МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO 14533-1

Первое издание
2012-09-15

Процессы, элементы данных и документы в торговле, промышленности и администрировании. Долгосрочные профили подписей.

Часть 1.

Долгосрочные профили подписей для усовершенствованных электронных подписей CMS

Processes, data elements and documents in commerce, industry and administration — Long term signature profiles —

Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)

Ответственность за подготовку русской версии несёт GOST R (Российская Федерация) в соответствии со статьёй 18.1 Устава ISO

Ссылочный номер
ISO 14533-1:2012(R)

Содержание

Страница

Предисловие

Международная организация по стандартизации (ISO) является всемирной федерацией национальных организаций по стандартизации (комитетов-членов ISO). Разработка международных стандартов обычно осуществляется техническими комитетами ISO. Каждый комитет-член, заинтересованный в деятельности, для которой был создан технический комитет, имеет право быть представленным в этом комитете. Международные правительственные и неправительственные организации, имеющие связи с ISO, также принимают участие в работах. ISO работает в тесном сотрудничестве с Международной электротехнической комиссией (IEC) по всем вопросам стандартизации в области электротехники.

Международные стандарты разрабатываются в соответствии с правилами, установленными в Директивах ISO/IEC, Часть 2.

Основная задача технических комитетов состоит в подготовке международных стандартов. Проекты международных стандартов, одобренные техническими комитетами, рассылаются комитетам-членам на голосование. Их опубликование в качестве международных стандартов требует одобрения, по меньшей мере, 75 % комитетов-членов, принимающих участие в голосовании.

Следует иметь в виду, что некоторые элементы этого документа могут быть объектом патентных прав. ISO не должен нести ответственность за идентификацию какого-либо одного или всех патентных прав.

ISO 14533-1 был разработан Техническим комитетом ISO/TC 154, *Процессы, элементы данных и документы в области коммерции, промышленности и администрирования.*

ISO 14533 состоит из следующих частей, под общим названием *Процессы, элементы данных и документы в торговле, промышленности и администрировании. Долгосрочные профили подписей:*

— *Часть 1. Долгосрочные профили подписей для усовершенствованных электронных подписей CMS (CAdES)*

— *Часть 2. Долгосрочные профили подписей для усовершенствованных электронных подписей XML (XAdES)*

Введение

Цель данной части ISO 14533 состоит в обеспечении взаимодействия при реализации гарантии в отношении долгосрочных подписей, которая укрепляет доверие к электронным подписям в течение длительного времени. Технические условия на долгосрочные подписи, на которые производятся ссылки при каждой реализации, включают усовершенствованные электронные подписи CMS (системы управления информационным наполнением) (CAdES), разработанные Европейским институтом телекоммуникационных стандартов (European Telecommunications Standards Institute (ETSI)).

Процессы, элементы данных и документы в торговле, промышленности и администрировании. Долгосрочные профили подписей.

Часть 1.
Долгосрочные профили подписей для усовершенствованных электронных подписей CMS

1 Область применения

Данная часть ISO 14533 устанавливает элементы, включающие определённые в CMS усовершенствованные электронные подписи (CAdES), позволяющие удостоверять цифровую подпись в течение длительного периода времени.

Стандарт не содержит новые технические спецификации, относящиеся к самим цифровым подписям, и не накладывает новые ограничения на применение технических спецификаций для цифровых подписей, которые уже используются.

ПРИМЕЧАНИЕ Усовершенствованные электронные подписи CMS (CAdES) представляют собой расширенные технические условия для Синтаксиса криптографических сообщений (CMS), находящих широкое применение.

2 Нормативные ссылки

Следующие ссылочные документы обязательны для применения в настоящем документе. В случае датированных ссылок применяются только цитированные издания. При недатированных ссылках используется последнее издание ссылочного документа (включая все изменения).

ETSI TS 101 733 v1.8.1 (2009-11), *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*[1)]

3 Термины и определения

Для целей настоящего документа применяются термины и определения, указанные ниже.

