



**Экономический  
и Социальный Совет**

Distr.: General  
5 December 2011  
Russian  
Original: English

---

**Европейская экономическая комиссия**

Комитет по торговле

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

**Восемнадцатая сессия**

Женева, 15–17 февраля 2012 года

Пункт 5 предварительной повестки дня

**Рекомендации и стандарты СЕФАКТ ООН**

**Рекомендация № 37: Функциональная совместимость  
подписанных цифровых документов**

**Подготовлена Группой по проекту защищенности документов  
и сообщений XML Направления разработки программы по  
логистической цепи и представляется Бюро для сведения**

*Резюме*

Первоначальный проект рекомендации № 37 ЕЭК ООН о функциональной совместимости подписанных цифровых документов был представлен СЕФАКТ ООН на его шестнадцатой сессии и впоследствии в соответствии с решением 10-04 был представлен на утверждение в рамках межсессионного процесса. Замечания, полученные в ходе межсессионного процесса, обсуждались на семнадцатой сессии. Было решено до 12 сентября 2011 года вернуться к шагу 4 "Публичный обзор" открытого процесса разработки.

В настоящее время Направление разработки проекта по логистической цепи представляет обновленный проект настоящей рекомендации для сведения.

Бюро также подготовило пояснительную записку (ECE/TRADE/C/CEFACT/2012/8) в качестве справочной информации для рассмотрения данной темы Пленумом.

Предыдущая документация:

ECE/TRADE/C/CEFACT/2010/14 Рекомендация № 37: Функциональная совместимость подписанных цифровых документов

## Содержание

	<i>Стр.</i>
1. Предисловие .....	3
2. Резюме .....	3
2.1 Контекст .....	3
2.2. Рекомендация .....	4
2.3 Полезные эффекты и цели .....	5
3. Введение .....	6
3.1 Сфера охвата .....	6
3.2 Цель .....	6
3.3 Аудитория .....	8
4. Определения .....	8
5. Рекомендация .....	10
5.1 Предусмотренные в рекомендации признаки подписанного цифрового документа .....	10
5.2 Функциональные параметры признаков .....	10
5.3 Различия между подписанными цифровыми документами и подписанными бумажными документами .....	11
6. Заключение .....	11
7. Литература .....	12

## 1. Предисловие

Рекомендация о функциональной совместимости подписанных цифровых документов (РСПЦД) нацелена на повышение уровня функциональной совместимости цифровых документов в качестве одного варианта в конкретных ситуациях в целях содействия развитию безбумажной международной торговли.

Для достижения этой цели в рекомендации сформулирован ряд функциональных требований к подписанным цифровым документам, затрагивающих построение и связи между подписанной информацией, цифровыми опознавательными признаками и подписями подразумеваемых лиц, подписывающих информацию.

Рекомендация предназначена для использования организациями или физическими лицами, соглашающимися использовать подписанные цифровые документы.

Юридические вопросы, затрагиваемые настоящей рекомендацией, следует координировать с другими международными организациями.

В рекомендации не затрагиваются правовые аспекты электронных подписей, которые рассматриваются на международном уровне в других документах, например опубликованных Комиссией Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ). В ней также не затрагиваются вопросы удобства пользования и толкования подписанной информации.

Настоящая рекомендация не должна противоречить рекомендации 14 ЕЭК ООН "Удостоверение подлинности внешнеторговых документов средствами помимо подписи".

## 2. Резюме

### 2.1 Контекст

Многообразие стандартов электронной подписи способно затруднить в техническом или юридическом отношении подтверждение подписанных цифровых документов получателем. В некоторых случаях это может непосредственным образом влиять на способность организаций и государственных органов без риска для себя обмениваться цифровыми документами как между собой, так и с партнерами – управленческими и финансовыми структурами.

Применение этих рекомендуемых стандартов в конкретных ситуациях может также быть связано с проблемами соблюдения и дополнительными расходами, а также, возможно, с необходимостью регулятивных или других правовых механизмов, что также необходимо учитывать при определении типа того общего положительного результата, который предполагается достичь.

Для решения этой проблемы в основу настоящей рекомендации положен функциональный, а не технический подход к подписанным цифровым документам, позволяющий акцентировать внимание, прежде всего, на предмете, а не на методе.

