# Об утверждении Правил хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 11 августа 2026 года № 474/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 12 августа 2026 года № 39573

В соответствии с частью четвертой пункта 3 статьи 51 Цифрового кодекса Республики Казахстан, ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые правила хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре.

2. Признать утратившим силу:

1) приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ "Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 21549);

2) приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 17 марта 2023 года № 95/НҚ "О внесении изменений в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ "Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 32129).

3. Департаменту цифровых решений Министерства искусственного интеллекта и цифрового развития Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

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

2) размещение настоящего приказа на интернет-ресурсе Министерства искусственного интеллекта и цифрового развития 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 искусственного интеллекта и цифрового развития Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

4. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра искусственного интеллекта и цифрового развития Республики Казахстан.

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

*Заместитель Премьер-Министра –*
*Министр искусственного интеллекта и*
*цифрового развития Республики Казахстан* *Ж. Мадиев*

"СОГЛАСОВАН"
Министерство торговли и интеграции
Республики Казахстан

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

Утверждены приказом
Заместитель Премьер-
Министра – Министр
искусственного интеллекта
и цифрового развития
Республики Казахстан
от 11 августа 2026 года
№ 474/НҚ

## Правила хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре

### Глава 1. Общие положения

1. Настоящие Правила хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре (далее – Правила) разработаны в соответствии с частью четвертой пункта 3 статьи 51 Цифрового Кодекса Республики Казахстан (далее – Кодекс) и определяют порядок хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре.

2. В настоящих Правилах применяются следующие понятия:

1) аппаратный криптографический модуль (Hardware Security Module) (далее – HSM ) – аппаратный модуль, предназначенный для обеспечения безопасности криптографических ключей при их создании, использовании и хранении, а также выполнения криптографических операций с их использованием;

2) биометрическая аутентификация – процесс сравнения и проверки соответствия биометрических данных для цели установления личности;

3) облачный закрытый ключ электронной цифровой подписи (далее – облачный закрытый ключ ЭЦП) – закрытый ключ электронной цифровой подписи, который создается, хранится и используется в облачном хранилище закрытых ключей электронной цифровой подписи;

4) 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 аутентификации);

5) удостоверяющий центр (далее – УЦ) – юридическое лицо, созданное в соответствии с законодательством Республики Казахстан, которое подтверждает достоверность сертификатов открытых ключей электронной цифровой подписи, принадлежность и действительность открытых ключей электронной цифровой подписи ;

6) защищенный носитель ключевой информации – специализированный носитель, в котором для защиты хранящихся закрытых ключей электронной цифровой подписи используются средства криптографической защиты информации, имеющие сертификат соответствия требованиям национального стандарта Республики Казахстан СТ РК 1073 -2007 "Средства криптографической защиты информации. Общие технические требования" либо СТ РК 1073-2025 "Требования к информационной безопасности и процессам жизненного цикла";

7) хэш – значение фиксированной длины, получаемое из данных и применяемое для проверки их целостности;

8) электронная цифровая подпись (далее – ЭЦП) – цифровая запись (набор цифровых данных), созданная с использованием закрытого ключа электронной цифровой подписи и средств электронной цифровой подписи, подтверждающая достоверность электронного документа, его принадлежность и неизменность содержания;

9) средства электронной цифровой подписи – совокупность программного обеспечения и объектов цифровой инфраструктуры, используемых для создания и проверки подлинности электронной цифровой подписи;

10) открытый ключ электронной цифровой подписи – цифровые данные, предназначенные для подтверждения подлинности электронной цифровой подписи;

11) владелец сертификата открытого ключа электронной цифровой подписи (далее - владелец) – физическое или юридическое лицо, на имя которого выдан сертификат

открытого ключа электронной цифровой подписи, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в сертификате открытого ключа электронной цифровой подписи;

12) сертификат открытого ключа электронной цифровой подписи (далее – сертификат) – цифровая запись, удостоверенная электронной цифровой подписью удостоверяющего центра, которая служит для подтверждения соответствия электронной цифровой подписи требованиям, установленным Цифровым Кодексом Республики Казахстан;

13) облачное хранилище закрытых ключей электронной цифровой подписи (далее – облачное хранилище) – сервис удостоверяющего центра, позволяющий владельцу создавать, хранить, использовать и удалять закрытые ключи электронной цифровой подписи в аппаратном криптографическом модуле удостоверяющего центра после прохождения многофакторной аутентификации, одним из факторов которой является биометрическая;

14) закрытый ключ электронной цифровой подписи – цифровые данные, предназначенные для создания электронной цифровой подписи с использованием средств электронной цифровой подписи.

## Глава 2. Порядок хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре

3. Облачный закрытый ключ ЭЦП создается УЦ в облачном хранилище.

4. Облачный закрытый ключ ЭЦП генерируется строго внутри HSM и не извлекается из HSM в открытом виде.

