Описание технологии мобильной ЭЦП

версия 1.0

Реферат. Документ содержит описание технологии мобильной ЭЦП, созданной ЗАО «АВЕСТ» совместно с унитарным предприятием «Велком» и республиканским унитарным предприятием «Национальный центр электронных услуг».

Содержание

1. Введение

Мобильная ЭЦП – технология, которая позволяет гражданам использовать мобильный телефон в качестве надежного средства электронной цифровой подписи и для идентификации при получении услуг через Интернет или в устройствах самообслуживания (инфокиосках).

В Республике Беларусь технология мобильной ЭЦП создана ЗАО «АВЕСТ» совместно с унитарным предприятием «Велком» и республиканским унитарным предприятием «Национальный центр электронных услуг».

Абоненты УП «Велком» имеют возможность подключить услугу SIMiD для доступа к системе мобильной ЭЦП. Для этого абонент УП «Велком» должен обратиться в уполномоченный центр обслуживания клиентов для смены SIM на специализированную SIM с функцией ЭЦП, при этом телефонный номер сохраняется за абонентом.

Владелец SIM с подключенной услугой SIMiD может обратиться в любой регистрационный центр (далее – РЦ) республиканского удостоверяющего центра (далее – РУЦ) Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК), имеющий подключение к системе мобильной ЭЦП, для генерации ключей ЭЦП и выпуска сертификата открытого ключа. Услуги РЦ РУЦ ГосСУОК могут быть оказаны владельцу SIM непосредственно в уполномоченном центре обслуживания клиентов УП «Велком».

2. Задачи

Технология мобильной ЭЦП решает те же задачи, что и другие технологии ЭЦП: возможность пройти аутентификацию с использованием сертификата открытого ключа и возможность выработать ЭЦП.

С точки зрения удобства, главным отличием мобильной ЭЦП от других технологий является простота использования: нет необходимости в отдельном средстве ЭЦП (смарт-карте или USB-токене), не требуется установка и настройка программного обеспечения, все функции ЭЦП выполняет специализированная SIM–карта в мобильном телефоне. Технология мобильной ЭЦП может быть использована с любого компьютера, планшета или смартфона.

С точки зрения безопасности, главным преимуществом технологии мобильной ЭЦП является обязательность физического использования владельцем SIM своего телефона при любых операциях ЭЦП: он должен вводить известные только ему PIN-коды только на собственном мобильном телефоне. Это делает технологию мобильной ЭЦП более стойкой по сравнению с другими технологиями ЭЦП.

3. Организационная структура мобильной ЭЦП

Организационную инфраструктуру мобильной ЭЦП образуют:

- *Мобильный оператор*. Мобильный оператор предоставляет услуги связи на основе специализированной SIM, включая услуги передачи специализированных бинарных SMS.
- *Государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.* РЦ РУЦ ГосСУОК (включая регистрационные центры мобильного оператора) осуществляют операции управления ключами на SIM и выпускают сертификаты открытых ключей.
- *Сервер авторизации ГосСУОК.* Сервер авторизации ГосСУОК[1] предоставляет сервис идентификации и аутентификации владельцев SIM с функцией ЭЦП и сервис выработки ЭЦП. Сервер авторизации осуществляет взаимодействие с мобильным оператором для передачи специализированных бинарных SMS на SIM, также взаимодействует с ГосСУОК для получения сертификатов открытых ключей SIM и информации об их статусе.
- *Поставщики электронных услуг.* Поставщикам требуется надежная идентификация и аутентификация своих пользователей, а также возможность выработки ЭЦП пользователем с соблюдением требований Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи».
- *Абоненты мобильного оператора*, использующие SIM-карты с функцией ЭЦП. Абоненты мобильного оператора, в случае получения SIM с функций ЭЦП, могут использовать сервер авторизации для надежной идентификации и аутентификации перед поставщиком электронных услуг, а также для выработки ЭЦП.

4. Технология мобильной ЭЦП

SIM с функцией ЭЦП создана на основе высокопроизводительного защищенного микроконтроллера. SIM соответствует стандартам GSM/3GPP/LTE (2G/3G/4G) в части услуг связи. Дополнительно SIM содержит приложение ЭЦП, которое соответствует спецификации SIM Application Toolkit согласно стандартам GSM/3GPP/LTE (2G/3G/4G).

