СРАВНИТЕЛЬНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ ПОДХОДОВ К АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В СИСТЕМАХ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

В.А. Герасимов

Научно-исследовательский институт технической защиты информации, г. Минск, Республика Беларусь

Аннотация. Проведен теоретический анализ безопасности трех подходов к аутентификации пользователя в Hardware Security Module (HSM) для систем электронной цифровой подписи на основе виртуальной инфраструктуры: 1) централизованный контроль на основе данных активации подписи (авторский подход); 2) разделение ключа с кворумом M-of-N; 3) разделение ключа с хранением части на стороне пользователя. Проведен анализ соответствия перечисленных подходов стандарту PKCS#11, определяющему унифицированный интерфейс взаимодействия с HSM. Предложены модели для расчета вероятностей успешной атаки для этих подходов. Обосновано, что авторский подход обеспечивает оптимальный баланс между безопасностью и сложностью реализации.

Ключевые слова: электронная цифровая подпись; виртуальная инфраструктура; HSM; аутентификация; данные активации подписи; PKCS#11.

COMPARATIVE ANALYSIS OF SECURITY OF USER AUTHENTICATION APPROACHES IN ELECTRONIC DIGITAL SIGNATURE SYSTEMS BASED ON VIRTUAL INFRASTRUCTURE

V.A. Gerasimov
Research Institute for Technical Protection of Information,
Minsk, Republic of Belarus

Abstract. A theoretical security analysis of three approaches to user authentication in the Hardware Security Module (HSM) for electronic digital signature systems based on a virtual infrastructure is performed: 1) centralized control based on signature activation data (the author's approach); 2) key sharing with M-of-N quorum; 3) key sharing with storage of a part on the user side. An analysis of the compliance of the listed approaches with the PKCS#11 standard, which defines a unified interface for interaction with the HSM, is carried out. Models for calculating the probabilities of a successful attack for these approaches are proposed. It is substantiated that the author's approach provides an optimal balance between security and implementation complexity.
Keywords: electronic digital signature; virtual infrastructure; HSM; authentication; signature activation data; PKCS#11.

Введение

Обеспечение безопасности личного ключа является критической задачей при выработке электронной цифровой подписи (ЭЦП). Использование HSM, т. е. аппаратных модулей безопасности, позволяет минимизировать риски компрометации, однако вопрос надежной аутентификации пользователя перед HSM остается предметом научных дискуссий [1, 2]. Стандарт PKCS#11 определяет платформонезависимый программный интерфейс для взаимодействия с криптографическими устройствами [5]. Этот стандарт поддерживается большинством современных HSM и криптографических токенов, что делает его важным критерием при оценке практической применимости рассматриваемых подходов. Существующие решения можно классифицировать на три категории: централизованные протоколы с активацией подписи, схемы разделения ключа с пороговым доступом (кворум) и схемы с распределенным хранением ключа между HSM и клиентом. Целью данной работы является сравнительный анализ указанных подходов с точки зрения безопасности, соответствия стандарту PKCS#11 и практической реализуемости.

Основная часть

В рамках исследования были рассмотрены три подхода аутентификации и доступа к ключу в HSM для создания ЭЦП в системах на основе виртуальной инфраструктуры.

Подход 1. Протокол активации подписи с использованием ДАП (авторский). Пользователь хэширует документ и аутентифицируется, генерируя уникальные данные активации подписи (ДАП). Хэш документа через сервер подписи и ДАП (по защищенному каналу) поступают в HSM, который после проверки ДАП вырабатывает подпись ключом пользователя. Важной особенностью является то, что вызов криптографических функций HSM осуществляется от имени СП, но только при наличии валидных ДАП.

Подход 2. Разделение ключа по схеме M-of-N. Личный ключ K разделяется на N частей (например, 5) с использованием алгоритма разделения секрета Шамира [3] и распределяется по независимым HSM. Для сборки ключа и подписания необходимо получить и объединить M частей (например, 3) от разных модулей.

Подход 3. Разделение ключа на две части (HSM и клиент). Ключ K разделен на две компоненты: K_{HSM}, хранящуюся в HSM, и K_{client}, хранящуюся в защищенной области на устройстве пользователя. Подпись генерируется путем объединения результатов вычислений от обеих частей.

Результаты сравнительного анализа подходов с учетом вероятностных моделей и соответствия стандарту PKCS#11.

