ПРОЕКТ

МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНКОМСВЯЗЬ РОССИИ)

ПРИКАЗ

_____ № _____

Об утверждении формата электронной подписи, обязательного для реализации всеми средствами электронной подписи

В соответствии с положениями пункта 5 части 4 статьи 8 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880; 2013, № 27, ст. 3477; 2014, № 11, ст. 1098; № 26, ст. 3390; 2016, № 1, ст. 65),

ПРИКАЗЫВАЮ:

1. Утвердить Формат электронной подписи, обязательный для реализации всеми средствами электронной подписи, согласно приложению к настоящему приказу.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

Министр Н.А. Никифоров

Приложение
к приказу Минкомсвязи России
от _____№_____

ФОРМАТ
ЭЛЕКТРОННОЙ ПОДПИСИ, ОБЯЗАТЕЛЬНЫЙ ДЛЯ РЕАЛИЗАЦИИ ВСЕМИ СРЕДСТВАМИ ЭЛЕКТРОННОЙ ПОДПИСИ

1. Настоящий Формат разработан в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (далее - Федеральный закон).

2. Для целей Формата используются следующие основные понятия, определенные в статье 2 Федерального закона:

1) электронная подпись (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) ключ ЭП - уникальная последовательность символов, предназначенная для создания ЭП;

3) ключ проверки ЭП - уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее - проверка ЭП);

4) удостоверяющий центр (далее - УЦ) - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Федеральным законом;

5) сертификат ключа проверки ЭП - электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

6) квалифицированный сертификат ключа проверки ЭП (далее - квалифицированный сертификат) - сертификат ключа проверки ЭП, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП (далее - уполномоченный федеральный орган);

7) владелец сертификата ключа проверки ЭП - лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки ЭП;

8) аккредитация УЦ - признание уполномоченным федеральным органом

соответствия УЦ требованиям Федерального закона;

9) средства ЭП - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП;

10) средства УЦ - программные и (или) аппаратные средства, используемые для реализации функций УЦ;

11) участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

3. Настоящий Формат устанавливает требования к структуре и содержанию информации ЭП.

4. При включении в состав ЭП дополнительной информации требования к её назначению и расположению в структуре ЭП определяются в техническом задании на разработку (модернизацию) средств ЭП и УЦ.

5. В составе ЭП должна размещаться информация об исходном электронном сообщении, алгоритмах хеширования и подписи, параметрах криптографических алгоритмов, времени создания ЭП, сертификат ключа проверки электронной подписи, цепочка сертификации и иные, установленные в соответствии с настоящим Форматом сведения.

6. В соответствии с настоящим Форматом средства электронной подписи должны обеспечивать возможность создания нескольких ЭП под одним документом, сохраняя всю необходимую информацию в сообщении.

7. Для включения в состав ЭП используются следующие виды данных:

SEQUENCE Используется для описания структуры данных, состоящей из различных типов.

INTEGER Целое число.

OBJECT IDENTIFIER Последовательность целых чисел.

UTCTime Временной тип, содержит 2 цифры для определения года

GeneralizedTime Расширенный временной тип, содержит 4 цифры для обозначения года.

SET Описывает структуру данных разных типов.

UTF8String Описывает строковые данные.

NULL специальное значение (псевдозначение), означающее, что значение поля не определено.

BIT STRING Тип для хранения последовательности бит.

8. Структура ЭП в форме электронного документа, определенная в соответствии со спецификацией абстрактной синтаксической нотации версии один <*>, должна иметь следующий общий вид:

<*> Справочно: Спецификация абстрактной синтаксической нотации версии один определена в ГОСТ Р ИСО/МЭК 8824-1-2001 "Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации"

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

Версия синтаксиса ЭП зависит от сертификатов, типа подписываемых данных и информации о подписывающих сторонах.

9. Настоящим Форматом устанавливаются следующие значения полей (структур) ЭП:

DigestAlgorithmIdentifiers включает в себя идентификаторы используемых алгоритмов хеширования и ассоциированные с ними параметры.

EncapsulatedContentInfo содержит подписываемые данные (Content) вместе с их типом (Content Type).

В поле CertificateSet должна быть включена информация о сертификатах ключа проверки ЭП, позволяющая установить цепочку сертификатов, отражающих путь сертификации от удостоверяющего центра, выдавшего сертификат ключа проверки ЭП, до каждой из подписывающих сторон. В данное поле может быть включена информация о сертификатах подписывающих сторон.

В поле CertificateRevocationList (RevocationInfoChoices) должна быть включена информация о статусе отзыва сертификатов, достаточная для определения действительности сертификата ключа проверки ЭП подписывающей стороны на момент проверки.

В структуре SignerInfoы содержится информация о каждой подписывающей стороне электронного документа.

Версия синтаксиса version определяется значением Signer ID.

Signer ID определяет открытый ключ подписывающей стороны (subjectKeyIdentifier) или сертификат его открытого ключа, необходимый для проверки подлинности подписи (issuerAndSerialNumber).