http://dx.doi.org/10.35596/1729-7648-2023-29-4-50-57

Оригинальная статья
Original paper

УДК 004.056.55

СЕРВИС ДЛЯ ПРОВЕРКИ СЕРТИФИКАТОВ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

И. О. ТОЛОХ, С. Ю. МИХНЕВИЧ, А. Ю. СЕНКЕВИЧ

Белорусская государственная академия связи (г. Минск, Республика Беларусь)

Поступила в редакцию 21.02.2023

Аннотация. В законодательстве Республики Беларусь в настоящее время установлена одинаковая юридическая сила для идентичных документов на бумажном носителе и в электронном виде, имеющих обязательный реквизит – электронную цифровую подпись. В статье рассмотрена система управления открытыми ключами электронной цифровой подписи в Республике Беларусь, приведены понятия и определения, связанные с этой системой. Проанализированы технические нормативные правовые акты в области криптографической защиты электронных документов. Обоснована необходимость проверки сертификатов открытых ключей электронной цифровой подписи. Описаны возможные варианты процедуры проверки сертификатов открытых ключей, показаны их преимущества и недостатки. С использованием открытых криптографических библиотек и общедоступных инструментов разработан онлайн-сервис для проверки сертификатов открытых ключей.

Ключевые слова: электронная цифровая подпись, открытый ключ, сертификат, бот, личный ключ, криптографические стандарты, электронные услуги, отзыв сертификатов, удостоверяющий центр.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Толох, И. О. Сервис для проверки сертификатов электронных документов / И. О. Толох, С. Ю. Михневич, А. Ю. Сенкевич // Цифровая трансформация. 2023. Т. 29, № 4. С. 50–57. http://dx.doi.org/10.35596/1729-7648-2023-29-4-50-57.

SERVICE FOR VERIFICATION OF ELECTRONIC DOCUMENT'S CERTIFICATES

IGOR O. TOLOKH, SVETLANA YU. MIKHNEVICH, ALENA YU. SIANKEVICH

Belarusian State Academy of Communications (Minsk, Republic of Belarus)

Submitted 21.02.2023

Abstract. The legislation of the Republic of Belarus currently establishes the same legal force for identical documents on paper and in electronic form, which have a mandatory requisite - an electronic digital signature. The article considers the system for managing public keys of electronic digital signature in the Republic of Belarus, as well as the concepts and definitions associated with this system. The technical normative legal acts in the field of cryptographic protection of electronic documents are analyzed. The necessity of verification of certificates of public keys of electronic digital signature is substantiated. Possible variants of the procedure for verifying public key certificates are described, their advantages and disadvantages are shown. An online service for checking public key certificates has been developed using open cryptographic libraries and public tools.

Keywords: electronic digital signature, public key, certificate, bot, private key, cryptographic standards, electronic services, certificate revocation, certification authority.

Conflict of interests. The authors declare no conflict of interests.

For citation. Tolokh I. O., Mikhnevich S. Yu., Siankevich A. Yu. (2023) Service for Verification of Electronic Document's Certificates. *Digital Transformation.* 29 (4), 50–57. http://dx.doi.org/10.35596/1729-7648-2023-29-4-50-57 (in Russian).

Введение

В современном мире в связи с быстрым развитием информационных технологий происходит их повсеместное внедрение во все сферы деятельности человека [1]. Вместе с их преимуществами, такими как удобство доступа к информации, ускорение обмена и распространения информации, появляются проблемы, связанные с подтверждением целостности и подлинности электронных документов. В настоящее время в сфере делопроизводства для решения этих вопросов широко используется электронная цифровая подпись (ЭЦП), которая обеспечивает контроль достоверности (целостности и подлинности) информации и подтверждение авторства. Применение ЭЦП возможно не только в электронном делопроизводстве. С 1991 г. идет обсуждение вопроса о защите авторских прав в киберпространстве [2]. Так, в Российской Федерации с 2012 г. действует сервис Itismine!, обеспечивающий постановку ЭЦП со штампом времени посредством веб-ресурса. Его оригинальность в том, что он направлен на защиту объектов авторского права. Созданная инфраструктура работы с ЭЦП создает предпосылки для использования ЭЦП в различных сферах деятельности [3, 4].

