УДК 004.622

Д.В. Сазонова, ассист.;
В.В. Козловский, ст. преп.
(БГТУ, г. Минск)

ТЕХНОЛОГИИ ИСПОЛЬЗОВАНИЯ ОБЛАЧНОЙ ЭЦП

Первое упоминание термина «электронная цифровая подпись» было сделано в 1976 году криптографами Уитфилдом Диффи и Мартином Хеллманом.

В дальнейшем получили распространение стандарты электронной цифровой подписи (далее – ЭЦП) на схемах Эль-Гамаля (стандарты DSA в США и ГОСТ Р 34.10-94 в России) и Шнора (стандарт СТБ 1176.2-99 в Республики Беларусь и KCDSA,EC-KCDSA в Южной Кореи) которые представляли из себя криптосистемы с открытым ключом, основанные на трудности вычисления дискретных логарифмов в конечном поле.

В настоящее время в качестве алгоритмов ЭЦП применяются ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм с открытым ключом, использующийся для построения и проверки ЭЦП при помощи криптографии на эллиптических кривых. В Республике Беларусь это стандарт СТБ 34.101.45-2013.

По основному функциональному назначению алгоритм ЭЦП предназначен для контроля целостности и подлинности электронных документов. При выработке подписи используется личный ключ, который находится в распоряжении владельца.

Для придания юридической значимости ЭЦП в Республике Беларусь в 2009 году был принят Закон «Об электронном документе и электронной цифровой подписи» (далее – Закон), в который вносились изменения и дополнения, расширяющие правовое поле в этой области, приравняв ЭЦП к аналогу собственноручной подписи.

В Законе термин «электронная цифровая подпись» определен как последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности, а также для иных целей [2]. ЭЦП признана аналогом собственноручной подписи.

Для практического использования ЭЦП и создания юридически значимы электронных документов в РБ создана Государственная система управления открытыми ключами (ГосСУОК), определяющая технологию использования ЭЦП.

ГосСУОК предназначена для обеспечения возможности получения всеми заинтересованными организациями и физическими лицами

информации об открытых ключах и их владельцах в Республике Беларусь и представляет собой систему взаимосвязанных и аккредитованных в ней поставщиков услуг.

ГосСУОК строится как иерархическая инфраструктура открытых ключей и состоит из корневого удостоверяющего центра, подчиненного ему республиканского удостоверяющего центра и регистрационных центров.

Основные компоненты ГосСУОК:

– регистрационный центр;

– удостоверяющий центр;

– центр атрибутных сертификатов.

ГосСУОК осуществляет распространение открытых ключей в виде сертификатов.

Конечными пользователями ГосСУОК выступают физические лица и организации, которые являются владельцами сертификатов, атрибутных сертификатов и (или) доверяющими сторонами [3].

Корневой удостоверяющий центр является базовым компонентом ГосСУОК и занимает высшее положение в единой иерархической инфраструктуре доверия открытых ключей, реализуемой ГосСУОК.

Порядок функционирования корневого удостоверяющего центра и процедура издания самоподписанного сертификата определяются политикой применения сертификатов.

Владельцем сертификата является организация или физическое лицо, являющееся владельцем личного ключа, на базе которого выработан открытый ключ, значение которого включено в этот сертификат.

На основании сертификатов физических лиц, работающих в государственных органах и других государственных организациях, а также иных физических лиц центр атрибутных сертификатов издает атрибутные сертификаты в соответствии с политикой применения вышеупомянутых сертификатов. В атрибутных сертификатах содержится информация о полномочиях таких физических лиц.

Доверяющие стороны могут запрашивать в республиканском удостоверяющем центре сертификаты и атрибутные сертификаты любого пользователя ГосСУОК и использовать их для проверки электронной цифровой подписи электронного документа. Перед установлением доверия к электронному документу доверяющие стороны обязаны:

– убедиться в действительности сертификата и атрибутного сертификата, включая их проверку на отзыв или истечение срока действия;

– удостовериться, что в атрибутном сертификате содержится информация о полномочиях физического лица на подписание электронного документа определенного типа.

В качестве носителя личного ключа ЭЦП пользователя используются аппаратные средства трех видов: специальный USB-token, специализированная SIM-карта, ID-карта гражданина РБ. Однако данные носители личного ключа имеет ряд недостатков.

