Об утверждении Правил формирования и проверки подлинности электронной цифровой подписи

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 21 августа 2026 года № 500/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 24 августа 2026 года № 39672

В соответствии с подпунктом 4) пункта 1 статьи 55 Цифрового кодекса Республики Казахстан, ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила формирования и проверки подлинности электронной цифровой подписи.

2. Признать утратившими силу:

1) приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 "Об утверждении Правил проверки подлинности электронной цифровой подписи" (зарегистрированный в Реестре государственной регистрации нормативных правовых актов под № 12864);

2) приказ Министра информации и коммуникаций Республики Казахстан от 30 декабря 2016 года № 316 "О внесении изменения в приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 "Об утверждении Правил проверки подлинности электронной цифровой подписи" (зарегистрированный в Реестре государственной регистрации нормативных правовых актов под № 14759).

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*

Утверждены приказом
Заместитель Премьер-
Министра – Министр
искусственного интеллекта
и цифрового развития
Республики Казахстан
от 21 августа 2026 года
№ 500/НҚ

Правила формирования и проверки подлинности электронной цифровой подписи

Глава 1. Общие положения

1. Настоящие Правила формирования и проверки подлинности электронной цифровой подписи (далее – Правила) разработаны в соответствии с подпунктом 4) пункта 1 статьи 55 Цифрового кодекса Республики Казахстан (далее – Кодекс) и устанавливают порядок формирования и проверки подлинности электронной цифровой подписи в электронном документе.

2. В настоящих Правилах применяются следующие понятия:

1) сервис списка отозванных сертификатов открытого ключа электронной цифровой подписи – сервис, предоставляющий список отозванных сертификатов открытого ключа электронной цифровой подписи, сформированный в соответствии с RFC 5280;

2) удостоверяющий центр – 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;

3) объектный идентификатор (далее – OID) – уникальная иерархическая последовательность числовых идентификаторов, присваиваемая цифровому объекту для его однозначной идентификации в международном дереве идентификаторов объектов;

4) владелец сертификата – 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;

5) сервис метки времени – онлайн-сервис удостоверяющего центра, предоставляющий квитанцию метки времени, подтверждающую существование электронной цифровой подписи в электронном документе на момент формирования квитанции метки времени, в соответствии с RFC 3161 и RFC 5816;

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

7) цифровая система – функционально связанный комплекс цифровых ресурсов, использующий объекты цифровой инфраструктуры с целью обеспечения создания, сбора, обработки, хранения и распространения цифровых данных, а также автоматизирующий взаимодействие субъектов цифровой среды и (или) обеспечивающий оказание услуг в цифровой среде;

8) электронный документ – цифровая запись, подтверждение достоверности, принадлежности и неизменности которой обеспечено с помощью электронной цифровой подписи;

9) 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;

10) 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 Кодексом;

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

12) сервис проверки статуса сертификата открытого ключа электронной цифровой подписи (Online Certificate Status Protocol, далее – OCSP) – онлайн-сервис удостоверяющего центра, предоставляющий OCSP-квитанцию, содержащую сведения об отзыве сертификата открытого ключа электронной цифровой подписи либо об отсутствии такого отзыва на момент выдачи OCSP-квитанции в соответствии с RFC 6960;

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

14) формат CAdES (CMS Advanced Electronic Signatures, далее – CAdES) – формат электронной цифровой подписи на основе CMS;

15) формат CMS (Cryptographic Message Syntax, далее – CMS) – формат криптографических сообщений, используемый для формирования и проверки электронной цифровой подписи;

16) формат PAdES (PDF Advanced Electronic Signatures, далее – PAdES) – формат электронной цифровой подписи для документов в формате PDF;

17) формат PDF (Portable Document Format, далее – PDF) – формат электронного документа, поддерживающий встроенное размещение электронной цифровой подписи;

18) стандарт X.509 – стандарт, определяющий форматы данных и процедуры распределения открытых ключей с помощью сертификата открытого ключа электронной цифровой подписи;

19) формат XAdES (XML Advanced Electronic Signatures, далее – XAdES) – формат электронной цифровой подписи для документов в формате XML;

20) расширяемый язык разметки XML (eXtensible Markup Language, далее – XML) – расширяемый язык разметки, используемый для хранения и передачи данных в структурированном и машиночитаемом формате.

Глава 2. Формирование и проверка подлинности электронной цифровой подписи

Параграф 1. Формирование электронной цифровой подписи

3. Формирование ЭЦП осуществляется владельцем сертификата либо цифровой системой с использованием закрытого ключа ЭЦП.