Проверка сертификатов электронных документов

В соответствии с законодательством Республики Беларусь электронная цифровая подпись – последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности, а также для иных целей, предусмотренных Законом Республики Беларусь от 28 декабря 2009 г. № 113-З[1] и иными законодательными актами. Одинаковые по содержанию документы, созданные организацией или физическим лицом на бумажном носителе и в электронной форме, имеют одинаковую юридическую силу. С 15 сентября 2016 г. банки Республики Беларусь используют сертификаты открытых ключей проверки электронной цифровой подписи, изданные Республиканским удостоверяющим центром Государственной системы управления открытыми ключами (ГосСУОК) проверки электронной цифровой подписи Республики Беларусь, для идентификации и аутентификации юридических и физических лиц, в том числе индивидуальных предпринимателей, адвокатов, нотариусов и их представителей.

Для проверки электронной цифровой подписи используется открытый ключ – последовательность символов, соответствующая определенному личному (закрытому) ключу, доступная для всех заинтересованных организаций или физических лиц. Открытый ключ распространяется в виде атрибутивных сертификатов (или сертификатов). Сертификат открытого ключа (СОК) – электронный документ, изданный удостоверяющим центром (УЦ), содержащий сведения, подтверждающие принадлежность указанного в нем открытого ключа определенной организации или физическому лицу. Помимо этой информации, сертификат содержит информацию о его владельце, эмитенте, сроке действия и включает также другие атрибуты.

Инфраструктура открытого ключа (ИОК) – инфраструктура, позволяющая управлять открытыми ключами для поддержания услуг аутентификации, контроля целостности, обеспечения конфиденциальности и (или) невозможности отказа от авторства. ИОК включает:

– регистрационный центр (РЦ) – объект системы, предназначенный для регистрации пользователей;

– корневой удостоверяющий центр (КУЦ) – УЦ в верхней позиции иерархической структуры ИОК;

– конечных пользователей – это пользователи, приложения или системы, являющиеся владельцами СОК и использующие ИОК.

[1] Об электронном документе и электронной цифровой подписи: Закон Респ. Беларусь от 28 декабря 2009 г. № 113-З: в ред. от 8 ноября 2018 г. № 143-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2021.

В Республике Беларусь структурой управления открытыми ключами является ГосСУОК, положение о которой разработано Оперативно-аналитическим центром при Президенте Республики Беларусь. ГосСУОК работает с 2014 г., и на сегодняшней день выдано почти 1,5 млн ЭЦП, а в системе ведомственного документооборота работает более 15 000 организаций.

В соответствии с Регламентом деятельности Республиканского удостоверяющего центра ГосСУОК проверки ЭЦП Республики Беларусь юридическое или физическое лицо, полагающееся на достоверность сведений, содержащихся в сертификате открытого ключа, и (или) электронную цифровую подпись (далее − доверяющая сторона), могут запрашивать сертификаты любого пользователя ГосСУОК и использовать их для проверки электронной цифровой подписи электронного документа. Прежде чем установить доверие к электронному документу, доверяющие стороны обязаны:

− удостовериться в действительности сертификата. Списки отозванных сертификатов (СОС) регулярно публикуются и обновляются. Обновление может происходить при истечении срока действия (например, в связи с изменением имени, названия организации и т. д.). Периодичность обновления устанавливается организацией, проводящей эту работу;

− убедиться, что в атрибутном сертификате содержатся сведения о полномочиях физического лица на подписание электронного документа определенного типа.

Форматы сертификата и электронного документа определены в документах СТБ 34.101.19 и СТБ 34.101.23, входящих в систему криптографических стандартов Республики Беларусь, схема которых представлена на рис. 1.

