МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)

INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO/IEC 24824-3— 2013

Информационные технологии

ОБЩИЕ ПРАВИЛА ПРИМЕНЕНИЯ ASN. 1

Безопасность быстрых сетевых услуг

Часть 3

(ISO/IEC 24824-3:2008, IDT)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены в ГОСТ 1.0—2015 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2015 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Государственный научно-исследовательский и конструкторско-технологический институт «ТЕСТ» (ФГУП ГосНИИ «ТЕСТ») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 5

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 14 ноября 2013 г. № 44)

За принятие проголосовали.

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Минэкономики Республики Армения
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 11 июня 2014 г. № 567-ст межгосударственный стандарт ГОСТ ISO/IEC 24824-3—2013 введен в действие в качестве национального стандарта Российской Федерации с 1 сентября 2015 г.

5 Настоящий стандарт идентичен международному стандарту ISO/IEC 24824-3:2008 «Информационные технологии. Общие правила применения ASN.1. Безопасность быстрых сетевых услуг. Часть 3» («Information technology — Generic applications of ASN.1: Fast infoset security. Part 3», IDT).

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

6 ВВЕДЕН ВПЕРВЫЕ

7 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

*Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «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, оформление, 2018

В Российской Федерации 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

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

Информационные технологии

ОБЩИЕ ПРАВИЛА ПРИМЕНЕНИЯ ASN.1

Безопасность быстрых сетевых услуг

Часть 3

Information technology. Generic applications of ASN.1. Fast infoset security.
Part 3

Дата введения — 2015—09—01

1 Область применения

В настоящем стандарте определены четыре канонических алгоритма быстрого инфо-набора, которые могут быть использованы в применении W3C XML-подписи, а также предоставлены URI для этих алгоритмов.

В настоящем стандарте также определены расширения уровня приложения к правилам обработки W3C XML шифрования для шифрования части XML инфо-набора (см. 8.1), сериализированного как документ быстрого инфо-набора, и дешифрования зашифрованной части (см. 8.3), сериализированной как документ быстрого инфо-набора.

В настоящем стандарте не рассматривается использование любых получившихся элементов информации W3C XML-подписи или элементов информации W3C XML шифрования.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные документы. Для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных — последнее издание ссылочного документа (включая все изменения к нему).

2.1 Идентичные рекомендации и международные стандарты

- ITU-T Recommendation X.891 (2005) | ISO/IEC 24824-1:2007, Information technology — Generic applications of ASN.1: Fast infoset (Рекомендация МСЭ-Т X.891 (2005) | ISO/IEC 24824-1:2007 Информационные технологии. Общие правила применения ASN.1. Быстрые команды)

2.2 Дополнительные ссылки

- ISO/IEC 10646:2003[1)] Information technology — Universal Multiple-Octet Coded Character Set (UCS) (ISO/IEC 10646:2003 Информационные технологии. Универсальный многооктетный набор кодированных символов (UCS))

- W3C Canonical XML:2001, W3C Canonical XML Version 1.0, W3C Recommendation, Copyright © [15 March 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), gost.e-ecolog.ru

gost.e-ecolog.ru нический XML: 2001, Канонический XML версия 1.0, Рекомендация консорциума W3C, © [15.03.2001] Консорциум Всемирной паутины (Массачусетский технологический институт, Национальный институт исследований в области компьютерной обработки данных и автоматики, Университет Кэйо), gost.e-ecolog.ru)

[1)] Заменен на ISO/IEC 10646:2017.

Издание официальное

- W3C XML Encryption:2002, XML Encryption Syntax and Processing, W3C Recommendation, Copyright © [10 December 2002] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), gost.e-ecolog.ru REC-xmlenc-core-20021210 (Шифрование XML:2002, Синтаксис и обработка шифрования XML, Рекомендация консорциума W3C, © [10.12.2002] Консорциум Всемирной паутины (Массачусетский технологический институт, Национальный институт исследований в области компьютерной обработки данных и автоматики, Университет Кэйо), gost.e-ecolog.ru)

- W3C Exclusive Canonical XML:2002, W3C Exclusive XML Canonicalization Version 1.0, W3C Recommendation, Copyright © [18 July 2002] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), gost.e-ecolog.ru TR/2002/REC-xml-exc-c14n-20020718 (Исключающий канонический XML:2002, Исключающая канонизация XML версия 1.0, Рекомендация консорциума W3C, © [18.07.2002] Консорциум Всемирной паутины (Массачусетский технологический институт, Национальный институт исследований в области компьютерной обработки данных и автоматики, Университет Кэйо), http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718)

- W3C XML Information Set:2004, XML Information Set (Second Edition), W3C Recommendation, Copyright © [04 February 2004] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), gost.e-ecolog.ru REC-xml-infoset-20040204 (XML информационный набор:2004, XML информационный набор (второе издание), Рекомендация консорциума W3C, © [04.02.2004] Консорциум Всемирной паутины (Массачусетский технологический институт, Национальный институт исследований в области компьютерной обработки данных и автоматики, Университет Кэйо), gost.e-ecolog.ru)