4. Перед формированием ЭЦП осуществляются следующие проверки сертификата подписывающего лица:

1) криптографическая проверка подлинности сертификата путем проверки ЭЦП удостоверяющего центра;

2) проверка срока действия сертификата с установлением того, что срок его действия наступил и не истек;

3) проверка отсутствия сведений об отзыве сертификата посредством онлайн-сервиса OCSP, а при его недоступности посредством сервиса списка отозванных сертификатов. При использовании сервиса списка отозванных сертификатов применяется актуальный список отозванных сертификатов (Certificate Revocation List, далее – CRL) и промежуточный список отозванных сертификатов (Delta Certificate Revocation List, далее – delta CRL). Использование delta CRL является не обязательным и применяется для уточнения сведений об отзыве сертификата в период действия CRL;

4) проверка области и целей использования сертификата, в соответствии с политикой применения сертификатов удостоверяющего центра.

5. В отношении документов, для которых требуется подтверждение момента формирования ЭЦП либо ее проверка после истечения срока действия сертификата или его отзыва, подтверждением даты и времени формирования ЭЦП являются дата и

время, указанные в квитанции метки времени. Для подтверждения момента формирования ЭЦП квитанция метки времени формируется непосредственно после формирования ЭЦП.

6. При отсутствии квитанции метки времени невозможно достоверно подтвердить дату и время существования ЭЦП на определенный момент времени.

7. Для формирования ЭЦП применяются следующие основные форматы:

1) CAdES – для документов любого формата (на основе CMS, совместимого с PKCS #7);

2) PAdES – для документов в формате PDF;

3) XAdES – для структурированных XML-документов.

Допускается применение иных форматов ЭЦП при условии обеспечения возможности проверки ЭЦП в соответствии с настоящими Правилами.

8. Формат CAdES содержит:

1) структурные элементы:

подписываемые данные либо их хэш, позволяющее однозначно установить подписанные данные;

значение ЭЦП;

алгоритм формирования ЭЦП;

сертификат подписывающего лица;

атрибут "messageDigest" (OID: 1.2.840.113549.1.9.4) – содержит хэш подписываемых данных;

атрибут "signingCertificateV2" (OID: 1.2.840.113549.1.9.16.2.47) – содержит хэш сертификата подписывающего лица, использованного при формировании подписи;

атрибут "contentType" (OID: 1.2.840.113549.1.9.3) – определяет тип подписываемых данных.

2) дополнительные (опциональные) структурные элементы:

квитанция метки времени (OID: 1.2.840.113549.1.9.16.2.14) – содержит дату и время , сформированные сервисом метки времени, и подтверждает момент формирования ЭЦП;

сведения об отзыве сертификата (OID: 1.2.840.113549.1.9.16.2.24) – OCSP-квитанция либо CRL;

сертификаты цепочки сертификации (OID: 1.2.840.113549.1.9.16.2.23) – содержат сертификаты, необходимые для построения и проверки цепочки сертификации от проверяемого сертификата до доверенного корневого сертификата удостоверяющего центра с учетом промежуточных сертификатов;

иные атрибуты – могут включаться по усмотрению формирующей стороны при условии, что их использование не препятствует проверке ЭЦП.

9. Формат PAdES содержит:

1) структурные элементы:

подписываемый документ;

сертификат подписывающего лица;

запись "ByteRange" – определяет диапазоны байтов подписываемого документа;

запись "SubFilter" – определяет использование формата ЭЦП CAdES;

запись "Contents" – содержит значение ЭЦП.

2) дополнительные (опциональные) структурные элементы ЭЦП в формате PAdES включают атрибуты, в соответствии с пунктом 9 настоящих Правил.

10. Формат XAdES содержит:

1) структурные элементы:

подписываемый документ;

элемент "SignedInfo" – содержит канонизированное представление данных, подлежащих подписанию, включая ссылки на них, их хэш и сведения о применяемых алгоритмах;

элемент "SignatureValue" – содержит значение ЭЦП;

элемент "KeyInfo" – содержит сертификат подписывающего лица либо сведения для его однозначной идентификации и получения;

элемент "SignedProperties" – содержит подписываемые свойства ЭЦП.

2) дополнительные (опциональные) структурные элементы:

квитанция метки времени – содержит дату и время, сформированные сервисом метки времени, и подтверждает момент формирования ЭЦП;

сведения об отзыве сертификата – OCSP-квитанция либо CRL;

иные элементы и атрибуты – могут включаться по усмотрению формирующей стороны при условии, что их использование не препятствует проверке ЭЦП.

11. При подписании электронного документа допускается использование одной или нескольких ЭЦП.

12. Электронный документ допускает наличие одной или нескольких ЭЦП. Добавление каждой последующей ЭЦП осуществляется способом, предусмотренным соответствующим форматом ЭЦП, с сохранением возможности проверки ранее сформированных ЭЦП.