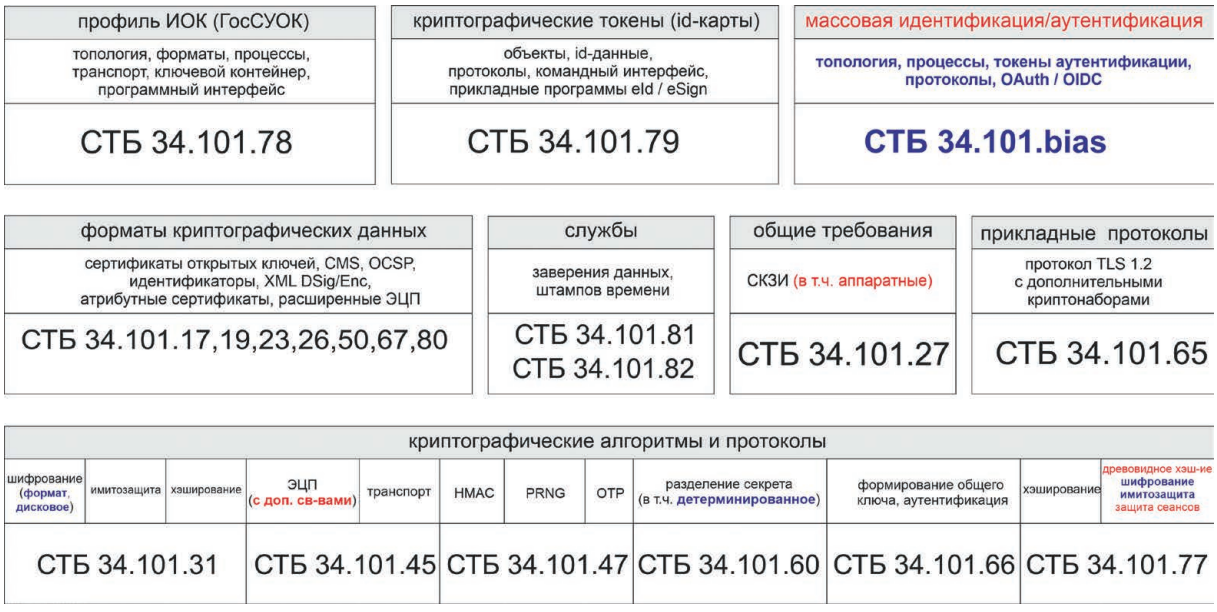

Рис. 1. Криптографические стандарты Республики Беларусь
Fig. 1. Cryptographic standards of the Republic of Belarus

Стандарт СТБ 34.101.19 определяет форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей, а также процедуры проверки их подлинности. Связь открытого ключа с его владельцем обеспечивает УЦ посредством сертификата (рис. 2). Проверка УЦ того, что пользователь владеет личным ключом, соответствующим открытому ключу, может основываться на применении протоколов (также известных как алгоритмы доказательства владения), на предъявлении личного ключа или на утверждении владельца открытого и личного ключа. Сертификат имеет ограниченный срок действия, указанный в атрибутах. Пользователи должны иметь возможность самостоятельно проверять СОК. Например, если по какой-либо причине УЦ отзывает ранее выданный СОК, пользователи должны иметь возможность узнать о том, что был отзыв, чтобы не использовать сертификат, к которому отсутствует доверие. Поэтому сертификаты могут передаваться по небезопасным каналам передачи данных и храниться в незащищенных хранилищах. СОС являются одним из способов, которые могут быть использованы для уведомления пользователей об отзыве СОК.

Рис. 2. Связь открытого ключа с его владельцем
Fig. 2. Linking a public key to its owner

В СТБ 34.101.19 определяется формат СОС, включая способ его расширения и совокупность расширений СОС. Как для СОК, так и для СОС могут определяться дополнительные расширения, которые окажутся полезными в конкретных приложениях.

Пользователь, для которого требуется информация об открытом ключе, должен проверить подлинность сертификата, содержащего требуемый открытый ключ. Если у пользователя подписавшего сертификат, нет доверенного значения открытого ключа УЦ, названия УЦ и связанной с ним информации (например, такой как срок действия или ограничения, накладываемые на имена), то для проверки СОК может потребоваться дополнительный сертификат. Как правило, необходимы цепочка сертификатов, содержащая проверяемый сертификат, подписанный одним из УЦ, и, возможно, дополнительные сертификаты УЦ, подписанные другими УЦ. Такие цепочки, называемые маршрутами сертификации, требуются потому, что пользователь открытого ключа изначально имеет только ограниченное число доверенных значений открытых ключей, принадлежащих УЦ.

