ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 17090-4— 2016

Информатизация здоровья

ИНФРАСТРУКТУРА С ОТКРЫТЫМ КЛЮЧОМ

Часть 4

Электронные подписи медицинских документов

(ISO 17090-4:2014, IDT)

Издание официальное

Москва
Стандартинформ
2017

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Министерства здравоохранения Российской Федерации» (ЦНИИОИЗ Минздрава) и Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава — постоянным представителем ISO TC 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2016 г. № 2104-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 17090-4:2014 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 4. Электронные подписи медицинских документов» (ISO 17090-4:2014 «Health informatics — Public key infrastructure — Part 4: Digital signatures for healthcare documents», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2017

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Прикладные системы 2
4.1 Целевая система 2
4.2 Процесс создания 3
4.3 Процесс проверки 4
4.4 Спецификация CAdES 10
4.5 Спецификация XAdES 14
Приложение А (справочное) Целевые сценарии 19
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 21
Библиография 22

Введение

Перед системой здравоохранения стоит проблема сокращения расходов с помощью перехода от бумажного документирования процессов к электронному. В новых моделях оказания медицинской помощи особо подчеркивается необходимость совместного использования сведений о пациенте расширяющимся кругом медицинских специалистов, выходящего за рамки традиционных организационных барьеров.

Персональная медицинская информация обычно передается с помощью электронной почты, удаленного доступа к базе данных, электронного обмена данными и других приложений. Среда Интернет предоставляет высокоэффективные и доступные средства обмена информацией, однако она не безопасна и при ее использовании необходимо принимать дополнительные меры обеспечения конфиденциальности и неприкосновенности личной жизни. Усиливаются такие угрозы безопасности, как случайный или преднамеренный несанкционированный доступ к медицинской информации, и системе здравоохранения необходимо иметь надежные средства защиты, минимизирующие риск несанкционированного доступа.

Каким же образом система здравоохранения может обеспечить соответствующую эффективную и в то же время экономичную защиту передачи данных через сеть Интернет? Решение этой проблемы может быть обеспечено с помощью технологии цифровых сертификатов и инфраструктуры открытых ключей (ИОК).

Для правильного применения цифровых сертификатов требуется сочетание технологических, методических и административных процессов, обеспечивающих защиту передачи конфиденциальных данных в незащищенной среде с помощью «шифрования с открытым ключом» и подтверждение идентичности лица или объекта с помощью «сертификатов». В сфере здравоохранения в это сочетание входят средства аутентификации, шифрования и электронной подписи, предназначенные для выполнения административных и клинических требований конфиденциальности доступа и передачи медицинских документов индивидуального учета. Многие из этих требований могут быть удовлетворены с помощью служб, использующих применение цифровых сертификатов (включая шифрование, целостность информации и электронные подписи). Особо эффективно использование цифровых сертификатов в рамках официального стандарта защиты информации. Многие организации во всем мире начали использовать цифровые сертификаты подобным образом.

Если обмен информацией должен осуществляться между медицинским прикладным программным обеспечением разных организаций, в том числе относящихся к разным ведомствам (например, между информационными системами больницы и поликлиники, оказывающих медицинскую помощь одному и тому же пациенту), то интероперабельность технологий цифровых сертификатов и сопутствующих политик, регламентов и практических приемов приобретает принципиальное значение.

Для обеспечения интероперабельности различных систем, использующих цифровые сертификаты, необходимо создать систему доверительных отношений, с помощью которой стороны, ответственные за обеспечение прав личности на защиту персональной информации, могут полагаться на политики и практические приемы и, в дополнение, на действительность электронных сертификатов, выданных другими уполномоченными организациями.

Во многих странах система цифровых сертификатов используется для обеспечения безопасного обмена информацией в пределах национальных границ. Если разработка стандартов также ограничена этими пределами, то это приводит к несовместимости политик и регламентов удостоверяющих центров (УЦ) и центров регистрации (ЦР) разных стран.

Технология цифровых сертификатов активно развивается в рамках определенных направлений, не специфичных для здравоохранения. Непрерывно проводится важнейшая работа по стандартизации и, в некоторых случаях, по правовому обеспечению. С другой стороны, поставщики медицинских услуг во многих странах уже используют или планируют использовать цифровые сертификаты. Настоящий стандарт призван удовлетворить потребность в управлении данным интенсивным международным процессом.

Настоящий стандарт содержит общие технические, эксплуатационные и методические требования, которые должны быть удовлетворены для обеспечения использования цифровых сертификатов в целях обмена медицинской информацией в пределах одного домена, между доменами и за пределами

границ одной юрисдикции. Его целью является создание основ глобальной интероперабельности. Настоящий стандарт изначально предназначен для поддержки трансграничного обмена данными на основе цифровых сертификатов, однако он также может служить руководством по широкому использованию цифровых сертификатов в здравоохранении на национальном или региональном уровнях. Интернет все шире используется как средство передачи медицинских данных между организациями здравоохранения и является единственным реальным вариантом для трансграничного обмена данными в этой сфере.

Серия стандартов ИСО 17090 должна рассматриваться как единое целое, поскольку каждая из четырех ее частей вносит свой вклад в определение того, как цифровые сертификаты могут использоваться для обеспечения сервисов безопасности в системе здравоохранения, включая аутентификацию, конфиденциальность, целостность данных и технические возможности поддержки качества электронной подписи.

В настоящем стандарте представлены профили электронной подписи, специфичные для сферы здравоохранения. Они основаны на стандарте организации ETSI и профиле этого стандарта, определенном в спецификациях CAdES и XAdES.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

ИНФРАСТРУКТУРА С ОТКРЫТЫМ КЛЮЧОМ

Часть 4

Электронные подписи медицинских документов

Health informatics. Public key infrastructure. Part 4. Digital signatures for healthcare documents

Дата введения — 2018—01—01

1 Область применения

В настоящем стандарте приведены минимальные требования к созданию и проверке электронных подписей и соответствующих сертификатов, а также к их форматам, способствующие обеспечению возможности обмена электронными подписями и предотвращения некорректных или юридически не признаваемых электронных подписей.

Кроме того, в настоящем стандарте определено доказываемое соответствие политике ИОК, необходимое в сфере здравоохранения. В настоящем стандарте признаются форматы долговременной электронной подписи, обеспечивающие целостность и неоспоримость длительно хранящейся электронной медицинской информации.

В целях улучшения и гарантирования интероперабельности в сфере здравоохранения настоящий стандарт соответствует стандартам ISO/ETSI, определяющим форматы долговременной электронной подписи.

Никакие ограничения на субъект подписываемых данных и их формат в настоящем стандарте не накладываются.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы, полное или частичное содержание которых неразрывно связано с настоящим стандартом. Если в ссылке указана дата публикации, то должен использоваться только цитируемый документ. Если дата в ссылке не указана, то должно использоваться последнее издание документа (включая все поправки):

ISO 17090-1:2008, Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services (Информатизация здоровья. Инфраструктура с открытым ключом. Часть 1. Структура и общие сведения)

ISO 17090-3:2008, Health informatics — Public key infrastructure — Part 3: Policy management of certification authority (Информатизация здоровья. Инфраструктура с открытым ключом. Часть 3. Управление политиками центра сертификации)

3 Термины и определения

В настоящем стандарте применены термины по ИСО 17090-1, а также следующие термины с соответствующими определениями:

3.1 **цепочка сертификатов** (certification path): Упорядоченная последовательность сертификатов, связывающая проверяемый сертификат с сертификатом доверенного удостоверяющего центра.

