УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ АКТИВАЦИИ ПОДПИСИ В СИСТЕМЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

В.А. Герасимов
Государственное предприятие «Научно-исследовательский институт технической защиты информации», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается система электронной цифровой подписи на основе виртуальной инфраструктуры и ее преимущества перед традиционными решениями. Внедрение такой системы позволяет пользователям избежать необходимости хранения личных ключей, однако связано с таким риском информационной безопасности, как взлом сервера. Для минимизации этого риска предложен протокол активации подписи, который обеспечивает контроль над использованием личного ключа. Автор статьи анализирует реализации протокола активации подписи, основывающиеся на различных методах аутентификации. Представлены ключевые характеристики и проект разработанного протокола активации подписи, направленный на повышение уровня безопасности. В результате исследования определены уязвимости и векторы атак, что позволяет в дальнейшем совершенствовать протоколы активации подписи и повысить доверие пользователей к системе электронной цифровой подписи на основе виртуальной инфраструктуры.
Ключевые слова: облачная электронная цифровая подпись на основе виртуальной инфраструктуры; данные активации подписи; протокол активации подписи.

COMPARATIVE ANALYSIS OF SIGNATURE ACTIVATION PROTOCOLS IN AN ELECTRONIC DIGITAL SIGNATURE SYSTEM BASED ON A VIRTUAL INFRASTRUCTURE

V.A. Herasimov
Scientific production republican unitary enterprise "Research institute for technical protection of information", Minsk, Republic of Belarus

Abstract. The article discusses an electronic digital signature system based on a virtual infrastructure and its advantages over traditional solutions. The implementation of such a system allows users to avoid the need to store private keys, however, it is associated with such an information security risk as hacking the server. To minimize this risk, a signature activation protocol has been proposed that provides control over the use of a private key. The author of the article analyzes the implementation of the signature activation protocol based on various authentication methods. The key characteristics and draft of the developed signature activation protocol aimed at increasing the security level are presented. As a result of the study, vulnerabilities and attack vectors were identified, which makes it possible to further improve signature activation protocols and increase user confidence in an electronic digital signature system based on a virtual infrastructure.
Keywords: cloud-based electronic digital signature based on virtual infrastructure; signature activation data; signature activation protocol.

Введение

Система электронной цифровой подписи на основе виртуальной структуры (далее – облачная ЭЦП) имеет очевидные преимущества для пользователей по сравнению с традиционными решениями использования электронной цифровой подписи, основанными на использовании USB-токенов или специальных SIM-карт (далее – ЭЦП).

Несмотря на обозначенное преимущество системы облачной ЭЦП, следует отметить, что ее эксплуатация сопряжена со следующими рисками информационной безопасности:

– взлома сервера [1];

– компрометация сервера

Для минимизации указанных рисков необходимо применять протокол активации подписи (далее – ПАП). Этот протокол реализуется между двумя сторонами: клиентской программой пользователя (далее – КПП) и сервером подписи (далее – СП). Основная задача протокола заключается в том, чтобы сервер получил разрешение от пользователя на использование его ключа для подписи определенного документа.

Консорциум облачной подписи (Cloud Signature Consortium, далее – CSC) [2] представляет собой объединение компаний и научных учреждений, занимающееся разработкой технических стандартов в сфере облачной ЭЦП. На данный момент ключевым документом, созданным в рамках CSC, является спецификация, которая описывает программный интерфейс (API) для взаимодействия со службами облачной подписи, а также шаги, необходимые для получения электронного документа.

В рамках анализа уязвимостей ПАП, а также анализа векторов атак на существующие системы, использующие ПАП, были выполнены следующие задачи:

– определены ключевые характеристики и особенности различных протоколов активации подписи;

– проанализированы преимущества и недостатки каждого протокола с точки зрения безопасности, производительности и удобства использования;

– сформирован проект ПАП, который опирается на данные [3], полученные при анализе.

Наиболее значимые результаты проведенного исследования представлены далее.