Также в СТБ 34.101.19 определены два класса сертификатов: УЦ и конечных пользователей. Сертификаты УЦ, в свою очередь, можно разделить на три класса: кросс-сертификаты, самоизданные и самоподписанные сертификаты. Кросс-сертификаты – это сертификаты УЦ, в которых эмитент и субъект СОК являются двумя разными сторонами. Кросс-сертификаты указывают на доверенные отношения между двумя УЦ. Самоизданные – это сертификаты УЦ, в которых эмитент и субъект являются одной и той же стороной. Такие сертификаты выдаются для внесения изменений в политику или деятельность УЦ. Самоподписанные – это самоизданные сертификаты, ЭЦП которых можно проверить с помощью открытого ключа из данного сертификата. Самоподписанные сертификаты предназначены для использования открытого ключа в качестве начала маршрута сертификации, т. е. точки доверия.

При выдаче сертификата предполагается, что он может быть использован на протяжении всего срока действия. Однако вследствие различных обстоятельств сертификат может стать недействительным до истечения срока действия. Такими обстоятельствами могут быть смена имени, изменение характера связи субъекта с УЦ (например, сотрудник разрывает договор с организацией), а также компрометация или подозрение на компрометацию соответствующего личного ключа. При этих обстоятельствах УЦ должен отозвать сертификат.

В СТБ 34.101.19 предусмотрен один способ отзыва сертификатов – каждый УЦ периодически выдает подписанную структуру данных, которая называется списком отозванных сертификатов. СОС – это общедоступный список с отметкой времени, подписанный УЦ или эмитентом СОС, в котором указаны отозванные сертификаты. Каждый отозванный сертификат можно найти в СОС

по серийному номеру. Каждая информационная система, использующая сертификат, не только проверяет его целостность и срок действия, но и обращается к допустимому по сроку действия СОС для подтверждения того, что серийный номер сертификата отсутствует в этом списке. Значение «допустимый по сроку действия» может различаться в разных системах, но обычно оно означает самый последний выпущенный СОС. Новый СОС выпускается периодически (например, ежечасно, ежедневно, еженедельно). Запись добавляется в СОС при следующем обновлении списка после уведомления о необходимости отзыва СОК. Запись об отзыве не должна удаляться из СОС до того, пока она не появится в одном СОС, выпущенном после окончания срока действия отозванного сертификата. Достоинство такого способа отзыва – то, что СОС могут распространяться таким же образом, что и сертификаты: через небезопасные каналы передачи данных и незащищенные хранилища.

Ограничение для способа отзыва с использованием СОС заключается в том, что периодичность процесса отзыва ограничена периодичностью выпуска СОС. Например, если в настоящее время зарегистрировали отзыв, то системы, использующие сертификаты, не будут уведомлены об этом, пока все выпущенные списки СОС не обновятся. В зависимости от частоты выпуска СОС это может занять час, день, неделю. Стандартные наборы атрибутов сертификатов были определены в серии X.500 спецификаций. Программные реализации проверки СОК, соответствующие настоящему стандарту, должны иметь возможность обработки следующих стандартных типов атрибутов в именах эмитента и субъекта:

– страна, организация, организационная единица, определитель уникального имени, название государства или области, обычное имя, серийный номер;

– местоположение, должность, фамилия, имя, отчество, инициалы, псевдоним.

Обработка СОС начинается с предположения, что сертификат не отозван. Алгоритм проверяет СОС один или более раз до тех пор, пока статус сертификата не будет определен как отозванный или пока не будет проверено достаточное количество СОС для проверки всех кодов причин. Процедуры проверки маршрута сертификации основаны на алгоритме, который проверяет связь между уникальным именем субъекта (альтернативным именем субъекта) и открытым ключом субъекта. Проверка маршрута сертификата ограничивается условиями, указанными в сертификатах в маршруте, и входными данными, представленными проверяющим участником.

Входными данными алгоритма является точка доверия. Точка доверия представляет собой совокупность следующей информации: доверенное значение открытого ключа, уникальное имя владельца соответствующего личного ключа (например, субъект удостоверяющего центра), идентификатор алгоритма электронной цифровой подписи, параметры открытого ключа (если они имеются) и период действия ключа (если он установлен). Выбор точки доверия зависит от политики: в качестве точки доверия могут выступать: корневой УЦ в иерархической ИОК; УЦ, выдавший сертификат (или несколько сертификатов) проверяющей стороне; любой иной УЦ в сети ИОК.

Процедура верификации маршрута остается неизменной и не зависит от выбора точки доверия. Кроме того, разные приложения могут использовать различные точки доверия или доверять маршрутам, начинающимся с любой точки доверия из заданного набора. В большинстве случаев сертификат является сертификатом конечного пользователя, но может быть и сертификатом УЦ, так как открытый ключ может использоваться для целей, отличных от проверки подписи сертификата. Для проверки связи между именем и открытым ключом субъекта необходимо иметь цепочку сертификатов, которые поддерживают такую связь.

Стандарт СТБ 34.101.23 определяет синтаксис криптографических сообщений, которые используются для обеспечения конфиденциальности, контроля целостности и подлинности данных при их передаче и хранении. Документ устанавливает форматы криптографических сообщений, правила создания и обработки сообщений. Синтаксис базируется на инкапсуляции – вложении одной структуры данных в другую. Система управления содержимым (CMS) допускает многократную вложенность: один контейнер, содержащий вложенные данные, может быть частью другого контейнера. Например, стороны могут подписывать ранее инкапсулированные данные, которые уже содержат ЭЦП. CMS позволяет подписывать произвольные атрибуты, например текущее время, вместе с обрабатываемым сообщением и добавлять другие атрибуты к выработанной ЭЦП. CMS поддерживает различные инфраструктуры открытых ключей, в том числе инфраструктуру, заданную в СТБ 34.101.19 и основанную на сертификатах открытых ключей.

Значения типов CMS определяются с помощью базовых правил кодирования ACH.1. Результатом кодирования является строка октетов. Большинство коммуникационных систем имеют средства надежной передачи строк октетов. Тем не менее известны системы, в которых такие средства отсутствуют. CMS позволяет описывать данные многих типов. Тип данных задается специальным идентификатором. CMS связывает идентификатор с самими данными. Для этого должен использоваться криптографический контейнер, формат которого определяется типом ContentInfo ACH.1.

СТБ 34.101.23 определяет семь типов данных: неструктурированные, подписанные, конвертованные, хэшированные, шифрованные, аутентифицируемые и аутентифицируемые конвертованные. Дополнительные типы данных могут быть определены в других ТНПА, основанных на СТБ 34.101.23. При этом дополнительные типы должны быть отличны от CHOICE. Программы реализации, которые претендуют на соответствие настоящему стандарту, должны поддерживать контейнер Contentinfo и неструктурированные, подписанные и конвертованные данные, также могут поддерживаться и остальные типы.

Неструктурированные данные – это произвольные строки октетов, например текстовые сообщения, интерпретация которых зависит от конкретного применения. Такие строки не обязательно имеют внутреннюю структуру, хотя структура может быть, и она может описываться, например, с помощью ACH.1.

Подписанные данные – это произвольные данные, дополненные несколькими ЭЦП, выработанными одной или несколькими сторонами. Отсутствие ЭЦП не считается ошибкой.

Конвертованные данные – зашифрованные данные вместе с зашифрованными для одного или нескольких получателей ключами шифрования данных. Комбинация зашифрованных данных и одного из зашифрованных ключей является цифровым конвертом для соответствующего получателя. В цифровой конверт могут быть помещены данные любого типа, данные могут адресоваться любому числу получателей, для шифрования ключей могут применяться любые поддерживаемые получателем методы. При шифровании данных ключ выбранного алгоритма шифрования вырабатывается случайным образом. Данные (строка октетов) дополняются до определенной длины, а затем зашифровываются с помощью выработанного ключа.

Хэшированные данные – это данные вместе с вычисленным для них хэш-значением. Обычно такой тип применяется для контроля целостности данных и используется в качестве вложенного контейнера при формировании конвертованных данных.

Шифрованные данные – данные любого типа, зашифрованные на некотором ключе. В отличие от конвертованных, в шифрованных не содержится информация ни о получателях, ни о ключах шифрования. Управление ключами шифрования должно осуществляться другими, отличными от использованных в конвертованных данных, способами. Типичное применение – защита данных при хранении на локальных устройствах с помощью шифрования на ключе, построенном по паролю.

Аутентифицируемые данные – это данные любого типа вместе с имитовставкой и зашифрованными для одного или нескольких получателей ключами имитозащиты. Имитовставка и зашифрованный ключ имитозащиты получателя используются им для проверки целостности данных. Контроль целостности может обеспечиваться для любого числа получателей.

