Universitatea Tehnică a Moldovei

DEZVOLTAREA INFRASTRUCTURII PENTRU ASIGURAREA ȘI MENTENANȚA PROTECȚIEI CRIPTOGRAFICE A DATELOR PERSONALE A PAȘAPORTULUI BIOMETRIC

РАЗРАБОТКА ИНФРАСТРУКТУРЫ ДЛЯ ОБЕСПЕЧЕНИЯ И ПОДДЕРЖКИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ БИОМЕТРИЧЕСКОГО ПАСПОРТА

Student: Kutukova Diana

Conducător: conf. univ., dr. Pușneac Iurie

Chișinău – 2019

Ministerul Educaţiei Culturii şi Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Programul de masterat "Securitatea Informațională de Sisteme și Rețele de Comunicații"

Admis la susţinere

Şef departament: dr. Nicolaev P.

„__"_____ 2020

DEZVOLTAREA INFRASTRUCTURII PENTRU ASIGURAREA ȘI MENTENANȚA PROTECȚIEI CRIPTOGRAFICE A DATELOR PERSONALE A PAȘAPORTULUI BIOMETRIC

РАЗРАБОТКА ИНФРАСТРУКТУРЫ ДЛЯ ОБЕСПЕЧЕНИЯ И ПОДДЕРЖКИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ БИОМЕТРИЧЕСКОГО ПАСПОРТА

Teză de master

Masterand: _____ **(Kutukova Diana)**

Conducător: _____ **(Pușneac Iurie)**

Chişinău – 2019

REZUMAT

Teza de master este dedicată dezvoltării infrastructurii pentru asigurarea și mentenanța protecției criptografice a datelor personale al pașaportului biometric.

A fost efectuată analiza standardelor și cerințelor internaționale pentru protecția criptografică și verificarea datelor personale stocate în cipul pașaportului.

A fost elaborată o infrastructură generală care oferă posibilitatea de a lucra cu pașapoarte biometrice naționale și străine. A fost determinată compoziția acestei structuri, funcțiile de bază, relațiile interne și externe.

Au fost dezvoltate instrumentele criptografice pentru autentificarea și protecția confidențialității datelor „sensibile" din cipul pașaportului folosind biblioteca OpenSSL.

Au fost analizate posibilitățile funcționale a platformei software EJBCA, care permite crearea și mentenanța activității autorităților de certificare.

Au fost analizate actualitatea și posibilitatea utilizării infrastructurii dezvoltate în țările care doar încep să introducă pașapoartele biometrice și în domenii unde cardurile cu cip sunt folosite pentru stocarea informației critice.

SUMMARY

The diploma is dedicated to the development of the infrastructure for ensuring and maintaining the cryptographic protection of the biometric passport personal data.

The analysis of international standards and requirements for cryptographic protection and verification of personal data stored in the passport chip has been carried out.

A common infrastructure that provides the opportunity to work with national and foreign biometric passports has been developed. It's composition, basic functions, internal and external relations has been determined.

Cryptographic tools for authentication validation and privacy protection of passport chip sensitive data using the OpenSSL library have been developed.

The functionality of the EJBCA software platform, which allows to create and maintain the work of certification authorities, has been analyzed.

The relevance and the possibility of using the developed infrastructure in countries that are just starting to introduce biometric passports, and in other domains where cards with chips are used to store critical information, have been analyzed.

Р Е З Ю М Е

Данная работа посвящена разработке инфраструктуры для обеспечения и поддержки криптографической защиты персональных данных биометрического паспорта.

Проведен анализ международных стандартов и требований к криптографической защите и проверке персональных данных, хранящихся в чипе паспорта.

Разработана общая инфраструктура, обеспечивающая возможность работы с национальными и зарубежными биометрическими паспортами. Определен ее состав, основные функции, внутренние и внешние связи.

Разработаны криптографические средства проверки достоверности и защиты конфиденциальности «чувствительных» данных чипа паспорта с помощью библиотеки OpenSSL.

Проанализированы функциональные возможности программной платформы EJBCA, позволяющей создавать и поддерживать работу центров сертификации.

Проанализирована актуальность и возможность применения разработанной инфраструктуры в странах, которые только приступают к внедрению биометрических паспортов, и в смежных областях, где для хранения критически важной информации используются карточки с чипами.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современный мир становится все более мобильным. Количество людей, пересекающих государственные границы, постоянно увеличивается. В связи с этим возрастают требования к методам и средствам пограничного контроля. Проблема обеспечения быстрой и надежной проверки паспортов становится все более актуальной.