Проверка подписанных цифровых документов не должна требовать от сторон предварительного согласования каких-либо процессов, для того чтобы проверяющий мог получить четкое представление о положении вещей по следующему разумному перечню вопросов:

- параметры подписей (дата, место, вид обязательств);
- целостность подписанной информации, где это положительным образом предполагается;
- целостность и действительность цифровых опознавательных признаков подразумеваемых подписавших лиц и степени надежности, которую они призваны обеспечить, в соответствии с правилами подразумеваемых удостоверяющих сторон, соглашениями между пользователями, а также с применимыми регулятивными нормами;
- надежность подразумеваемых удостоверяющих центров.

В настоящей рекомендации излагается ряд функциональных требований к созданию и проверке подписанных цифровых документов в целях повышения их функциональной совместимости с учетом того, что в случае ее принятия со временем может потребоваться внесение изменений.

Помимо отмеченных здесь конкретных вопросов, основное внимание в рекомендации уделяется функциональной совместимости, и она не изучалась в общеюридическом разрезе или в связи с конкретными национальными законами, а соблюдение этих стандартов не дает каких-либо гарантий признания или юридической силы любого подписанного цифрового документа в любой правовой системе.

В том что касается правительств, законодательных органов, судебных властей, реализующих структур, пользователей или других сторон, рекомендация не ставит цели решения вопроса о том, будет ли ее использование юридически признаваться законодательством любой страны или в международных операциях. Использование принципов, изложенных в настоящей рекомендации, не обязательно будет иметь большую доказательственную силу в любом судебном разбирательстве, чем любые допустимые методы предоставления или подтверждения такой информации в качестве доказательства.

## **2.2. Рекомендация**

В настоящей рекомендации любым организациям или сторонам, принимающим решение обмениваться с другими сторонами подписанными цифровыми документами, предлагается применять следующие принципы в целях максимальной функциональной совместимости:

Подписанные цифровые документы:

- ДОЛЖНЫ содержать однозначно идентифицируемое содержание;
- ДОЛЖНЫ иметь одну и более чем одну подпись;
- ДОЛЖНЫ однозначным образом содержать все необходимые опознавательные признаки.

Каждая подпись, содержащаяся в цифровом документе:

- МОЖЕТ иметь дату подписания и другие признаки;
- ДОЛЖНА относиться ко всему содержанию документа;
- МОЖЕТ иметь одну или более чем одну контрподпись.

Ключевые слова "ДОЛЖЕН" или "МОЖЕТ", используемые в этом разделе, следует толковать следующим образом:

- "ДОЛЖЕН": означает, что данное требование представляет собой абсолютное требование данной спецификации;
- "МОЖЕТ": означает, что требование имеет факультативный характер. Решение, которое не предусматривает конкретный вариант, должно обеспечивать функциональную совместимость с другим решением, которое его предусматривает, хотя, возможно, и с уменьшенной функциональностью.

Аналогичным образом решение, которое предусматривает данный вариант, должно быть подготовлено для функциональной совместимости с другим решением, которое его не предусматривает (за исключением, разумеется, функции, обеспечиваемой данным вариантом).

## 2.3 Полезные эффекты и цели

В настоящей рекомендации хозяйственным, административным и финансовым организациям предлагается ряд стандартных функциональных требований, призванных повысить функциональную совместимость создания и подтверждения подписанных цифровых документов при условии согласования и применения соответствующих им стандартов и технических решений с учетом издержек для пользователей, связанных с регламентациями, развитием инфраструктуры и практической деятельностью.

Эти положительные результаты могут быть получены при широко доступных в настоящее время технологиях и продуктах, включая проекты с открытым кодом.

Ее цели:

- повышение эффективности и надежности создания и подтверждения подписанного цифрового документа, полученного от другой стороны;
- повышение функциональной совместимости подписанных цифровых документов, что в свою очередь должно способствовать повышению доверия;
- определение широкого и при этом координированного пути ускорения перехода на безбумажные технологии.

### **3. Введение**

#### **3.1 Сфера охвата**

С начала 90-х годов было разработано, предложено и принято большое число технических стандартов на подписанные цифровые документы. Примеры таких стандартов приводятся в разделе 7 – Литература.

Однако из-за многообразия стандартов, допускающих многовариантность и не содержащих указаний в отношении того, как ставить цифровые подписи на цифровые документы, возникла проблема функциональной несовместимости подписанных цифровых документов с синтаксической и семантической точек зрения, а также с точки зрения методов обработки.

Цель настоящей рекомендации – предложить конкретный подход к созданию и подтверждению подписанных цифровых документов при уделении основного внимания их функциональным аспектам в отличие от их технических аспектов.

Для секторов, для которых настоящая рекомендация в итоге признана подходящим решением, и там, где это приемлемо для участвующих сторон, акцент на функциональных аспектах позволяет определить общие функциональные признаки подписанного цифрового документа. Такие предусмотренные в настоящей рекомендации признаки секторальных решений с учетом других факторов, таких как затраты, регулятивная инфраструктура, практика в данном секторе и т.п., могут упростить и облегчить создание и проверку подписанных цифровых документов.

Настоящая рекомендация не затрагивает возможности выбора сторонами других методик, которые могут быть приняты системами или сторонами для реализации аналогичных целей.

В настоящей рекомендации содержится ряд функциональных требований, призванных содействовать функциональной совместимости создания и проверки подписанных цифровых документов в той мере, в какой это подходит для конкретных секторов и соответствующих сторон.

#### **3.2 Цель**

Цель настоящей рекомендации – облегчить обмен и проверку подписанных цифровых документов, которые могут иметь большое значение в хозяйственной практике, обеспечив или повысив их функциональную совместимость в той мере, в какой это подходит для конкретных секторов и соответствующих сторон. Ожидается, что ее использование ускорит "дематериализацию" цифровых документов, содействуя созданию, проверке и функциональной совместимости подписанных цифровых документов.

Для конечного пользователя использование цифровых подписей предполагает выполнение трех основных процедур:

- определение объема содержания документа, к которому относится цифровая подпись;
- подписание соответствующего документа (соответствующих документов) или их частей;

- проверка подписи (подписей) под документом, включая выявление параметров подписи.

Конкретная региональная практика в областях электронных торгов и электронного фактурирования показывает, что, когда та или иная сторона подписывает документ, используя для этого свои программные средства обозначения реквизитов и подписи, необходимо решить ряд проблем 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: возможны случаи, когда программа, используемая для проверки подписи, или формат подписи не позволяет определить назначение подписи (например, хотело ли подписавшее лицо удостоверить целостность документа или же оно хотело только подтвердить свое согласие с его содержанием и т.д.);
- проблема подтверждения цифровых реквизитов: программа, используемая для подтверждения подписи, может оказаться не в состоянии определить надежность цифровых реквизитов или их действительность на дату и время подписания.

Возможность проверить подлинность подписи имеет исключительно важное значение, например, на этапе подведения итогов или объявления победителя на торгах при проведении государственных закупок, поскольку неподтвержденность подписи может привести к тому, что конкурсные предложения будут по ошибке признаны недействительными и отклонены или же используемые процедуры проверки могут вызвать задержки и уменьшить экономию расходов, которую предполагалось достичь благодаря использованию цифровых подписей.

Для решения первых двух проблем может потребоваться, чтобы все созданные подписи представлялись в формате, воспринимаемом всеми пакетами программного обеспечения, используемыми для проверки этих подписей.

Таким образом, основные положительные результаты предлагаемых признаков подписанных цифровых документов заключаются в следующем:

- содействие повышению доверия на основе предоставления возможностей создания и проверки подписанных цифровых документов и удобства работы с ними;
- содействие совместимости подписанных цифровых документов с помощью функционального общего знаменателя, независимо от используемого технического формата;
- упрощение применения цифровых подписей в производственных и архивных приложениях, с тем чтобы облегчить замену функции "печать" функцией "подписать" или "удостоверить".

### 3.3 Аудитория

Настоящий документ предназначен главным образом для организаций, сторон и систем, которым приходится решать следующие задачи:

- обмен подписанными цифровыми документами;
- выбор формата подписанных цифровых документов, приемлемого для конкретного проекта "дематериализации";
- отслеживание информационных технологий на предмет их возможного использования для цифровых подписей и цифрового архивирования;
- обеспечение функциональной совместимости подписанных цифровых документов.

## 4. Определения

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

УЭП: усиленная электронная подпись

СУЭП: усиленная электронная подпись с использованием СКС

Подписанный цифровой документ: цифровой документ или другая информация, которые могут использоваться для подтверждения надежности или неповрежденности подписанной информации, либо согласование сторонами или использование системой процедур для достижения этого. Он не определяет конкретной стороны, которая фактически произвела данное действие, в отсутствие дополнительных процедур и технологий

СКС: синтаксис криптографического сообщения

Соподпись: подпись, относящаяся к тому же содержимому, что и другая подпись, или сопоставимое средство обозначения соответствующей стороны согласно практике, применяемой в данном секторе

Лицо, проставляющее контрподпись: лицо, являющееся держателем данных, необходимых для создания контрподписи, и действующее либо от своего имени, либо от имени другого лица, которое оно представляет, либо сопоставимое средство обозначения соответствующей стороны согласно применяемой в данном секторе практике

Контрподпись: подпись, относящаяся к другой подписи (подписанное содержимое контрподписи само по себе является подписью); может быть также названа "иерархической подписью"

Информационное сообщение: информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, магнитных, оптических или аналогичных средств, включая электронный обмен данными, электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими (статья 4, определение, Конвенция ООН об электронной торговле)

Цифровой документ: документ в цифровой форме, используемый для передачи информации либо для ее представления пользователю, либо для ее обработки тем



КЭТ или Конвенция ООН об электронной торговле: Конвенция Организации Объединенных Наций об использовании электронных сообщений в международных договорах, Официальные отчеты Генеральной Ассамблеи, шестидесятая сессия, A/RES/60/21 (иначе называемая Конвенция ООН об электронной торговле или КЭТ)

Электронная подпись: данные в электронной форме, которые содержатся в информационном сообщении, приложены к нему или логически ассоциируются с ним и могут быть использованы для определения подписавшего лица в связи с информационным сообщением и для подтверждения согласия подписавшего лица с информацией, содержащейся в информационном сообщении (литература 1)

ЕИСС: Европейский институт по стандартизации в области связи

ЕС: Европейский союз

Информация: включает все виды цифровых файлов [нужно ли определение "файла"?] и содержимого, включая, но не ограничиваясь ими, "документы, а также информационные сообщения любого вида"

РГПИ: Рабочая группа проектирования Интернета

ИСО: Международная организация по стандартизации

ПУЭП: усиленная электронная подпись в среде PDF

PDF: машиннонезависимый формат документа

КСОК: криптографический стандарт с открытым ключом

ЗПЗ: запрос о представлении замечаний

Подписавшее лицо: лицо, являющееся держателем данных, необходимых для создания подписи, и действующее либо от своего имени, либо от имени лица, которое оно представляет

Подписанное содержимое: данные, содержащиеся в подписанном цифровом документе, который подписан подразумеваемым подписавшим лицом (подразумеваемыми подписавшими лицами)

ТС: техническая спецификация

ЮНСИТРАЛ: Комиссия Организации Объединенных Наций по праву международной торговли

Экс-УЭП: усовершенствованная электронная подпись с использованием средств XML

XML: расширяемый язык разметки

XMLDSIG: цифровая подпись в формате XML

## 5. Рекомендация

В настоящем разделе излагается рекомендация.

### 5.1 Предусмотренные в рекомендации признаки подписанного цифрового документа

В рекомендации предлагаются признаки подписанных цифровых документов, призванные обеспечить максимальную функциональную совместимость между созданием и подтверждением подписанных цифровых документов.

Эти признаки задаются как набор функциональных параметров.

### 5.2 Функциональные параметры признаков

В этом пункте излагаются функциональные параметры предлагаемых признаков подписанного цифрового документа.

Ключевые слова "ДОЛЖЕН" и "МОЖЕТ", используемые в этом разделе, следует толковать следующим образом:

- "ДОЛЖЕН": это слово означает, что данное требование представляет собой абсолютное требование спецификации;
- "МОЖЕТ": данное слово означает, что данное требование является полностью факультативным. Решение, которое не предусматривает конкретный вариант, ДОЛЖНО быть подготовлено таким образом, чтобы оно обеспечивало функциональную совместимость с другим решением, которое предусматривает данный вариант, хотя и, возможно, с меньшими функциональными свойствами. Таким же образом решение, которое не предусматривает конкретный вариант, ДОЛЖНО быть подготовлено таким образом, чтобы оно обеспечивало функциональную совместимость с другим решением, которое не предусматривает данный вариант (за исключением, разумеется, функции, обеспечиваемой данным вариантом).

Подписанный цифровой документ, соответствующий предлагаемым признакам подписанного цифрового документа:

- ДОЛЖЕН содержать однозначно идентифицируемое содержание с указанием его вида и, факультативно, названия;
- ДОЛЖЕН иметь одну или более чем одну подпись;
- ДОЛЖЕН четко определенным образом содержать все соответствующие цифровые опознавательные признаки.

Каждая подпись, содержащаяся в подписанном цифровом документе, соответствующем предлагаемым признакам подписанного цифрового документа:

- ДОЛЖНА относиться ко всему содержимому;
- МОЖЕТ содержать элементы, которые должны быть подписаны подписью, такие как:
  - дата подписания, определяющая момент времени, когда, по утверждению подразумеваемого подписавшего лица, оно выполнило процедуру подписания;

- местонахождение подписавшего лица, представляющее собой мнемокод адреса, ассоциируемого с подписавшим лицом в данной географической точке, например городе;
- указание концепции подписи, определяющей в точности роль и обязательства, которые подразумеваемое подписавшее лицо намерено взять на себя в отношении подписанного документа;
- вид обязательства, ассоциируемого с подписью: четкое указание удостоверяющей стороне на то, что, подписав данный документ, та иллюстрирует обязательство конкретного вида от имени подразумеваемого подписавшего лица;
- роль (роли) подразумеваемого подписавшего лица; указывает, в каком качестве (каких качествах) или в какой должности (должностях) действовало подразумеваемое подписавшее лицо, подписывая данный документ;
- указание цифровых реквизитов подразумеваемого подписавшего лица и его подразумеваемых удостоверятелей;
- МОЖЕТ быть проставлено одной контрподписью или несколькими контрподписями;
- МОЖЕТ содержать отметку времени.

### 5.3 Различия между подписанными цифровыми документами и подписанными бумажными документами

Многие элементы одинаковы для подписанных документов обоих видов, однако имеются некоторые важные различия, например следующие:

- реквизиты подразумеваемых подписавших лиц не всегда присутствуют в бумажных документах;
- реквизиты подразумеваемых удостоверятелей подразумеваемого подписавшего лица, как правило, отсутствуют в бумажных документах;
- наоборот, подписанные бумажные документы, как правило, имеют собственноручные подписи, хотя в практике делопроизводства также распространены штампы или факсимильные подписи, в то время как не предполагается, что цифровая подпись в электронном цифровом документе будет иметь графическое отображение, если только одновременно не используются другие технологии, такие как динамическая подпись. Обычно только компьютерная программа способна произвести сложные математические расчеты, необходимые для проверки цифровой подписи.

## 6. Заключение

Представленное в настоящем документе описание признаков подписанного цифрового документа в той мере, в какой оно принято организациями, системами или сторонами, преследует цель а) способствовать дематериализации бумажного документооборота за счет упрощения (одновременно с учетом регулятивных и инфраструктурных механизмов и издержек, связанных с этим) и облегчения процедур создания и проверки подписанных цифровых документов и б) содействовать их использованию в прикладных программах для веде-

ния деловых операций в контекстах или ситуациях, когда это необходимо или соответствует договоренности.

## 7. Литература

PKCS#7: <http://www.rsa.com/rsalabs/node.asp?id=2129>

S/MIME: <http://www.ietf.org/rfc/rfc3851.txt>

CMS: <http://www.ietf.org/rfc/rfc3852.txt>

XMLDSIG: <http://www.w3.org/TR/xmlsig-core/>

CAdES (ETSI TS 101 733): <http://www.etsi.org>

EANCOM digital signature:

[http://www.gs1.org/docs/ecom/eancom/eancom\\_Digital\\_Signature.pdf](http://www.gs1.org/docs/ecom/eancom/eancom_Digital_Signature.pdf)

Signed PDF (ISO/DIS 32000): [http://www.adobe.com/devnet/pdf/pdf\\_reference.html](http://www.adobe.com/devnet/pdf/pdf_reference.html)  
or otherwise

[http://www.iso.org/iso/fr/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=51502](http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502)

XAdES (ETSI TS 101 903): <http://www.etsi.org>

PADES (ETSI TS 102 778): <http://www.etsi.org>

---