Электронный сервис проверки сертификатов электронных документов

На едином портале электронных услуг реализована функция проверки сертификатов ЭЦП при вводе необходимой информации. Однако с увеличением потока электронных документов появляется необходимость автоматической проверки сертификатов подлинности ЭЦП. Сервис онлайн-проверки должен быть максимально доступен (например, реализован на открытом веб-сервере, в виде Telegram-бота и т. д.). Для реализации онлайн-сервиса проверки электронных документов целесообразно использовать открытые криптографические библиотеки и общедоступные инструменты. В данной статье выбраны следующие:

– OpenSSL (протоколы SSL/TLS, криптографические форматы, унификация работы с криптографическими алгоритмами);

– Bee2 (криптографические алгоритмы РБ);

– Bee2evp (встраивание Bee2 в OpenSSL);

– Python (интеграция, Telegram-бот).

OpenSSL – это криптографический пакет с открытым исходным кодом, который предназначен для работы с протоколами SSL/TLS, сертификатами открытых ключей, списками отозванных сер-

тификатов, электронными документами и другими криптографическими форматами. OpenSSL поддерживает разнородную зарубежную криптографию, но, к сожалению, не отечественную. Криптографические алгоритмы Республики Беларусь встраиваются в OpenSSL с помощью программной библиотеки Bee2 и плагина Bee2evp. Алгоритмы реализованы в Bee2, а в Bee2evp эти реализации «обернуты» интерфейсами схемы EVP, которая поддерживается в OpenSSL. Библиотека Bee2 и плагин Bee2evp разработаны в НИИ прикладных проблем математики и информатики Белорусского государственного университета. Они распространяются на условиях GNU GeneralPublicLicense версии 3. Трехуровневая конструкция OpenSSL[Bee2evp[Bee2]] использована в серверной части разработанного авторами статьи онлайн-сервиса проверки достоверности электронных документов. Клиентская часть представлена Telegram-ботом. Бот обрабатывает следующие команды: /cert – проверить сертификат; /doc– проверить электронный документ.

В Telegram-боте, приведенном на рис. 3, реализованы две основные функции: проверить документ и проверить сертификат. Работают они по схожему принципу – на вход подается электронный документ, который проверяется на валидность, и на выходе мы получаем ответ в виде статуса ответа.

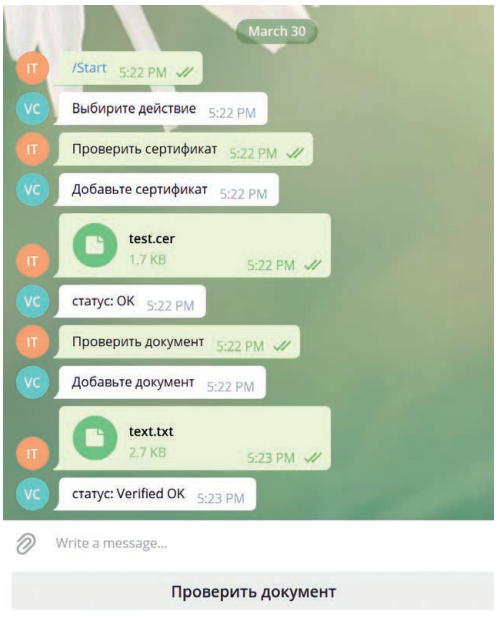

Рис. 3. Telegram-бот проверки сертификата открытого ключа
Fig. 3. Telegram bot to check public key certificate

Проверка сертификатов происходит следующим образом. При использовании кнопки «Проверить сертификат» появляется предложение отправить его. После отправки выполняется проверка сертификата – проверяется его штамп времени, кто его подписал и не находится ли сертификат в списке отозванных. Если все в порядке, получаем ответ OK, если нет – в статусе ответа будет выведена определенная ошибка в зависимости от того, что именно произошло. Проверка документа реализуется схожим образом: на вход подается документ, который должен содержать сертификат с подписью. Сначала проверяется подпись на документе: если она подлинная, то переходим к проверке подлинности сертификата. Если с ним тоже все в порядке, то ответ будет OK, а если произошла ошибка, то она будет выдана в статусе (рис. 3) [5].

Результатом работы бота является статус корректности сертификата или документа. Бот использует предустановленные сертификаты корневого и Республиканского удостоверяющих центров ГосСУОК, загружает отозванные этими центрами списки сертификатов. Также бот проверяет, что сертификат лица, подписавшего документ, действительно выдан Республиканским удостоверяющим центром, что срок действия сертификата включает момент проверки и что сертификат не включен в список отозванных.

Заключение

Обоснована необходимость создания сервиса по проверке сертификатов открытых ключей электронной цифровой подписи. Описаны общедоступные инструменты и криптографические

библиотеки для их создания. Разработан Telegram-бот для проверки сертификата открытого ключа электронной цифровой подписи и представлен его интерфейс.

Список литературы

1. Курочкина, Е. А. Возможности использования электронно-цифровой подписи в современных условиях / Е. А. Курочкина, Т. М. Тарасова // Наука и образование транспорту. 2020. № 1. С. 253–256.
2. Niva Elkin-Koren. Copyrights in Cyberspace – Rights without Laws // *Chicago-Kent Law Review*. 1998. Vol. 73, Iss. 4. P. 1156–1199.
3. Злотникова, Г. К. Влияние инфраструктуры открытых ключей на экономическую и информационную безопасность предприятия / Г. К. Злотникова, И. С. Денисов // Книга «Фундаментальная и прикладная наука: состояние и тенденции развития». Петрозаводск, 2022. С. 263–276.
4. Акушуев, Р. Т. Инфраструктура открытых ключей / Р. Т. Акушуев // Modern Science. 2020. № 1–2. С. 213–215.
5. Михневич, С. Ю. Онлайн-проверка достоверности электронных документов / С. Ю. Михневич, И. О. Толох // International Journal of Information and Communication Technologies. 2021.

References

1. Kurochkina E. A., Tarasova T. M. (2020) Possibilities of Using Electronic Digital Subscription in Modern Conditions. *Science and Education Transport*. (1), 253–256 (in Russian).
2. Niva Elkin-Koren (1998) Copyrights in Cyberspace – Rights without Laws. *Chicago-Kent Law Review*. 73 (4), 1156–1199.
3. Zlotnikova G. K., Denisov I. S. (2022) Influence of Public Key Infrastructure on the Economic and Information Security of an Enterprise. *Book "Fundamental and Applied Science: State and Development Trends"*. Petrozavodsk. 263–276 (in Russian).
4. Akushuev R. T. (2020) Public Key Infrastructure. *Modern Science*. (1–2), 213–215 (in Russian).
5. Mikhnevich S. Yu., Tolokh I. O. (2021) Online Check for Availability of Electronic Documents. *International Journal of Information and Communication Technology* (in Russian).

Вклад авторов

Толох И. О. осуществил реализацию сервиса.
Михневич С. Ю. и Сенкевич А. Ю. обосновали и выполнили постановку задачи.

Authors' contribution

Tolokh I. O. implemented the service.
Mikhnevich S. Yu. and Siankevich A. Yu. substantiated completed the statement of the problem.

Сведения об авторах

Толох И. О., лаборант кафедры инфокоммуникационных технологий Белорусской государственной академии связи

Михневич С. Ю., к.ф.-м.н., доцент, заведующий кафедрой инфокоммуникационных технологий Белорусской государственной академии связи

Сенкевич А. Ю., лаборант кафедры инфокоммуникационных технологий Белорусской государственной академии связи

Адрес для корреспонденции

220076, Республика Беларусь,
г. Минск, ул. Ф. Скорины, 8/2
Белорусская государственная академия связи
Тел.: +375 17 356-96-06
E-mail: s.mikhnevich@bsac.by
Михневич Светлана Юрьевна

Information about the authors

Tolokh I. O., Laboratory Assistant at the Department of Infocommunication Technologies of the Belarusian State Academy of Communications

Mikhnevich S. Yu., Cand. of Sci., Associate Professor, Head at the Department of Infocommunication Technologies of the Belarusian State Academy of Communications

Siankevich A. Yu., Laboratory Assistant at the Department of Infocommunication Technologies of the Belarusian State Academy of Communications

Address for correspondence

220076, Republic of Belarus,
Minsk, F. Skoriny St., 8/2
Belarusian State Academy of Communications
Tel.: +375 17 356-96-06
E-mail: s.mikhnevich@bsac.by
Mikhnevich Svetlana Yurievna