Параграф 2. Проверка подлинности электронной цифровой подписи

13. Данные необходимые для проверки ЭЦП в электронном документе:

1) электронный документ либо его хэш;

2) ЭЦП электронного документа;

3) сертификат подписывающего лица;

4) сертификат удостоверяющего центра, выдавшего сертификат подписывающего лица, а также промежуточные сертификаты удостоверяющих центров до доверенного корневого сертификата удостоверяющего центра;

5) квитанция метки времени – опционально;

6) OCSP-квитанция либо CRL (delta CRL при наличии) удостоверяющего центра, выдавшего сертификат подписывающего лица.

14. Проверка подлинности ЭЦП включает:

1) криптографическую проверку ЭЦП в электронном документе;

2) проверку сертификата подписывающего лица;

3) проверку квитанции метки времени (при наличии).

При отсутствии квитанции метки времени проверка подлинности ЭЦП осуществляется на момент проверки ЭЦП. При наличии действительной квитанции метки времени проверка подлинности ЭЦП осуществляется на момент времени, указанный в квитанции метки времени.

15. Криптографическая проверка ЭЦП осуществляется путем сопоставления значения хэша проверяемых данных с результатом выполнения алгоритма проверки ЭЦП с использованием открытого ключа ЭЦП, содержащегося в соответствующем сертификате.

Проверка ЭЦП в электронном документе осуществляется с использованием открытого ключа ЭЦП, содержащегося в сертификате подписывающего лица. Электронный документ содержит сертификат каждого подписывающего лица либо обеспечивает возможность его получения. Отсутствие указанного сертификата исключает возможность проверки ЭЦП.

Несоответствие результата криптографической проверки ЭЦП значению хэша проверяемых данных означает отрицательный результат проверки подлинности ЭЦП.

16. Проверка сертификата подписывающего лица осуществляется с использованием средств криптографической защиты информации и включает:

1) проверку срока действия сертификата на момент проверки подлинности ЭЦП, включая все сертификаты в цепочке сертификации от проверяемого сертификата до доверенного корневого сертификата удостоверяющего центра с учетом промежуточных сертификатов. Истечение срока действия хотя бы одного сертификата в цепочке сертификации на момент проверки подлинности ЭЦП означает отрицательный результат проверки;

2) проверку отсутствия сведений об отзыве сертификата посредством сервиса OCSP либо CRL (delta CRL при наличии) согласно пунктам 18 и 19 настоящих Правил. Наличие сведений об отзыве сертификата означает отрицательный результат проверки;

3) проверку корректности построения цепочки сертификации от сертификата подписывающего лица до доверенного корневого сертификата удостоверяющего центра, включая промежуточные сертификаты удостоверяющих центров. Некорректное построение цепочки сертификации означает отрицательный результат проверки;

4) проверку соответствия номера политики сертификата и назначения ключа, определяемого расширениями Key Usage и Extended Key Usage, условиям

использования сертификата, установленным политикой применения сертификатов соответствующего удостоверяющего центра.

Отрицательный результат хотя бы одной из проверок, предусмотренных настоящим пунктом, означает отрицательный результат проверки подлинности ЭЦП.

17. Проверка квитанции метки времени включает:

1) проверку подлинности ЭЦП квитанции метки времени в соответствии с пунктами 15 и 16 настоящих Правил;

2) проверку наличия сведений, позволяющих определить сервис метки времени либо удостоверяющий центр, сформировавший и подписавший метку времени, а также подтверждение того, что сертификат сервиса метки времени выдан удостоверяющим центром, выдавшим проверяемый сертификат;

3) проверку наличия в сертификате сервиса метки времени назначения ключа, предназначенного для формирования квитанций метки времени (timeStamping);

4) проверку соответствия значения хэша, содержащегося в квитанции метки времени, значению хэша данных, в отношении которых сформирована ЭЦП.

Квитанция метки времени признается действительной по результатам всех проверок, предусмотренных настоящим пунктом. Отрицательный результат проверки квитанции метки времени означает отрицательный результат проверки подлинности ЭЦП.

18. Проверка CRL и delta CRL (при наличии) включает:

1) проверку соответствия структуры CRL формату X.509, корректности ASN.1/ DER-кодирования;

2) проверку наличия сведений, позволяющих определить удостоверяющий центр, сформировавший и подписавший CRL;

3) проверку соответствия CRL проверяемому сертификату путем установления, что CRL сформирован удостоверяющим центром, выдавшим проверяемый сертификат;

4) криптографическую проверку ЭЦП CRL путем сопоставления значения хэша подписываемых данных CRL (TBSCertList) с результатом выполнения алгоритма проверки ЭЦП CRL с использованием открытого ключа ЭЦП, содержащегося в сертификате удостоверяющего центра, выпустившего соответствующий CRL. Несоответствие результата криптографической проверки ЭЦП CRL значению хэша подписываемых данных CRL означает отрицательный результат проверки CRL;

5) проверку периода действия CRL или delta CRL на момент проверки подлинности ЭЦП. Истечение периода действия CRL или delta CRL на момент проверки подлинности ЭЦП означает отрицательный результат проверки.

