МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO 14533-2

Первое издание
2012-09-15

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

Часть 2.
Долгосрочные профили подписей для усовершенствованных электронных подписей XML

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 14533-2:2012
https://standards.iteh.ai/c...
3a5a...-2012

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

Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

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

Ссылочный номер
ISO 14533-2:2012(R)

© ISO 2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 14533-2:2012
https://standards.iteh.ai/catalog/standards/sist/38cd461e-1716-4dbc-b9d2-3a5a712475ca/iso-14533-2-2012

ДОКУМЕНТ ЗАЩИЩЁН АВТОРСКИМ ПРАВОМ

© ISO 2012

Все права сохраняются. Если не указано иное, никакую часть настоящей публикации нельзя копировать или использовать в какой-либо форме или каким-либо электронным или механическим способом, включая фотокопии и микрофильмы, без предварительного письменного согласия ISO по адресу, указанному ниже, или членов ISO в стране регистрации пребывания.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Опубликовано в Швейцарии

Содержание

Страница

Предисловие iv

Введение v

1 Область применения 1

2 Нормативные ссылки 1

3 Термины и определения 1

4 Символы 2

5 Требования 2

6 Долгосрочные профили подписей 3
6.1 Определённые профили 3
6.2 Представление требуемого уровня 3
6.3 Стандарт по установке требуемого уровня 4
6.4 Действия, выполняемые, когда опциональный элемент не реализуется 4
6.5 XAdES-T профиль 5
6.6 XAdES-A профиль 6
6.7 Данные валидации временной метки 8

Приложение A (нормативное) **Декларация соответствия поставщиков и его приложения** 9

Приложение B (нормативное) **Структура знака временной метки** 14

Библиография 16

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 14533-2:2012
https://standards.iteh.ai/catalog/standards/sist/38cd461e-1716-4dbc-b9d2-3a5a712475ca/iso-14533-2-2012

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 14533-2 был разработан Техническим комитетом ISO/TC 154, *Процессы, элементы данных и документы в области коммерции, промышленности и администрирования*.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 14533-2:2012
3a5a712475ca/iso-14533-2-2012

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

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

© ISO 2012 – Все права сохраняются

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 XML (расширяемый язык маркировки) (XAdES), разработанные Европейским институтом телекоммуникационных стандартов (European Telecommunications Standards Institute (ETSI)).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 14533-2:2012
https://standards.iteh.ai/catalog/standards/sist/38cd461e-1716-4dbc-b9d2-3a5a712475ca/iso-14533-2-2012

© ISO 2012 – Все права сохраняются

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 14533-2:2012
https://standards.iteh.ai/catalog/standards/sist/38cd461e-1716-4dbc-b9d2-3a5a712475ca/iso-14533-2-2012

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

Часть 2.
Долгосрочные профили подписей для усовершенствованных электронных подписей XML

1 Область применения

Данная часть ISO 14533 устанавливает элементы, включающие определённые в XML усовершенствованные электронные подписи (XAdES), 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ПРИМЕЧАНИЕ Усовершенствованные электронные подписи XML (XAdES) представляют собой расширенные технические условия для расширяемого языка разметки (XML), находящего широкое применение.

ISO 14533-2:2012
https://standards.iteh.ai/catalog/standards/sist/38cd461e-1716-4dbc-b9d2-3a5a712475ca/iso-14533-2-2012

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).

ISO 14533-1, *Процессы, элементы данных и документы в торговле, промышленности и администрировании. Долгосрочные профили подписей. Часть 1. Долгосрочные профили подписей для усовершенствованных электронных подписей CMS*

ETSI TS 101 903 v1.4.1 (2009-06), *XML Advanced Electronic Signatures (XAdES)*[1)]

3 Термины и определения

Для целей настоящего документа применяются термины и определения, указанные в ISO 14533-1 и ниже в тексте.

3.1
подпись XML
XML signature
синтаксис подписи и обработка данного сообщения

ПРИМЕЧАНИЕ Подпись XML определена в справке *Синтаксис и обработка подписи XML*, Рекомендации W3C, 12 февраля 2002 г.

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

© ISO 2012 – Все права сохраняются

3.2
усовершенствованная электронная подпись XML
XML advanced electronic signature
XAdES
общее обозначение усовершенствованных электронных подписей XML, определённое в ETSI TS 101 903, для которых подписант может быть идентифицирован, а любое нелегальное изменение данных определено

3.3
XAdES с временем
XAdES with time
XAdES-T
усовершенствованная электронная подпись XML, определённая в ETSI TS 101 903, содержащая информацию, позволяющую определить SigningTime (например, временную метку подписи)

3.4
архивное XAdES
archival XAdES
XAdES-A
усовершенствованная электронная подпись XML, определённая в ETSI TS 101 903, содержащая информацию, позволяющую определить любые незаконные изменения информации, относящейся к подписи, включая предмет подписи и данные валидации (например, временную метку архива)

3.5
элемент подписи
signature element
элемент выполняющий роль маршрута к подписи XML. Могут быть два или более элемента подписи для одного объекта подписи

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 14533-2:2012
https://standards.iteh.ai/catalog/standards/sist/38cd461e-1716-4dbc-b9d2-3a5a712475ca/iso-14533-2-2012

4 Символы

Следующие символы используются для указания “требуемого уровня”.

— C Договорный

— M Обязательный

— O Опциональный

5 Требования

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

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

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

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

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

 © ISO 2012 – Все права сохраняются

b) подробные спецификации, относящиеся к обработке любых элементов, которую требует уровень “Договорный” в профиле XAdES-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 XAdES-T и данных XAdES-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 XAdES:

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

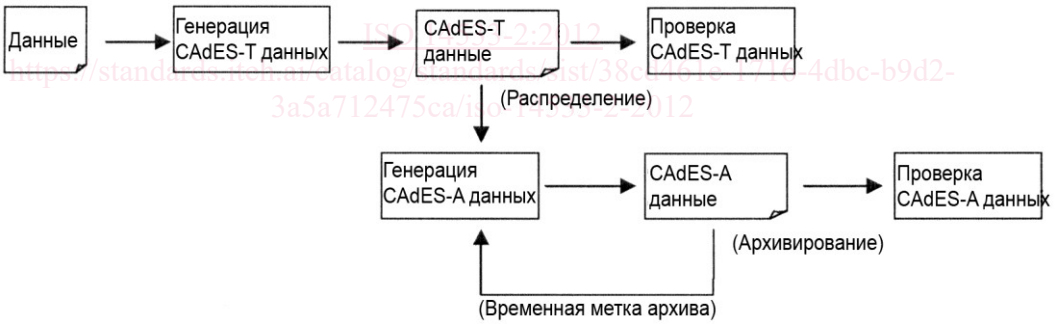

Рисунок 1 — Связь между данными XAdES-T и данными XAdES-A

6.2 Представление требуемого уровня

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

b) Опциональный (O) Элементы, требуемый уровень которых “Опциональный”, могут быть реализованы по решению исполнителя программы.

© ISO 2012 – Все права сохраняются

c) Договорный (C) Элементы, требуемый уровень которых “Договорный”, могут быть реализованы по решению исполнителя программы, при условии, что подробные спецификации по его обработке предоставляются отдельно.

6.3 Стандарт по установке требуемого уровня

Требуемый уровень каждого элемента, составляющего данные XAdES-T и данные XAdES-A, должен быть установлен в соответствии со следующими требованиями.

a) Требуемый уровень должен быть “Обязательный” для элементов, для которых требуемый уровень “Обязательный” согласно определению XAdES, и которые необходимы для генерирования и валидации долгосрочных подписей. Элементы, требуемый уровень которых “Опциональный” в определении XAdES, определяются как “Обязательный”, “Опциональный” или “Договорный”.

b) Требуемый уровень должен быть “Договорный” для элементов, определённых внешними источниками данных.

   ПРИМЕР OtherCertificateFormat.

c) Требуемый уровень должен быть “Договорный” для элементов, предназначенных для взаимодействия с некоторыми приложениями.

   ПРИМЕР DataObjectFormat.

d) Требуемый уровень должен быть “Договорный” для элементов, включающих зависящий от операции фактор.

   ПРИМЕРЫ Сертификат атрибута; отметка времени.

   ПРИМЕЧАНИЕ Временная метка архивного типа, определённая в ISO/IEC 18014-2, включена в “Отметки времени или другие методы.”

e) Требуемый уровень должен быть “опциональный” для элементов, содержащих только ссылочную информацию.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 14533-2:2012
https://standards.iteh.ai/catalog/standards/sist/38cd461e-1716-4dbc-b9d2-

6.4 Действия, выполняемые, когда опциональный элемент не реализуется

Следующие действия должны быть выполнены, когда данные XAdES, использованные при транзакции валидации, содержат нереализованный элемент.

a) Когда требуемый уровень элемента верхнего уровня является обязательным и один или более опциональный элемент низшего уровня должен быть выбран, или один или более подходящие опциональные элементы должны быть выбраны, валидатор должен выполнять меры предосторожности, учитывающие, что валидация требует выполнения вышеупомянутых элементов; в противном случае валидация не может быть выполнена.

   ПРИМЕР При транзакции валидации элемент BasicOCSPResponse детектируется когда только выполняется обработка элементов CertificateList, среди всех других опциональных элементов в RevocationValues.

b) Когда CounterSignature является нереализованным элементом, валидатор должен выполнять меры предосторожности, учитывающие, что валидация требует реализации вышеупомянутого элемента; в противном случае валидация не может быть выполнена.

c) Опциональные элементы, другие, чем указанные выше, могут игнорироваться при реализации.

 © ISO 2012 – Все права сохраняются

6.5 XAdES-T профиль

6.5.1 Общие положения

Требуемые уровни составляющих элементов данных XAdES-T указаны в 6.5.2 и 6.5.3.

6.5.2 Элемент подписи

В Таблице 1 установлены требуемые уровни каждого составляющего элемента подписи XML. Требуемый уровень должен быть “Договорный” для любого элемента, не перечисленного в Таблице 1.

Таблица 1 — Элемент подписи

Элемент или атрибут [a]	Требуемый уровень	ETSI TS 101 903 v1.4.1 Ссылка
Id attribute	M [b]	4.4
ds:SignedInfo	M	4.4
ds:CanonicalizationMethod	M	4.4
ds:SignatureMethod	M	4.4
ds:Reference	M	4.4
ds:Transforms	O	4.4
ds:DigestMethod	M	4.4
ds:DigestValue	M	4.4
ds:SignatureValue	M	4.4
ds:KeyInfo	O [c]	4.4
ds:Object	M	4.4

[a] Префикс “ds” соответствует области имени подписи XML.

[b] “Опциональный” в подписи XML, но “Обязательный” в ETSI TS 101 903.

[c] Требуется либо ds:KeyInfo (информация службы ключей) или SigningCertificate (Таблица 3). Если выбрано ds:KeyInfo (Обязательный в ETSI TS 101 903 v1.1.1), в качестве субэлемента должен быть включён X.509 элемент данных, определённый в подписи XML.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 14533-2:2012
https://standards.iteh.ai/catalog/standards/sist/38cd461e-171e-4dbc-b9d2-
3a5c71f475ce/iso-14533-2-2012

6.5.3 Элемент объект, элемент SignedProperties, элемент UnsignedProperties

Таблицы 2, 3 и 4 устанавливают требуемые уровни элементов, которые определяют подписанные атрибуты и неподписанные атрибуты. Требуемый уровень должен быть “Договорный” для всех подписанных и неподписанных элементов атрибутов, не перечисленных в Таблицах 2, 3 и 4.

ПРИМЕЧАНИЕ Неподписанные элементы атрибутов, не перечисленные в Таблицах 2, 3 и 4, включают, но не ограничиваются этим, CompleteCertificateReferences и CompleteRevocationReferences указанные в Таблице 5. Данные XAdES-T, к которым добавлены CompleteCertificateReferences и CompleteRevocationReferences, могут быть сделаны соответствующими профилю XAdES-T путём отдельного обеспечения обработки этих элементов.

© ISO 2012 – Все права сохраняются