- W3C XML Signature:2002, XML-Signature Syntax and Processing, W3C Recommendation, Copyright © [12 February 2002] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), gost.e-ecolog.ru (XML-подпись:2002, Синтаксис и обработка XML-подписи, Рекомендация консорциума W3C, © [12.02.2002] Консорциум Всемирной паутины (Массачусетский технологический институт, Национальный институт исследований в области компьютерной обработки данных и автоматики, Университет Кэйо), gost.e-ecolog.ru TR/2002/REC-xmldsig-core-20020212)

- W3C XPath:1999, XML Path Language (XPath) Version 1.0, W3C Recommendation, Copyright © [16 November 1999] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), gost.e-ecolog.ru gost.e-ecolog.ru ith:1999, Язык XML Path (XPath) версия 1.0, Рекомендация консорциума W3C, © [16.11.1999] Консорциум Всемирной паутины (Массачусетский технологический институт, Национальный институт исследований в области компьютерной обработки данных и автоматики, Университет Кэйо), gost.e-ecolog.ru)

3 Термины и определения

В настоящем стандарте применены следующие термины по международным стандартам:

3.1 Заимствованные термины

В настоящем стандарте использованы следующие термины по ISO/IEC 8824-1:

a) документ быстрого инфо-набора (fast infoset document);

b) элемент информации (information item);

c) исходный словарь (initial vocabulary);

d) XML инфо-набор (XML infoset).

3.2 Дополнительные термины

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.2.1 **расширения уровня приложения (для W3C шифрования)** (application-level extensions (for W3C Encryption)): Определяют действия, которые должны быть приняты приложением, если правила W3C шифрования не полностью определяют действия, которые должны быть приняты.

3.2.2 **канонический алгоритм быстрого инфо-набора** (canonical Fast Infoset algorithm): Алгоритм, который используется как входной XML инфо-набор (см. W3C XML информационный набор) или набор узлов XPath (см. W3C XPath) и формирует выходной канонический документ быстрого инфо-набора.

3.2.3 **канонический документ быстрого инфо-набора** (canonical fast infoset document): Документ быстрого инфо-набора, сформированный каноническим алгоритмом быстрого инфо-набора.

3.2.4 **канонический XML алгоритм** (canonical XML algorithm): Алгоритм, который принимает на входе XML инфо-набор, правильно построенный XML-документ или набор узлов XPath, и формирует на выходе правильно построенный XML-документ в канонической форме.

Примечание — Канонические XML алгоритмы в настоящий момент определяются W3C каноническим XML и W3C исключающим каноническим XML.

3.2.5 **канонический XML-документ** (canonical XML document): Правильно построенный XML-документ, сформированный каноническим XML алгоритмом.

3.2.6 **часть элемента (XML инфо-набора)** (element part (of an XML infoset)): Информационный элемент **element** (и все информационные элементы, которые являются производными информационного элемента **element**).

3.2.7 **часть содержимого элемента (XML инфо-набора)** (element content part (of an XML infoset)): Все информационные элементы в свойстве **[children]** информационного элемента **element** (и информационные элементы, которые являются производными этих информационных элементов).

4 Сокращения

В настоящем стандарте применены следующие сокращения:

URI — Uniform Resource Identifier (унифицированный идентификатор ресурса);

UTF-8 — Universal Transformation Function 8-bit (универсальный формат преобразования 8-бит) (см. ISO/IEC 10646, приложение D);

W3C — World Wide Web Consortium (Консорциум Всемирной паутины).

5 Нотация

5.1 В настоящем стандарте **`полужирный шрифт Courier New`** используется для нотации ASN.1, а **полужирный шрифт Arial** — для W3C XML синтаксиса и имен информационных элементов XML информационного набора.

5.2 Названия свойств информационных элементов пишутся **полужирным шрифтом Arial** и заключаются в квадратные скобки (например, **[children]**)

5.3 URI пишутся **полужирным шрифтом Arial** и заключаются в кавычки.

НАПРИМЕР: «

gost.e-ecolog.ru

.

6 Канонические алгоритмы быстрого инфо-набора

6.1 Требования к каноническим алгоритмам быстрого инфо-набора

6.1.1 Следующие подпункты определяют ввод и общие требования к каноническим алгоритмам быстрого инфо-набора. Определенные алгоритмы быстрого инфо-набора (которые ссылаются на этот пункт) рассмотрены в 6.4.

6.1.2 Канонический алгоритм быстрого инфо-набора должен определить канонический XML алгоритм, который используется в концептуальном процессе преобразования (см. 6.1.5).

Примечание — Этот стандарт не определяет канонические XML алгоритмы. Алгоритмы, используемые в 6.4, определяются в W3C каноническом XML и W3C исключающем каноническом XML.

6.1.3 Канонический алгоритм быстрого инфо-набора должен определить URI, который используется для объявления алгоритма в информационных элементах W3C XML-подписи (см. 7.2).

6.1.4 Канонический алгоритм быстрого инфо-набора должен представить канонический документ быстрого инфо-набора для преобразования следующих вводов:

a) XML инфо-набора;

b) набора узлов XPath, произведенного правильно построенным XML-документом, когда он преобразован, как определено в 6.1.5, a).

Примечания

1 Поддержка наборов узлов XPath должна гарантировать, что настоящий стандарт является совместимым с XML стандартами, связанными с безопасностью. W3C канонический XML и W3C исключающий канонический XML

используют модель данных XPath (см. W3C XPath, п. 5). W3C XML-подпись описывает преобразования, используя XPath для канонизации и фильтрации (см. W3C XML-подпись, 6.5 и 6.6.3 соответственно).

2 Ввод набора узлов XPath, произведенного XML-документом, построенным неправильно, не поддерживается для канонизации быстрого инфо-набора (и, следовательно, для W3C XML-подписей, произведенных при помощи канонического алгоритма быстрого инфо-набора).

6.1.5 Концептуальные шаги преобразования, выполняемые каноническим алгоритмом быстрого инфо-набора, с целью произвести канонический документ быстрого инфо-набора, должны быть следующими:

a) входной XML быстрый инфо-набор или ввод набора узлов XPath преобразовываются (каноническим XML алгоритмом), чтобы произвести канонический XML-документ, как определено в 6.2;

b) канонический XML-документ анализируется, чтобы произвести XML быстрый инфо-набор; это будет канонический XML быстрый инфо-набор;

c) канонический XML быстрый инфо-набор сериализируется как канонический документ быстрого инфо-набора, с определенными ограничениями, указанными в 6.3.

Примечание — При реализации можно оптимизировать шаги так, чтобы XML инфо-набор или набор узлов XPath были преобразованы непосредственно к каноническому документу быстрого инфо-набора, не производя промежуточных канонических XML-документов, при этом получив такой же результат, как будто все шаги выполнялись.

6.1.6 Сериализируя в канонический документ быстрого инфо-набора, порядок атрибутов должен быть порядком соответствующего канонического XML-документа.

Примечания

1 Информационные элементы **attribute** среди свойств **[namespace attributes]** и **[attributes]** информационных элементов **element** не упорядочиваются (см. W3C XML информационный набор, 2.2). Пункт 6.1.6 сохраняет порядок документов информационных элементов attributes, произведенных из парсинга канонического XML-документа.

2 W3C канонический XML (канонический XML алгоритм) расширяет порядок документов наборов узлов XPath (см. W3C XPath, п. 5) так, что пространство имен элемента и приписанные узлы канонически упорядочиваются (см. W3C канонический XML, 2.2).

6.2 Требования к каноническим XML алгоритмам для использования каноническими алгоритмами быстрого инфо-набора

6.2.1 Следующий пункт определяет требования для канонического XML алгоритма, которые он должен удовлетворить для того, чтобы он мог использоваться при определении канонического алгоритма быстрого инфо-набора.

Примечание — Алгоритмы, определенные в W3C каноническом XML и W3C исключающем каноническом XML, удовлетворяют этим требованиям.

6.2.2 Канонический XML алгоритм, используемый в определении канонического алгоритма быстрого инфо-набора, должен быть способен преобразовывать (в правильно построенный канонический XML-документ) все те входные данные, которые поддерживает канонический алгоритм быстрого инфо-набора (см. 6.1.4).

Примечание — Такие канонические XML алгоритмы определяются W3C каноническим XML и W3C исключающим каноническим XML.

6.3 Ограничения при сериализации XML инфо-набора в канонический документ быстрого инфо-набора

Примечание — Эта сериализация является шагом c) в п. 6.1.5, который используется в создании октетов для подписи.

6.3.1 Значения типа **`NonIdentifyingStringOrIndex`** (см. МСЭ-Т X.891 | ISO/IEC 24824-1, 7.14) должны состоять из альтернативы **`literal-character-string`** с компонентом **`add-to-table`**, установленным как **`FALSE`**.

6.3.2 Кодировка UTF-8 (см. ISO/IEC 10646) должна использоваться для всех символьных строк, представленных как значения типа **`EncodedCharacterString`** (см. МСЭ-Т X.891 | ISO/IEC 24824-1, 7.17).

Примечание — Такие символьные строки будут связаны с последовательностями смежных символьных информационных элементов и свойствами **[normalized value]** информационных элементов **attribute**.

6.3.3 Последовательность смежных символьных информационных элементов, запускающихся с первого символьного информационного элемента, у которой нет никакого предыдущего символьного элемента непосредственно в свойстве **[children]**, до информации о последнем знаке, у которой нет никакого дальнейшего символьного информационного элемента непосредственно в свойстве **[children]**, должна быть представлена единственным значением типа **`CharacterChunk`** (см. МСЭ-Т X.891 | ISO/IEC 24824-1, 7.7).

6.3.4 Если последовательность смежных символьных информационных элементов превышает максимум, разрешенный для значения типа **`CharacterChunk`** (2^{32}), то должны быть последовательные значения типа **`CharacterChunk`** для каждой максимальной последовательности смежных символьных информационных элементов.

6.3.5 У канонического документа быстрого инфо-набора не должно быть исходного словаря. Компонент **`initial-vocabulary`** значения типа **`Document`** должен отсутствовать (см. МСЭ-Т X.891 | ISO/IEC 24824-1, 7.2.1).

6.3.6 Таблица словаря (см. МСЭ-Т X.891 | ISO/IEC 24824-1, п. 6), не может содержать двойные записи в таблице. МСЭ-Т X.891 | ISO/IEC 24824-1, 7.13.7 применяется с таким ограничением, что действие 7.13.7, b) не должно выполняться, если идентичная символьная строка будет существовать в текущем содержимом применяемой таблицы.

