

**Об утверждении Правил подтверждения подлинности электронной цифровой подписи доверенной третьей стороной Республики Казахстан**

Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 23 февраля 2015 года № 149. Зарегистрирован в Министерстве юстиции Республики Казахстан 2 апреля 2015 года № 10615.

      Сноска. Заголовок в редакции приказа и.о. Министра информации и коммуникаций Республики Казахстан от 29.03.2018 № 121 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

      Сноска. Преамбула в редакции приказа Министра по инвестициям и развитию РК от 09.12.2015 № 1186 (вводится в действие со дня его первого официального опубликования).

      1. Утвердить прилагаемые Правила подтверждения подлинности иностранной электронной цифровой подписи доверенной третьей стороной Республики Казахстан.

      2. Комитету связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан (Сарсенов С.С.) обеспечить:

      1) в установленном законодательством порядке 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 на официальное опубликование в периодических печатных изданиях и информационно-правовой системе "Әділет" республиканского государственного предприятия на праве хозяйственного ведения "Республиканский центр правовой информации Министерства юстиции 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 вице-министра по инвестициям и развитию Республики Казахстан Жумагалиева А.К.

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

|  |  |
| --- | --- |
|
Исполняющий обязанности |
 |
|
Министра по инвестициям и развитию |
 |
|
Республики Казахстан |
Ж. Касымбек |

|  |  |
| --- | --- |
|   | Утвержденыприказом Министрапо инвестициям и развитиюРеспублики Казахстанот 23 февраля 2015 года № 149 |

 **Правила**
**подтверждения подлинности электронной цифровой подписи доверенной третьей стороной Республики Казахстан**

      Сноска. Правила в редакции приказа и.о. Министра информации и коммуникаций Республики Казахстан от 29.03.2018 № 121 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

 **Глава 1. Общие положения**

      1. Настоящие Правила подтверждения подлинности электронной цифровой подписи доверенной третьей стороной Республики Казахстан (далее – Правила), разработаны в соответствии с подпунктом 13) пункта 1 статьи 5 Закона Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи" (далее – Закон) и определяют порядок подтверждения подлинности электронной цифровой подписи доверенной третьей стороной Республики Казахстан.

      2. В настоящих Правилах используются следующие основные понятия:

      1) 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);

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

      3) доверенная третья сторона Республики Казахстан (далее – ДТС РК) информационная система, осуществляющая в рамках трансграничного взаимодействия подтверждение подлинности иностранной электронной цифровой подписи и электронной цифровой подписи, выданной на территории Республики Казахстан;

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

      5) сервис подтверждения подлинности регистрационных свидетельств (Validation of Public Key Certificates) (далее – VPKC) – сервис ДТС РК осуществляющий проверку принадлежности и действительности открытого ключа электронной цифровой подписи одного или нескольких регистрационных свидетельств;

      6) доверенная третья сторона иностранного государства (далее – ДТС иностранного государства) – организация, наделенная в соответствии с законодательством иностранного государства правом осуществлять деятельность в автоматизированном режиме по проверке электронной цифровой подписи в электронных документах в фиксированный момент времени в отношении лица, подписавшего электронный документ;

      7) квитанция проверки электронной цифровой подписи (далее – квитанция) – электронный документ, удостоверенный ЭЦП ДТС РК и подтверждающий подлинность ЭЦП;

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

      9) сервис подтверждения подлинности документов подписанных электронной цифровой подписью (Validation of Digitally Signed Document) (далее – VSD) – сервис ДТС РК осуществляющий проверку подлинности ЭЦП.

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

      3. Участниками информационного обмена с ДТС РК являются:

      1) удостоверяющие центры;

      2) ДТС иностранных государств;

      3) пользователи информационных систем, интегрированных с ДТС РК.

 **Глава 2. Порядок подтверждения подлинности электронной цифровой подписи доверенной третьей стороной Республики Казахстан**

      4. ЭЦП сформированная с использованием регистрационных свидетельств, полученных в удостоверяющих центрах Республики Казахстан, проверяются информационными системами в соответствии с Правилами проверки подлинности электронной цифровой подписи, утвержденными приказом Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 12864) (далее – Правила проверки подлинности ЭЦП).

      В случае если электронный документ направляется в информационную систему иностранных государств, ДТС РК выдает квитанцию на основе запросов от информационных систем Республики Казахстан, для подтверждения подлинности ЭЦП в иностранных государствах. ДТС РК перед выдачей квитанции осуществляет проверку ЭЦП и регистрационного свидетельства в соответствии с Правилами проверки подлинности ЭЦП, при этом ИС осуществляет проверки предусмотренные подпунктами 2), 3) и 4) пункта 1 статьи 10 Закона.

