Об утверждении Правил проверки подлинности электронной цифровой подписи

Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187. Зарегистрирован в Министерстве юстиции Республики Казахстан 14 января 2016 года № 12864.

В соответствии с подпунктом 10) пункта 1 статьи 5 Закона Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи"

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила проверки подлинности электронной цифровой подписи.

2. Комитету связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан (Қазанғап Т.Б.) обеспечить:

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

2) в течение десяти календарных дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан направление его копии в печатном и электронном виде на официальное опубликование в периодические печатные издания и информационно-правовую систему "Әділет", а также в Республиканский центр правовой информации для внесения в эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) размещение настоящего приказа на интернет-ресурсе Министерства по инвестициям и развитию Республики Казахстан и на интранет-портале государственных органов;

4) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства по инвестициям и развитию Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1), 2) и 3) пункта 2 настоящего приказа.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра по инвестициям и развитию Республики Казахстан.

4. Настоящий приказ вводится в действие со дня его первого официального опубликования и распространяется на правоотношения, возникшие с 1 января 2016 года.

Министр
по инвестициям и развитию
Республики Казахстан А. Исекешев

Утверждены
приказом Министра
по инвестициям и развитию
Республики Казахстан
от 9 декабря 2015 года № 1187

Правила
проверки подлинности электронной цифровой подписи

Сноска. Правила в редакции приказа Министра информации и коммуникаций РК от 30.12.2016 № 316 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Глава 1. Общие положения

1. Настоящие Правила проверки подлинности электронной цифровой подписи (далее – Правила) разработаны в соответствии с подпунктом 10) статьи 5 Закона Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи" (далее – Закон) и определяют порядок проверки подлинности электронной цифровой подписи информационной системой на этапе создания и функционирования информационной системы.

2. В настоящих Правилах применяются следующие понятия:

1) средство криптографической защиты информации (далее – СКЗИ) – средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами;

2) список отозванных регистрационных свидетельств (далее – СОРС) – часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования);

3) удостоверяющий центр – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

4) регистрационное свидетельство – документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом;

5) электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи;

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

8) хеш - преобразование массива входных данных произвольной длины в битовую сторону фиксированной длины;

9) хеш-функция - функция отображения последовательности байт в последовательность байт фиксированного размера.

Глава 2. Порядок проверки подлинности электронной цифровой подписи

3. На этапе создания и функционирования информационной системы, при получении электронного документа, содержащего регистрационное свидетельство подписывающей стороны, в информационной системе реализуется функционал проверки подлинности ЭЦП, осуществляющий следующие проверки:

1) проверку ЭЦП в электронном документе;

2) проверку регистрационного свидетельства подписывающей стороны.

4. Информационная система проверяет ЭЦП на электронном документе, путем использования открытого ключа ЭЦП, который содержится в регистрационном свидетельстве подписывающей стороны. Электронный документ должен содержать регистрационное свидетельство подписывающей стороны.

5. Проверка ЭЦП осуществляется в обратном порядке, по которому производилась подпись документа, по следующей схеме:

1) с помощью открытого ключа ЭЦП отправителя дешифруется хэш сообщения (подпись отправителя);

2) с помощью хэш-функции вычисляется контрольная сумма оригинального сообщения.

На данном этапе производится сверка двух контрольных сумм, если они равны, то ЭЦП считается верной (определен положительный результат проверки ЭЦП), если не равны, то ЭЦП считается не действительной (определен отрицательный результат проверки ЭЦП).

6. Информационная система в случае, если определен положительный результат проверки ЭЦП проверяет регистрационные свидетельства подписывающей стороны путем выполнения следующих проверок с использованием СКЗИ и средств ЭЦП удостоверяющего центра:

1) проверка срока действия регистрационного свидетельства. Проверка сроков действия от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;

2) проверка регистрационного свидетельства на отозванность (аннулирование). Проверка регистрационного свидетельства на отозванность (аннулирование) осуществляется одним из следующих методов:

на основе СОРС удостоверяющего центра. Данный метод проверки подтверждает, аннулировано ли проверяемое регистрационное свидетельство на момент начала срока действия СОРС удостоверяющего центра;

онлайн проверка регистрационного свидетельства на аннулирование, основанная на протоколе On-line Certificate Status Protocol (далее – OCSP). Данный метод проверки подтверждает аннулировано ли проверяемое регистрационное свидетельство на момент формирования квитанции OCSP;

на основе дополнительного СОРС. Данный сервис используется совместно с сервисом СОРС. Данный метод проверки подтверждает, аннулировано ли проверяемое регистрационное свидетельство на момент начала срока действия дополнительного СОРС удостоверяющего центра;

3) проверка области использования ЭЦП регистрационного свидетельства. Проверка заключается в проверке значения поля регистрационного свидетельства " использование ключа" (KeyUsage). Значения "Цифровая подпись" и "Неотрекаемость", содержащиеся в поле "использование ключа", означают что, это регистрационное свидетельство используется для ЭЦП. Значения "Цифровая подпись" и "Шифрование ключей", содержащиеся в поле "использование ключа", означают что, это регистрационное свидетельство используется для аутентификации;

4) проверка номера политики регистрационного свидетельства и разрешенных способах его использования. Политика проверяемого регистрационного свидетельства содержит разрешенные и запрещенные способы использования регистрационного свидетельства (например: регистрационное свидетельство используется в информационной системе "Казначейство-клиент"), это означает, что данное регистрационное свидетельство не может использоваться в других информационных системах, за исключением информационной системы "Казначейство-клиент";

5) проверка построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;

6) проверка метки времени. Проверка квитанции метки времени осуществляется для электронных документов долговременного хранения. Квитанция метки времени формируется в момент подписания электронного документа при определении положительного результата проверки ЭЦП, тем самым являясь доказательством подписания документа в указанный момент времени.

Метка времени является доказательством наличия ЭЦП в указанный в квитанции момент времени;

7) проверка полномочий лица подписавшего документ. Механизмы проверки полномочий осуществляются информационной системой. Проверка полномочий осуществляется при наличии информации об этом в регистрационном свидетельстве.

При несоответствии ЭЦП или регистрационного свидетельства требованиям одной из вышеуказанных проверок, за исключением подпункта 6) и 7) настоящего пункта, ЭЦП или регистрационное свидетельство считается недействительным (определен отрицательный результат проверки ЭЦП и регистрационного свидетельства).

7. Техническая реализация проверки подлинности ЭЦП и регистрационного свидетельства возлагается на информационную систему.

8. При удостоверении (установлении) подлинности ЭЦП с использованием СКЗИ удостоверяющего центра после проведения процедуры проверки ЭЦП (определен положительный результат проверки ЭЦП и регистрационного свидетельства), а также при соответствии условиям согласно подпунктам 2), 3) и 4) пункта 1 статьи 10 Закона, электронный документ, полученный посредством информационной системы, признается равнозначным документу, подписанному собственноручной подписи с одинаковыми юридическими последствиями.

9. При выявлении несоответствия ЭЦП (определен отрицательный результат проверки ЭЦП) после проведения процедуры проверки подлинности ЭЦП с использованием СКЗИ, а также при несоответствии условиям согласно подпунктам 2), 3) и 4) пункта 1 статьи 10 Закона, электронный документ, полученный посредством информационной системы, не признается равнозначным документу, подписанному собственноручной подписи.