Самое эффективное решение этой проблемы на данный момент – использование биометрического паспорта с чипом. Паспорт (чип) содержит информацию, необходимую и достаточную для надежной идентификации его владельца, а также позволяет автоматически считывать и проверять данные, что ускоряет процесс пограничной проверки.

Однако для обслуживания биометрического паспорта нужна специальная инфраструктура, которая обеспечивала бы его эффективную поддержку на протяжении всех этапов жизненного цикла. Каждая страна должна создать у себя подобную инфраструктуру, руководствуясь общими международными правилами (стандартами).

Инфраструктура, во-первых, должна обеспечить тщательную проверку достоверности данных о владельце паспорта, а во-вторых, исключить какую-либо возможность несанкционированного чтения содержащихся в паспорте “чувствительных” персональных данных о владельце, таких, например, как отпечатки пальцев. Кроме того, для поддержания системы защиты паспорта и контроля доступа к данным инфраструктуру следует своевременно обновлять. Таким образом, обе эти задачи могут быть успешно решены с помощью методов и средств современной криптографии, технологии PKI и защищенных коммуникаций.

Целью работы является разработка инфраструктуры для обеспечения и поддержки криптографической защиты персональных данных, содержащихся в биометрическом паспорте.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Проанализировать международный опыт в области защиты и проверки персональных данных, хранящихся в чипе биометрического паспорта;
2. Проанализировать международные стандарты и требования к криптографической защите данных, хранящихся в чипе;
3. Для вымышленной страны Utopia определить состав и разработать общую инфраструктуру, обеспечивающую возможность работы с национальными и зарубежными биометрическими паспортами;

4. Проанализировать функциональные возможности современного программного обеспечения и выбрать оптимальный инструмент для практической реализации элементов криптографической защиты данных;
5. Разработать криптографические средства, обеспечивающие достоверность данных, хранящихся в чипе биометрического паспорта. Создать соответствующие центры сертификации, ключи и сертификаты;
6. Разработать криптографические средства, обеспечивающие защиту хранящихся в чипе “чувствительных” персональных данных от несанкционированного доступа. Создать соответствующие центры сертификации, ключи и сертификаты;
7. Выполнить сквозной пример, демонстрирующий все процедуры, связанные с созданием реальных криптографических средств защиты биометрического паспорта.

БИБЛИОГРАФИЯ

1. https://ru.wikipedia.org/wiki/Биометрический_паспорт ***- Понятие биометрического паспорта***

2. ICAO Document 9303: Машиносчитываемые проездные документы. Часть 10. Логическая структура данных (LDS) для хранения биометрических и других данных на бесконтактной интегральной схеме (ИС) Издание седьмое, 2015 ***- Логическая структура данных***

3. https://ru.wikipedia.org/wiki/SHA-2 ***- Функция хеширования SHA 256***

4. https://ru.wikipedia.org/wiki/RSA - ***Алгоритм RSA***

5. https://en.wikipedia.org/wiki/Hardware_security_module ***-Назначение HSM***

6. https://en.wikipedia.org/wiki/Electronic_signature#Digital_signature ***- Digital signature***

7. *Горбатов В. С , Полянская О. Ю.*Г67 Основы технологии PKI. - М.:Горячая линия-Телеком, 2004. -248 с - ***Введение; Сертификаты открытых ключей X.509***

8. ICAO Document 9303: Машиносчитываемые проездные документы. Часть 12. Инфраструктура открытых ключей для МСПД Издание седьмое, 2015 ***- Роли и обязанности CSCA и DS в инфраструктуре открытых ключей***

9. HoonJae Lee Trend of ePassport in Korea ***- Протокол аутентификации***

10. Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1 Version 2.10, 20. March 2012 – ***Механизм EAC***

11. Common Certificate Policy for the Extended Access Control Infrastructure for Travel and Residence Document Isissued by EU Member States, BSI TR-03139 Version 2.2, 31. July 2018 ***- Понятие и функции CVCA, DVCA, IS в инфраструктуре EAC***

12. https://doc.primekey.com/ejbca/ejbca-introduction ***- Функциональные возможности EJBCA***

13. https://ru.wikipedia.org/wiki/OpenSSL - ***Функциональные возможности OpenSSL***

14. *Ivan Ristić* OpenSSL Cookbook. A guide to the most frequently used OpenSSL features and commands 2013, -55 с. ***- Описание команд библиотеки OpenSSL***

15. https://www.openssl.org/docs/man1.1.1/man1/ ***- Команды библиотеки OpenSSL***