată?...59	
1.2.9	Particularitățile sistemului identicatorului electronic.....	60
2.	ANALIZA METODELOR DE IMPLEMENTARE A TEHNOLOGIEI DE IDENTIFICARE ELECTRONICĂ.....	63
2.1.	Tehnologiile coexistente pentru autorizarea în lumea virtuală.....	63
2.2.	Tehnologii mobile, locale și la distanță.....	64
2.3.	Rețeaua Intranet Moldcell.....	66
2.4.	Interconectarea existentă VPN dintre Moldcell și „CNAM”.....	67
2.5.	Securitatea tranzacției.....	69
2.6.	Identificarea prin intermediul telefonului mobil.....	71
2.6.1.	Identificarea mobilă din partea clientului.....	71
2.6.1.1.	Procesul înregistrării utilizatorului.....	72
2.6.1.2.	Procesul de autentificare.....	73

2.6.1.3. Procesul de semnare.....	73
2.6.2. Identificarea electronică mobilă prin intermediul serverului.....	74
2.6.2.1. Procesul de înregistrare a utilizatorului.....	75
2.6.2.2. Procesul de autentificare cu tehnologia HSM.....	75
2.6.2.3. Procesul de semnare digitală a documentelor electronice.....	76
2.7. Cerințele pentru semnăturile digitale/ electronice.....	77
3. PROIECTAREA INFRASTRUCTURII DE TELECOMUNICAȚII A SISTEMULUI DE IDENTIFICARE ELECTRONIC.....	79
3.1. Identificatorul electronic în Republica Moldova.....	79
3.2. Optimizarea capacității rețelei mobile.....	79
3.2.1. Realizarea procedurii de CP swap la registrul abonaților locali	81
3.2.2. Integrarea semnalizării HSL între MGW1-HLR.....	83
3.3. Integrarea centrului de mesaje în rețeaua Core.....	84
3.4. Unificarea Platformei MSSP.....	87
3.5. Stabilirea cartelelor USIM securizate.....	91
3.6. Introducerea tehnologiei VPN între Platforma MSSP și Autoritatea de Certificare..	96
3.7. Structura detaliată a rețelei identificatorului electronic e-ID proiectate.....	100
CONCLUZII.....	103
BIBLIOGRAFIE.....	105