3.1
долгосрочная подпись
long term signature
подпись, позволяющая в течение длительного времени выполнять её проверку с помощью специальных мер в целях определения незаконных изменений содержащейся в ней информации, включая определение времени создания подписи, исполнителя данной подписи, и контрольных данных

1) Доступно на http://pda.etsi.org/pda/queryform.asp

3.2
профиль
profile
правило, применяемое для гарантирования операционной совместимости, относящееся к вспомогательным элементам ссылочной спецификации, диапазону значений, и т.д.

3.3
требуемый уровень
required level
уровень требований к реализации каждого элемента, включённого в профиль

3.4
синтаксис криптографического сообщения
cryptographic message syntax
CMS
синтаксис, относящийся к подписи, каталогу, аутентификации, и кодированию данного сообщения

ПРИМЕЧАНИЕ Синтаксис криптографического сообщения определён в IETF RFC 5652.

3.5
усовершенствованная электронная подпись CMS
CMS advanced electronic signature
CAdES
электронная подпись, определённая в ETSI TS 101 733, для которой может быть определён подписант и любые незаконные изменения данных

3.6
CAdES с включением времени
CAdES with time
CAdES-T
усовершенствованная электронная подпись CMS, определённая в ETSI TS 101 733, содержащая информацию для определения времени подписания

ПРИМЕР Метка времени подписи.

3.7
архивные данные CAdES
archival CAdES
CAdES-A
усовершенствованная электронная подпись CMS, определённая в ETSI TS 101 733, содержащая информацию, позволяющую определять любые незаконные изменения информации, содержащейся в подписи, включая субъекта подписи и критерий правильности

ПРИМЕР Временная метка архива.

3.8
информация о контенте
content information
данные структуры, определяющие контент CMS

3.9
подписанные данные
signed data
структура данных, определяющая подписанные данные в CMS или связанные данные

3.10
информация о подписанте
signerinfo
структура данных, определяющая информацию о подписи для каждого подписанта или связанные данные

3.11
подписанный атрибут
signed attribute
информация о подписи, относящаяся к предмету подписи

3.12
неподписанный атрибут
unsigned attribute
информация о подписи, не относящаяся к предмету подписи

ПРИМЕЧАНИЕ Временной штамп подписи и архивный штамп подписи являются неподписанными атрибутами.

3.13
данные валидации
validation data
информация сертификата и отзыва, используемая для валидации подписи и временного штампа

3.14
полномочия определения отметки времени
timestamping authority
TSA
доверенная третья сторона, уполномоченная предоставить подтверждение, что определённые данные имелись к определённому моменту времени

3.15
маркер отметки времени
timestamp token
TST
объект данных, устанавливающий связь предоставления данных с определённым моментом времени, являющийся свидетельством существования этих данных перед указанным моментом времени

3.16
отметка времени подписи
signature timestamp
отметка времени, закреплённая для анализа подписи в целях идентификации времени существования подписи

3.17
отметка времени архива
archive timestamp
отметка времени, закреплённая в информации, относящейся к подписи, включающая субъект подписи и данные валидации, в целях определения любых незаконных изменений

3.18
точка доверия
trust anchor
источник доверия, предоставляемый в виде сертификата ключа подписи или ключа общего пользования, используемый системой проверки для подтверждения достоверности электронной подписи, и обычно сертификат ключа подписи, выпущенный доверенным корневым органом сертификации

3.19
пользующаяся доверием третья сторона
trusted third party
TTP
орган обеспечения безопасности, или его агент, пользующийся доверием другой организации, связанной с работами в области обеспечения безопасности

3.20
организация по сертификации
certification authority
CA
центр, которому доверены разработка и присваивание сертификата ключа подписи

ПРИМЕЧАНИЕ Организации по сертификации могут, по собственному решению, разрабатывать и присваивать ключи организациям.

3.21
сертификат
certificate
информация относительно общественно раскрытого ключа в качестве части асимметричной пары ключей для предприятия, подписанная органом сертификации для предотвращения подделки

3.22
сертификация по атрибутам
attribute certificate
сертификат, содержащий указание работы, квалификации, должности, и других атрибутов и значений атрибутов

3.23
информация об отзыве
revocation information
информация, выпущенная органом сертификации в отношении сертификата, аннулированного в течение заданного периода

ПРИМЕЧАНИЕ Эта информация может быть рассмотрена для определения, действует или нет сертификат в текущее время.