При положительном результате всех проверок, предусмотренных настоящим пунктом, результат проверки CRL или delta CRL является положительным. При отрицательном результате хотя бы одной из указанных проверок результат проверки CRL или delta CRL является отрицательным.

19. Проверка OCSP-квитанции включает:

1) проверку соответствия структуры OCSP-квитанции требованиям стандарта OCSP , корректности ASN.1/DER-кодирования;

2) проверку наличия сведений, позволяющих определить сервис OCSP либо удостоверяющий центр, сформировавший и подписавший OCSP-квитанцию, а также подтверждение того, что сертификат сервиса OCSP выдан удостоверяющим центром, выдавшим проверяемый сертификат;

3) проверку соответствия OCSP-квитанции проверяемому сертификату путем сопоставления идентификаторов сертификата, указанных в OCSP-квитанции, с данными проверяемого сертификата;

4) криптографическую проверку ЭЦП OCSP-квитанции путем сопоставления значения хэша подписываемых данных OCSP-квитанции с результатом выполнения алгоритма проверки ЭЦП OCSP-квитанции с использованием открытого ключа ЭЦП, содержащегося в сертификате сервиса OCSP либо удостоверяющего центра, подписавшего OCSP-квитанцию. Несоответствие результата криптографической проверки ЭЦП OCSP-квитанции значению хэша подписываемых данных OCSP-квитанции означает отрицательный результат проверки OCSP-квитанции;

5) проверку наличия в сертификате сервиса OCSP либо удостоверяющего центра назначения ключа, предназначенного для подписания OCSP-квитанций (OCSPSigning);

6) проверку того, что момент предоставления OCSP-квитанции (thisUpdate) не предшествует моменту проверки подлинности ЭЦП. Статус, содержащийся в OCSP-квитанции, характеризует состояние проверяемого сертификата исключительно на момент еҰ предоставления и не распространяется на иные моменты времени.

7) проверку наличия в OCSP-квитанции статуса "good" для проверяемого сертификата. Наличие статуса "revoked" означает отрицательный результат проверки. Статус "unknown" означает отсутствие у сервиса OCSP сведений о статусе проверяемого сертификата; поскольку статус "unknown" не позволяет подтвердить отсутствие сведений об отзыве сертификата, его наличие также означает отрицательный результат проверки.

При положительном результате всех проверок, предусмотренных настоящим пунктом, результат проверки OCSP-квитанции является положительным. При отрицательном результате хотя бы одной из указанных проверок результат проверки OCSP-квитанции является отрицательным.

20. При положительном результате проверки подлинности ЭЦП и соблюдении условий, предусмотренных пунктом 2 статьи 49 Кодекса, электронный документ, признается равнозначным документу, подписанному собственноручной подписью, и имеет одинаковые юридические последствия.

21. Отрицательный результат проверки полномочий лица, подписавшего электронный документ от имени юридического лица в соответствии с пунктом 2 статьи

61 Кодекса, не влияет на результат проверки подлинности ЭЦП. Правовые последствия отсутствия соответствующих полномочий определяются законодательством Республики Казахстан.

22. При формировании и (или) проверке подлинности ЭЦП с использованием цифровой системы владелец цифровой системы обеспечивает соблюдение требований настоящих Правил к процессам формирования и (или) проверки подлинности ЭЦП.

23. В случае формирования ЭЦП владельцем сертификата самостоятельно, без использования цифровой системы, соблюдение требований настоящих Правил при формировании ЭЦП обеспечивается владельцем сертификата. В случае проверки подлинности ЭЦП без использования цифровой системы соблюдение требований настоящих Правил при проверке подлинности ЭЦП обеспечивается лицом, осуществляющим такую проверку.

24. Визуальная форма представления сведений об ЭЦП, включая штрих-код, двухмерный матричный штриховой код или графическое изображение, не используется в качестве самостоятельного средства проверки подлинности ЭЦП в соответствии с настоящими Правилами.

В случае если цифровая система при подписании электронного документа формирует штрих-код, двухмерный матричный штриховой код или графическое изображение, содержащие электронный документ либо сведения, необходимые для его получения, такая цифровая система обеспечивает возможность получения электронного документа, в отношении которого осуществляется проверка подлинности ЭЦП, в соответствии с пунктом 4 статьи 61 Кодекса и настоящими Правилами.