Для USB-токена:

– наличие адаптированного программного обеспечения только для ОС Windows;

– невозможность применения с рядом мобильных систем (iOS);

– дополнительные затраты на приобретение;

– возможность выхода из строя.

Для специализированной SIM-карты:

– невозможность автономного применения;

– зависимость от оператора сотовой связи и иных информационных систем;

– дополнительные затраты на приобретение;

– возможность выхода из строя.

Для ID-карты гражданина РБ:

– невозможность применения с рядом мобильных устройств, не имеющих NFC;

– дополнительные затраты на приобретение ридера смарт-карт;

– возможность выхода из строя.

В любом случае пользователю необходимо иметь некоторое устройство, используемое в качестве носителя личного ключа ЭЦП.

Новое решение, позволяющее отказаться от наличие индивидуального устройства хранение личного ключа – это переход к использованию технологии облачной ЭЦП.

Главное отличие технологии облачной ЭЦП от традиционной является место хранения личного ключа пользователя и выполнение криптографической операции выработки ЭЦП. При построении инфраструктуры облачной ЭЦП таким местом является HSM (hardware security module) – аппаратный модуль безопасности, схема которого представлена на рис. 1.

Базовые HSM являются корнем доверия, который защищает инфраструктуру открытых ключей от взлома, позволяя создавать ключи на протяжении всего жизненного цикла инфраструктуры, а также обеспечивая масштабируемость всей архитектуры безопасности.

Внедрение и роль HSM становится основополагающей. HSM выполняет роль аппаратного устройства, которое защищает все криптографические процессы путем создания, управления и защиты клю-

чей, используемых для шифрования и дешифрования конфиденциальных данных, критически важных для информации и безопасности большинства организаций.

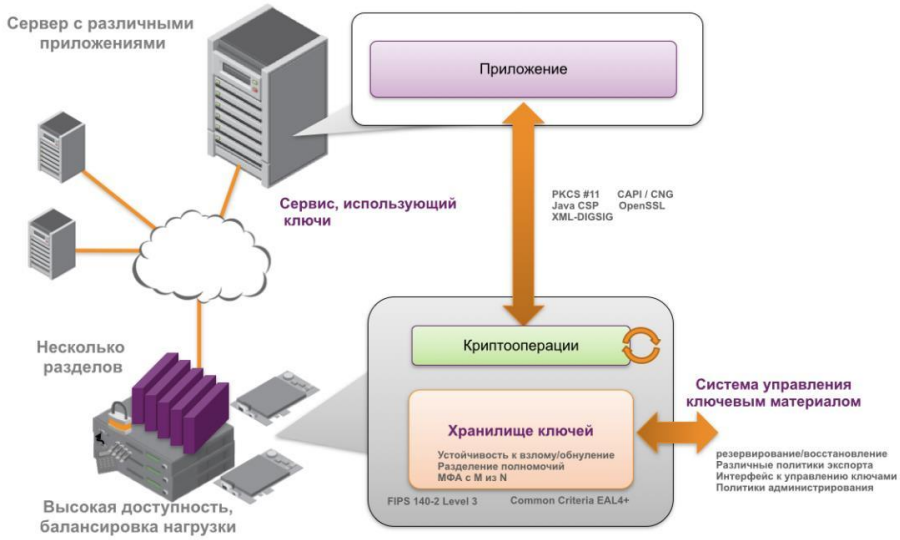

Рисунок 1 – Схема аппаратного модуля безопасности HSM

Однако для безопасного использования технологии облачной ЭЦП недостаточно одного HSM. Необходимо выстроить инфраструктуру с дополнительными элементами. Инфраструктура облачной ЭЦП представлена на рис. 2. HSM на приведенном рисунке выполняет роль «Устройство создания подписи».