3.24
усиленная служба безопасности
enhanced security service
ESS
необязательно усиленная служба, относящаяся к подписи, включающая, но не ограничивающаяся, предоставлением информации, идентифицирующей SigningCertificate и информацией, относящейся к типу подписи

4 Символы

Следующие символы используются для указания “требуемого уровня”.

— C Договорный

— M Обязательный

— O Опциональный

5 Требования

5.1 Генерирование или валидация данных CAdES-T соответствует настоящей части ISO 14533, при условии, что выполняются следующие требования:

a) все типы обработки элементов, которые требуют уровень “Обязательный” в профиле CAdES-T, определённом в данной части ISO 14533, должны быть включены;

b) подробные спецификации, относящиеся к обработке любых элементов, которую требует уровень “Договорный” в профиле CAdES-T, определённом в данной части ISO 14533, должны быть включены.

5.2 Генерирование или валидация данных CAdES-A соответствует настоящей части ISO 14533, при условии, что выполняются следующие требования:

a) все типы обработки элементов, которые требует уровень “Обязательный” в профиле CAdES-A, определённом в данной части ISO 14533, должны быть включены;

b) подробные спецификации, относящиеся к обработке любых элементов, которую требует уровень “Договорный” в профиле CAdES-A, определённом в данной части ISO 14533, должны быть включены.

5.3 Когда используется оценка соответствия первой стороны, реализующая сторона должна сделать заявление о соответствии данной части ISO 14533 путём раскрытия заявления о соответствии поставщика и его приложения (см. Приложение A), содержащего описание статуса реализации (и спецификаций для всех элементов типа “Договорный”).

ПРИМЕЧАНИЕ Рисунок 1 показывает позиционирование генерирования и валидации данных CAdES-T и данных CAdES-A.

6 Долгосрочные профили подписей

6.1 Определённые профили

В целях создания возможности проверки электронных подписей в течение длительных периодов времени, должна существовать возможность определения любых незаконных изменений информации, относящейся к подписям, включая объект информации и данные валидации, а также должна быть гарантирована операционная совместимость. Для выполнения этих требований данная часть ISO 14533 определяет два профиля, относящиеся к CAdES:

a) профиль CAdES-T: профиль, соответствующий генерированию и валидации данных CAdES-T;

b) профиль CAdES-A: профиль, соответствующий генерированию и валидации данных CAdES-A.

На Рисунке 1 показана взаимосвязь между данными CAdES-T и данными CAdES-A.

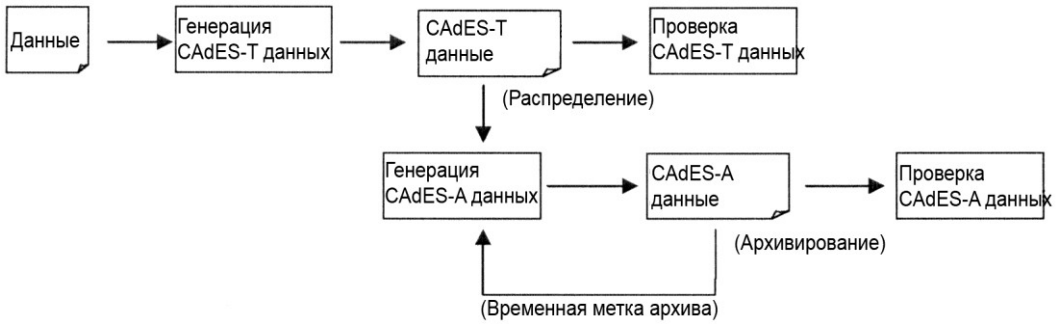

Рисунок 1 — Связь между данными CAdES-T и данными CAdES-A

6.2 Представление требуемого уровня

Данная часть ISO 14533 определяет следующие методы представления требуемого уровня (в виде профилей) каждого элемента, соответствующего данным CAdES-T и данным CAdES-A.

a) Обязательные (M) Элементы, которые требуют уровень “Обязательный”, должны быть реализованы без ошибок. Если такой элемент имеет опциональные субэлементы, должен быть выбран не менее чем один субэлемент. Любой элемент, требуемый уровень которого “Обязательный”, и который является одним из субэлементов опционального элемента, должен быть выбран во всех случаях, когда выбран опциональный элемент.