Издание официальное

3.2 **проверка цепочки сертификатов** (certification path validation): Проверка каждого сертификата цепочки вплоть до сертификата доверенного удостоверяющего центра, включая проверку вхождения в списки отозванных сертификатов.

3.3 **хэш-функция** (hash function): Метод вычислений, позволяющий генерировать случайное значение фиксированной длины по данным произвольной длины.

Примечания

1 Сгенерированное значение, называемое «хэш-кодом», обладает свойством односторонности (исходные данные не могут быть вычислены по этому значению) и малой вероятностью получения одинакового значения (коллизии) по двум различным данным.

2 Если при отправке/получении данных хэш-код был вычислен на стороне отправителя и совпал с хэш-кодом, вычисленным получателем данных, то благодаря этим свойствам можно с высокой степенью доверия утверждать, что данные не были искажены в процессе передачи.

4 Прикладные системы

4.1 Целевая система

Следующие системы являются целевыми для настоящего стандарта:

a) библиотека электронной подписи, включающая в себя функции вычисления и проверки электронной подписи, предназначенная для использования компонентами медицинских информационных систем;

b) программы вычисления и проверки электронной подписи, которые могут использоваться автономно или вместе с компонентами медицинских информационных систем.

К числу целевых не относятся следующие системы:

a) компоненты медицинских информационных систем, не связанные с непосредственной обработкой электронной подписи;

b) компоненты медицинских информационных систем, которые обрабатывают электронную подпись и результаты ее проверки с помощью библиотеки электронной подписи, специальной программы электронной подписи или специальной программы проверки электронной подписи;

c) интерфейс прикладных программ и пользовательский интерфейс. На рисунке 1 показан пример уровней обработки. В этом примере прикладной уровень электронной подписи (библиотека электронной подписи, программа электронной подписи или программа проверки электронной подписи) является целевой системой для настоящего стандарта, а следующий уровень, а также криптопровайдер и PKCS#11 к целевым системам не относятся.

В ИОК, предназначенной для использования в сфере здравоохранения, предполагается, что, согласно подпункту 7.6.2.12 ИСО 17090-3:2008, устройства хранения секретных ключей, используемые их владельцами, должны соответствовать стандартам, уровень которых равен уровню 1 Федерального стандарта США FIPS-140-2 или превышает его. Кроме того, секретные ключи могут храниться не только на смарт-картах, как показано на рисунке, но также на USB-токенах, в программных токенах и т. д.

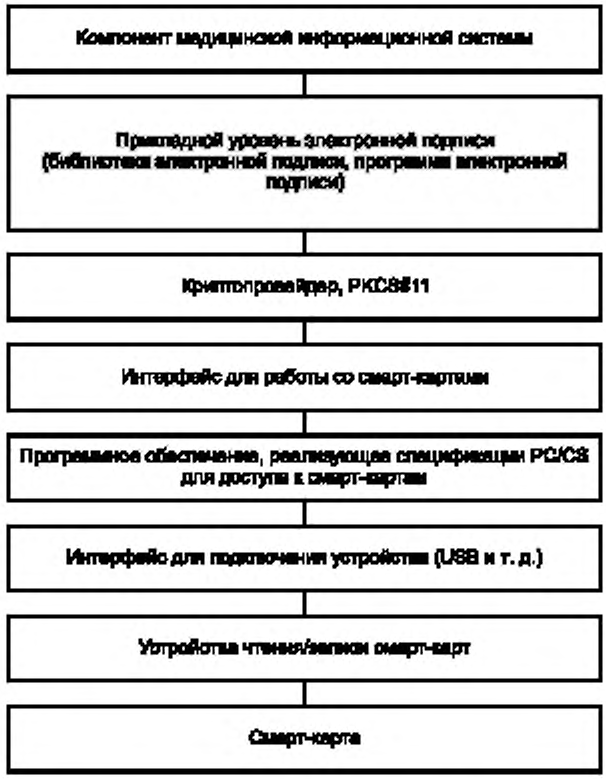


Рисунок 1 — Пример спецификации уровней обработки электронной подписи

4.2 Процесс создания

Формат электронной подписи, описанный в настоящем стандарте, основан на спецификациях усовершенствованной электронной подписи, приведенных в стандартах организации ETSI CAdES (CMS Advanced Digital Signature [[5]]) и XAdES (XML Advanced Digital Signature [[6]]).

В зависимости от назначения электронной подписи в этих спецификациях определены разные форматы, а именно:

- ES: формат, в котором предусмотрены значение электронной подписи, собственно данные, а также информация о подписанте;

- ES-T: расширение формата ES, в котором добавлена метка времени подписи, полученная от доверенной службы времени и используемая для доказательства момента постановки подписи,

- ES-C: расширение формата ES-T, в котором добавлены ссылки на доказательства подлинности,

- ES-X: расширение формата ES-C, в котором добавлена защита ссылок на доказательства подлинности;

- ES-X Long: расширение формата ES-C, в котором добавлена информация об отзыве сертификатов, необходимая для проверки подписи;

- ES-A: формат, в который включена архивная метка времени, предназначенная для защиты подписи, меток времени и доказательств подлинности.

Взаимосвязи различных типов формата электронной подписи показаны на рисунке 2.

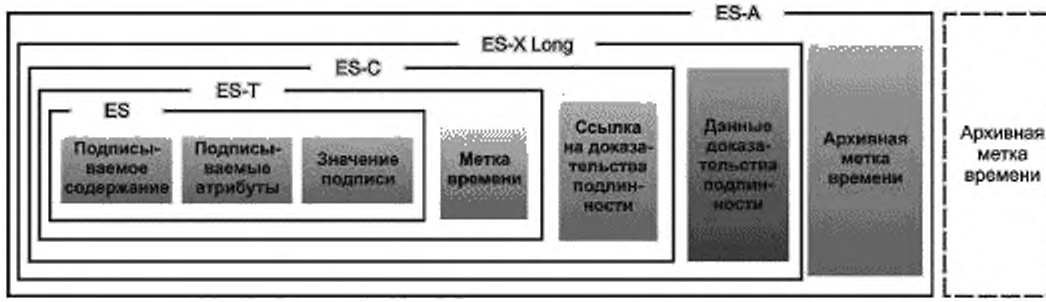


Рисунок 2 — Типы формата электронной подписи

В настоящем стандарте описаны только профили ES-T и ES-A. Другие форматы рассматриваются как промежуточные, предназначенные для генерирования ES-T или ES-A, и не входят в область применения настоящего стандарта.

Формат электронной подписи основан на спецификациях усовершенствованной электронной подписи, предложенных организацией ETSI. В настоящем стандарте описаны формат CAdES [[5]], основанный на спецификации CMS (Cryptographic Message Syntax — синтаксис криптографических сообщений), и формат XAdES [[6]], основанный на спецификации XML Advanced Digital Signature (усовершенствованная электронная подпись XML-документов).