Основная часть

В настоящее время существует несколько реализаций ПАП [2], которые предоставляют возможность создания электронного документа с использованием технологии облачной ЭЦП использующих либо один из видов аутентификации из перечня или же их комбинацию:

– базовая аутентификация (Basic Authentication) (рис. 1, а);

– OAuth2 аутентификация (OAuth2 with Authentication Code flow) (рис. 1, б);

– аутентификация с использованием PIN (credenal protected by a PIN) (рис. 2, а);

– аутентификация с использованием OTP (credenal protected by an «online» OTP (based on SMS)) (рис. 2, б);

– аутентификация с использованием PIN и OTP (credenal protected by a PIN and an «online» OTP (based on SMS)) (рис. 3).

В общем виде, любой из ПАП разделяется на блоки.

1. Блок SysAuth - пользователь проходит аутентификацию как субъект системы электронного документооборота.

2. Блок Submit: пользователь инициирует подпись документов без атрибутов.

3. Блок CredAuth1: начало аутентификации пользователя на доступ к личному ключу.

4. Блок AddSignedAttrs: добавление подписываемых атрибутов.

5. Блок Confirm: пользователь дает согласие на подпись документов.

6. Блок CredAuth2: завершение аутентификации пользователя на доступ к личному ключу.

7. Блок IssueDAP: выпуск данных активации подписи (далее – ДАП).

8. Блок Sign: подпись документов.

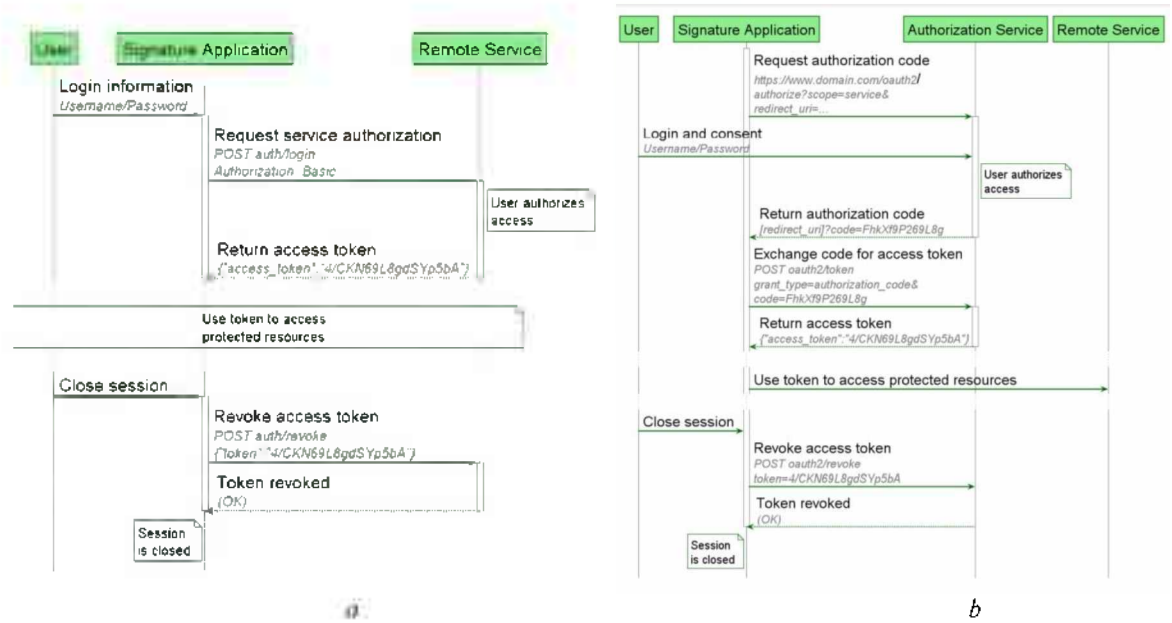
9. Блок AddUnsignedAttrs: добавление неподписываемых атрибутов.

Разработанный в рамках исследования ПАП опирается на протоколы, использующие PIN-код к личному ключу пользователя и OTP-пароль, а также дополнительные механизмы защиты информации [3].

Разработанный ПАП может противостоять следующим атакам.