Результаты сравнительного анализа подходов
Results of the approaches comparative analysis

Параметр / Угроза	Подход 1	Подход 2	Подход 3
1	2	3	4
Вероятность компрометации ключа	$p \cdot q$ $(\sim 10^{-9})$	$\sum_{k=M}^{N} C_N^k p^k (1-p)^{N-k}$ $(\sim 10^{-8})$	$p \cdot p_c$ $(\sim 10^{-5})$
Соответствие PKCS#11	Полное (стандартная функция C_Sign с атрибутом CKA_ALWAYS_AUTHENTICATE; вызов от имени СП)	Частичное (требуются проприетарные расширения)	Частичное (требуется экспортируемый ключ, CKA_EXTRACTABLE = true)
Стойкость к сговору	Высокая (требуется участие пользователя)	Низкая (возможен сговор M операторов)	Средняя
Зависимость от безопасности клиента	Низкая (клиент только генерирует ДАП)	Очень низкая (ключ не хранится у клиента)	Высокая (часть ключа – у клиента)
Сложность реализации	Низкая	Высокая (синхронизация, управление долями)	Средняя

Заключение

1. Авторский подход может быть реализован с использованием стандартных механизмов (C_Sign с атрибутом CKA_ALWAYS_AUTHENTICATE) [2; 5]. Важной особенностью является то, что вызов криптографических функций осуществляется от имени сервера подписи, но только при наличии валидных ДАП, что гарантируется аппаратными механизмами HSM. Распределенный подход M-of-N требует проприетарных расширений API [3], а подход с разделением ключа – установки атрибута CKA_EXTRACTABLE, что снижает безопасность [5].

2. Авторский подход превосходит по теоретической стойкости подход с кворумом M-of-N при типичных значениях вероятностей компрометации.

3. Подход с разделением ключа на две части демонстрирует критическую зависимость от безопасности клиентской среды, что делает его наименее предпочтительным для систем с высокими требованиями к защите.

4. Авторский подход демонстрирует наилучший баланс между количественными показателями безопасности, соответствием отраслевым стандартам и сложностью реализации, что делает его предпочтительным для внедрения в системах электронной цифровой подписи на основе виртуальной инфраструктуры [1, 2, 4].

Список использованных источников

1. Герасимов, В. А. Механизмы защиты информации при выработке облачной электронной цифровой подписи / В. А. Герасимов, М. А. Казловский, О. В. Бойправ // Комплексная защита информации: материалы XXVIII науч.-практ. конф. — Гомель: БелГУТ, 2023. — С. 257–261.

2. Герасимов, В. А. Использование системы облачной электронной подписи для организации электронного голосования / В. А. Герасимов, М. А. Казловский // Цифровая трансформация. — 2024. — Т. 30, № 1. — С. 52–62.

3. Шамир, А. Как разделить секрет / А. Шамир // Коммуникации АКМ. — 1979. — Т. 22, № 11. — С. 612–613.

4. Герасимов, В. А. Метод обнаружения событий информационной безопасности в системах облачной подписи / В. А. Герасимов, О. В. Бойправ // Цифровая трансформация. — 2024. — Т. 30, № 2. — С. 77–84.

5. RSA Laboratories. PKCS #11 v2.40: Cryptographic Token Interface Standard. — 2015. — 422 с.

References

1. Herasimau V. A., Kazlouski M. A., Boiprav O. V. (2023) Information protection mechanisms in the development of cloud-based electronic digital signatures. *Integrated*

Information Protection: Proceedings of the XXVIII Scientific and Practical Conference. Gomel, BelSUT, pp. 257–261. (In Russian)

2. Herasimau V. A., Kazlouski M. A. (2024) Using a Cloud-Based Electronic Signature System for Organizing Electronic Voting. *Digital Transformation*. 30 (1), 52–62. (In Russian)

3. Shamir A. (1979) How to share a secret. *Communications of the ACM*. 22 (11), 612–613.

4. Gerasimov V. A., Boyprav O. V. (2024) Method for Information Security Events Detection in a Cloud Signature Systems. *Digital Transformation*. 30 (2), 77–84. (In Russian)

5. RSA Laboratories. (2015) *PKCS #11 v2.40: Cryptographic Token Interface Standard*.

Сведения об авторе

Герасимов В. А., магистр, сотрудник Научно-исследовательского института технической защиты информации, e-mail: vger@niitzi.by.

Information about the author

Gerasimov V., Master of Science, Researcher at the Research Institute for Technical Protection of Information, e-mail: vger@niitzi.by.