Профиль CAdES, определяющий обязательные/необязательные элементы, необходимые для создания подписи в форматах ES-T и ES-A, описан в 4.4; в 4.5 описан профиль XAdES представления форматов ES-T и ES-A на языке XML.

4.3 Процесс проверки

В настоящем подразделе приведен краткий обзор основных процессов проверки. В настоящем стандарте не предусмотрены методы проверки необязательных атрибутов. Если данные подписи содержат необязательные атрибуты, то они должны правильно проверяться в соответствии с другими спецификациями, политиками или руководствами.

4.3.1 Проверка подписи в формате ES

4.3.1.1 Процессы проверки подписи в формате ES

Ниже описаны процессы проверки электронной подписи в формате ES. Порядок выполнения этих процессов не должен изменяться (см. рисунок 3).

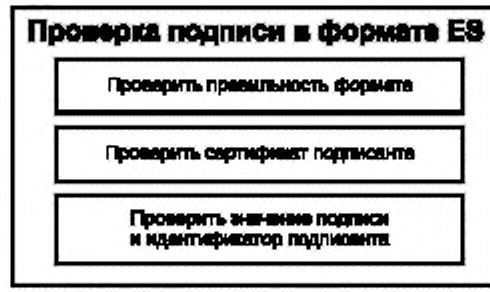


Рисунок 3 — Процессы проверки подписи в формате ES

Процессы проверки осуществляются следующим образом.

a) Проверка формата данных подписи:

1) проверить правильность формата электронной подписи.

b) Проверка сертификата подписанта.

Для проверки действительности сертификата подписанта выполняются следующие действия:

1) выполнить проверку цепочки сертификатов, описанную в документе RFC 5280;

2) выполнить проверку расширений сертификата, предусмотренных в ИОК здравоохранения;

c) Проверка значения подписи и идентификатора подписанта.

При этой проверке выполняются следующие действия:

1) проверить значение подписи, используя открытый ключ подписанта;

2) проверить идентификатор подписанта, указанный в сертификате.

Объяснения к указанным выше процессам приведены в приложении А.

4.3.1.2 Описание процессов проверки

Описание процессов проверки приведено в таблице 1.

Таблица 1 — Описание процессов проверки

Процесс проверки	Описание
a) Проверка формата данных подписи	Должно быть проверено выполнение следующих условий: - структура данных подписи соответствует установленному формату; - данные подписи содержат все элементы, указанные обязательными в профиле; - номер версии данных подписи правилен
b) Проверка сертификата подписанта	1) Проверка цепочки сертификатов описана в документе RFC 5280: - построить и проверить цепочку сертификатов для сертификата подписанта
	2) Проверить расширения сертификата подписанта, предусмотренные в ИОК здравоохранения: - реализации настоящего стандарта должны обеспечивать выполнение функций проверки следующих элементов: - идентификатор политики сертификации, принятой в ИОК здравоохранения; - значение атрибута hcRole, указанное в сертификате подписанта; - метод проверки не входит в область применения настоящего стандарта. В приложениях могут быть выбраны наиболее подходящие методы
c) Проверка значения подписи и идентификатора подписанта	1) Проверить значение подписи с помощью открытого ключа подписанта. Должны быть выполнены следующие действия: - вычислить хэш-код подписанных данных и убедиться, что он совпадает с хэш-кодом сообщения, указанным в подписи; - проверить значение подписи и подписанных атрибутов, используя открытый ключ подписанта
	2) Проверить соответствие идентифицирующей информации, указанной в сертификате подписанта: - убедиться, что идентификатор подписанта совпадает с атрибутами сертификата подписанта, содержащимися в данных подписи

4.3.2 Проверка подписи в формате ES-T

4.3.2.1 Процессы проверки подписи в формате ES-T

В настоящем подразделе описаны процессы проверки электронной подписи в формате ES-T.

Порядок выполнения этих процессов не должен изменяться. См. рисунок 4.

Процессы проверки осуществляются следующим образом:

Проверка метки времени подписи:

1) проверить сертификат доверенной службы, предоставляющей метки времени подписи;

2) проверить значение подписи метки, полученной от этой службы;

3) проверить отпечаток сообщения в метке времени.

Проверка действительности подписи на момент, указанный в метке времени:

1) убедиться, что подпись подписанта была действительная на момент, указанный в метке времени;

2) проверить приемлемость доверенного удостоверяющего центра.

Указанные выше процессы разъясняются в приложении А.

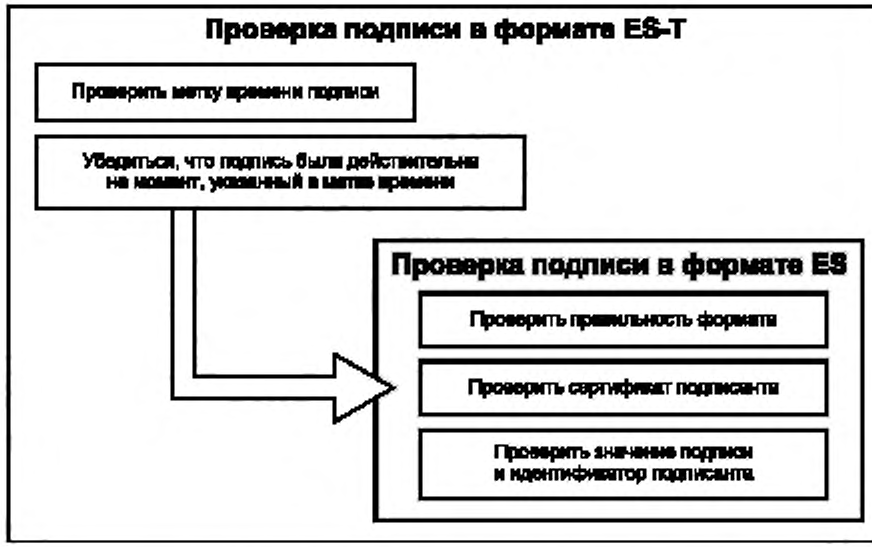


Рисунок 4 — Процессы проверки подписи в формате ES-T

4.3.2.2 Описание процессов проверки

Описание процессов проверки приведено в таблице 2.

Таблица 2 — Описание процессов проверки

Процесс проверки	Описание
a) Проверка метки времени подписи	1) Проверить сертификат доверенной службы, предоставляющей метки времени подписи. Должны быть выполнены следующие действия проверки: - проверить цепочку сертификатов в соответствии с документом RFC 5280; - убедиться, что сертификат доверенной службы времени содержит расширенный ключ использования в целях предоставления меток времени
	2) Проверить подпись доверенной службы времени, предоставляющей метки времени. Проверить значение подписи метки времени, используя открытый ключ, содержащийся в сертификате доверенной службы времени
	3) Проверить отпечаток сообщения в метке времени: - вычислить хэш-код подписи подписанта и убедиться, что он совпадает с отпечатком сообщения в метке времени
b) Проверка формата ES на момент метки времени подписи	1) Проверить формат ES на момент метки времени подписи: - проверить, что сертификат подписанта был действителен на момент, указанный в метке времени подписи.
	2) Проверить приемлемость доверенного удостоверяющего центра: - проверка подписи может выполняться спустя длительное время после создания данных в формате ES-T. В момент ее проверки доверенный удостоверяющий центр, действительный на момент создания подписи, может оказаться закрытым или скомпрометированным. В этом случае проверяющий должен убедиться в приемлемости удостоверяющего центра; - например, подписант и проверяющий могли заключить соглашение об удостоверяющем центре (к примеру, в виде политики подписи) и контролировать его выполнение для защиты от компрометации УЦ, либо проверяющий может обратиться к доверенной третьей стороне, контролирующей историю информации о проверке сертификатов. Эти методы не входят в область применения настоящего стандарта

4.3.3 Проверка подписи в формате ES-A

4.3.3.1 Процессы проверки подписи в формате ES-A

В настоящем подразделе описаны процессы проверки электронной подписи в формате ES-A. Порядок выполнения этих процессов не должен изменяться. См. рисунок 5.