1. Перехват аутентификатора, при котором противник перехватывает аутентификаторы в момент их ввода пользователем и определяет по ним будущие аутентификаторы.
2. Угадывание аутентификатора, когда противник угадывает аутентификатор в ходе выполнения протокола аутентификации.
3. Подбором аутентификатора, при котором противник в последовательных сеансах аутентификации пытается угадать аутентификатор, проверяя различные его варианты.
4. Перехват сообщений протокола, при котором противник перехватывает сообщения протокола и обрабатывает их, надеясь получить информацию, которая позволит выдать себя за пользователя.
5. Противник посередине встраивается во взаимодействие между пользователем и системой во время выполнения протокола аутентификации;
6. Повторное использование данных аутентификации, которые уже ранее использовался законным пользователем;

Противник пытается использовать метод подмены ответов, при котором вмешивается в передачу данных между сторонами протокола и в ответ на аутентификатор одного пользователя возвращает данные другого.



a b

Рис. 1. Вид ПАП: *a* – Базовая аутентификация *a*; *b* – OAuth2 аутентификация
Fig. 1. Form SAP: *a* – Basic Authentication; *b* – OAuth2 with Authentication Code flow

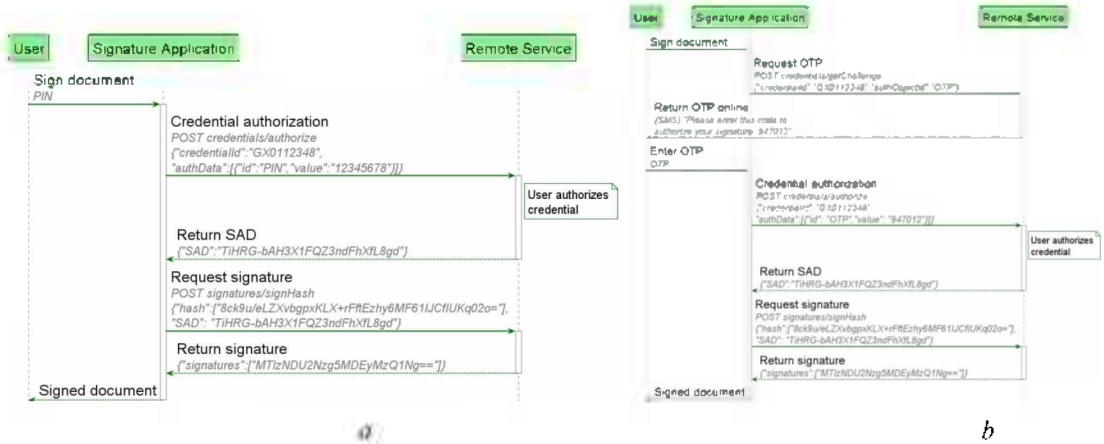


Рис. 2. Вид ПАП: *a* – Аутентификация с использованием PIN: *b* – Аутентификация с использованием OTP
Fig. 2. Form SAP: *a* – PIN authentication: *b* – OTP authentication

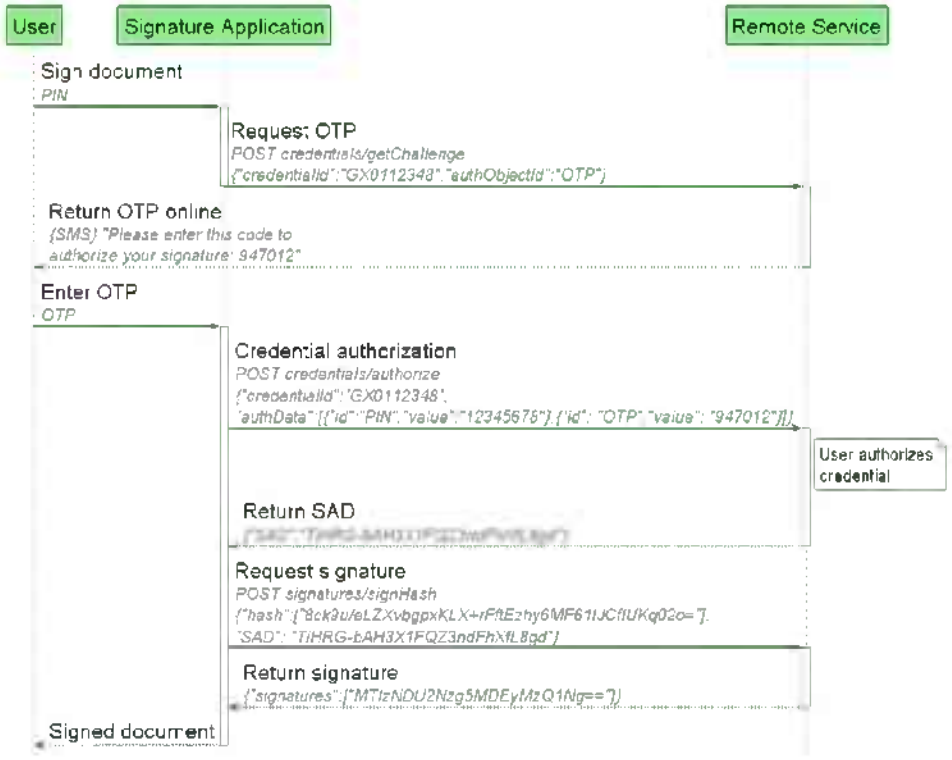


Рис. 3. ПАП, использующий аутентификацию, основанную на PIN и OTP
Fig. 3. SAP using PIN-code and OTP-based authentication

Заключение

Использование ПАП позволяет существенно повысить уровень контроля над данными, обеспечивая дополнительную аутентификацию и защиту от подмены подписываемого документа [3]. Тем не менее, даже с внедрением ПАП, остается возможность атаки со стороны злоумышленников.

Модификация ПАП направлена на минимизацию рисков при работе с технологией облачной ЭЦП. В дальнейшем исследования будут направлены на анализ уязвимости существующих систем, использующих облачную ЭЦП, чтобы обеспечить их безопасность и эффективность. Таким образом, сочетание

современных технологий и надежных протоколов аутентификации станет ключевым аспектом в поднятии уровня доверия граждан технологии облачной ЭЦП.

Список использованных источников

1. Сазонова. Д. В.Технологии использования облачной ЭЦП / Д. В. Сазонова, В. В. Козловский // Информационные технологии. Физика и математика : материалы 88-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 29 января – 16 февраля 2024 г. – Минск: БГТУ, 2024. – С. 30-35.

2. Теоретическая и прикладная криптография : материалы II Междунар. науч. конф., Минск. 19–20 окт. 2023 г. / Белорус. гос. ун-т ; редкол.: Ю. С. Харин (гл. ред.) [и др.]. – Минск : БГУ, 2023. – С. 250-260.

3. Герасимов, В. А. Механизмы защиты информации при выработке облачной электронной цифровой подписи / В. А. Герасимов // *Комплексная защита информации : материалы XXVIII научно-практической конференции*. г. Гомель. 23-25 мая 2023 г. / Белорусский государственный университет транспорта. – Гомель. 2023. – С. 257–261.

4. Josang A., Alfayyadh B. Robust WYSIWYS: A Method for Ensuring that What You See Is What You Sign // Sixth Australasian Information Security Conference (AISC 2008). т. 81. – Wollongong, NSW, Australia : ACS. 2008. – С. 53–58.

References

1. Sazonova, D. V. Technologies for using cloud EDS / D. V. Sazonova, V. V. Kozlovsky // Information technologies. Physics and Mathematics : materials of the 88th Scientific and Technical Conference of the teaching staff, researchers and aspirants (with international participation), Minsk, January 29 – February 16, 2024 – Minsk: BSTU, 2024. – pp. 30-35. (inRussian)

2. Theoretical and Applied cryptography : proceedings of the II International Scientific Conference. Minsk, October 19-20, 2023 / Belarusian State University ; editor: Yu. S. Kharin (chief editor) [and others]. – Minsk : BSU, 2023. – pp. 250-260. (inRussian)

3. Gerasimov, V. A. Information protection mechanisms in the development of cloud-based electronic digital signatures / V. A. Gerasimov // Integrated information protection : proceedings of the XXVIII scientific and practical conference, Gomel, May 23-25, 2023 / Belarusian State University of Transport. Gomel, 2023. pp. 257-261. (inRussian)

4. Josang A., Alfayad B. Reliable WYSIWYS: a method to ensure that what you see corresponds to what you sign // Sixth Australasian Conference on Information Security. (AISC, 2008). vol. 81. – Wollongong, New South Wales, Australia : ACS. 2008. – pp. 53-58.

Сведения об авторе

Герасимов В.А., магистр, сотрудник. Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», vger@niitzi.by.

Information about the author

Gerasimov V.A., Master's degree, employee, Scientific production republican unitary enterprise "Research institute for technical protection of information", vger@niitzi.by.