      5. ЭЦП сформированная с использованием регистрационных свидетельств полученных в удостоверяющих центрах иностранных государств проверяются в ДТС РК, на основе запросов от иностранных информационных систем.

      6. ДТС РК проверяет подлинность ЭЦП при выполнении следующих условий:

      1) проверяемый электронный документ удостоверен ЭЦП физического или юридического лица;

      2) в ДТС РК зарегистрирован ДТС иностранного государства или удостоверяющий центр, выдавший проверяемое регистрационное свидетельство.

      7. Для проверки подлинности ЭЦП пользователь или ИС отправляет в ДТС РК, один из следующих запросов:

      1) электронный запрос VSD – согласно приложению 1 к настоящим Правилам;

      2) электронный запрос VPKC – согласно приложению 2 к настоящим Правилам;

      3) электронный запрос XML – согласно приложению 3 к настоящим Правилам.

      ДТС РК принимает запросы размером не более 100 мегабайт.

      8. Формы электронного запроса, квитанции и схем данных основных реквизитов квитанции приведены в приложениях 1, 2, 3, 4 и 5 к настоящим Правилам.

      9. На основании полученного ответа от удостоверяющего центра и (или) ДТС иностранного государства, ДТС РК формирует ответ в виде квитанции, являющейся необходимой и достаточной для подтверждения подлинности ЭЦП на территории Республики Казахстан.

      10. Подтверждение подлинности ЭЦП и (или) регистрационного свидетельства ДТС РК осуществляется бесплатно.

      11. Виды ответов от ДТС РК:

      1) квитанция со статусом "Проверено" ("Подтверждено"), в случае положительной проверки;

      2) квитанция со статусом "Не проверено" ("Не подтверждено"), в случае отрицательной проверки. При получении квитанции со статусом "Не проверено" пользователь информационной системы получает соответствующее оповещение через средства информационной системы;

      3) квитанция со статусом "Невозможно проверить" ("Нерасшифровано", "ошибка", "отказ"), в случае несоответствия структуры электронного запроса VSD, либо отсутствия регистрации удостоверяющего центра, либо ДТС иностранного государства в ДТС РК.

      Подтверждение подлинности ЭЦП и (или) регистрационного свидетельства считается удостоверенной, в случае наличия квитанций со статусом "Проверено", полученной пользователем или ИС в ДТС РК.

      12. ДТС РК хранит информацию о полученных запросах в базе данных, используя уникальные идентификаторы транзакций в течение пяти лет.

      13. По истечении срока хранения информация о полученных запросах поступает на архивное хранение в ДТС РК.

|  |  |
| --- | --- |
|   | Приложение 1 к Правилам подтвержденияподлинности электроннойцифровой подписи довереннойтретьей сторонойРеспублики Казахстан |

 **Электронный запрос VSD**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|
№ п/с |
Наименование
поля сообщения |
Тип поля сообщения |
Смысловое содержание |
Обязательность |
|
DVCSRequestInformation (запрос) |
|
1. |
requestInformation->version |
integer |
Версия запроса. По умолчанию 1 |
Нет |
|
2. |
requestInformation->service |
ServiceType |
Тип сервиса.
VSD – 2 |
Да |
|
3. |
requestInformation->nonce |
integer |
Зарезервированное поле (не используется) |
Нет |
|
4. |
requestInformation->requestTime |
DVCSTime |
Может содержать одно из значений на выбор – время по UTC (genTime), метка времени (timeStampToken) |
Нет |
|
5. |
requestInformation->requester |
GeneralNames |
Может содержать одно из значений на выбор – otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID |
Нет |
|
6. |
requestInformation->requestPolicy |
PolicyInformation |
Политика запроса |
Нет |
|
7. |
requestInformation->dvcs |
GeneralNames |
Может содержать одно из значений на выбор – otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID |
Нет |
|
8. |
requestInformation->dataLocations |
GeneralNames |
Может содержать одно из значений на выбор – otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID |
Нет |
|
9. |
requestInformation->extensions |
Extensions |
Дополнительная информация |
Нет |
|
10. |
data |
Data |
Проверяемые данные |
Да |
|
11. |
transactionIdentifier |
GeneralName |
Идентификатор транзакции |
Да |

|  |  |
| --- | --- |
|   | Приложение 2 к Правилам подтвержденияподлинности электроннойцифровой подписи довереннойтретьей стороной Республики Казахстан |

