УДК 004.056.5

РАЗРАБОТКА МУЛЬТИПЛАТФОРМЕННОГО СЕРВИСА ДЛЯ РАБОТЫ С ГОСТ-КРИПТОГРАФИЕЙ

Гранцев Г.А., Белоусова В.И.

ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина»,

Екатеринбург, Россия

Georgy.Grantsev@urfu.me

Аннотация. Рассмотрены подходы к реализации кроссплатформенного криптографического веб-сервиса для работы с открытыми ключами электронной подписи с применением в сценариях шифрования данных на открытый ключ получателя, проверки электронной подписи, а также усовершенствования электронной подписи от CAdES-BES до типа CAdES-T.

Ключевые слова: ЭЦП, электронная подпись, шифрование данных, ГОСТ-стандартизированная криптография, веб-сервис, криптопровайдер, CAdES, метка времени, TSP.

DEVELOPMENT OF A MULTIPLATFORM SERVICE FOR WORK WITH GOST CRYPTOGRAPHY

Grantsev G.A., Belousova V.I.

Ural Federal University, Ekaterinburg, Russia

Georgy.Grantsev@urfu.me

Annotation. Approaches to the implementation of a cross-platform cryptographic web service for working with public keys of an electronic signature using data encryption with the recipient's public key, verification of an electronic signature, as well as finalization of an electronic signature from CAdES-BES to the CAdES-T type are considered.

Keywords: EDS, electronic signature, data encryption, GOST standardized cryptography, web service, cryptographic service provider, CAdES, timestamp, TSP.

Введение

Криптографические алгоритмы в современном мире широко применяются для обеспечения неавторизованного доступа к информации при передаче или хранении (шифрование), целостности данных и проверки наличия в них изменений, для подтверждения авторства информации (ЭЦП). В Российской Федерации использование ЭЦП регламентируется законодательством: для ведения юридически-значимого документооборота необходима ЭЦП, соответствующая государственным стандартам (Федеральный закон № 63-ФЗ «Об электронной подписи» [1], Приказ ФСБ России от 27.12.2011 N 796 [2]), например, ГОСТ Р 34.10–2012 [3]. Так же, операторы персональных данных при обработке и их передачи используют технические меры для обеспечения безопасности персональных данных (Федеральный закон № 152-ФЗ «О персональных данных» [4]), например, сертифицированные СКЗИ, реализующие ГОСТ-стандартизированные алгоритмы, например, ГОСТ 28147–89 [5].

Практическая ценность разрабатываемого инфраструктурного веб-сервиса – использование стандартизированных криптографических алгоритмов на предприятии, что позволит другим сервисам/продуктам предприятия не поддерживать свою реализацию данного функционала.

Ключевая особенность разрабатываемого веб-сервиса – мультиплатформенность, то есть возможность развертывания на различных ОС (Windows, Linux). Данная возможность является особенно актуальной в современных реалиях, исходя из возможности регионального ограничения пользователей в использовании различного программного обеспечения.

Основная часть

Рассмотрены различные подходы к передаче двоичных данных (файлов произвольного формата) по протоколу HTTP, описана методика тестирования производительности, плюсы и минусы указанных методов, на основании которых было принято решение о выборе конкретного способа.

Изучен интерфейс CAPILite криптопровайдера КриптоПро CSP 5.0 [6], использование которого позволяет реализовывать различный криптографический функционал на уровне прикладного приложения или сервиса.

В ходе разработки был реализован кроссплатформенный веб-сервис, отвечающий требованиям, поставленным в работе. Стоит дополнительно отметить, что поддержка доставки логов веб-сервиса в Hercules [7] реализована благодаря использованию набора библиотек Vostok [7], имеющего данный функционал. Так же реализован механизм авторизации на основе утверждений при использовании внешнего (по отношению к разрабатываемому) сервиса API-ключей.

