

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра методов оптимального управления

Аннотация к дипломной работе

**РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, РЕАЛИЗУЮЩЕГО
КРИПТОГРАФИЧЕСКИЙ ИНТЕРФЕЙС ДОСТУПА К ГРУППАМ
ДАННЫХ, РАЗМЕЩЕННЫМ НА ИДЕНТИФИКАЦИОННОЙ КАРТЕ
ГРАЖДАНИНА РЕСПУБЛИКИ БЕЛАРУСЬ**

Гарбуз Егор Сергеевич

Научный руководитель – зам. нач. отдела – нач. сектора

НП РУП «НИИ ТЗИ» Шуманский Д.И.

Минск, 2020

РЕФЕРАТ

Дипломная работа, 54 с., 13 рис., 4 табл., 10 источников.

ИДЕНТИФИКАЦИОННАЯ КАРТА, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ID-КАРТА, ТЕРМИНАЛ, РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ГРУППЫ ДАННЫХ, РАЗРАБОТКА, АЛГОРИТМ, КРИПТОГРАФИЯ

Объектом исследования является идентификационная карта гражданина Республики Беларусь, способы взаимодействия с программным обеспечением, расположенным на ID-карте, программное обеспечение, требуемое для реализации чтения групп данных с идентификационной карты соответствующее государственным стандартам Республики Беларусь.

Цель работы – проанализировать варианты создания программного обеспечения, для взаимодействия с идентификационной картой, соответствующее международным стандартам, регламентирующих требования к ID-картам и способам взаимодействия с ними. Разработать программное обеспечение основываясь на государственных стандартах Республики Беларусь. Реализовать и встроить всю необходимую криптографическую поддержку, для безопасного и защищённого взаимодействия в ЕСИФЮЛ.

Для решения и исследования поставленной задачи используются следующие методы: фреймворк Qt Creator языка с++ для разработки программного обеспечения, библиотека базовых криптографических алгоритмов для криптографической поддержки, библиотека WinSCard для взаимодействия с идентификационной картой на ОС Windows, библиотека QtWebApp для реализации сервисной части.

Результатом работы является работающее многопоточное программное обеспечения, реализующее криптографический интерфейс доступа к группам данных, размещенным на идентификационной карте гражданина Республики Беларусь.

ABSTRACT

Thesis, 54 p., 13 Fig., 4 table., 10 sources.

ID CARD, SOFTWARE, ID CARD, TERMINAL, SOFTWARE DEVELOPMENT, DATA GROUPS, DEVELOPMENT, ALGORITHM, CRYPTOGRAPHY

The object of the research is the identification card of a citizen of the Republic of Belarus, methods of interaction with the software located on the ID card, software required for reading groups of data from the ID card that meets the state standards of the Republic of Belarus.

The purpose of this work is to analyze options for creating software for interacting with an ID card that meets international standards that regulate the requirements for ID cards and how to interact with them. Develop software based on the state standards of the Republic of Belarus. Implement and integrate all necessary cryptographic support for secure and secure interaction in the UISILE.

The following methods are used to solve and research this problem: the C++ Qt Creator framework for software development, the library of basic cryptographic algorithms for cryptographic support, the WinSCard library for interacting with an ID card on Windows, and the QtWebApp library for implementing the service part.

The result is a working multithreaded software that implements a cryptographic interface for accessing data groups placed on the identification card of a citizen of the Republic of Belarus.