 **Электронный запрос VPKC**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|
№ п/с |
Наименование
поля сообщения |
Тип поля сообщения |
Смысловое содержание |
Обязательность |
|
DVCSRequestInformation (запрос) |
|
1. |
requestInformation->version |
integer |
Версия запроса. По умолчанию 1 |
Нет |
|
2. |
requestInformation->service |
ServiceType |
Тип сервиса.
VPKC – 3 |
Да |
|
3. |
requestInformation->nonce |
integer |
Зарезервированное поле (не используется) |
Нет |
|
4. |
requestInformation->requestTime |
DVCSTime |
Может содержать одно из значений на выбор – время по UTC (genTime), метка времени (timeStampToken) |
Нет |
|
5. |
requestInformation->requester |
GeneralNames |
Может содержать одно из значений на выбор – otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID |
Нет |
|
6. |
requestInformation->requestPolicy |
PolicyInformation |
Политика запроса |
Нет |
|
7. |
requestInformation->dvcs |
GeneralNames |
Может содержать одно из значений на выбор – otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID |
Нет |
|
8. |
requestInformation->dataLocations |
GeneralNames |
Может содержать одно из значений на выбор – otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID |
Нет |
|
9. |
requestInformation->extensions |
Extensions |
Дополнительная информация |
Нет |
|
10. |
data |
Data |
Проверяемые данные |
Да |
|
11. |
transactionIdentifier |
GeneralName |
Идентификатор транзакции |
Да |

|  |  |
| --- | --- |
|   | Приложение 3 к Правилам подтвержденияподлинности электроннойцифровой подписи довереннойтретьей стороной Республики Казахстан |

 **Электронный запрос XML**

|  |
| --- |
|
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:doc="urn:EEC:SignedData:v1.0:
EDoc" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" targetNamespace=
"urn:EEC:SignedData:v1.0:EDoc" elementFormDefault="qualified" attributeFormDefault="unqualified">
   <xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation=
"http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd#"/>
   <xs:element name="SignedDoc" type="doc:SignedDocType">
      <xs:annotation>
         <xs:documentation>Электронный документ</xs:documentation>
      </xs:annotation>
   </xs:element>
   <xs:complexType name="SignedDocType">
      <xs:annotation>
         <xs:documentation>Тип данных "Электронный документ"</xs:documentation>
      </xs:annotation>
      <xs:sequence>
         <xs:element name="Data">
            <xs:annotation>
               <xs:documentation>Блок содержимого электронного документа</xs:documentation>
            </xs:annotation>
            <xs:complexType>
               <xs:complexContent>
                  <xs:extension base="doc:DataType">
                     <xs:attribute name="Id" type="xs:ID" use="required"/>
                  </xs:extension>
               </xs:complexContent>
            </xs:complexType>
         </xs:element>
         <xs:element ref="ds:Signature" minOccurs="0">
            <xs:annotation>
               <xs:documentation>Квитанция доверенной третьей стороны</xs:documentation>
            </xs:annotation>
         </xs:element>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="DataType">
      <xs:annotation>
         <xs:documentation>Тип блока содержимого электронного документа</xs:documentation>
      </xs:annotation>
      <xs:sequence>
         <xs:element ref="ds:Signature" maxOccurs="unbounded">
            <xs:annotation>
               <xs:documentation>Электронная цифровая подпись (электронная подпись)</xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="SignedContent">
            <xs:annotation>
               <xs:documentation>Блок подписываемых данных</xs:documentation>
            </xs:annotation>
            <xs:complexType>
               <xs:sequence>
                  <xs:any namespace="##any" processContents="lax" maxOccurs="unbounded">
                     <xs:annotation>
                        <xs:documentation>Структура видов электронных документов (сведений)</xs:documentation>
                     </xs:annotation>
                  </xs:any>
               </xs:sequence>
               <xs:attribute name="Id" type="xs:ID" use="required">
                  <xs:annotation>
                     <xs:documentation>Атрибут-идентификатор блока подписываемых данных</xs:documentation>
                  </xs:annotation>
               </xs:attribute>
               <xs:attribute name="DocInstance" type="xs:anyURI" use="required">
                  <xs:annotation>
                     <xs:documentation>Уникальный идентификатор электронного документа</xs:documentation>
                  </xs:annotation>
               </xs:attribute>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
   </xs:complexType>
</xs:schema> |

|  |  |
| --- | --- |
|   | Приложение 4к Правилам подтвержденияподлинности электроннойцифровой подписи довереннойтретьей стороной Республики Казахстан |