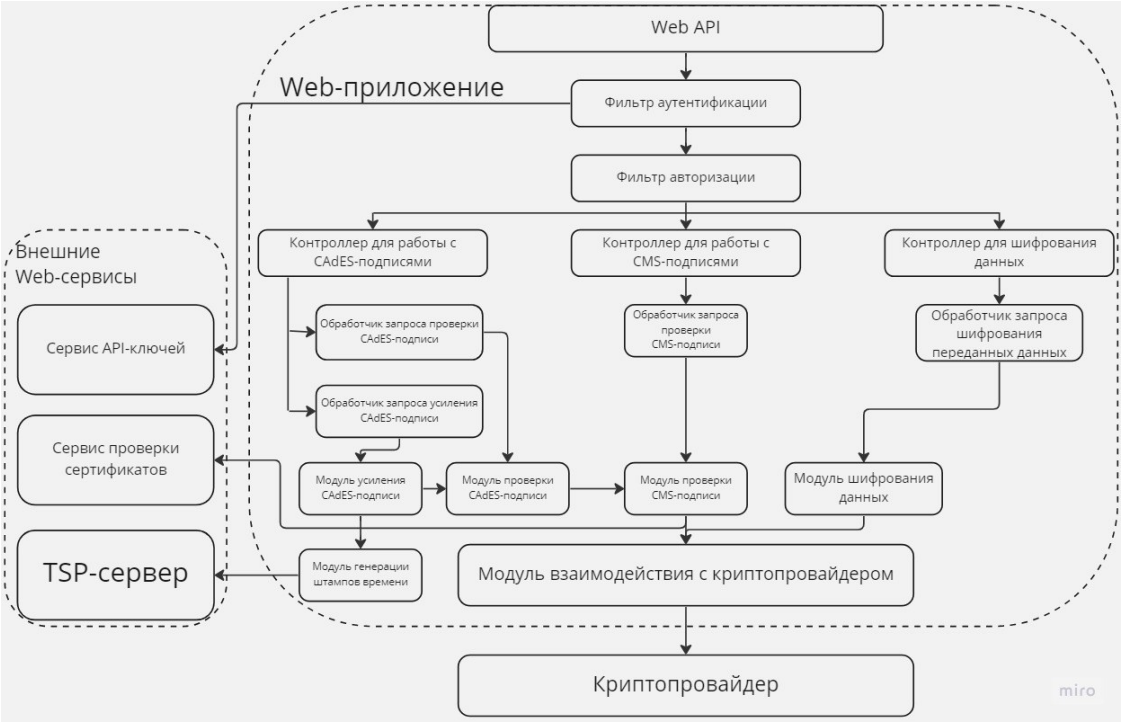

Рисунок 2 - Архитектура разработанного веб-сервиса

Заключение

В ходе работы была достигнута поставленная цель, а именно был спроектирован и разработан инфраструктурный веб-сервиса для работы с ГОСТ-стандартизированными криптографическими алгоритмами, работающего с открытыми ключами (для ассиметричной криптографии), имеющего возможность развертывания на различных ОС. В разработанном веб-сервисе реализован функционал поточной проверки электронной

подписи, поточного шифрования данных, проверки электронных подписей в формате CAdES-BES, CAdES-T, а также усовершенствование электронной подписи от формата CAdES-BES до формата CAdES-T. Разработанный веб-сервис имеет возможность интеграции с инфраструктурой предприятия.

Библиографический список

1. Об электронной подписи [Электронный ресурс]: Федеральный закон РФ от 06.04.2011 № 63-ФЗ // Официальный интернет-портал правовой информации. - 2022 г. - с изм. и допол. в ред. от 28.12.2022.

2. Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра [Электронный ресурс]: Приказ ФСБ России от 27.12.2011 № 796 // Доступ из справ. правовой системы «КонсультантПлюс». - 2022 г. - с изм. и допол. в ред. от 13.04.202

3. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Текст]: дата введения 2013-01-01. – М.: Стандартинформ, 2018. – 20 с.

4. О персональных данных [Текст]: Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ // Официальный интернет-портал правовой информации. - 2022 г. - с изм. и допол. в ред. от 14.07.2022.

5. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Текст]: дата введения 1990-05-01. – М.: ИПК Издательство стандартов, 1996. – 28 с.

6. КриптоПро CAPILite Руководство программиста (CAPILite) [Электронный ресурс]: http://cpdn.cryptopro.ru/default.asp?url=content/capilite_trunk/html/Titul.html (дата обращения 23.03.2023).

7. Vostok Docs [Электронный ресурс]: https://github.com/vostok (дата обращения: 23.03.2023).