При этом HSM:

1) соответствует не ниже третьего уровня безопасности в соответствии с требованиями, установленными национальным стандартом Республики Казахстан СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования" либо СТ РК 1073-2025 "Требования к информационной безопасности и процессам жизненного цикла";

2) спроектирован с физической защитой периметра (защита от вскрытия корпуса), предусматривающей использование датчиков вскрытия с автоматическим удалением закрытых ключей электронной цифровой подписи УЦ при нарушении целостности корпуса HSM.

5. Архивирование облачных закрытых ключей ЭЦП осуществляется в целях обеспечения восстановления работоспособности облачного хранилища при отказе основного оборудования, аварийных ситуациях, утрате работоспособности HSM, а также при проведении мероприятий по замене, модернизации или переносу оборудования.

Архивирование облачных закрытых ключей ЭЦП из HSM допускается исключительно в зашифрованном виде с применением механизма разделения ключа шифрования по схеме M из N (не менее 3 из 5), части которого хранятся на защищенных носителях ключевой информации. Восстановление из архива на резервном оборудовании должно быть возможно только при наличии не менее M компонентов из N.

Допускается многоуровневая схема управления ключами при условии, что конечная зависимость от M компонентов из N сохраняется для любого сценария восстановления.

Архивные копии облачных закрытых ключей ЭЦП хранятся до удаления соответствующих облачных закрытых ключей ЭЦП в случаях, предусмотренных пунктом 8 настоящих Правил.

Уничтожение архивных копий облачных закрытых ключей ЭЦП осуществляется в порядке, установленном внутренними документами удостоверяющего центра.

6. При создании облачного закрытого ключа ЭЦП и выпуске сертификата заявитель :

1) предоставляет согласие на сбор и обработку персональных данных;

2) проходит многофакторную аутентификацию, включающую биометрическую аутентификацию на основе изображения лица с подтверждением, что изображение лица принадлежит живому человеку, исключающим использование фотографии, видеозаписи или иного имитирующего материала, осуществляемую непосредственно при создании облачного закрытого ключа ЭЦП;

3) устанавливает пароль на облачный закрытый ключ ЭЦП.

Допускается использование встроенных средств устройства пользователя, обеспечивающих защищ¥нное хранение пароля и контроль доступа к нему.

7. Созданный облачный закрытый ключ ЭЦП сохраняется в HSM в зашифрованном виде. В качестве секретного значения, используемого для криптографической защиты облачного закрытого ключа ЭЦП, применяется пароль, установленный владельцем, который не хранится в удостоверяющем центре. Для проверки пароля в HSM хранится его хэш. Пароль восстановлению не подлежит. В случае утраты пароля использование соответствующего облачного закрытого ключа ЭЦП не допускается.

8. Облачный закрытый ключ ЭЦП удаляется из облачного хранилища в следующих случаях:

1) при отзыве сертификата облачного закрытого ключа ЭЦП;

2) при истечении срока действия сертификата облачного закрытого ключа ЭЦП.

9. Использование облачного закрытого ключа ЭЦП осуществляется после прохождения владельцем многофакторной аутентификации, включающей подтверждение пароля и биометрическую аутентификацию на основе изображения

лица с подтверждением, что изображение лица принадлежит живому человеку, исключающим использование фотографии, видеозаписи или иного имитирующего материала.

10. Подписание электронных документов осуществляется в памяти HSM путем передачи подписываемого файла либо его хэша в HSM. Передаваемые данные не подлежат хранению после завершения операции подписания.

11. При аутентификации владельца в УЦ передача данных аутентификации осуществляется в зашифрованном виде, при этом их шифрование производится на стороне владельца с использованием персонального компьютера либо мобильного устройства.

12. В случае выявления факта компрометации облачного закрытого ключа ЭЦП владельца сертификата УЦ отзывает сертификат ЭЦП и публикует информацию об отзыве в следующем списке отозванных сертификатов ЭЦП и онлайн-сервисе проверки статуса отзыва сертификата ЭЦП.

13. УЦ обеспечивает протоколирование следующих событий:

1) формирование облачного закрытого ключа ЭЦП;

2) использование облачного закрытого ключа ЭЦП;

3) удаление (стирание) облачного закрытого ключа ЭЦП.

Срок хранения протоколов событий составляет 3 (три) года с даты истечения срока действия сертификата.

При протоколировании действий фиксируется следующая информация:

1) идентификатор владельца (учҰтная запись);

2) дата и время события (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС) ;

3) наименование источника события (компонент или сервис системы, где произошло действие);

4) IP адрес клиента или сессии;

5) описание события;

6) результат операции (успех/неуспех и код или причина отказа).

14. Программно-аппаратное обеспечение облачного хранилища размещается на территории Республики Казахстан в соответствии с едиными требованиями в сферах цифровизации и обеспечения кибербезопасности.

15. Защита облачного закрытого ключа ЭЦП обеспечивается комплексом организационных, программных и технических мероприятий в соответствии с требованиями, установленными едиными требованиями в сферах цифровизации и обеспечения кибербезопасности.

16. УЦ обеспечивает отсутствие возможности подписания электронных документов с использованием облачного закрытого ключа ЭЦП без многофакторной аутентификации.