Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 30 октября 2020 года № 21549.

В соответствии с подпунктом 13-3) пункта 1 статьи 5 Закона Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи" ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре.

2. Комитету государственных услуг Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в установленном законодательном порядке обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Министр цифрового развития,
инноваций и аэрокосмической
промышленности Республики Казахстан *Б. Мусин*

"СОГЛАСОВАН"
Министерство торговли и интеграции
Республики Казахстан

"СОГЛАСОВАН"

Комитет национальной безопасности
Республики Казахстан

Утверждены
приказом Министра цифрового
развития, инноваций и
аэрокосмической
промышленности
Республики Казахстан
от 27 октября 2020 года
№ 405/НҚ

Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре

Глава 1. Общие положения

1. Настоящие Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре (далее- Правила) разработаны в соответствии с Законом Республики Казахстан "Об электронном документе и электронной цифровой подписи" (далее - Закон) и определяют порядок создания, использования, и хранения закрытых ключей электронной цифровой подписи в облачных сервисах.

Сноска. Пункт 1 – в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 17.03.2023 № 95/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

2. В настоящих Правилах применяются следующие понятия:

1) биометрическая аутентификация – комплекс мер, идентифицирующих личность на основании физиологических и неизменных биологических признаков;

2) блокчейн - информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования;

3) многофакторная аутентификация – способ проверки подлинности пользователя при помощи комбинации различных параметров, в том числе генерации и ввода паролей или аутентификационных признаков (цифровых сертификатов, токенов, смарт-карт, генераторов одноразовых паролей и средств биометрической идентификации);

4) удостоверяющий центр (далее - УЦ) - юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу

электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

5) владелец регистрационного свидетельства (далее - владелец) – физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;

6) электронная цифровая подпись (далее - ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

7) открытый ключ ЭЦП - последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

8) закрытый ключ ЭЦП - последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;

9) средства электронной цифровой подписи - совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи;

10) облачная ЭЦП – сервис удостоверяющего центра, позволяющий создавать, использовать, хранить и удалять закрытые ключи электронной цифровой подписи в HSM удостоверяющего центра, где доступ к закрытому ключу осуществляется владельцем удалҰнно посредством не менее двух факторов аутентификации, одним из которых является биометрическая;

11) хэш – преобразование массива входных данных произвольной длины в битовую сторону фиксированной длины;

12) аппаратный криптографический модуль (Hardware Security Module) (далее - HSM) - аппаратный криптографический модуль предназначенный для шифрования информации и управления открытыми и закрытыми ключами ЭЦП.

Сноска. Пункт 2 – в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 17.03.2023 № 95/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Глава 2. Порядок создания закрытых ключей ЭЦП в удостоверяющем центре

3. Закрытые ключи ЭЦП создаются УЦ:

1) на носителе ключевой информации владельца, которая передается владельцу;

2) в облачной ЭЦП.

4. Закрытые ключи ЭЦП облачной ЭЦП генерируются строго внутри HSM. Закрытый ключ не извлекается из HSM в открытом виде.

При этом HSM:

1) соответствует не ниже третьего уровня безопасности в соответствии с требованиями, установленными СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования";

2) спроектирован с физической защитой периметра (защита от вскрытия корпуса), использующей датчики для определения факта вскрытия корпуса и последующего удаления ключевой информации, необходимой для HSM.

3) соответствует нормам эффективности защиты и методикам оценки защищенности информации и технических средств согласно требованиям действующего законодательства Республики Казахстан.

5. Архивирование ключевой информации с HSM возможно только в зашифрованном виде и только с разделением ключа шифрования по схеме M из N (не менее 3 из 5). Ключи шифрования по схеме M из N хранятся на защищенных токенах. Для государственных УЦ N токенов постоянно хранится в уполномоченном органе в сфере информатизации, в органах национальной безопасности и у УЦ. Защищенные токены используются только при восстановлении архива на резервном HSM.