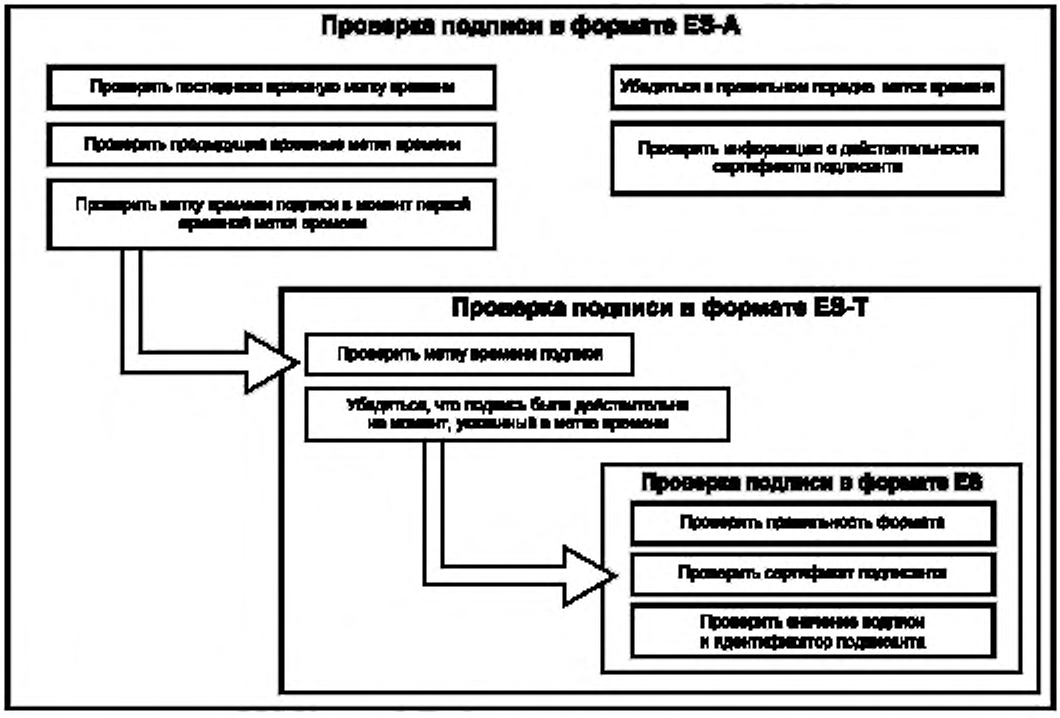


Рисунок 5 — Процессы проверки подписи в формате ES-A

Процессы проверки осуществляются следующим образом:

a) Проверка последней архивной метки времени.

Проверить, что последняя архивная метка времени действительна на момент проверки подписи:

1) проверить сертификат доверенной службы, предоставившей последнюю архивную метку времени;

2) проверить подпись доверенной службы, предоставившей последнюю архивную метку времени;

3) проверить соответствие последней архивной метки времени и целевых данных метки времени.

b) Проверка предыдущих архивных меток времени, если таковые есть.

Проверить, что метка времени была действительной на момент архивирования подписанных данных:

1) проверить сертификат доверенной службы, предоставившей архивную метку времени;

2) проверить подпись доверенной службы, предоставившей архивную метку времени;

3) проверить соответствие архивной метки времени и целевых данных метки времени;

4) проверить, что доверенный удостоверяющий центр архивной метки времени приемлем.

c) Проверка информации о действительности сертификата подписанта:

1) проверить действительность цепочки сертификатов, архивированной в данных о действительности сертификата;

2) проверить приемлемость доверенного удостоверяющего центра;

3) проверить действительность информации об отзыве сертификатов, включенной в данные о действительности сертификата;

4) проверить приемлемость доверенного удостоверяющего центра, предоставившего информацию об отзыве сертификатов;

d) Проверка метки времени подписи.

Проверить приемлемость метки времени подписи:

1) проверить, что метка времени подписи была действительной на момент архивирования;

2) проверить приемлемость доверенного удостоверяющего центра, указанного в метке времени подписи.

e) Проверить правильность данных формата ES на момент, указанный в метке времени подписи:

1) проверить, что данные формата ES были действительны на момент, указанный в метке времени подписи,

2) проверить приемлемость доверенного удостоверяющего центра.

f) Проверить правильность порядка моментов меток времени и моментов выпуска информации об отзыве сертификатов.

Объяснения к указанным выше процессам приведены в приложении А.

4.3.3.2 Описание процессов проверки

Описание процессов проверки приведено в таблице 3.

Таблица 3 — Описание процессов проверки

Процесс проверки	Описание
a) Проверка последней архивной метки времени	1) Проверить сертификат доверенной службы, предоставившей последнюю архивную метку времени Должны быть выполнены следующие действия проверки: - проверить действительность сертификата на момент проверки; - убедиться, что сертификат доверенной службы времени содержит расширенный ключ использования в целях предоставления меток времени
	2) Проверить подпись доверенной службы, предоставившей последнюю архивную метку времени: - проверить значение подписи метки времени, используя открытый ключ, содержащийся в сертификате доверенной службы времени
	3) Проверить отпечаток сообщения в метке времени: вычислить хэш-код целевых полей архива и убедиться, что он совпадает с отпечатком сообщения в метке времени
b) Проверка предыдущей архивной метки времени, если таковая имеется	1) Проверить сертификат доверенной службы, предоставившей архивную метку времени: - проверить действительность сертификата доверенной службы, предоставившей архивную метку времени в момент, указанный в архивной метке времени предыдущего поколения. Связь с моментом проверки показана на рисунке 6
	2) Проверить подпись доверенной службы, предоставившей архивную метку времени
	3) Проверить соответствие архивной метки времени и данных отпечатка
	4) Проверить, что доверенный удостоверяющий центр архивной метки времени приемлем: - действие сертификата удостоверяющего центра могло завершиться к моменту проверки архивной метки времени; - чтобы проверить действительность этого сертификата, следует убедиться в его приемлемости у удостоверяющего центра. Соответствующие методы не входят в область применения настоящего стандарта
c) Проверка информации о действительности сертификата подписанта	1) Проверить действительность цепочки сертификатов, архивированной в данных о действительности сертификата
	2) Проверить приемлемость доверенного удостоверяющего центра, выпустившего сертификат

Окончание таблицы 3

Процесс проверки	Описание
	3) Проверить действительность информации об отзыве сертификатов, включенной в данные о действительности сертификата: - сравнить время выпуска информации об отзыве сертификатов с временем архивирования и следует убедиться, что эта информация приемлема
	4) Проверить приемлемость доверенного удостоверяющего центра, предоставившего информацию об отзыве сертификатов: - следует убедиться, что удостоверяющий центр, выпустивший сертификат, которым подписана информация об отзыве, был приемлем на время проверки действительности этого сертификата
d) Проверка метки времени подписи в момент первой архивной метки времени	1) Проверить, что метка времени подписи была действительной в момент первой архивной метки времени: - выполнить процедуру, описанную в настоящей таблице, для момента первой архивной метки времени. Проверьте, что сертификат доверенной службы времени был действительным в момент первой архивной метки времени
	2) Проверить приемлемость доверенного удостоверяющего центра, указанного в метке времени подписи: - действие сертификата удостоверяющего центра могло завершиться к моменту проверки сертификата подписанта; - чтобы проверить действительность сертификата удостоверяющего центра, следует убедиться в его приемлемости у удостоверяющего центра. Соответствующие методы не входят в область применения настоящего стандарта
e) Проверка действительности подписи подписанта на момент метки времени подписи	1) Проверить подпись подписанта на основе процедур, описанных в приложении А, используя информацию об отзыве сертификатов, проверенную с помощью процесса c). Следует убедиться, что сертификат подписанта был действителен на момент метки времени подписи
	2) Проверить приемлемость корневого доверенного удостоверяющего центра цепочки сертификатов, построенной для сертификата подписанта: - действие сертификата удостоверяющего центра могло завершиться к моменту проверки сертификата подписанта; - чтобы проверить действительность сертификата удостоверяющего центра, убедитесь в его приемлемости у удостоверяющего центра. Соответствующие методы не входят в область применения настоящего стандарта
f) Проверка порядка моментов времени и их соответствия	Проверить соответствие моментов времени, не участвующих в описанном выше процессе: - следует убедиться в правильном соответствии моментов меток времени подписи и архивных меток времени

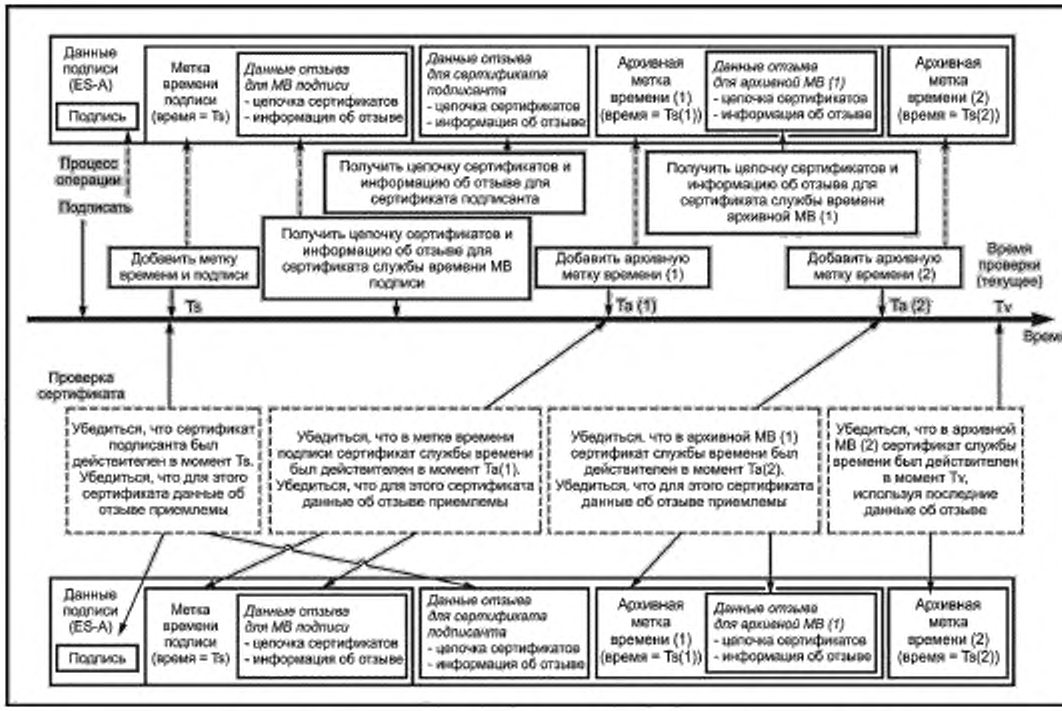


Рисунок 6 — Связь моментов времени при проверке подписи в формате ES-A (в случае двух архивных меток времени)

4.4 Спецификация CAdES

В настоящем подразделе описаны требования к созданию или проверке данных, соответствующих спецификации CAdES.

В таблице 4 описаны связи профилей, определенных в настоящем стандарте, а в таблице 5 описана структура данных, соответствующих спецификации CAdES. В таблицах 6, 7 и 8 описаны профили, определенные в настоящем стандарте, а в таблице 9 — элементы данных, взятые из спецификации CAdES.

4.4.1 Профиль долговременной подписи

Чтобы электронная подпись могла быть проверена спустя длительное время после ее создания, должно быть идентифицируемо время подписи, при этом должны выявляться все несанкционированные изменения подписанных данных, включая субъект информации и сведения об отзыве сертификатов. Кроме того, должна обеспечиваться интероперабельность. В настоящем стандарте приведены определения следующих двух профилей, удовлетворяющих предыдущим требованиям, предъявляемым к спецификациям CAdES:

a) Профиль CAdES-T

Профиль, относящийся к генерации и проверке данных, соответствующих спецификации CAdES-T.

b) Профиль CAdES-A

Профиль, относящийся к генерации и проверке данных, соответствующих спецификации CAdES-A.

На рисунке 7 показаны отношения между данными, соответствующими спецификациям CAdES-T и CAdES-A.

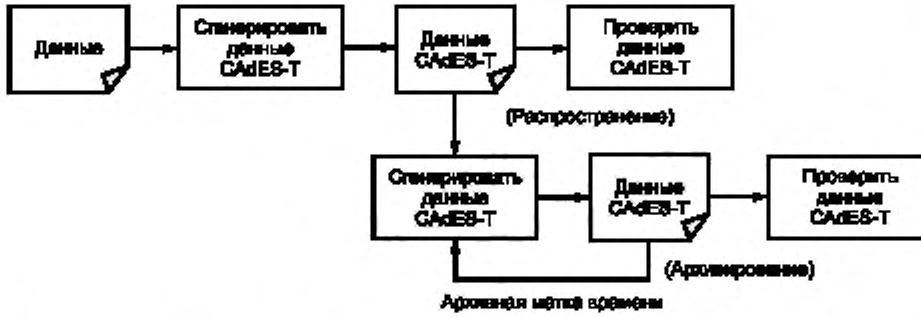


Рисунок 7 — Отношения между данными, соответствующими спецификациям CAdES-T и CAdES-A

4.4.2 Представление степени обязательности

В настоящем стандарте определены следующие методы представления степени обязательности (как профиля) каждого элемента, входящего в состав данных CAdES-T и CAdES-A:

a) Обязательный (O)

Элементы, у которых степень обязательности равна «O», должны быть реализованы. Если такой элемент имеет необязательные подчиненные элементы, то хотя бы один из них должен быть выбран. Любой элемент, имеющий степень обязательности «O» и являющийся подчиненным элементом необязательного элемента, должен быть выбран, если выбран этот необязательный элемент.

b) Необязательный (H)

Реализация элементов, у которых степень обязательности равна «H», оставлена на усмотрение разработчика.

c) Условный (У)

Реализация элементов, у которых степень обязательности равна «У», оставлена на усмотрение разработчика. Должны быть составлены детальные спецификации обработки любого элемента со степенью обязательности «У». Например, разработчик предоставляет спецификации таких элементов, раскрывая объявление поставщика о соответствии и приложение к нему (см. ИСО 14533-1:2012, приложение А, или ИСО 14533).

d) Запрещенный (З)

Элементы с уровнем обязательности «З» не должны присутствовать в данных. При проверке запрещенный элемент может игнорироваться.

4.4.3 Профиль CAdES-T

Состав элемента ContentInfo представлен в таблице 4.

Таблица 4 — Состав элемента ContentInfo

Элемент	Обязательность	Значение
ContentType	O	Id-signedData
Content	O	SignedData

Состав элемента SignedData представлен в таблице 5.

Таблица 5 — Состав элемента SignedData

Элемент	Обязательность	Значение
CMSVersion	O	
DigestAlgorithmIdentifiers	O	
EncapsulatedContentInfo	O	
—eContentType	O	

Окончание таблицы 5

Элемент	Обязательность	Значение
—eContent	Н	
CertificateSet (certificates)	Н	
—Certificate	Н	
—AttributeCertificateV2	З	
—OtherCertificateFormat	З	
RevocationInfoChoices (crls)	Н	
—CertificateList	Н	
—OtherRevocationInfoFormat	У	
SignerInfos	О	
—single	Н	
—parallel	Н	

Состав элемента SignerInfo представлен в таблице 6.

Таблица 6 — Состав элемента SignerInfo

Элемент	Обязательность	Значение
CMSVersion	О	
SignerIdentifier	О	
—IssuerAndSerialNumber	Н	
—SubjectKeyIdentifier	Н	
DigestAlgorithmIdentifier	О	
SignedAttributes	О	
SignatureAlgorithm	О	
SignatureValue	О	
UnsignedAttributes	О	

Состав элемента SignedAttributes представлен в таблице 7. Все элементы подписываемых и неподписываемых атрибутов, не перечисленные в таблицах 7 и 8, должны иметь степень обязательности «У».

Таблица 7 — Состав элемента SignedAttributes

Элемент	Обязательность	Значение
ContentType	М	
MessageDigest	М	
SigningCertificateReference	М	
—ESSSigningCertificate	Н[а)]	
—ESSSigningCertificateV2	Н[а)]	
—OtherSigningCertificate	З	

Окончание таблицы 7

Элемент	Обязательность	Значение
SignatureAlgorithmIdentifier	У	
SigningTime	Н[b)]	
ContentReference	У	
ContentIdentifier	У	
ContentHint	У	
CommitmentTypeIndicatio	У	
SignerLocation	У	
SignerAttribute	У	
ContentTimestamp	У	
[a)] Должен быть выбран либо элемент ESSSigningCertificate, либо элемент ESSSigningCertificateV2. [b)] Если элемент не реализован, его можно игнорировать.		

Дополнительные неподписываемые атрибуты представлены в таблице 8.

Таблица 8 — Дополнительные неподписываемые атрибуты

Элемент	Обязательность	Значение
CounterSignature	Н	
Signing-time	О	
—SignatureTimestamp	О	Метка времени, определенная в документе RFC 3161
—Time-Mark и т. д.	З	

4.4.4 Профиль CAdES-A

Профиль CAdES-A определен как расширенная форма профиля CAdES-T, к которой добавлены неподписываемые атрибуты, приведенные в таблице 0. Все элементы, не перечисленные в таблице 9, должны иметь степень обязательности «У».

Таблица 9 — Дополнительные неподписываемые атрибуты

Элемент	Обязательность	Значение
CompleteCertificateRefs	О (Н при проверке)	
CompleteRevocationRefs	О (Н при проверке)	
—CompleteRevRefs CRL	Н	
—CompleteRevRefs OCSP	Н	
—OtherRevRefs	З	
Ссылки на сертификаты атрибутов	З	
Ссылки на атрибуты отзыва	З	
CertificateValues	О	
—CertificateValues	Н	

Окончание таблицы 9

Элемент	Обязательность	Значение
—Certificates (сертификаты, контролируемые доверенной службой)	З	
RevocationValues	О	
—CertificateList	Н	
—BasicOCSPResponse	Н	
—OtherRevVals	З	
—Информация об отзыве, контролируемая доверенной службой	З	
CAdES-C-timestamp	З	
Ссылка на сертификаты и списки отзыва с метками времени	З	
Архивирование	О	
—ArchiveTimestampV2 id-aa-48	Н	Метка времени, определенная в документе RFC 3161
—ArchiveTimestamp id-aa-27	Н	Метка времени, определенная в документе RFC 3161
—TimeMark и т. д.	З	

4.5 Спецификация XAdES

В настоящем подразделе приведены детали требований к генерации и проверке электронной подписи, соответствующей спецификации XAdES.

Подраздел 4.5.1 содержит обзор профилей, определенных в настоящем стандарте, а в подразделе 4.5.2 показана структура, соответствующая спецификации XAdES. В подразделах 4.5.3, 4.5.4 и в таблице 14 приведены требования к профилям.

4.5.1 Определяемые профили долговременной подписи

Чтобы электронная подпись могла быть проверена спустя длительное время после ее создания, должна быть обеспечена интероперабельность. Должно быть идентифицируемо время подписи, при этом должны выявляться все несанкционированные изменения подписанных данных, включая субъект информации и сведения об отзыве сертификатов. В настоящем стандарте приведены определения следующих двух профилей, удовлетворяющих предыдущим требованиям, предъявляемым к спецификациям XAdES.

a) Профиль XAdES-T

Профиль, относящийся к генерации и проверке данных, соответствующих спецификации XAdES-T.

b) Профиль XAdES-A

Профиль, относящийся к генерации и проверке данных, соответствующих спецификации XAdES-A.

На рисунке 8 показаны отношения между данными, соответствующими спецификациям XAdES-T и XAdES-A.

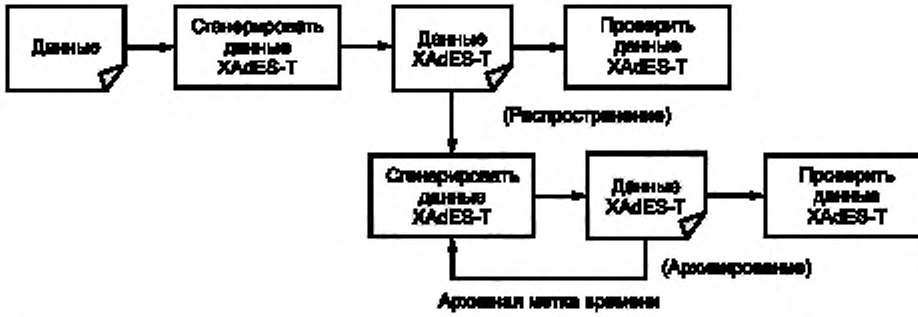


Рисунок 8 — Отношения между данными, соответствующими спецификациям XAdES-T и XAdES-A

4.5.2 Представление степени обязательности

В настоящем стандарте определены следующие методы представления степени обязательности (как профиля) каждого элемента, входящего в состав данных XAdES-T и XAdES-A.

a) Обязательный (O)

Элементы, у которых степень обязательности равна «O», должны быть реализованы без ошибок. Если такой элемент имеет необязательные подчиненные элементы, то хотя бы один из них должен быть выбран. Любой элемент, имеющий степень обязательности «O» и являющийся подчиненным элементом необязательного элемента, должен быть выбран, если выбран этот необязательный элемент.

b) Необязательный (H)

Реализация элементов, у которых степень обязательности равна «H», оставлена на усмотрение разработчика.

c) Условный (У)

Реализация элементов, у которых степень обязательности равна «У», оставлена на усмотрение разработчика. Должны быть составлены детальные спецификации обработки любого элемента со степенью обязательности «У». Например, разработчик предоставляет спецификации таких элементов, раскрывая объявление поставщика о соответствии и приложение к нему (см. ИСО 14533-1:2012, приложение А, или ИСО 14533).

d) Запрещенный (З)

Элементы с уровнем обязательности «З» не должны присутствовать в данных. При проверке запрещенный элемент может игнорироваться.

4.5.3 Требования к представлению подписи в соответствии со спецификацией XAdES-T

Все элементы, не перечисленные в таблицах 10, 11, 12 и 13, должны иметь степень обязательности «У».

Таблица 10 — Элемент Signature

Элемент или атрибут	Обязательность	Условие
Атрибут ID элемента ds:Signature	O (см. примечание 1)	
ds:SignedInfo	O	
—ds:CanonicalizationMethod	O	C14n
—ds:SignatureMethod	O	
—ds:Reference	O	
—ds:Transforms	O	
—ds:DigestMethod	O	
—ds:DigestValue	O	
ds:SignatureValue	O	

Окончание таблицы 10

Элемент или атрибут	Обязательность	Условие
ds:KeyInfo	Н (см. примечание 2)	
ds:Object	О	

Примечания
1 Атрибут не обязателен в спецификации XML Signature, но обязателен в спецификации XAdES.
2 Должен присутствовать либо элемент ds:KeyInfo, либо элемент SigningCertificate (см. таблицу 12). Если выбран элемент ds:KeyInfo (обязателен в спецификации XAdES v1.1.1), то элемент данных X.509, определенный в спецификации XML Signature, должен быть включен как субэлемент.

Таблица 11 — Элемент Object

Элемент	Обязательность	Условие
QualifyingProperties	О	В атрибуте target должно быть указано значение атрибута ID элемента Signature
—SignedProperties	О	
—UnsignedProperties	Н	
QualifyingPropertiesReferнce	У	

Таблица 12 — Элемент SignedProperties

Элемент	Обязательность	Условие
SignedSignatureProperties	О	
—SigningTime	Н (см. примечание 1)	
—SigningCertificate	Н (см. примечания 1 и 2)	
—SignaturePolicyIdentifier	У	
—SignatureProductionPlace	У	
—SignerRole	У	
SignedDataObjectProperties	У	
—DataObjectFormat	У	
—CommitmentTypeIndication	У	
—AllDataObjectsTimeStamp	У	
—IndividualDataObjectTimeStamp	У	

Примечания
1 Атрибут обязателен в спецификации XAdES v1.1.1.
2 Должен присутствовать либо элемент SigningCertificate, либо элемент ds:KeyInfo (см. таблицу 10).

Таблица 13 — Элемент UnsignedProperties

Элемент	Обязательность	Условие
UnsignedSignatureProperties	О	
—CounterSignature	Н	
—Trusted signing time	О	
—SignatureTimeStamp	О	Метка времени, определенная в документе RFC 3161[a)]

Окончание таблицы 13

Элемент	Обязательность	Условие
—TimeMark или другой метод	З	
UnsignedDataObjectProperties	У	
[a] Используется спецификация метки времени, определенная в документе RFC 3161, поскольку методы получения метки времени, ее сохранения в данных формата XAdES и метод ее проверки строго описаны в стандартах.		

4.5.4 Требования к представлению подписи в соответствии со спецификацией XAdES-A

Профиль XAdES-A определен как расширенная форма профиля XAdES-T. Степень обязательности каждого элемента, входящего в элемент UnsignedSignatureProperties, определенного в спецификации XAdes и приведенного в таблице 14, должна соответствовать этой таблице. Если элемент не включен в эту таблицу, то он должен иметь степень обязательности «У».

Таблица 14 — Элемент UnsignedSignatureProperties

Элемент или метод обработки	Обязательность	Условие
CompleteCertificateRefs	Н (см. примечание 1)	
CompleteRevocationRefs	Н (см. примечание 1)	
—CRLRef	Н	
—OCSPRef	Н	
—OtherRef	З	
AttributeCertificateRefs	З	
AttributeRevocationRefs	З	
SigAndRefsTimeStamp	З	
—нераспределенная обработка	З	
— распределенная обработка	З	
RefsOnlyTimeStamp	З	
—нераспределенная обработка	З	
— распределенная обработка	З	
CertificateValues	М	
—EncapsulatedX509Certificate	Н	
—OtherCertificate	З	
—Сертификаты, контролируемые доверенной службой	З	
RevocationValues	М	
—CRLValues	Н	
—OCSPValues	Н	
—OtherValues	З	
—Информация об отзыве, контролируемая доверенной службой	З	
AttrAuthoritiesCertValues	З	
AttributeRevocationValues	З	

Окончание таблицы 14

Элемент или метод обработки	Обязательность	Условие
Архивирование	О	
—ArchiveTimeStamp	О	
—нераспределенная обработка	О	Метка времени, определенная в документе RFC 3161[a]
— распределенная обработка	З	
—TimeMark или другой метод	З	
Любое неподписываемое свойство подписи, определенное в любой другой версии спецификации XAdES	У	

[a] Используется спецификация метки времени, определенная в документе RFC 3161, поскольку методы получения метки времени, ее сохранения в данных формата XAdES и метод ее проверки строго описаны в стандартах.

Примечания

1 Атрибут обязателен в спецификации XAdES v1.1.1.

2 Курсивом выделены методы обработки.

3 Элементы AttrAuthoritiesCertValues, AttributeRevocationValues, нераспределенная обработка и распределенная обработка не определены в версиях спецификации XAdES v1.1.1 и v1.2.1. Элементы AttributeCertificateRefs и AttributeRevocationRefs также не определены в версии v1.1.1.

Приложение А
(справочное)

Целевые сценарии

А.1 Категории целевых сценариев

Электронные подписи добавляются к исходным электронным данным в целях неоспоримости. В повседневной деятельности в сфере здравоохранения можно выделить следующие категории целевых сценариев:

a) электронные подписи документов, отправляемых внешним организациям, например направления (информация об осмотре пациента и его лечении) и информация о лечении;

b) электронная подпись для целей электронного хранения документов в течение срока, установленного действующими нормативными документами;

c) электронная подпись других внутренних документов, например результатов лабораторных тестов и протоколов лучевых исследований;

d) электронная подпись, добавленная к электронным копиям бумажных документов, полученных с помощью сканирования;

e) электронная подпись журналов доступа.

Для каждого из этих классов приводится соответствующий сценарий, представляющий собой типичный пример, а не полное описание.

А.1.1 Электронные подписи документов, отправляемых внешним организациям

Медицинские организации направляют внешним организациям различные документы («распечатки»). Для передачи внешним организациям следующие документы должны быть преобразованы в электронный формат:

- выписной эпикриз;
- запрос выписки из медицинской карты;
- направление;
- запрос медицинской карты;
- результаты клинического испытания.

При преобразовании этих документов в электронный формат подразумевается их длительное хранение. Следовательно, в этом случае может пригодиться долговременная электронная подпись, описанная в настоящем стандарте. Ниже приведены типичные сценарии ее применения к разным типам документов.

Выписной эпикриз, выписка из медицинской карты

Проверка действительности электронной подписи может потребоваться, когда на стороне получателя необходимо определить авторство документа, а также такие атрибуты его автора, как официально присвоенная квалификация.

При преобразовании этих документов в электронную форму добавление электронной подписи позволяет получателю без труда определить авторство документа и ту информацию об авторе, которая передается в атрибуте профессиональной роли hcRole. Таким образом, этот сценарий может быть достаточно эффективным.

Направление

В медицинских организациях, предоставляющих клиническую информацию другим организациям, направление, выданное пациенту стационаром или клиникой, должно быть подписано врачом или заверено печатью организации. При преобразовании направления в электронную форму требуется также электронная подпись. На стороне получателя необходимость проверки электронной подписи может существовать столь долго, сколько это направление у него хранится. Таким образом, этот сценарий может быть достаточно эффективным.

Запрос выписки из медицинской карты

Этот сценарий описывает передачу пациенту выписки из его медицинской карты. По этому сценарию медицинская организация передает пациенту информацию, что требует как обеспечения ее аутентичности, так и усиленного свойства неоспоримости. Таким образом, этот сценарий может быть достаточно эффективным.

Результаты клинического испытания

Когда результаты клинического испытания создаются в электронной форме, то обработка персональной информации должна осуществляться в соответствии с юридическими требованиями, принятыми в данной стране. Так как результаты клинических испытаний должны храниться длительный срок, то будет полезна долговременная электронная подпись, описанная в настоящем стандарте.

А.1.2 Электронная подпись для хранения документов

Например, к числу документов, хранение которых требуется японским законодательством, относятся:

- медицинские карты (ведущиеся врачами, например стоматологами и т. д.);
- истории родов (ведущиеся акушерами);
- инструкции по зубопротезированию (предназначенные зубным техникам);
- карты вызова скорой помощи (заполняемые врачами или фельдшерами скорой помощи);
- дневники учета работы врача стоматолога-ортодонта;
- карты лучевой нагрузки (ведущиеся рентгенолаборантами);

- рецепты (выписываемые врачами);
- дневники операций (в стационаре);
- статистические карты выбывших из стационара.

Сценарии оцифровки этих документов рассматриваются следующим образом. В общем случае нормативные сроки их хранения превышают сроки действия сертификатов электронной подписи, но возможность проверки подписи должна быть обеспечена в течение всего срока хранения. Для этого требуется долговременная электронная подпись, описанная в настоящем стандарте.

Документы, хранение которых регламентируется законодательством

Для этих документов добавление электронной подписи регламентируется законодательством.

В этом случае используется следующая процедура добавления электронной подписи:

- при создании документа должна быть добавлена электронная подпись автора;
- при хранении подписанного документа должны быть обеспечены целостность и неоспоримость его содержания.

Документы, хранение которых не регламентируется законодательством

Поскольку эти документы хранятся не в связи с требованиями законодательства, то добавление к ним электронной подписи не является необходимым. Однако для обеспечения целостности и неоспоримости содержания рекомендуется использовать электронную подпись. Процедура добавления электронной подписи та же, что и для документов, хранение которых регламентируется законодательством.

А.1.3 Электронная подпись других внутренних документов

К ним относятся те внутренние документы, которые не относятся к числу тех, хранение которых требуется действующим законодательством. К таким документам могут относиться результаты лабораторных тестов и протоколы лучевых исследований, используемые только для внутренних нужд медицинских организаций. Хотя для таких документов может осуществляться ряд проверок, они не обязательно рассматриваются как самостоятельные, поскольку в медицинских организациях системы ввода заказов/передачи результатов являются встроенными компонентами систем ведения электронной медицинской карты. В электронной подписи таких документов может быть использовано значение атрибута профессиональной роли hcRole «заказ» (contracts).

А.1.4 Электронная подпись, добавленная к электронным копиям бумажных документов, полученных с помощью сканирования

При преобразовании медицинской карты в электронную форму с помощью сканера изображений и последующем уничтожении исходных бумажных документов оператор (или администратор) должен подписать полученный электронный образ, чтобы принять на себя ответственность за аутентичность информации. Электронные медицинские карты должны проверяться на предмет возможной фальсификации. При преобразовании бумажных медицинских карт в электронную форму необходима более высокая степень доверия к цепочке авторизации по сравнению со случаем, когда медицинская карта изначально создается в электронной форме.

А.1.5 Электронная подпись журналов доступа

Журналы доступа к электронным медицинским картам содержат большие объемы данных. Те записи журналов доступа, срок хранения которых превышает установленное значение, должны архивироваться. Во избежание фальсификации архивированных записей журналов доступа может требоваться, чтобы они были подписаны системным администратором.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 17090-1:2008	IDT	ГОСТ Р ИСО 17090-1—2009 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 1. Структура и общие сведения»
ISO 17090-3:2008	IDT	ГОСТ Р ИСО 17090-3—2010 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 3. Управление политиками центра сертификации»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:
- IDT — идентичные стандарты.

Библиография

[1] ISO 14533 (все части):2012, Processes, data elements and documents in commerce, industry and administration — Long term signature profiles

[2] ISO 17090-2:2008, Health informatics — Public key infrastructure — Part 2: Certificate profile

[3] ISO 27799, Health informatics — Information security management in health using ISO/IEC 27002

[4] ISO/IEC 18014-2:2009, Information technology — Security techniques — Time-stamping services — Part 2: Mechanisms producing independent tokens

[5] ETSI/TS 101 733: CMS Advanced Electronic Signatures

[6] ETSI/TS 101 903: XML Advanced Electronic Signatures

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, инфраструктура с открытым ключом, защита данных, электронная подпись, медицинский документ

Редактор *А.Ф. Колчин*
Технический редактор *В.Ю. Фотиева*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.Е. Кругова*

Сдано в набор 11.01.2017. Подписано в печать 10.02.2017. Формат 60 ×84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,93. Тираж 24 экз. Зак. 349.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru