Проект

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНЦИФРЫ РОССИИ)

ПРИКАЗ

_____ № _____

Москва

О внесении изменений в формат электронной подписи, обязательный для реализации всеми средствами электронной подписи, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 14 сентября 2020 г. № 472

В соответствии с пунктом 5 части 4 статьи 8 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и абзацем третьи пункта 1 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418, п р и к а з ы в а ю :

Внести изменения в формат электронной подписи, обязательный для реализации всеми средствами электронной подписи, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 14 сентября 2020 г. № 472 «Об утверждении Формата электронной подписи, обязательного для реализации всеми средствами электронной подписи» (зарегистрирован Министерством юстиции Российской Федерации 29 октября 2020 г., регистрационный № 60631), согласно приложению.

Министр М.И. Шадаев

Приложение
к приказу Министерства
цифрового развития,
связи и массовых коммуникаций
Российской Федерации
от _____ № _____

ИЗМЕНЕНИЯ,
которые вносятся в формат электронной подписи, обязательный для реализации всеми средствами электронной подписи, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций от 14 сентября 2020 г. № 472

1. Пункт 5 изложить в следующей редакции:

«5. Структура ЭП должна соответствовать синтаксису криптографических сообщений, основанному на инкапсуляции криптографических данных внутри структуры ContentInfo, связывающей тип содержимого (contentType) с самим содержимым (content) и имеющей следующий общий вид:

```
ContentInfo ::= SEQUENCE {
    contentType        ContentType,
    content        [0] EXPLICIT ANY DEFINED BY contentType }

ContentType ::= OBJECT IDENTIFIER
```

Поле contentType должно содержать тип «подписанные данные» (id-signedData) с объектным идентификатором вида «1.2.840.113549.1.7.2».

Поле content должно содержать структуру SignedData, описывающую структуру и содержимое ЭП и имеющую следующий вид:

```
SignedData ::= SEQUENCE {
    version              CMSVersion,
    digestAlgorithms     DigestAlgorithmIdentifiers,
    encapContentInfo     EncapsulatedContentInfo,
    certificates     [0] IMPLICIT CertificateSet OPTIONAL,
    crls             [1] IMPLICIT RevocationInfoChoices OPTIONAL,
    signerInfos          SignerInfos }».
```

2. Абзац первый пункта 5.4 изложить в следующей редакции:

«5.4. В поле certificates (тип CertificateSet) включается информация о сертификатах подписывающих сторон. Данное поле может содержать полный набор иерархически обусловленной последовательности сертификатов, где каждый последующий сертификат подписан ЭП, основанной на предшествующем сертификате. В данное поле также может включаться дополнительная информация о сертификатах.».

3. В пункте 5.4.1 слова «Поле signatureAlgorithm (тип SignatureAlgorithmIdentifier) определяет идентификатор использованного алгоритма ЭП и связанные с ним параметры:» заменить словами «Поле signatureAlgorithm (тип AlgorithmIdentifier) определяет идентификатор использованного алгоритма ЭП и связанные с ним параметры.», слова «SignatureAlgorithmIdentifier ::= AlgorithmIdentifier» исключить.

4. Пункт 5.4.3 изложить в следующей редакции:

«5.4.3. Поля v1AttrCert (типа AttributeCertificateV1) и v2AttrCert (типа AttributeCertificateV2) определяют атрибутивные сертификаты версии 1 и версии 2 соответственно, которые могут содержать дополнительные атрибуты, права или информацию, не входящую в X.509, и применению не подлежат.».

5. Пункт 5.4.4 признать утратившим силу.

6. В абзаце первом пункта 5.5.1 после слов «список аннулированных» дополнить словами «и досрочно прекративших действие».

7. Пункт 5.6 изложить в следующей редакции:

«5.6. В поле signerInfos (тип SignerInfos) содержится информация о каждой подписывающей стороне электронного документа.

```
SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
  version                 CMSVersion,
  sid                     SignerIdentifier,
  digestAlgorithm         DigestAlgorithmIdentifier,
  signedAttrs             [0]  IMPLICIT SignedAttributes OPTIONAL,
  signatureAlgorithm      SignatureAlgorithmIdentifier,
  signature               SignatureValue,
  unsignedAttrs           [1]  IMPLICIT UnsignedAttributes OPTIONAL }

SignatureAlgorithmIdentifier ::= AlgorithmIdentifier
```

Поле signedAttrs должно присутствовать в структуре SignerInfo.».

8. Пункт 5.6.5 дополнить абзацем следующего содержания:

«В качестве неподписываемого атрибута в структуру ЭП может быть включена информация о метке доверенного времени, порядок создания и проверки которой утвержден приказом Минцифры России от 6 ноября 2020 г. № 580 «Об утверждении порядка создания и проверки метки доверенного времени» (зарегистрирован Министерством юстиции Российской Федерации 28 декабря 2020 г., регистрационный № 61867). Для включения указанной информации используется атрибут id-aa-timeStampToken с объектным идентификатором вида «1.2.840.113549.1.9.16.2.14».».

9. В пункте 6.1 цифры «1.2.840.113549.1.3» заменить цифрами «1.2.840.113549.1.9.3».

10. Абзац пятый пункта 6.2 изложить в следующей редакции:

«Результат функции, отображающей строки бит в строки бит фиксированной длины и удовлетворяющей указанным условиям, должен быть добавлен в атрибут id-messageDigest с объектным идентификатором вида «1.2.840.113549.1.9.4»;».

11. в пункте 6.3 цифры «1.2.840.113549.1.9» заменить цифрами «1.2.840.113549.1.9.16.2.47».

12. Пункт 7 изложить в следующей редакции:

«7. Структура заявления на выдачу сертификата, предоставляемого заявителем в УЦ, должна иметь следующий вид:

CertificationRequest ::= SEQUENCE {
certificationRequestInfo CertificationRequestInfo,
signatureAlgorithm AlgorithmIdentifier {{Signature Algorithms}},
signature BIT STRING}, где

certificationRequestInfo - подписываемая информация;

signatureAlgorithm - информация об алгоритме ЭП, который использовался при формировании ЭП данных поля certificationRequestInfo структуры CertificationRequest;

signature - ЭП данных поля certificationRequestInfo структуры CertificationRequest, сформированная с использованием алгоритма, указанного в SignatureAlgorithm.».

13. В пункте 7.1 слова «описанной в ГОСТ Р ИСО/МЭК 9594-8» заменить словами «описанной в ГОСТ Р ИСО/МЭК 9594-8-98», слова «при этом он должен быть равен» заменить словами «при этом идентификатор digestParamSet должен быть равен», слова «в соответствии с ГОСТ Р ИСО/МЭК 8825-1» заменить словами «в соответствии с ГОСТ Р ИСО/МЭК 8825-1-2003».

14. Абзац первый пункта 7.2 изложить в следующей редакции:

«7.2. Поле signatureAlgorithm структуры CertificationRequest имеет тип AlgorithmIdentifier. Поле algorithm структуры AlgorithmIdentifier содержит идентификатор алгоритма ЭП и связанных с ним параметров, который используется при формировании ЭП структуры CertificationRequestInfo с использованием ключа ЭП:».

15. В третьем и пятом абзацах пункта 7.3 слово «BITSTRING» заменить словами «BIT STRING».