6. Перед созданием закрытого ключа ЭЦП и выпуском регистрационного свидетельства ЭЦП владелец дает согласие на сбор и обработку персональных данных.

Владелец проходит аутентификацию:

1) удаленно, с использованием многофакторной аутентификации, одним из методов является биометрическая аутентификация;

2) в центре регистрации УЦ с использованием биометрической аутентификации, при необходимости пройдя процедуру сбора биометрических данных, УЦ обеспечивает хранение биометрических данных.

Владелец дает согласие на хранение закрытого ключа ЭЦП в облачной ЭЦП УЦ.

7. После создания, закрытый ключ ЭЦП сохраняется в HSM в зашифрованном виде с использованием стандарта ГОСТ 28147-89. В качестве секретных значений участвуют пароль, заданный владельцем который в УЦ не хранится. УЦ, для проверки пароля от закрытого ключа владельца, хранит хэш пароля в HSM.

Глава 3. Порядок использования закрытых ключей ЭЦП, хранящихся в удостоверяющем центре

8. При использовании закрытых ключей ЭЦП, хранящихся в УЦ, владелец проходит многофакторную аутентификацию, одним из методов является биометрическая аутентификация.

9. Подписание электронных документов осуществляется в памяти HSM путем передачи подписываемого файла или его хэш в HSM.

10. При аутентификации владельца в УЦ, передача пароля от владельца (браузер, мобильное приложение) в HSM производится в зашифрованном виде, при этом шифрование пароля производится на стороне владельца, в персональном компьютере или смартфоне.

11. Восстановление пароля от закрытого ключа ЭЦП в облачной ЭЦП не осуществляется.

12. УЦ предоставляет владельцу закрытого ключа облачной ЭЦП доступ к информации о всех подписанных электронных документах через личный кабинет УЦ. Срок хранения информации обо всех подписанных электронных документах составляет не менее одного года после истечения срока действия регистрационного свидетельства владельца.

13. В случае выявления факта компрометации закрытых ключей электронной подписи владельцев регистрационных свидетельств, УЦ незамедлительно публикует на своем интернет-ресурсе информацию о данном факте и принятых мерах по минимизации нанесенного ущерба.

14. УЦ обеспечивает протоколирование следующих событий:

1) формирование закрытого ключа ЭЦП облачной ЭЦП;

2) использование закрытого ключа ЭЦП облачной ЭЦП;

3) удаление (стирание) закрытого ключа ЭЦП облачной ЭЦП.

Срок хранения протоколов работы составляет один год с даты истечения срока действия регистрационного свидетельства.

При протоколировании действий записывается следующая информация:

1) идентификатор владельца;

2) дата, время;

3) событие.

15. Протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Применяемая для этого блокчейн доступна в Интернет.

Глава 4. Порядок хранения закрытых ключей ЭЦП в удостоверяющем центре

16. УЦ обеспечивает защиту закрытых ключей ЭЦП в УЦ.

17. Срок хранения закрытых ключей ЭЦП в облачной ЭЦП описывается в правилах применения регистрационных свидетельств УЦ утверждаемых УЦ в соответствии подпункта 2-1) пункта 1 статьи 21 Закона.

18. Согласно пункта 92 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 (далее - ЕТ), программно-аппаратное обеспечение облачной ЭЦП размещается на территории Республики Казахстан.

19. Защита закрытых ключей обеспечивается комплексом организационных, программных и технических мероприятий в соответствии с требованиями описанные в ЕТ.

20. УЦ обеспечивает отсутствие возможности подписания электронных документов с использованием закрытых ключей ЭЦП облачной ЭЦП без многофакторной аутентификации.

Сноска. Пункт 20 – в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 17.03.2023 № 95/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

21. Выполнение требований настоящих Правил является необходимым условием при аккредитации УЦ в соответствии с Правилами проведения аккредитации удостоверяющих центров, утвержденных приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 1 июня 2020 года № 224/НҚ (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 20815).