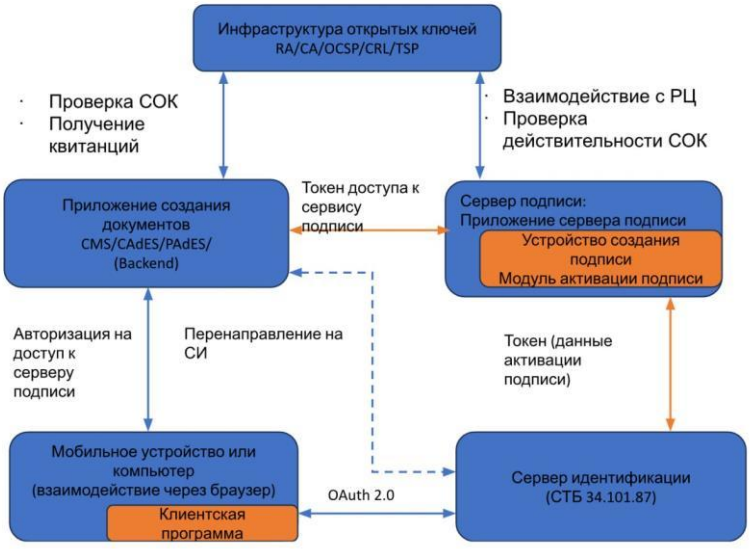

Рисунок 2 – Инфраструктура облачной ЭЦП

В инфраструктуру облачной подписи (ИОП) входят следующие компоненты:

1. Сервер подписи (СП) состоит:

– приложение сервера подписи (ПСП);

– модуль активации подписи (МАП);

– устройства создания подписи (УСП);

2. Приложение создания документов (ПСД);

3. Сервер идентификации (СИ);

4. Клиентское приложение (КП);

5. Внешние компоненты, с которыми взаимодействует ИОП:

– регистрационный центр (РЦ);

– удостоверяющий центр (УЦ);

– служба штампа времени (СШВ) и онлайн проверки статуса сертификатов (OCSP).

Сервис цифровой подписи – это масштабируемая платформа с поддержкой API для выработки цифровых подписей, которая обеспечивает:

1. Цифровую подпись хэша любого документа или цифровую транзакцию в настройке инфраструктуры открытых ключей;

2. Выдачу сертификата подписи;

3. Поддержку мировых доверенных служб (AATL и Microsoft Root);

4. Хранение приватных ключей на базе HSM;

5. Проверку отзыва, требуемого для аудита;

6. Продвинутые электронные печати и после аккредитации квалифицированные подписи, соответствующие стандарту стран Евросоюза (eIDAS).

Эксперты заявляют, что информация, хранящаяся на облачном сервере, лучше защищена и исключает доступ третьих лиц.

Это объясняется это тем, что носитель, где содержится сертификат с паролями, у владельца можно запросто украсть и подписать за него электронный документ. Следственно, пользователь должен надёжно хранить свой токен, и так бывает не всегда.

К преимуществам облачной ЭЦП можно отнести:

1. Удаленное применение;

2. Отсутствие рисков потери или повреждения физического носителя;

3. Высокая степень защиты;

4. Стоимость ниже традиционной ЭП;

5. Быстрое получение;

Правообладатель ЭЦП – удостоверяющий центр. Эта организация несёт ответственность за сохранность и неприкосновенность электронного ключа, а не то лицо, на кого оформлен сертификат облачной цифровой подписи.

Электронную цифровую подпись имеет право получить:

1. Должностное лицо в компании, которое будет использовать ее для выполнения своих должностных обязанностей.

2. Индивидуальный предприниматель для ведения отчетности по своей деятельности.

3. Физическое лицо, которое может использовать ЭПЦ в личных целях.

В зависимости от собственного статуса, владелец ЭЦП может использовать ее в различных целях. К примеру, ИП или юрлицо может:

1. Подавать налоговые декларации

2. Платить налоги и получать информацию обо всех заложенностях и переплатах

3. Отправлять отчеты в ФФЗН, Белгосстрах, Белстат и другие госорганы

4. Работать с электронными счет-фактурами

Физические лица могут использовать ЭЦП при подписании договоров на оказание услуг, договоров кредитования, страхования, а также крупных сделках купли-продажи.

Однако пока подобная услуга не стала популярной. ЭПЦ используют в основном компании и ИП.

ЛИТЕРАТУРА

1. СТБ 34.101.45-2013 Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых. [Электронный ресурс] – Режим доступа: https://apmi.bsu.by/resources/std.html. – Дата доступа: 25.01.2024.

2. Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи». [Электронный ресурс] – Режим доступа: https://etalonline.by/document/?regnum=h10900113. – Дата доступа: 28.01.2024.

3. Регламент деятельности республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь республиканского унитарного предприятия «Национальный центр электронных услуг» [Электронный ресурс] – Режим доступа: https://nces.by/wp-content/uploads/reglament-rc-ruc.pdf. – Дата доступа: 29.01.2024.