[1] Местонахождение Сервера авторизации ГосСУОК – центр обработки данных республиканского унитарного предприятия «Национальный центр электронных услуг»

Приложение ЭЦП хранит личный ключ ЭЦП и выполняет криптографические операции с личным ключом: все операции выполняются только внутри SIM, личный ключ не покидает пределов SIM. Для проведения операций входные данные должны быть переданы на SIM в виде служебных («бинарных») SMS согласно 3GPP TS 23.040, результаты обработки возвращаются также в виде «бинарных» SMS.

Приложение ЭЦП на SIM реализует сервис идентификации и аутентификации владельца SIM с использованием сертификата открытого ключа согласно СТБ 34.101.19. После завершения аутентификации приложение ЭЦП на SIM устанавливает защищенное соединение[2] с сервером авторизации с использованием криптографических алгоритмов и протоколов согласно СТБ 34.101.31, СТБ 34.101.45, СТБ 34.101.47.

Приложение ЭЦП на SIM также реализует сервис выработки ЭЦП электронного документа согласно СТБ 34.101.45: приложение ЭЦП вырабатывает ЭЦП для хэш-значения, присланного сервером по защищенному соединению в бинарной SMS, выработанное значение ЭЦП возвращается на сервер также по защищенному соединению. Формат формируемого электронного документа соответствует требованиям СТБ 34.101.23.

Для подтверждения своего согласия на прохождение идентификации и аутентификации владелец SIM должен ввести на телефоне PIN1, для подтверждения своего согласия на выработку ЭЦП — ввести PIN2. Длина PIN1 составляет 4 цифры, PIN2 — 5 цифр. После 5 неудачный попыток ввода каждого PIN-кода доступ к сервисам идентификации/аутентификации и выработки ЭЦП блокируется. PIN коды могут быть разблокированы путем ввода PUK-кода. После 3-х неудачный попыток ввода PUK-кода приложение ЭЦП на SIM блокируется.

Сервер авторизации предоставляет поставщикам услуг программный интерфейс для идентификации и аутентификации владельцев SIM, для выработки ими электронной цифровой подписи. Программный интерфейс сервера авторизации доступен по протоколу Oauth2 с обеспечением защиты информации по протоколу TLS согласно СТБ 34.101.65.

В целом, SIM с функцией ЭЦП во взаимодействии с сервером авторизации реализует набор национальных стандартных криптографических алгоритмов в соответствии с Положением о криптографической защите информации Оперативно-аналитического центра при Президенте Республики Беларусь (приказ Оперативно-

[2] При создании защищенного соединения не используется криптографическая защита информации, предоставляемая оборудованием мобильного оператора. Вместо этого сервер авторизации и SIM самостоятельно организуют криптографическую защиту передаваемой информации согласно требованиям национального законодательства Республики Беларусь.

аналитического центра при Президенте Республики Беларусь 30.08.2013 № 62 в редакции приказа 16.01.2015 № 3).

5. Типовой порядок применения

Порядок использования сервера авторизации для идентификации и аутентификации пользователя приведен на рис. 1:

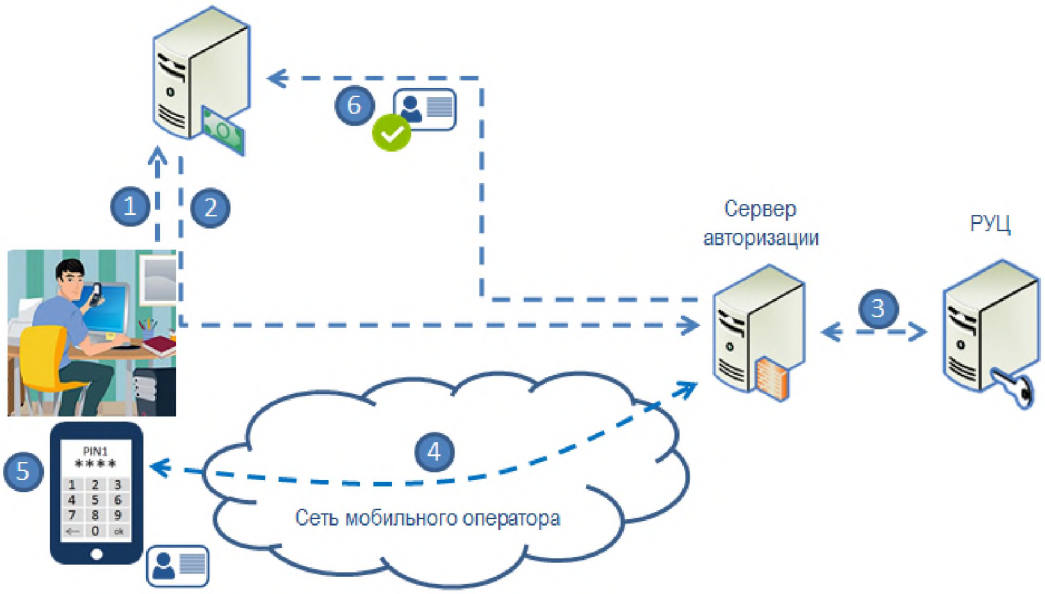

Рисунок 1 – Идентификация и аутентификация пользователя

1. Пользователь, который является владельцем SIM с ЭЦП, обращается на электронный ресурс поставщика за услугой.
2. Поставщик перенаправляет пользователя на сервер авторизации с обращением к сервису идентификации и аутентификации сервера. Пользователь указывает серверу свой телефонный номер.
3. Сервер определяет сертификат, выпущенный на данный телефонный номер, и проверяет его статус.
4. Сервер выполняет протокол аутентификации пользователя путем обмена с SIM бинарными SMS.
5. Для подтверждения согласия на прохождение идентификации и аутентификации на сервере с последующей передачей своих идентификационных данных поставщику услуг владелец SIM вводит на телефоне PIN1.
6. Сервер возвращает поставщику услуг результат аутентификации пользователя и подлинные идентификационные данные пользователя: Ф.И.О., паспортные данные, сертификат открытого ключа ЭЦП и др.

Порядок использования сервера авторизации для выработки ЭЦП приведен на рис. 2:

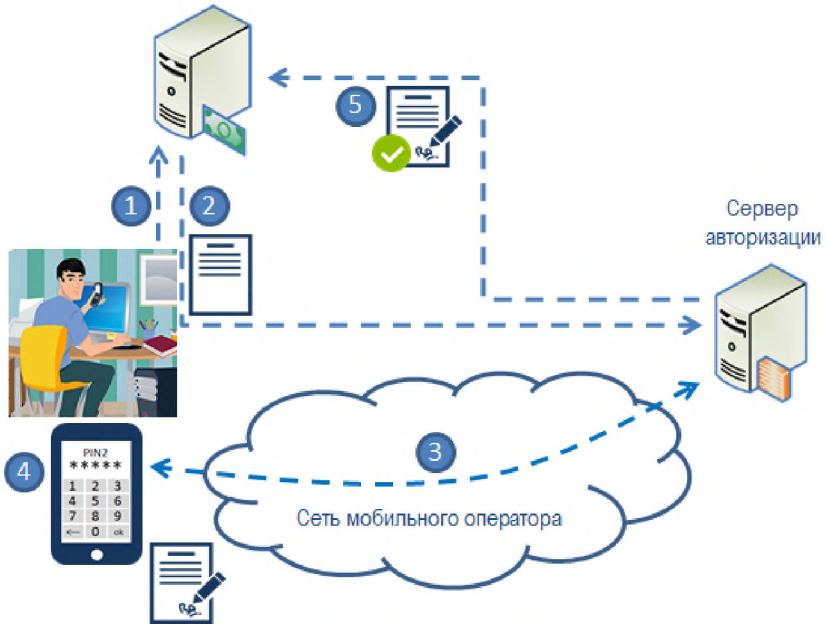

Рисунок 2 – Выработка ЭЦП пользователем

1. Пользователь желает оформить электронный документ на электронном ресурсе поставщика, например, подписать заявление или договор на получение электронной услуги, подать отчетность.
2. Поставщик перенаправляет пользователя на сервер авторизации с обращением к сервису выработки ЭЦП в рамках защищенного соединения, установленного между сервером и SIM: передается хэш-значение документа.
3. Сервер выполняет протокол выработки ЭЦП пользователя путем отправки бинарной SMS с хэш-значением документа и получения бинарной SMS с выработанной ЭЦП.
4. Для подтверждения своего согласия на выработку ЭЦП владелец SIM вводит на телефоне PIN2.
5. Сервер формирует электронный документ согласно СТБ 34.101.23, проверяет его подлинность и возвращает поставщику услуг, сформированный подлинный электронный документ.

В целом, сервер авторизации во взаимодействии с SIM с функцией ЭЦП реализует сервис идентификации и аутентификации владельца SIM, а также сервис выработки ЭЦП с соблюдением требований Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи».

6. Поставщики электронных услуг

Поставщики электронных услуг предоставляют доступ (через Интернет, через устройства самообслуживания и т.п.) к государственным, банковским и любым другим услугам, которые требуют проведения идентификации гражданина по паспорту и получения его собственноручной подписи на документах.

Поставщики заинтересованы в увеличении доступности своих услуг для пользователей (с соблюдением требований Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи») и в уменьшении расходов на эксплуатацию системы защиты информации.

Сервер авторизации предоставляет унифицированный программный интерфейс для идентификации и аутентификации граждан, для выработки ими электронной цифровой подписи независимо от используемого ими вида средства ЭЦП, в том числе с использованием SIM с функций ЭЦП. Сервер авторизации обеспечивает поддержку сертификатов открытых ключей, изданных РУЦ ГосСУОК, включая, атрибутные сертификаты.

В случае использования сервера авторизации поставщик электронных услуг избавлен от необходимости обеспечения совместимости с существующими и перспективными средствами ЭЦП, упрощается разработка и аттестация системы защиты информации – не требуется разработка подсистем аутентификации, управления полномочиями (авторизации) и электронной цифровой подписи.

В целом, взаимодействие с сервером авторизации позволяет поставщикам электронных услуг идентифицировать обратившегося гражданина и получить его электронную цифровую подпись на электронных документах. Это будет сделано в правовых рамках Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи», согласно которому электронная цифровая подпись по правовому статусу приравнивается к собственноручной подписи[3], электронный документ – к обычному документу[4], а сертификат ключа ЭЦП используется для идентификации его владельца[5].

---

[3] Статья 22 «*Подлинный электронный документ приравнивается к документу на бумажном носителе, подписанному собственноручно, и имеет одинаковую с ним юридическую силу.*»

[4] Статья 22 «*Если в соответствии с законодательством Республики Беларусь требуется, чтобы документ был оформлен в письменной форме, то электронный документ и его копия считаются соответствующими этому требованию.*»

[5] Статья 29 «*Государственная система управления открытыми ключами предназначена для обеспечения возможности получения всеми заинтересованными организациями и физическими лицами информации об открытых ключах и их владельцах в Республике Беларусь…* »; Статья 1 «*сертификат открытого ключа — электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенным организации или физическому лицу*»; Статья 26 «*… сертификат открытого*

7. Совместимость

SIM соответствует стандартам GSM/3GPP/LTE (2G/3G/4G) в части услуг связи и может быть использована в любых моделях телефонов, смартфонов и планшетов, совместимых с данными стандартами.

Приложение ЭЦП на SIM соответствует спецификации SIM Application Toolkit согласно стандартам GSM/3GPP/LTE (2G/3G/4G) и функции ЭЦП доступны на всех моделях телефонов, смартфонов и планшетов, совместимых с данными стандартами.

Пользовательский интерфейс приложения ЭЦП определяется характеристиками используемого телефона, смартфона или планшета. Такие характеристики как размер экрана, объем отображаемого на экране текста, доступные интерфейсные элементы определяют внешний вид пользовательского интерфейса приложения ЭЦП и могут влиять на его удобство для пользователей.

Проведенное тестирование показало совместимость технологии мобильной ЭЦП как с GSM телефонами различных производителей — и разного времени выпуска, — так и со смартфонами и планшетами под управлением различных ОС: Android, iOS, Windows Mobile, Symbian.

ключа должен содержать… информацию, однозначно идентифицирующую организацию или физическое лицо, являющиеся владельцем открытого ключа»