 **Электронная квитанция**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|
№ п/с |
Наименование
поля сообщения |
Тип поля сообщения |
Смысловое содержание |
Обязательность |
|
 |
DVCSResponse(ответ), 1-й вариант ответа |
|
1. |
dvCertInfo->version |
integer |
Версия запроса.
По умолчанию 1 |
Нет |
|
2. |
dvCertInfo->dvReqInfo |
DVCSRequestInformation |
Информация о запросе |
Да |
|
3. |
dvCertInfo->messageImprint |
DigestInfo |
Хэш-значение на данные из запроса |
Да |
|
4. |
dvCertInfo->serialNumber |
Integer |
Уникальный идентификатор запроса |
Да |
|
5. |
dvCertInfo->responseTime |
DVCSTime |
Может содержать одно из значений на выбор – время по UTC (genTime), метка времени (timeStampToken) |
Да |
|
6. |
dvCertInfo->dvStatus |
PKIStatusInfo |
Статус ответа |
Нет |
|
7. |
dvCertInfo->policy |
PolicyInformation |
Политика ответа |
Нет |
|
8. |
dvCertInfo->reqSignature |
SignerInfos |
Подпись запроса |
Нет |
|
9. |
dvCertInfo->certs |
TargetEtcChain  |
Ргеистрационные свидетельства |
Нет |
|
10. |
dvCertInfo->extensions |
Extensions |
Дополнительная информация |
Нет |
|
DVCSResponse(ответ), 2-й вариант ответа |
|
1. |
dvErrorNote->transactionStatus |
PKIStatusInfo |
Статус ответа |
Да |
|
2. |
dvErrorNote->transactionIdentifier |
GeneralName |
Идентификатор транзакции |
Нет |

|  |  |
| --- | --- |
|   | Приложение 5 к Правилам подтвержденияподлинности электроннойцифровой подписи довереннойтретьей стороной Республики Казахстан |

 **Схема данных основных реквизитов квитанции**

|  |
| --- |
|
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:rcpt="urn:EEC:TTP:v1.0:receipt" targetNamespace="urn:EEC:TTP:v1.0:receipt" elementFormDefault="qualified" attributeFormDefault="unqualified">
   <xs:element name="Receipt" type="rcpt:ReceiptType">
      <xs:annotation>
         <xs:documentation>Блок основных реквизитов квитанции</xs:documentation>
      </xs:annotation>
   </xs:element>
   <xs:complexType name="ReceiptType">
      <xs:annotation>
         <xs:documentation>Тип блока основных реквизитов квитанции</xs:documentation>
      </xs:annotation>
      <xs:sequence>
         <xs:element name="ReceiptId" type="xs:anyURI">
            <xs:annotation>
               <xs:documentation>Уникальный идентификатор сформированной квитанции</xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="DocId" type="xs:anyURI">
            <xs:annotation>
               <xs:documentation>Идентификатор электронного документа</xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="Report">
            <xs:annotation>
               <xs:documentation>Блок сведений о результатах проверки</xs:documentation>
            </xs:annotation>
            <xs:complexType>
               <xs:choice maxOccurs="unbounded">
                  <xs:element name="Success" type="rcpt:SuccessType"/>
                  <xs:element name="Error" type="rcpt:ErrorType"/>
               </xs:choice>
            </xs:complexType>
         </xs:element>
         <xs:element name="AttachedData" minOccurs="0">
            <xs:annotation>
               <xs:documentation>Блок дополнительных сведений в формате XML</xs:documentation>
            </xs:annotation>
            <xs:complexType>
               <xs:sequence>
                  <xs:any namespace="##any" processContents="lax" maxOccurs="unbounded"/>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:ID" use="required"/>
   </xs:complexType>
   <xs:complexType name="BaseReportType">
      <xs:annotation>
         <xs:documentation>Базовый тип элемента-отчета о проверке</xs:documentation>
      </xs:annotation>
      <xs:attribute name="Reference" type="xs:anyURI" use="optional"/>
   </xs:complexType>
   <xs:complexType name="SuccessType">
      <xs:annotation>
         <xs:documentation>Тип элемента, указывающего, что проверка ДТС выполнена успешно</xs:documentation>
      </xs:annotation>
      <xs:complexContent>
         <xs:extension base="rcpt:BaseReportType"/>
      </xs:complexContent>
   </xs:complexType>
   <xs:complexType name="ErrorType">
      <xs:annotation>
         <xs:documentation>Тип контейнера описания ошибки</xs:documentation>
      </xs:annotation>
      <xs:complexContent>
         <xs:extension base="rcpt:BaseReportType">
            <xs:sequence>
               <xs:element name="ReasonCode">
                  <xs:annotation>
                     <xs:documentation>Код ошибки</xs:documentation>
                  </xs:annotation>
                  <xs:simpleType>
                     <xs:restriction base="xs:string">
                        <xs:enumeration value="Signature.Error"/>
                        <xs:enumeration value="Signature.BadCertificate"/>
                        <xs:enumeration value="Document.AuthenticityError"/>
                     </xs:restriction>
                  </xs:simpleType>
               </xs:element>
               <xs:element name="ReasonText" type="xs:string" >
                  <xs:annotation>
                     <xs:documentation>Текстовое описание ошибки</xs:documentation>
                  </xs:annotation>
               </xs:element>
            </xs:sequence>
         </xs:extension>
      </xs:complexContent>
   </xs:complexType>
</xs:schema> |

 © 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан