Организация Объединенных Наций ECE/TRADE/C/CEFACT/2010/14

Экономический и Социальный Совет

Distr.: General
27 September 2010
Russian
Original: English

**Европейская экономическая комиссия**

Комитет по торговле

**Центр по упрощению процедур торговли и электронным деловым операциям**

**Шестнадцатая сессия**

Женева, 8−10 декабря 2010 года

Пункт 7 предварительной повестки дня

**Новые и пересмотренные стандарты и рекомендации**

# Рекомендация № 37: Рекомендация в отношении функциональной совместимости подписанных цифровых документов

**Представлено для утверждения Рабочей группой по архитектуре, проектно-конструкторским работам и строительству (ГТД-6)**

*Резюме*

В настоящей Рекомендации предлагается ряд функциональных требований, которым должны соответствовать подписанные цифровые документы в части их построения, а также в части взаимосвязи между подписанным контентом, сертификатами подписантов и подписями. ГТД-6 представляет Рекомендацию Пленарной сессии для утверждения.

GE.10-25028 (R) 161110 181110

# Содержание

# Предисловие

Рекомендация в отношении функциональной совместимости подписанных цифровых документов направлена на обеспечение большей функциональной совместимости цифровых документов, заверенных электронной подписью, в целях содействия развитию безбумажной международной торговли.

В Рекомендации сформулирован ряд функциональных требований, которым должны соответствовать подписанные цифровые документы в части их построения, а также в части взаимосвязи между подписанным контентом, сертификатами подписантов и подписями.

Рекомендация не затрагивает правовых аспектов электронных подписей, которые рассматриваются на международном уровне в других документах, в том числе в документах, опубликованных ЮНСИТРАЛ[1, 2, 3]. Она также не затрагивает вопросов, касающихся семантики, удобства пользования или толкования подписанного контента. Настоящая Рекомендация не противоречит Рекомендации 14 ЕЭК ООН "Удостоверение подлинности внешнеторговых документов средствами помимо подписи".

В целях содействия применению указанных требований в приложении B приводятся примеры технических решений с использованием некоторых из новейших стандартов, касающихся цифровых документов. В будущем это приложение может обновляться с учетом других возможных технических решений.

Ввиду настоятельной необходимости повышения функциональной совместимости в области проверки цифровых документов настоящая Рекомендация и приложения к ней представляются одновременно, что должно способствовать скорейшему практическому применению Рекомендации.

# Резюме

Цифровой документ (в отличие от бумажного) не имеет доказательной ценности, если не подкрепляется каким-либо механизмом, таким, например, как электронная подпись, позволяющим гарантировать его целостность и подлинность.

Однако многообразие стандартов электронной подписи может свести на нет возможность проверки подписанных цифровых документов. Это самым непосредственным образом влияет на способность предприятий и административно-управленческих органов без риска для себя обмениваться цифровыми документами как между собой, так и с административными и финансовыми структурами, выступающими их партнерами.

В этой связи в основу настоящей Рекомендации положен функциональный, а не технический подход к созданию и проверке подписанных цифровых документов, позволяющий акцентировать внимание прежде всего на предмете, а не на методе.

В результате проверки подписанного цифрового документа проверяющая сторона должна, как минимум, получить четкое представление о:

- параметрах подписей (дате, месте, виде обязательства);
- целостности подписанного контента;
- целостности и действительности сертификатов подписантов;
- надежности провайдеров сертификационных услуг.

Таким образом, в настоящей Рекомендации сформулированы простые общие требования в отношении создания и проверки подписанных цифровых документов, призванные способствовать повышению их функциональной совместимости с учетом того, что в случае принятия Рекомендации эти требования могут со временем потребовать корректировки.

# 1. Рекомендация № 37: Рекомендация в отношении функциональной совместимости подписанных цифровых документов

Настоящая Рекомендация призвана стимулировать структуры, желающие обмениваться подписанными цифровыми документами с другими структурами, к обеспечению максимальной функциональной совместимости таких документов за счет соблюдения следующего набора принципов:

Подписанный цифровой документ:

- ДОЛЖЕН содержать один единственный поддающийся идентификации контент;
- ДОЛЖЕН быть заверен одной или несколькими подписями;
- ДОЛЖЕН содержать все соответствующие четко определенные реквизиты.

Каждая подпись, содержащаяся в таком документе:

- МОЖЕТ содержать информацию о дате подписи и другие реквизиты;
- ДОЛЖНА относиться ко всему контенту;
- МОЖЕТ быть завизирована одной или несколькими контрподписями.

## 1.1 Преимущества

Настоящая Рекомендация содержит ряд простых стандартных требований, которые должны соблюдаться коммерческими, административными и финансовыми структурами при обмене защищенными документами и которые могут подкрепляться различными стандартными технологиями и продуктами, включая программы с открытым кодом.

Ее целями являются:

- повышение эффективности и надежности процедуры проверки подписанных цифровых документов, полученных от других сторон;
- повышение функциональной совместимости подписанных цифровых документов, что в свою очередь должно способствовать укреплению доверия;
- скоординированное расширение возможностей для ускорения темпов перехода на безбумажные технологии.

# 2. Контекст

## 2.1 Сфера охвата

1. С начала 90-х годов прошлого века было разработано и принято большое число технических стандартов, касающихся подписанных цифровых документов. Примеры таких стандартов приводятся в конце документа в примечаниях 4−12[4, 5, 6, 7, 8, 9, 10, 11, 12].

2. Однако из-за многообразия стандартов, допускающих поливариантность и не содержащих указаний в отношении того, как ставить цифровые подписи под документами, возникла проблема функциональной несовместимости под-

писанных цифровых документов с синтаксической и семантической точек зрения, а также с точки зрения методов их обработки.

3. В настоящем документе предлагается новый подход к созданию и проверке подписанных цифровых документов, делающий акцент на функциональных, а не на технических аспектах.

4. Акцент на функциональных аспектах позволяет определить общий функциональный профиль подписанных цифровых документов, что должно упростить и облегчить обмен электронными документами, имеющими доказательственную ценность, и их проверку.

5. Настоящая Рекомендация содержит набор функциональных требований, призванных облегчить разработку прикладных программ для создания и проверки функционально совместимых подписанных цифровых документов. В ней также приводятся примеры применения таких требований в отношении некоторых из последних технических стандартов, касающихся подписанных цифровых документов.

6. Для облегчения ссылок на Рекомендацию в настоящем документе используется ее сокращение − SDEIR ("Signed Digital Evidence Interoperability Recommendation").

### 2.2 Цель

7. Цель настоящего документа состоит в ускорении процесса "дематериализации" документооборота путем содействия созданию, проверке и обеспечению функциональной совместимости электронных документов, имеющих доказательственную ценность, и их интеграции в прикладные программы для ведения деловых операций.

8. Для конечного пользователя использование цифровых подписей предполагает выполнение двух основных процедур:

- процедуры подписания документа; и
- процедуры проверки подписи под документом.

9. Реальная практика проведения электронных торгов и выставления электронных счетов свидетельствует о том, что, когда та или иная сторона ставит свою электронную подпись под каким-либо документом, используя для этого соответствующее программное обеспечение, возникает ряд проблем, связанных с обеспечением его функциональной совместимости:

- проблема совместимости формата подписи: программы, предназначенные для проверки подписей, зачастую не воспринимают формат полученной цифровой подписи, или не могут соотнести такую подпись с соответствующим файлом, или вообще не могут ее найти;
- проблема определения семантического значения подписи: программа, используемая для проверки подписи, или формат подписи часто не позволяют определить назначение подписи (например, хотел ли подписант удостоверить подлинность документа или же он хотел только подтвердить свое согласие с его содержанием и т.д.);
- проблема проверки действительности сертификата: программа, используемая для проверки подписи, может оказаться не в состоянии определить, является ли сертификат действительным и не был ли он аннулирован на дату подписи.

10. Возможность проверить подпись имеет исключительно важное значение, например на этапе подведения итогов или объявления победителя торгов при осуществлении государственных закупок, поскольку неспособность удостовериться в подлинности подписи может привести к тому, что конкурсные предложения поставщиков будут по ошибке признаны недействительными и отклонены.

11. Для решения первых двух проблем необходимо, чтобы все подписи генерировались в формате, обеспечивающем возможность их проверки с помощью соответствующих пакетов программного обеспечения.

12. Таким образом, предлагаемая конфигурация подписанных цифровых документов призвана:

- способствовать повышению доверия посредством обеспечения возможностей для создания и проверки подписанных цифровых документов и работы с ними;
- обеспечить функциональную совместимость подписанных цифровых документов независимо от их технического формата посредством использования общего функционального знаменателя;
- упростить интеграцию цифровых подписей в бизнес-приложения и программы архивирования, с тем чтобы облегчить замену функции "print" ("печать") функцией "sign" ("подписать") или "certify" ("удостоверить").

### 2.3 Целевая аудитория

13. Настоящий документ предназначен главным образом для организаций и частных лиц, которым приходится решать проблемы, связанные с:

- обменом подписанными цифровыми документами в открытом режиме;
- выбором формата подписанного цифрового документа, который был бы приемлемым в контексте соответствующего проекта по дематериализации документооборота;
- мониторингом информационных технологий на предмет их возможного использования для целей цифровых подписей и архивирования документов, имеющих доказательную ценность;
- обеспечением функциональной совместимости, обратимости и действительности подписанных цифровых документов.

## 3. Определения

В данном разделе дается краткое определение терминов и сокращений, используемых в настоящем документе.

AdES: усовершенствованная электронная подпись

BES: базовая электронная подпись

CAdES: усовершенствованная электронная подпись с использованием CMS

ЕКС: Европейский комитет по стандартизации

Сертификат: сообщение данных или иная запись, подтверждающая наличие связи между подписантом и данными для создания подписи (примечание 2)

Подписанный цифровой документ: цифровой документ, который может быть представлен в качестве доказательства

CMS: синтаксис криптографического сообщения

CRL: список аннулированных сертификатов

ПСУ: поставщик сертификационных услуг: лицо, которое выдает сертификаты и может оказывать другие услуги, связанные с электронными подписями (примечание 1)

Соподпись: подпись, относящаяся к тому же контенту, что и другая подпись

Контрподписант: лицо, являющееся держателем данных, необходимых для создания контрподписи, и действующее либо от своего собственного имени, либо от имени другого лица, которое оно представляет

Контрподпись: подпись, относящаяся к другой подписи (подписанный контент контрподписи сам по себе является подписью); может быть также названа "иерархической подписью"

Электронная подпись: данные в электронной форме, которые содержатся в сообщении данных, приложены к нему или логически ассоциируются с ним и которые могут быть использованы для идентификации подписанта в связи с сообщением данных и для засвидетельствования того, что подписант согласен с информацией, содержащейся в сообщении данных (примечание 1)

EPES: электронная подпись, основанная на эксплицитной концепции

ЕИСС: Европейский институт по стандартизации в области связи

ЕС: Европейский союз

ИСО: Международная организация по стандартизации

ОРССИ: Организация по развитию стандартов структурированной информации

OCSP: протокол определения статуса сертификата в онлайновом режиме

PDF: кросс-платформенный формат электронных документов

PKCS: криптографический стандарт с публичным ключом

PKI: инфраструктура публичных ключей

RFC: запрос о представлении замечаний

SDEIR: Рекомендация в отношении функциональной совместимости подписанных цифровых документов

Подписант: лицо, являющееся держателем данных, необходимых для создания подписи, и действующее либо от своего собственного имени, либо от имени лица, которое оно представляет (примечание 1)

Подписанный контент: данные, содержащиеся в подписанном цифровом документе

SSCD: устройство для создания защищенных подписей

Trust anchor: сертификат, которому доверяет проверяющая сторона (часто называется "корневым" сертификатом)

TSL: список заслуживающих доверия поставщиков сертификационных услуг с информацией об их статусе

TSP: заслуживающий доверия поставщик сертификационных услуг

XAdES: усовершенствованная электронная подпись в формате XML

XML: расширяемый язык разметки

XMLDSIG: цифровая подпись в формате XML

## 4. Указания для пользователей по применению Рекомендации

14. В настоящем разделе описываются функциональные характеристики и управленческие требования, которые составляют суть Рекомендации.

### 4.1 Профиль подписанного цифрового документа согласно Рекомендации

15. Рекомендация определяет профиль подписанного цифрового документа, призванный обеспечить максимальную функциональную совместимость между созданием и проверкой подписанных цифровых документов.

16. Этот профиль задается набором функциональных требований.

### 4.2 Функциональные характеристики профиля

17. Функциональными характеристиками предлагаемого профиля подписанного цифрового документа являются:

- наличие одного единственного подписанного контента с указанием его вида и (факультативно) названия;
- наличие подписей и соподписей, относящихся к подписанному контенту;
- наличие контрподписей в качестве неподписанных реквизитов подписи или контрподписи;
- наличие подписанных реквизитов подписи и контрподписи, каковыми являются:
    - дата подписания, определяющая момент времени, когда, по утверждению подписанта, он выполнил процедуру подписания;
    - информация о местонахождении подписанта, представляющая собой мнемокод адреса, ассоциируемого с подписантом в данной географической точке, например городе;
    - ссылка на концепцию подписи, определяющую в точности роль и обязательства, которые подписант намерен взять на себя в отношении подписанных данных;
    - информация о виде обязательства, ассоциируемого с подписью (четкое указание на то, какое конкретно обязательство принял на себя подписант, поставив свою подпись под данными);
    - информация о том, в какой роли или на какой позиции действовал подписант (как указывается им самим), когда подписывал данные;
    - ссылки на сертификат подписанта и его удостоверителей;
- наличие временны́х меток в качестве неподписанных реквизитов подписи или контрподписи;
- сертификаты подписантов и контрподписантов и их удостоверители.

### 4.3 Различия между цифровыми и бумажными документами

18. Оба вида документов имеют между собой много общего, однако между ними есть и ряд важных различий, состоящих в следующем:

- бумажные документы не всегда содержат информацию, идентифицирующую подписантов;
- бумажные документы, как правило, не содержат информации, идентифицирующей предшественников подписантов;
- подписанные бумажные документы, как правило, содержат собственноручную подпись подписанта, тогда как цифровая подпись под электронным документом не имеет графической формы. Обычно только компьютерная программа способна произвести сложные математические расчеты, необходимые для проверки цифровой подписи.

### 4.4 Применение Рекомендации на практике

19. Инструкции для пользователей по применению Рекомендации − см. приложения A и B.

## 5. Заключение

20. Содержащееся в настоящем документе описание профиля подписанного цифрового документа призвано способствовать дематериализации бумажного документооборота за счет упрощения и облегчения процедур создания и проверки защищенных цифровых сообщений, имеющих доказательственную силу, и обмена ими, а также интеграции таких сообщений в прикладные программы для ведения деловых операций.

# Приложение A (ненормативное): функциональные имплементационные требования

## A.1 Уровни

Спецификация, закрепленная в рамках Рекомендации, предполагает использование уровней для дифференциации некоторых требований Рекомендации по степени их важности. В настоящей версии определяются два уровня:

- базовый ("Core") уровень (обозначает более простые требования, которые легче выполнить); и
- уровень 1 ("Level 1") (обозначает более жесткие требования Рекомендации, обеспечивающие большую функциональную совместимость, например требование о том, чтобы каждая подпись дополнялась подписанной датой этой подписи, а также требование, касающееся подписанных ссылок на всех удостоверителей и их сертификаты).

## A.2 Ключевые слова

Ключевые слова "ДОЛЖЕН", "НЕ ДОЛЖЕН", "ТРЕБУЕТСЯ", "СЛЕДУЕТ", "НЕ СЛЕДУЕТ", "РЕКОМЕНДУЕТСЯ", "МОЖЕТ" и "ФАКУЛЬТАТИВНЫЙ"/"НЕ ОБЯЗАТЕЛЬНО", используемые в настоящем документе (в указанном написании заглавными буквами) следует толковать в соответствии с RFC 2119[13].

## A.3 Виды применения

Спецификация предусматривает два различных прикладных профиля:

- создание электронных подписей в соответствии с требованиями Рекомендации;
- проверка электронных подписей в соответствии с требованиями Рекомендации.

## A.4 Требования

Ниже изложены 18 требований, устанавливаемых Рекомендацией. Этим требованиям соответствуют не все действующие технические стандарты, касающиеся цифровых подписей. В этой связи пользователям рекомендуется всякий раз проверять, поддерживает ли выбранный ими стандарт соответствующие требования. Подробная информация, касающаяся некоторых предлагаемых вариантов выполнения требований Рекомендации, содержится в техническом приложении к настоящему документу.

T1. Подписанный цифровой документ ДОЛЖЕН содержать один-единственный подписанный контент с указанием его вида и (ФАКУЛЬТАТИВНО) названия.

T2. Подписанный цифровой документ ДОЛЖЕН содержать как минимум одну подпись. Как минимум пять соподписей под подписанным цифровым документом ДОЛЖНЫ поддерживаться совместимой прикладной программой создания или проверки подписи. Если имеются дополнительные подписи, не поддерживаемые программой проверки, процедура проверки ДОЛЖНА быть объявлена незавершенной.

T3. Каждая подпись ДОЛЖНА относиться ко всему подписанному контенту, т.е. к содержащимся в нем данным, а также к информации о его виде и (ФАКУЛЬТАТИВНО) названии.

T4. Подпись МОЖЕТ быть скреплена одной или несколькими контрподписями. Как минимум пять контрподписей ДОЛЖНЫ поддерживаться совместимой прикладной программой создания или проверки подписи. Если имеются дополнительные контрподписи, не поддерживаемые программой проверки подписи, процедура проверки должна быть объявлена незавершенной.

T5. Контрподпись ДОЛЖНА скреплять одну-единственную подпись или контрподпись и НЕ ДОЛЖНА скреплять подписанный контент или что-либо еще. Контрподпись ДОЛЖНА включаться в качестве неподписанного реквизита подписи или контрподписи, которую она скрепляет.

T6. Контрподпись МОЖЕТ быть скреплена одной или несколькими контрподписями. Как минимум одна контрподпись, скрепляющая другую контрподпись, ДОЛЖНА поддерживаться совместимой прикладной программой создания или проверки подписи. При наличии дополнительных уровней контрподписей, не поддерживаемых программой проверки подписи, процедура проверки должна быть объявлена незавершенной.

T7. Подпись или контрподпись МОЖЕТ содержать максимум одну временну́ю метку. Временна́я метка ДОЛЖНА включаться в качестве неподписанного реквизита подписи или контрподписи.

T8. Подписанный цифровой документ ДОЛЖЕН содержать сертификаты подписантов и контрподписантов, на которые должны указывать подписанные ссылки, упомянутые в [T9].

T9. Подпись или контрподпись ДОЛЖНА содержать подписанную недвусмысленную ссылку на сертификат подписанта или контрподписанта. Данное требование призвано установить четкую связь между подписантом и его подписью и обеспечить условия для того, чтобы проверяющей стороне не пришлось "гадать" по поводу сертификата подписанта или контрподписанта в связи с проверкой подписи.

T10−базовое. Подписанный цифровой документ МОЖЕТ содержать сертификаты удостоверителей подписанта или контрподписанта, на которые могут указывать или не указывать подписанные ссылки, упомянутые в [T11−базовое].

T10−уровень 1. Подписанный цифровой документ ДОЛЖЕН содержать сертификаты всех удостоверителей подписанта и контрподписанта, на которые должны указывать подписанные ссылки, упомянутые в [T11−уровень 1].

T11−базовое. Подпись или контрподпись МОЖЕТ содержать подписанные ссылки на сертификаты удостоверителей подписанта или контрподписанта. Такая возможность призвана облегчить получение информации, необходимой для проверки сертификата подписанта или контрподписанта.

T11−уровень 1. Подпись или контрподпись ДОЛЖНА содержать все подписанные ссылки на сертификаты удостоверителей подписанта или контрподписанта. Данное требование призвано не допустить, чтобы проверяющей стороне пришлось "разыскивать" сертификат того или иного

удостоверителя в связи с проверкой сертификатов подписанта или контрподписанта.

T12−базовое. Подпись или контрподпись МОЖЕТ содержать одну подписанную дату подписи.

T12−уровень 1. Подпись или контрподпись ДОЛЖНА содержать одну подписанную дату подписи.

T13. Подпись или контрподпись МОЖЕТ содержать максимум одно подписанное указание местонахождения подписанта.

T14. Подпись или контрподпись МОЖЕТ содержать максимум одну подписанную ссылку на концепцию подписи.

T15. Подпись или контрподпись МОЖЕТ содержать одно или несколько подписанных указаний на то, в каком качестве выступает подписант.

T16−базовое. Подпись или контрподпись МОЖЕТ содержать максимум одну подписанную ссылку на вид обязательства.

T16−уровень 1. Ссылка на вид обязательства (при наличии таковой) ДОЛЖНА указывать на один из следующих видов обязательств (Виды обязательств, перечисленные в настоящем требовании, взяты из стандартов CAdES и XAdES. Со временем их перечень может измениться.):

- доказательство авторства, подтверждающее, что подписант является автором подписанного контента, но не является ни стороной, одобрившей его, ни его отправителем. Данный вид обязательства имеет важное значение в связи с необходимостью представления в некоторых случаях гарантий целостности и подлинности документа, не подразумевающих каких-либо других обязательств. Примером могут служить электронные счета-фактуры[14], которым необходима защита лишь в части обеспечения их целостности и подлинности. Другим примером использования данного вида обязательств служат контракты (в частности, договоры подряда), которые должны быть защищены их составителями лишь в части их целостности и подлинности, но при этом требуют одобрения со стороны получателей;
- доказательство одобрения, свидетельствующее о том, что подписант одобрил подписанный контент;
- доказательство происхождения, свидетельствующее о том, что подписант признает, что он создал и одобрил подписанный контент и является его отправителем;
- доказательство отправления, подтверждающее, что сторона, представившая такое доказательство, является отправителем подписанного контента, но не обязательно его автором;
- доказательство получения, свидетельствующее о том, что подписант подтверждает получение подписанного контента;
- доказательство доставки, подтверждающее, что инстанция, поставившая временну́ю метку, доставила подписанный контент в местный банк сообщений, доступный для получателя этого контента.

T17-базовое. Подпись или контрподпись МОЖЕТ содержать и другие подписанные реквизиты. Такие другие реквизиты НЕ ОБЯЗАТЕЛЬНО должны поддерживаться программой проверки, совместимой с Рекомендацией.

T17-уровень 1. Подпись или контрподпись НЕ ДОЛЖНА содержать других подписанных реквизитов.

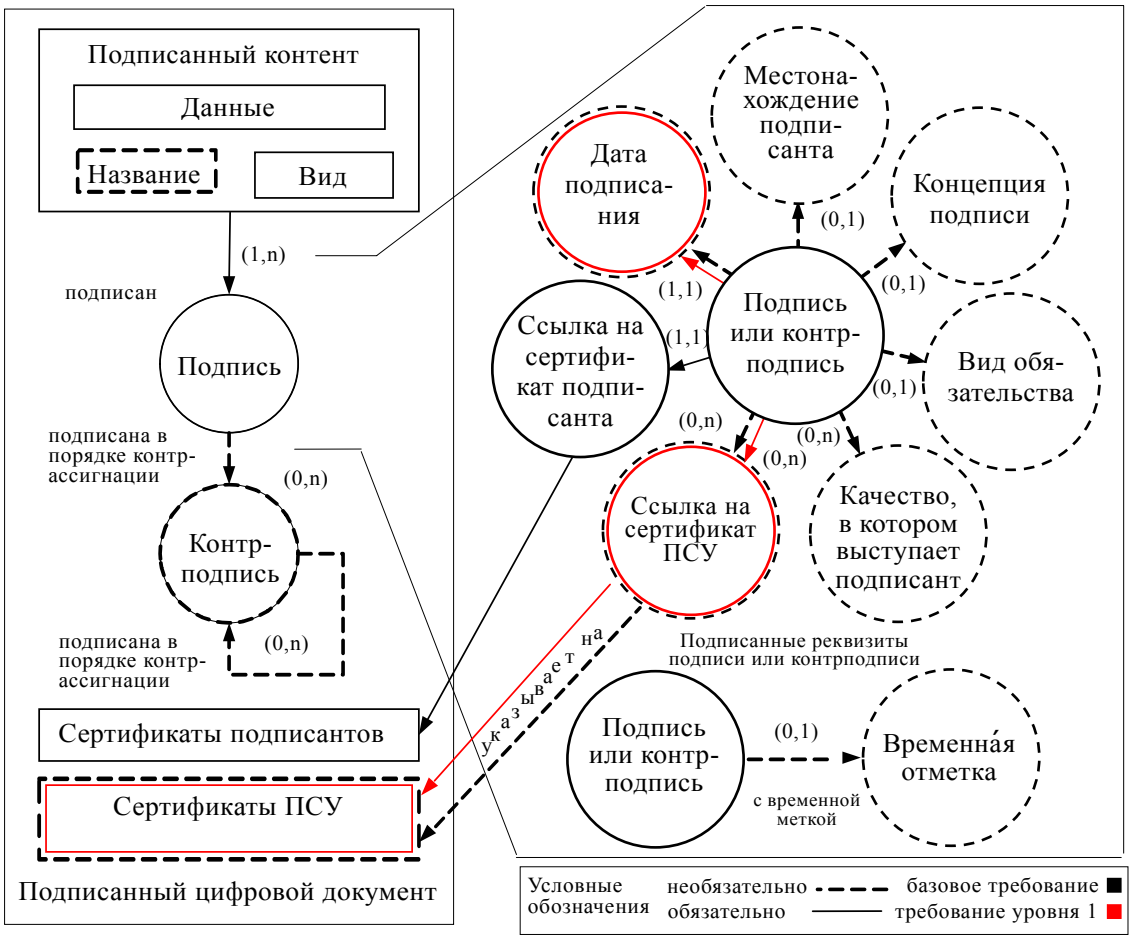
T18. Подпись или контрподпись МОЖЕТ содержать и другие неподписанные реквизиты. Такие другие неподписанные реквизиты НЕ ОБЯЗАТЕЛЬНО должны поддерживаться программой проверки, совместимой с Рекомендацией. Наличие неподдерживаемых неподписанных реквизитов НЕ ДОЛЖНО влиять на толкование подписи проверяющей стороной.

### A.5 Схематическая модель цифрового документа, соответствующего требованиям Рекомендации

В настоящем разделе в схематическом виде показаны структура и построение подписанного цифрового документа, соответствующего требованиям Рекомендации.

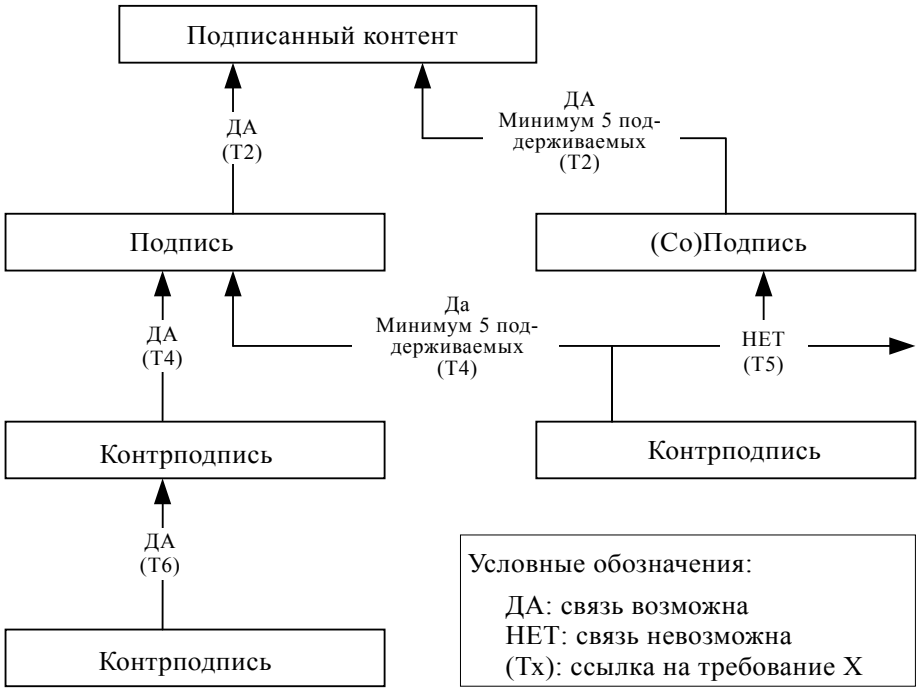
Иллюстрацией общей структуры и построения подписанного цифрового документа, соответствующего требованиям Рекомендации, служит следующая диаграмма. Требования 17 и 18 на диаграмме не отображены.

**Цифровой документ, отвечающий требованиям Рекомендации: общая структура и построение**



На нижеследующей диаграмме показаны взаимосвязи между подписями, соподписями и контрподписями цифрового документа, соответствующего требованиям Рекомендации.

**Цифровой документ, соответствующий требованиям Рекомендации: взаимосвязи между подписями**




## A.6 Процедура проверки согласно требованиям Рекомендации

Проверка подписанного цифрового документа может производиться подписантом, получателем сообщения или любой заинтересованной третьей стороной.

*A.6.1 Проверка соответствия Рекомендации*

Проверка подписанного цифрового документа проводится в два этапа:

- проверка соблюдения требований T1 и T2, относящихся к подписанному цифровому документу в целом;
- проверка каждой подписи, относящейся к подписанному цифровому документу.

В результате проверки подписанного цифрового документа ДОЛЖЕН быть зафиксирован его статус:

- ПРОШЕЛ ПРОВЕРКУ: подписанный цифровой документ успешно прошел проверку; это означает, что были соблюдены требования T1 и T2 и что все подписи успешно прошли проверку;
- НЕ ПРОШЕЛ ПРОВЕРКУ, что означает, что требования T1 и/или T2 не были соблюдены и/или одна или несколько подписей или контрподписей не прошли проверку (о причинах того, почему результат проверки оказался отрицательным, должно быть сообщено отправителю документа).

*A.6.2 Проверка подписи*

Временна́я ссылка, используемая в процессе проверки подписи, позволяет убедиться в действительности подписи на момент ее создания. Характер такой ссылки зависит от концепции удостоверения подписи. Для целей временно́й привязки могут использоваться:

- временна́я метка, проставляемая заслуживающим доверия источником;
- момент времени, когда подписант выполнил, по его указанию, процедуру подписания;
- время, указанное проверяющей стороной.

Рекомендуемая процедура проверки каждой подписи или контрподписи, имеющейся в подписанном цифровом документе, включает следующие этапы:

1. извлечение из подписи сертификата подписанта и его проверка на предмет применимости к подписи; проверка целостности подписанного контента;

2. выбор временно́й ссылки в соответствии с избранной концепцией удостоверения подписи;

3. если временна́я ссылка имеет форму временно́й метки, производится проверка подписи временно́й метки;

4. проверка целостности всех сертификатов, имеющих отношение к подписи, с использованием сертификатов, содержащихся в подписи, или любых других средств, доступных проверяющей стороне;

5. проверка всех сертификатов, имеющих отношение к подписи, на предмет их действительности на момент времени, согласно временно́й ссылке, о которой говорится в пункте 2;

6. проверка информации об аннулировании сертификатов на момент времени, указанный во временно́й ссылке, о которой говорится в пункте 2, применительно к каждому сертификату, упомянутому в пункте 4, с использованием информации, содержащейся в подписи (в случае ее наличия и уместности);

7. сообщение проверяющей стороне информации о результате проверки, включая информацию об использовавшейся временно́й ссылке (см. пункт 2) и сертификате подписанта, а также следующую информацию (при наличии таковой):

   - информацию о дате и времени подписания;
   - информацию о местонахождении подписанта;
   - информацию о том, в каком качестве выступает подписант;
   - информацию о концепции подписи или ссылку на нее;
   - информацию о виде обязательства.

Информация об аннулировании сертификата должна учитывать разрыв во времени между отзывом сертификата и публикацией информации об этом.

В процессе проверки подписи ДОЛЖНЫ также соблюдаться требования T3−T18 (в случае их применимости).

Если из концепции подписи или из принципов, которых придерживается провайдер сертификационных услуг, выдавший сертификат подписанту, вытекают какие-либо дополнительные требования к процедуре проверки, эти требования СЛЕДУЕТ принять во внимание.

Результатом[15] проверки подписи должно быть одной из следующих заключений:

- ПРОШЛА ПРОВЕРКУ (если подпись успешно прошла все этапы проверки);
- НЕ ПРОШЛА ПРОВЕРКУ (если подпись не прошла один или несколько этапов проверки);
- ПРОВЕРКА НЕ ЗАВЕРШЕНА (если отсутствует какая-либо информация, необходимая для проверки подписи).

Если подпись не прошла проверку или если проверка подписи не может быть завершена, проверяющая сторона должна получить четкое сообщение о причинах этого. Программа проверки должна стремиться завершить процедуру проверки даже в случае обнаружения ошибки и должна выдавать полную информацию о выявленных проблемах.

### A.7 Обратная совместимость

Любые изменения в профиле подписанного цифрового документа должны обеспечивать обратную совместимость с предыдущими версиями. Нельзя допустить, чтобы из-за эволюции профиля подписанные цифровые документы, созданные в соответствии с его предыдущими версиями, становились несовместимыми, неправомерными или неинтероперабельными.

### A.8 Возможные направления эволюции профиля подписанного цифрового документа, соответствующего требованиям Рекомендации

Совершенствованию профиля подписанного цифрового документа, соответствующего требованиям Рекомендации, могут способствовать многие подвижки.

Под влиянием таких подвижек может возникнуть потребность в инкорпорировании в него данных, необходимых для целей долгосрочной проверки подписанных цифровых документов, таких как AdES-A (примечание 15) (уровень 2), или механизмов для проверки действительности сертификатов подписантов, таких как TSL[16] (уровень 2).

Будущие версии Рекомендации должны также обеспечивать возможность учета реквизитов самих сертификатов (условные сертификаты, SSCD и т.д.).

Кроме того, будущие усовершенствованные версии Рекомендации могут обеспечить поддержку:

- прилагаемых подписей (отдельных подписей и большого числа пакетов подписанных контентов)[17];
- кинематики подписи.

## Приложение B (ненормативное): руководящие принципы, касающиеся технического решения, реализующего требования Рекомендации

Профиль подписанного цифрового документа, определяемый Рекомендацией, нельзя использовать без технического решения, реализующего и поддерживающего его требования и параметры.

### B.1 Обзор возможных технических решений

В качестве технических решений, реализующих требования Рекомендации, уже изучены и одобрены три следующих стандарта цифровой подписи:

- цифровая подпись в формате XAdES (на основе стандарта ETSI TS 101 903 v1.4.1). Этот формат, реализуемый с помощью соответствующего решения, упоминается ниже как формат X-SDEIR. Описание такой реализации будет дано в одной из будущих обновленных версий настоящего технического приложения;
- цифровая подпись в формате CAdES (на основе стандарта ETSI TS 101 733 v1.8.1). Этот формат, реализуемый с помощью соответствующего решения, упоминается ниже как формат C-SDEIR. Описание такой реализации дается в разделе B.4: описание формата C-SDEIR.
- цифровая подпись в формате PAdES (на основе стандарта ETSI TS 102 778 v1.1.1). Этот формат, реализуемый с помощью соответствующего решения, упоминается ниже как формат P-SDEIR. Описание такой реализации дается в разделе B.5: описание формата P-SDEIR.

К изучению этих стандартов цифровой подписи под углом зрения технических решений, предусмотренных Рекомендаций, побудили следующие основные причины:

- они соответствуют Директиве 1999/93/ЕС Европейского парламента и Европейского совета от 13 декабря 1999 года о базовых нормативных требованиях Сообщества к электронным подписям[18];
- они привязаны к стандартам ЕИСС;
- в настоящее время одним из технических комитетов ИСО (ISO TC 154[19]) ведется работа с целью утвердить эти форматы в качестве стандартов ИСО:
  - XAdES − ISO/CD 14533-2[20]
  - CAdES − ISO/CD 14533-1[21]
  - PAdES − ISO 32000-2[22].

### B.2 Сравнение технических решений

Наличие нескольких технических решений позволяет разработчикам программного обеспечения выбрать формат подписанного цифрового документа, в наибольшей степени соответствующий их потребностям.

Формат X-SDEIR в наибольшей степени подходит для XML-контента (сохраненного в виде читаемого текста), а также для целей интеграции цифровых подписей в прикладные программы для ведения деловых операций. Этот фор-

мат совместим с форматом цифровой подписи XAdES, признаваемым в качестве эталонного в Общем репозитарии для целей функциональной совместимости, ведущемся французской администрацией[23].

Формат C-SDEIR лучше всего подходит для подписания двоичного контента (сохраненного без изменений). Возможность легко выделить подписанный контент подписи обеспечивает гибкость в части хранения и проверки подписанных цифровых документов.

Формат P-SDEIR в наибольшей степени подходит для приложений, делающих акцент на доступе к контенту документа для целей проверки подписи. Однако этот формат зарезервирован для подписанного контента в формате PDF.

### B.3 Описание формата X-SDEIR

Описание этого формата будет дано в одной из будущих версий настоящего технического приложения.

### B.4 Описание формата C-SDEIR

Чтобы соответствовать требованиям Рекомендации, различные формы подписей в формате CAdES ДОЛЖНЫ иметь следующие характеристики:

- CAdES-BES: наличие данной характеристики необходимо для ссылки на сертификат подписанта в соответствии с базовыми требованиями Рекомендации (SDEIR Core). Чтобы соответствовать требованиям SDEIR Level 1, подпись ДОЛЖНА содержать ссылку на всю цепочку сертификатов, имеющих отношение к сертификату подписанта, а сам подписанный цифровой документ ДОЛЖЕН содержать все сертификаты, на которые делаются ссылки;
- CAdES-EPES: если используется концепция подписи, формат подписи должен быть совместимым с форматом CAdES-EPES и должен дополняться комбинацией идентификаторов объекта (OID) и универсального идентификатора ресурсов (URI), а также импринтом документа с изложением такой концепции с его алгоритмом;
- CAdES-T: если подпись должна содержать временную метку, она должна быть создана в формате CAdES-T.

Чтобы соответствовать требованиям SDEIR Core, файл SignedData, содержащийся в цифровой подписи в формате C-SDEIR, ДОЛЖЕН удовлетворять следующим условиям:

- поле encapContentInfo ДОЛЖНО содержать подписанный контент в поле eContent;
- поле сертификатов ДОЛЖНО содержать сертификат автора каждой подписи;
- поле clrs НЕ ДОЛЖНО содержать перечней аннулированных сертификатов (CRL);
- поле signerInfos ДОЛЖНО содержать подпись и, если имеются, соподписи;
- в отношении поля signedAttrs каждого поля SignerInfo ДОЛЖНЫ соблюдаться следующие требования:

- ДОЛЖЕН присутствовать один реквизит contentType, который ДОЛЖЕН содержать идентификатор объекта id-signedData (1.2.840.113549.1.7.2);
- ДОЛЖЕН присутствовать один реквизит messageDigest;
- ДОЛЖЕН присутствовать один реквизит signing-certificate-v2, который ДОЛЖЕН содержать ссылку на сертификат подписанта;
- ДОЛЖЕН присутствовать один реквизит content-hints. Поле content Type ДОЛЖНО содержать идентификатор объекта id-data (1.2.840.113549.1.7.1), а в отношении поля content Description ДОЛЖНЫ соблюдаться следующие требования:
  - ДОЛЖНА присутствовать информация о виде контента, которая ДОЛЖНА содержать ссылки на вид подписанного контента в формате MIME (например, Content-Type: text/plain ("вид контента: текст/читаемый");
  - одно описание контента является ФАКУЛЬТАТИВНЫМ. В случае его наличия оно ДОЛЖНО содержать файловое название подписанного контента (например, Content-Description: JCFV201.txt);
- МОЖЕТ присутствовать один реквизит signing-time, содержащий информацию о том, когда подписант, по его указанию, выполнил процедуру подписания;
- МОЖЕТ присутствовать один реквизит signer-location, содержащий мнемокод адреса, ассоциируемого с подписантом в конкретной географической точке;
- МОЖЕТ присутствовать один реквизит signature-policy-identifier, содержащий концепцию подписи. В случае наличия такого атрибута он может содержать либо поле signaturePolicyImplied (для имплицитной концепции), либо поле signaturePolicyId (для эксплицитной политики). Если присутствует поле signaturePolicyId, поле sigPolicyQualifiers является ФАКУЛЬТАТИВНЫМ, но при его наличии оно ДОЛЖНО содержать квалификатор spuri с указанием URL-адреса, по которому можно получить копию концепции подписи;
- МОЖЕТ присутствовать один реквизит signer-attributes. При наличии такого реквизита он ДОЛЖЕН содержать поле claimedAttributes с не скрепленной подписью информацией о том, в каком качестве выступает подписант. Каждое такое качество ДОЛЖНО быть закодировано в стандарте UTF8String;
- МОЖЕТ присутствовать один реквизит, идентифицирующий вид обязательства. При его наличии поле commitmentTypeidentifier должно содержать один из следующих параметров:
  - id-cti-ets-proofOfOrigin OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 1};
  - id-cti-ets-proofOfReceipt OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 2};

- id-cti-ets-proofOfDelivery OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 3};
- id-cti-ets-proofOfSender OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 4};
- id-cti-ets-proofOfApproval OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 5};
- id-cti-ets-proofOfCreation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 6};

- другие реквизиты присутствовать НЕ ДОЛЖНЫ;

- в отношении поля unsignedAttrs каждого поля SignerInfo ДОЛЖНЫ соблюдаться следующие требования:
  - может присутствовать один реквизит counter-signature. При наличии такого реквизита он ДОЛЖЕН содержать одну или несколько контрподписей, относящихся к соответствующей подписи;
  - МОЖЕТ присутствовать один реквизит signature-timestamp. При наличии такого реквизита он ДОЛЖЕН содержать один символ временно́й метки;
  - МОГУТ присутствовать и другие реквизиты.

Помимо требований, предъявляемых к подписи в формате C-SDEIR Core, подпись в формате C-SDEIR Level 1 ДОЛЖНА соответствовать также следующим дополнительным требованиям:

- поле сертификатов ДОЛЖНО содержать все сертификаты цепочки сертификатов, относящихся к каждой подписи;
- для каждого поля SignerInfo:
  - ДОЛЖЕН присутствовать подписанный реквизит signing-time;
  - подписанный реквизит signing-certificate-v2 ДОЛЖЕН содержать ссылки на все сертификаты цепочки сертификатов, имеющих отношение к сертификату подписанта.

Поскольку в данной спецификации не оговорен конкретный синтаксис, любая прикладная программа, пригодная для проверки подписи в формате CAdES, пригодна и для проверки цифрового документа в формате C-SDEIR.

## B.5 Описание формата P-SDEIR

### *B.5.1 Общие положения*

Документ в формате PDF может содержать большое число цифровых подписей и обладать всеми необходимыми качествами цифрового документа, соответствующего требованиям Рекомендации. В настоящем разделе дается подробное описание специфических характеристиках PDF-подписей, удовлетворяющих базовым требованиям и требованиям уровня 1 Рекомендации.

Форматом PDF-подписи, соответствующим требованиям Рекомендации, является формат PAdES Basic, определяемый стандартом ETSI TS 102 7786-2[24] и эквивалентный формату PDF-подписи, определяемому стандартом ISO/DIS 32000-1.

Следует отметить, что данное решение не поддерживает:

- контрподписей (требование T4 Рекомендации);
- концепции подписи (требование T14 Рекомендации);
- ссылки на то, в каком качестве выступает подписант (требование T15 Рекомендации).

Имплементационные примечания:

- если документ подлежит распечатке, он должен содержать дополнительные данные, благодаря которым читатель мог бы проверить его подлинность и целостность;
- что касается видимых подписей, то работа в этом направлении ведется Европейским институтом по стандартизации в области связи (ЕИСС) и Организацией по развитию стандартов структурированной информации (ОРССИ), однако на данном этапе такие подписи не входят в сферу охвата Рекомендации.

*B.5.2 Характеристики формата подписи P-SDEIR PAdES Basic*

Формат подписи, поддерживаемый форматом P-SDEIR, соответствует двум различным видам невидимых PDF-подписей, описываемым в пункте 8.7 стандарта ISO 32000-1:

- подпись, соответствующая требованиям Рекомендации, без указания вида обязательства или с указанием вида обязательства, отличного от "доказательства авторства", ДОЛЖНА быть реализована как "подпись под документом (или обычная подпись)";
- подпись, соответствующая требованиям Рекомендации, с указанием вида обязательства, равнозначного "доказательству авторства", ДОЛЖНА быть реализована как MDP-подпись ("modification detection and prevention"), которую называют также авторской или удостоверяющей подписью. MDP-подпись относится к виду 2.

Поскольку в данной спецификации также не оговорен конкретный синтаксис, любая прикладная программа, пригодная для проверки подписи в формате P-SDEIR Basic, пригодна и для проверки подписанного цифрового документа в формате P-SDEIR Core.

*B.5.2.1 Характеристики формата P-SDEIR Core*

Подпись в формате P-SDEIR Core имеет следующие характеристики (в соответствии со стандартом ISO 32000-1):

1. подпись кодируется с использованием синтаксиса CMS, определяемого форматом PKCS#7 (см. RFC 2315[25]);
2. используется субфильтр "adbe.pkcs7.detached";
3. подпись МОЖЕТ содержать временну́ю метку согласно RFC 3161[26];

4. подпись НЕ ДОЛЖНА содержать никаких ответов на запросы о статусе сертификатов (по протоколу OCSP[27]) и никаких перечней аннулированных сертификатов (CRL[28]) в качестве подписанных реквизитов;

5. подпись ДОЛЖНА содержать сертификат подписанта;

6. сертификат, дающий право подписи, должен быть скреплен подписью. Это может быть обеспечено посредством:

   • включения дополнительного подписанного реквизита (не определяемого в стандарте ISO 32000-1), содержащего дающий право подписи сертификат ESS V2. Данный реквизит ДОЛЖЕН содержать ссылку на сертификат подписанта; или

   • включения в сам документ (в ручном режиме) идентификационной метки сертификата, дающего право подписи;

7. подпись МОЖЕТ содержать дату подписи и информацию о месте и мотивах создания подписи;

8. информация о мотивах ДОЛЖНА соответствовать параметру, определяющему вид обязательства для целей удостоверения подписанного цифрового документа в форме [CommitmentType=<CommitmentTypeIdentifier>], где "Label" − эта строка, описывающая вид обязательства на языке подписи, и где CommitmentTypeIdentifier может иметь следующие значения: proof_of_origin, proof_of_receipt, proof_of_delivery, proof_of_approval, proof_of_sender. Пример: "[CommitmentType=proof_of_receipt] Proof of Receipt".

*B.5.2.2 Характеристики формата P-SDEIR (Level 1)*

Подпись в формате P-SDEIR Level 1 ДОЛЖНА дополнительно соответствовать следующим требованиям:

• требование 5 раздела 0 распространяется на все сертификаты цепочки сертификатов, имеющих отношение к сертификату подписанта;

• требование 6 раздела 0 распространяется на все сертификаты цепочки сертификатов, имеющих отношение к сертификату подписанта.

## Приложение C (нормативное): криптографические алгоритмы

Пользователям прикладных программ, соответствующих требованиям Рекомендации, следует учитывать, что криптографические алгоритмы постоянно эволюционируют и становятся все более эффективными.

В настоящем приложении содержатся руководящие указания в отношении разработки и соблюдения алгоритмов, предназначенных для целей создания и проверки электронных подписей.

Что касается создания электронных подписей, то желательно, чтобы прикладные программы, соответствующие требованиям Рекомендации, поддерживали как минимум следующие алгоритмы:

- алгоритмы хеширования: SHA-256
- алгоритмы подписи: RSA 2048

Что касается проверки подписей, то прикладные программы, соответствующие требованиям Рекомендации, ДОЛЖНЫ как минимум поддерживать следующие алгоритмы:

- алгоритмы хеширования: SHA-256
- алгоритмы подписи: RSA 2048

Для целей проверки подписей желательно, чтобы прикладные программы, соответствующие требованиям Рекомендации, поддерживали как минимум следующие алгоритмы:

- алгоритмы хеширования: SHA-1
- алгоритмы подписи: RSA 1024

Если конкретное решение, реализующее требования Рекомендации, предполагает использование особых алгоритмов (например, эллиптических кривых), рекомендуется обращаться к стандарту ETSI TS 102 176[29].

## Примечания

[1] Типовой закон об электронной торговле, принятый Комиссией Организации Объединенных Наций по праву международной торговли: http://www.uncitral.org/pdf/russian/texts/electcom/05-89450_Ebook.pdf

[2] Типовой закон об электронных подписях, принятый Комиссией Организации Объединенных Наций по праву международной торговли: http://www.uncitral.org/pdf/russian/texts/electcom/ml-elecsig-e.pdf

[3] Содействие укреплению доверия к электронной торговле: правовые вопросы международного использования электронных методов удостоверения подлинности и подписания: http://www.uncitral.org/pdf/russian/texts/electcom/08-55698_Ebook.pdf

[4] PKCS#7: http://www.rsa.com/rsalabs/node.asp?id=2129

[5] S/MIME: http://www.ietf.org/rfc/rfc3851.txt

[6] CMS: http://www.ietf.org/rfc/rfc3852.txt

[7] XMLDSIG: http://www.w3.org/TR/xmldsig-core/

[8] CAdES (ETSI TS 101 733): http://www.etsi.org

[9] EANCOM digital signature: http://www.gs1.org/docs/ecom/eancom/eancom_Digital_Signature.pdf

[10] Signed PDF (ISO/DIS 32000): http://www.adobe.com/devnet/pdf/pdf_reference.html или http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502

[11] XAdES (ETSI TS 101 903): http://www.etsi.org

[12] PAdES (ETSI TS 102 778): http://www.etsi.org

[13] Ключевые слова: http://www.faqs.org/rfcs/rfc2119.html

[14] Директива Совета 2001/115/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0115:EN:HTML (7)-2-c)

[15] CWA 14171 on electronic signature verification: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf

[16] TSP Status List (ETSI TS 102 231): http://www.etsi.org

[17] Информацию о работе ЕИСС по теме "Прилагаемые подписи" (работа продолжается) см. на сайте" http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=31946

[18] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

[19] ISO TC 154 : http://www.iso.org/iso/iso_technical_committee.html?commid=53186

[20] ISO/CD 14533-2: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56025

[21] ISO/CD 14533-1: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56024

[22] ISO 32000-2 http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?ics1=37&ics2=100&ics3=99&csnumber=53041

[23] Используемый французской администрацией профиль цифровой подписи в формате XAdES: http://www.ietf.org/rfc/rfc2315.txt

[24] PAdES Basic (ETSI TS 102 778-2): http://www.etsi.org

[25] RFC 2315: http://www.ietf.org/rfc/rfc2315.txt

[26] Временна́я метка: RFC 3161: http://www.ietf.org/rfc/rfc3161.txt & X9.95: http://www.x9.org/news/pr050701

[27] Online Certificate Status Protocol (протокол онлайнового запроса статуса сертификата): http://www.ietf.org/rfc/rfc2560.txt

[28] Certificate Revocation List (список отозванных сертификатов: http://www.ietf.org/rfc/rfc5280.txt

[29] Algorithms and Parameters for Secure Electronic Signatures (ETSI TS 102 176): http://www.etsi.org