Примечание — Таблица CONTENT CHARACTER CHUNK и таблица ATTRIBUTE VALUE (см. МСЭ-Т X.891 | ISO/IEC 24824-1, 8.4) не будет содержать записей из-за ограничения, описанного в 6.3.1.

6.4 Канонические алгоритмы быстрого инфо-набора

6.4.1 Следующие пункты определяют четыре канонических алгоритма быстрого инфо-набора. В каждом случае определяется канонический XML алгоритм, который будет использоваться (см. 6.1.2) вместе с URI для алгоритма быстрого инфо-набора (см. 6.1.3).

6.4.2 «Включающий канонический алгоритм быстрого инфо-набора без комментариев» должен быть идентифицирован URI «**urn:fastinfoset:c14n:inclusive**» с использованием канонического XML алгоритма, определенного в W3C каноническом XML со вторым входным параметром (см. W3C канонический XML, 2.1), установленным как false.

Примечание — Второй входной параметр является булевской переменной, которая указывает, должны ли комментарии быть включены в каноническую форму, произведенную каноническим XML алгоритмом.

6.4.3 «Включающий канонический алгоритм быстрого инфо-набора с комментариями» должен быть идентифицирован URI «**urn:fastinfoset:c14n:inclusive:withcomments**» с использованием канонического XML алгоритма, определенного в W3C каноническом XML со вторым входным параметром (см. W3C канонический XML, 2.1), установленным как true.

6.4.4 «Исключающий канонический алгоритм быстрого инфо-набора без комментариев» должен быть идентифицирован URI «**urn:fastinfoset:c14n:exclusive**» с использованием канонического XML алгоритма, определенного в W3C исключающем каноническом XML, со вторым входным параметром (см. W3C исключающий канонический XML, п. 3), установленным как false. Этот алгоритм быстрого инфо-набора имеет параметр «InclusiveNamespace PrefixList» (см. W3C исключающий канонический XML, 1.1), который может быть нулем, и который переходит неизмененным в канонический XML алгоритм.

6.4.5 «Исключающий канонический алгоритм быстрого инфо-набора с комментариями» должен быть идентифицирован URI «**urn:fastinfoset:c14n:exclusive:withcomments**» с использованием канонического XML алгоритма, определенного в W3C исключающем каноническом XML, со вторым входным параметром (см. W3C исключающий канонический XML, п. 3), установленным как true. Этот алгоритм быстрого инфо-набора имеет параметр «InclusiveNamespace PrefixList» (см. W3C исключающий канонический XML, 1.1), который может быть нулем, и который переходит неизмененным в канонический XML алгоритм.

7 W3C XML-подпись и быстрый инфо-набор

7.1 В следующих подразделах определяется использование канонического алгоритма быстрого инфо-набора (см. 6.4).

7.2 Информационный элемент **Algorithm attribute** в свойстве **[attributes]** информационного элемента **CanonicalizationMethod element** (см. W3C XML-подпись, 4.3.1) или информационного элемента

Transform element (см. W3C XML-подпись, 4.3.3.4) должен иметь свойство **[normalized value]**, которое является URI, идентифицирующим канонический алгоритм быстрого инфо-набора (см. 6.1.3).

7.3 Если канонический алгоритм быстрого инфо-набора определяет канонический XML алгоритм (см. 6.1.2) ссылкой на W3C исключающий канонический XML, и параметр «InclusiveNamespace PrefixList» (см. W3C исключающий канонический XML, 1.1) дается как входной (см. 6.4.4 и 6.4.5), то параметр должен быть представлен так, как определено в W3C исключающий канонический XML, п. 4.

8 W3C XML шифрование и быстрый инфо-набор

W3C XML шифрование допускает (и настоящий стандарт также поддерживает) шифрование частей элементов и частей содержимого элементов XML быстрого инфо-набора.

8.1 Расширения уровня приложения для шифрования

8.1.1 Каждый элемент данных (см. W3C XML шифрование, 4.1), чтобы быть зашифрованным, должен быть частью элемента или частью содержимого элемента XML быстрого инфо-набора, выбранного шифрующим приложением.

8.1.2 Операции по обработке шифрования (определенные в W3C XML шифрование, 4.1) по отношению к части XML быстрого инфо-набора должны быть расширены для операций 3.2, 4 и 5.2 из W3C XML шифрование, 4.1, как определено в трех следующих пунктах.

8.1.3 Операция 3.2 из W3C XML шифрование, 4.1 должна быть расширена, чтобы получить октеты, которые будут зашифрованы следующим образом:

a) выбранная часть исходного XML быстрого инфо-набора (A) должна быть преобразована в полный XML быстрый инфо-набор (B) как определено в 8.2;

b) этот XML быстрый инфо-набор (B) должен быть сериализирован, используя МСЭ-Т X.891 | ISO/IEC 24824-1 с ограничением, что не будут использоваться внешние словари;

c) получившиеся октеты должны быть октетами, которые будут зашифрованы в операции 3.3 в W3C XML шифрование, 4.1.

8.1.4 Операция 4 в W3C XML шифрование, 4.1 должна быть расширена, чтобы включать информационный элемент **Type attribute** в свойство **[attributes]** информационного элемента **EncryptedData element** (см. W3C XML шифрование, 3.1), свойство **[normalized value]** которого должно быть одним из следующих:

a) если часть XML быстрого инфо-набора будет частью элемента, то **[normalized value]** информационного элемента **Type attribute** должно быть URI «**urn:fastinfoset:element**»;

b) если часть XML быстрого инфо-набора будет частью содержимого элемента, то **[normalized value]** информационного элемента **Type attribute** должно быть URI «**urn:fastinfoset:element-content**».

8.1.5 Операция 5.2 в W3C XML шифрование, 4.1 должна быть расширена так, что информационный элемент **EncryptedData element** (произведенный операцией 4 в W3C XML шифрование, 4.1, расширенной, как определено в 8.1.4) должен заменить часть XML быстрого инфо-набора, который был обработан в операции 3 (расширенной, как определено в 8.1.3).

8.2 Формирование полного XML инфо-набора из части XML инфо-набора

8.2.1 Формирование из части элемента XML инфо-набора

8.2.1.1 Полный XML быстрый инфо-набор должен быть сформирован с информационным элементом **document**, обладающим следующими свойствами:

a) свойством **[children]**, единственный член которого является копией (E, скажем) информационного элемента **element** (и всех его свойств, включая **[children]**), который является частью элемента исходного XML быстрого инфо-набора, который должен быть зашифрован;

b) свойством **[document element]**, которое является E.

8.2.1.2 Свойство **[namespace attributes]** у E (см. 8.2.1.1, a)) должно быть изменено так, чтобы оно не противоречило свойству **[in-scope namespaces]** у E.

Примечания

1 При реализации можно удалить любые неиспользованные информационные элементы пространства имен в свойстве **[in-scope namespaces]** у E (и его производных) перед тем, как свойство **[namespace attributes]** у E будет изменено.

2 Для более подробной информации о рекомендованной обработке информационных элементов, соответствующих объявлениям пространств имен по умолчанию и специфичным для XML информационным элементам **attribute**, см. W3C XML шифрование, 4.3.3.

8.2.2 Формирование из части содержимого элемента XML быстрого инфо-набора

8.2.2.1 Полный XML быстрый инфо-набор должен быть сформирован информационным элементом **document**, содержащим следующие свойства:

a) свойство **[children]**, единственный член которого является информационным элементом **element** (E, скажем), как определено в 8.2.2.2;

b) свойство **[document element]**, которое является E.

8.2.2.2 Информационный элемент **element** E (см. 8.2.2.1, a)) не должен иметь никакого значения для свойств **[namespace name]** и **[prefix]**, но должен иметь:

a) свойство **[local name] «content»**;

b) свойство **[children]**, которое является копией свойства **[children]** части содержимого элемента исходного XML быстрого инфо-набора;

c) свойство **[namespace attributes]** у E, которое согласуется со всеми свойствами **[in-scope namespaces]** информационных элементов **element** среди свойства **[children]** части содержимого элемента исходного XML.

Примечания

1 В реализации возможно удаление любых неиспользованных информационных элементов пространства имен в свойствах **[in-scope namespaces]** информационных элементов **element** (и производных) в свойстве **[children]** фрагмента XML быстрого инфо-набора перед тем, как свойство **[namespace attributes]** у E будет изменено.

2 Для более подробной информации о рекомендованной обработке информационных элементов, соответствующих объявлениям пространств имен по умолчанию и специфичным для XML информационным элементам **attribute**, см. W3C XML шифрование, 4.3.3.

8.3 Расширения уровня приложений для дешифрования

Операция 5.0 в W3C XML шифрование, 4.2 должна быть расширена, чтобы обработать информационный элемент **EncryptedData element**, который содержит информационный элемент **Type attribute** (см. W3C XML шифрование, 3.1) среди свойства **[attributes]**, свойство **[normalized value]** которого является одним из URI, определенных в 8.1.4. Для этого необходимо выполнить следующие шаги:

a) последовательность октетов, полученная в процессе операции 3 (см. W3C XML шифрование, 4.2), должна быть интерпретирована как документ быстрого инфо-набора;

b) XML быстрый инфо-набор должен быть получен в результате парсинга документа быстрого инфо-набора;

c) части этого XML быстрого инфо-набора должны использоваться для замены информационного элемента **EncryptedData element** следующим образом:

1) если URI — «**urn:fastinfoset:element**», то информационный элемент **element**, которой является свойством **[document element]** информационного элемента **document** XML быстрого инфо-набора, должен заменить информационный элемент **EncryptedData element**;

2) если URI — «**urn:fastinfoset:element-content**», то все информационные элементы в свойстве **[children]** информационного элемента **element**, который является свойством **[document element]** информационного элемента **document** XML быстрого инфо-набора, должны заменить информационный элемент **EncryptedData element**.

Приложение А
(справочное)

Примеры подписания и шифрования XML инфо-набора

А.1 Общее описание примеров

А.1.1 Все XML инфо-наборы в настоящем приложении будут представлены как XML-документы. Для краткости пространства имен URI и текстовый контент (base64 [IETF RFC 2045] закодированные октеты), которые не затрагиваются в настоящем приложении, будут сокращены или полностью удалены и представлены символами «...».

А.1.2 Криптографические алгоритмы, представленные в этом приложении, предназначены только для пояснения. Настоящий стандарт не гарантирует использование таких алгоритмов.

А.1.3 В настоящем приложении рассматриваются два примера: подписание XML инфо-набора (см. А.2) и подписание и шифрование XML инфо-набора (см. А.3).

А.1.4 XML инфо-набор, выбранный в каждом примере (чтобы быть подписанным или подписанным и зашифрованным), является следующим инфо-набором SOAP сообщений:

```
<soap:Envelope xmlns:soap=«...»>
  <soap:Body>
    <n:payment xmlns:n=«...»>1000</n:payment>
  </soap:Body>
</soap:Envelope>
```

А.1.5 Финальный подписанный или подписанный и зашифрованный инфо-набор SOAP сообщений соответствует указанному в OASIS Web Services Security [WSS] и WS-I Basic Profile [WS-I], за исключением того, что для подписания используется канонический алгоритм быстрого инфо-набора (см. 6.4), и зашифрованное содержимое определяется как документ быстрого инфо-набора (см. 8.1.4).

А.1.6 В примере представлены процессы, с помощью которых XML инфо-набор может быть подписан/проверен или подписан/проверен и зашифрован/дешифрован, поэтому точная информация о ключах, значениях подписей, значениях хэш-сумм и зашифрованных данных в примере не описывается.

А.1.6.1 Инфо-набор SOAP сообщений представляет собой простой пример платежного запроса на 1000 единиц от клиента к сервису. Чтобы гарантировать неизменность 1000 единиц, например при вмешательстве третьего лица, при передаче SOAP сообщения с использованием сети общего пользования, информационный элемент **soap:Body element** и содержимое могут быть подписаны, и получатель может проверить, что в содержимое не вмешивались и что оно не было подменено. Чтобы гарантировать, что сообщение смогут прочитать только доверенные стороны (и что платеж на 1000 единиц был запрошен), информационный элемент **soap:Body element** и содержимое могут быть подписаны, а затем содержимое может быть зашифровано.

А.2 Подписание и проверка инфо-набора SOAP сообщений

А.2.1 Подписанный инфо-набор SOAP сообщений

А.2.1.1 Подписанный инфо-набор SOAP сообщений инфо-набора SOAP сообщений из А.1.4, где тело SOAP подписано, представлен в приложении В.

А.2.1.2 Подписанный инфо-набор SOAP сообщений использует раздельную подпись, где подписываемый объект (информационный элемент **soap:Body element**) и подпись (информационный элемент **ds:Signature element**) отделены друг от друга.

А.2.2 Формирование подписанного инфо-набора SOAP сообщений

Примечание — Криптографические алгоритмы, используемые в этом подразделе, приводятся только в качестве примера. Использование SHA-1 исключается некоторыми организациями по стандартизации.

А.2.2.1 Процесс формирования подписи определяется в W3C XML-подпись, 3.1. Описание этого процесса на примере инфо-набора SOAP сообщений будет рассмотрено далее.

А.2.2.2 Подписывающее приложение формирует ссылки на объекты данных, которые должны быть подписаны, собирает эти ссылки и затем формирует подписанную информацию из цифровой подписи.

А.2.2.3 Подписывающее приложение выбирает, что единственным объектом данных, который будет подписан, является информационный элемент **soap:Body element** (и содержимое) инфо-набора SOAP сообщений из А.1.4.

А.2.2.4 Подписывающее приложение идентифицирует объект данных так, чтобы на него можно было сослаться. Объект данных идентифицируется добавлением информационного элемента **wsu:Id attribute** к информационному элементу **soap:Body element**, свойство которого **[normalized value]** является идентификатором «**TheBody**».

А.2.2.5 Подписывающее приложение выбирает, что преобразования для вычисления значения хэш-суммы по получающемуся объекту данных состоят из единственного преобразования, которое определяет «исключающий

канонический алгоритм быстрого инфо-набора без комментариев» (см. 6.4.4 и 7). Это приводит к появлению информационного элемента **ds:Transforms element**, который содержит одиночный дочерний информационный элемент **ds:Transform element** с информационным элементом **Algorithm attribute**, свойством **[normalized value]** которого является «**urn:fastinfoset:c14n:exclusive**».

А.2.2.6 Подписывающее приложение выбирает SHA-1 алгоритм хэширования (см. [FIPS 180-2]) и формирует значение хэш-суммы. Значение хэш-суммы формируется с применением единственного преобразования от объекта данных до последовательности октетов (которые преобразуются, используя SHA 1 алгоритм), следующим образом (см. 6.1.5):

a) входными данными в «исключающем каноническом алгоритме быстрого инфо-набора без комментариев» является набор узлов XPath информационного элемента **soap:Body element** и его дочерние информационные элементы инфо-набора SOAP сообщений из 1.4 (см. 6.1.5, a));

b) канонический XML-документ формируется из набора узлов XPath (см. 6.1.5, a)), используя канонический XML алгоритм, определенный в W3C, исключающий канонический XML (см. 6.4.4);

c) канонический XML-документ парсится, чтобы произвести XML инфо-набор (см. 6.1.5, b));

d) канонический XML инфо-набор сериализируется как канонический документ быстрого инфо-набора (см. 6.1.5, c)) с ограничениями на сериализацию, определенную в 6.3;

e) последовательность октетов, которая вводится в алгоритм хэширования SHA-1, является каноническим документом быстрого инфо-набора.

А.2.2.7 Формирование хэш-суммы приводит к появлению информационного элемента **ds:DigestMethod element** и информационного элемента **ds:DigestValue element**. Содержимое элемента информации **ds:DigestValue element** будет содержать символы с base64 кодированием (см. [IETF RFC 2045]) 160-разрядной хэш-суммы, сгенерированной алгоритмом SHA-1.

А.2.2.8 Подписывающее приложение формирует ссылку на объект данных, который подписывается. Это приводит к появлению информационного элемента **ds:Reference element**, у которого есть информация **URI attribute**, чье свойство **[normalized value]** является URI «**#TheBody**», которое ссылается на объект данных. Информационный элемент **ds:Reference element** содержит, как дочерние элементы информации об элементе, ранее полученные информационные элементы **ds:Transforms**, **ds:DigestMethod** и **ds:DigestValue element**.

А.2.2.9 Затем подписывающее приложение собирает ссылки и формирует подписанную информацию.

А.2.2.10 Подписывающее приложение выбирает «исключающий канонический алгоритм быстрого инфо-набора без комментариев» (см. 6.4.4 и 7) как алгоритм метода канонизации. Это приводит к производству элемента информации **ds:CanonicalizationMethod element** с элементом информации **Algorithm attribute**, свойство **[normalized value]** которого является «**urn:fastinfoset:c14n:exclusive**».

А.2.2.11 Подписывающее приложение выбирает алгоритм подписи RSA-SHA-1 (см. [IETF RFC 3447]) как метод подписи для вычисления значения подписи. Это приводит к появлению элемента информации **ds:SignatureMethod element**.

А.2.2.12 Подписывающее приложение формирует информацию, которая будет подписана, используя метод подписи. Это приводит к появлению элемента информации **ds:SignedInfo element**, который содержит, как дочерние информационные элементы, ранее полученные информационные элементы **ds:CanonicalizationMethod**, **ds:SignatureMethod** и **ds:Reference element**.

А.2.2.13 Подписывающее приложение выбирает ключ, который будет использован для подписи (в данном примере используется маркер доступа X.509, см. [ITU-T X.509]). Это приводит к появлению элементов информации **ds:KeyInfo** и **wsse:BinarySecurityToken element**.

А.2.2.14 Подписывающее приложение канонизирует элемент информации **ds:SignedInfo element**, чтобы произвести последовательность октетов (для ввода в метод подписи), в следующем порядке:

a) входными данными в «исключающем каноническом алгоритме быстрого инфо-набора без комментариев» является набор узлов XPath элемента информации **ds:SignedInfo element** и его дочерние информационные элементы (см. 6.1.5, a));

b) канонический XML-документ производится из набора узлов XPath (см. 6.1.5, a)), используя канонический XML алгоритм, определенный в W3C исключающий канонический XML (см. 6.4.4);

c) канонический XML-документ парсится, чтобы произвести XML инфо-набор (см. 6.1.5, b));

d) канонический XML инфо-набор сериализируется как канонический документ быстрого инфо-набора (см. 6.1.5, c)), с ограничениями на сериализацию, определенными в 6.3;

e) последовательность октетов, что вводится в RSA-SHA-1 алгоритм подписи, является каноническим документом быстрого инфо-набора.

А.2.2.15 Подписывающее приложение формирует значение подписи, применяя метод подписи к октетам, полученным из канонизации подписанной информации. Это приводит к появлению информационного элемента **ds:SignatureValue element**. Содержимое информационного элемента **ds:SignatureValue element** будет содержать символы в base64 кодировании (см. [IETF RFC 2045]) октета значения подписи, сформированного с помощью RSA-SHA1 алгоритма подписи.

А.2.2.16 Подписывающее приложение формирует подпись. Это приводит к появлению информационного элемента **ds:Signature element**, который содержит, как дочерний элемент информационных элементов, ранее произведенные информационные элементы **ds:SignedInfo**, **ds:SignatureValue** и **ds:KeyInfo element**.

A.2.2.17 Наконец, подписывающее приложение формирует SOAP блок заголовка безопасности веб-сервисов. Это приводит к появлению информационного элемента **wsse:Security element**, который содержит, как дочерний элемент информационных элементов, ранее произведенные элементы информации **wsse:BinarySecurityToken** и **ds:Signature element**.

A.2.3 Проверка подписанного инфо-набора SOAP сообщений

A.2.3.1 Процесс проверки подписи описан в W3C XML-подпись, 3.2. Ниже представлено описание этого процесса, применительно к примеру подписанного инфо-набора SOAP сообщений.

A.2.3.2 Основной процесс проверки требует проверки ссылок и проверки подписей.

A.2.3.3 Перед проверкой ссылок, проверяющее приложение должно канонизировать подписанную информацию и работать уже с канонизированной подписанной информацией. Все ссылки в следующих пунктах к информационным элементам внутри подписанной информации, представленной информационным элементом **ds:SignedInfo element** и содержимым, относятся к информационным элементам, представленным в канонической подписанной информации.

Примечание — Важно, чтобы лица и автоматизированные механизмы работали с подписанными данными, а не с оригинальными данными, см. W3C XML-подпись, 8.1.3.

A.2.3.4 Проверяющее приложение получает «исключающий канонической алгоритм быстрого инфо-набора без комментариев» для канонизации подписанной информации, представленной свойством **[normalized value]** информационного элемента **Algorithm attribute** в информационном элементе **ds:CanonicalizationMethod element**.

A.2.3.5 Проверяющее приложение канонизируют подписанную информацию следующим образом:

a) ввод в «исключающий канонический алгоритм быстрого инфо-набора без комментариев» является набором узлов XPath информационного элемента **ds:SignedInfo element** и его дочерних элементов информации (см. 6.1.5, a));

b) канонический XML-документ формируется из набора узлов XPath (см. 6.1.5) с использованием канонического XML алгоритма, указанного в W3C, исключающий канонический XML (см. 6.4.4);

c) канонический XML-документ парсится для формирования XML инфо-набора (см. 6.1.5, b));

d) канонический XML инфо-набор сериализуется как канонический документ быстрого инфо-набора (см. 6.1.5, c)) с ограничениями на сериализацию, указанными в 6.3;

e) канонический документ быстрого инфо-набора парсится для формирования XML инфо-набора, из которого получается подписанная информация, представленная информацией **ds:SignedInfo element**.

A.2.3.6 Далее проверяющее приложение определяет, что для проверки ссылок есть одна ссылка на проверку, представленная информационным элементом **ds:Reference element**.

A.2.3.7 Проверяющее приложение получает объект данных для хэширования путем разыменования URI «**#TheBody**», которое представлено свойством **[normalized value]** информации **URI attribute** в информационном элементе **ds:Reference element**, и выполняет преобразования объекта данных, представленные информационным элементом **ds:Transforms element**.

A.2.3.8 Разыменование достигается путем поиска инфо-набора SOAP сообщений, чтобы идентифицировать элемент информации **element**, который имеет элемент информации **wsu:Id attribute** со свойством **[normalized value]**, равным идентификатору «**TheBody**». В этом случае, набор узлов XPath элемента информации **soap:Body element** и его дочерние элементы информации идентифицируются как объект данных для хэширования.

A.2.3.9 Преобразования состоят из одного преобразования, представленного информационным элементом **ds:Transforms element**, который определяет «исключающий канонический алгоритм быстрого инфо-набора без комментариев» (см. 6.4.4 и 7), представленного информационным элементом **Algorithm attribute** (в элементе информации **ds:Transforms element**), свойство **[normalized value]** которого является «**urn:fastinfoset:c14n:exclusive**».

A.2.3.10 Проверяющее приложение выполняет преобразование объекта данных в последовательность октетов (которые являются вводом в алгоритм хэширования) следующим образом:

a) ввод в «исключающий канонический алгоритм быстрого инфо-набора без комментариев» является набором узлов XPath информационного элемента **soap:Body element** и его дочерних элементов информации инфо-набора SOAP сообщений из A.1.4 (см. 6.1.5, a));

b) канонический XML-документ формируется из набора узлов XPath (см. 6.1.5, a)) с использованием канонического XML алгоритма, указанного в W3C исключающем каноническом XML (см. 6.4.4);

c) канонический XML-документ парсится для получения XML инфо-набора (см. 6.1.5, b));

d) канонический XML инфо-набор сериализуется как канонический документ быстрого инфо-набора (см. 6.1.5, c)), с ограничениями на сериализацию, указанными в 6.3;

e) последовательность октетов, что подается на вход алгоритма хэширования, является каноническим документом быстрого инфо-набора.

A.2.3.11 Проверяющее приложение хэширует последовательность октетов для получения хэш-суммы с использованием SHA-1 алгоритма хэширования, представленного информационным элементом **ds:DigestMethod element**.

A.2.3.12 Проверяющее приложение сравнивает полученную хэш-сумму со значению хэш-суммы в ссылке, представленной содержимым информационного элемента **ds:DigestValue element**. Если есть какие-либо несоответствия, то проверка считается неудавшейся.

A.2.3.13 Затем проверяющее приложение проверяет подпись.

A.2.3.14 Проверяющее приложение получает ключевую информацию, представленную элементами информации **ds:KeyInfo** и **wsse:BinarySecurityToken element** (в данном примере используется маркер доступа X.509, см. [ITU-T X.509]).

A.2.3.15 Проверяющее приложение, для получения значения подписи, подписывает последовательность октетов, являющуюся каноническим документом быстрого инфо-набора, полученным в A.2.3.5 с использованием RSA-SHA-1 алгоритма подписи, представленного свойством **[normalized value]** информационного элемента **Algorithm attribute** в информационном элементе **ds:SignatureMethod element**.

A.2.3.16 Наконец, проверяющее приложение подтверждает, что полученное значение подписи такое же, как значение подписи в подписанной информации, представленной содержимым информационного элемента **ds:SignatureValue element**.

A.3 Шифрование и дешифрование инфо-набора SOAP сообщений

A.3.1 Подписанный и зашифрованный инфо-набор SOAP сообщений

A.3.1.1 Подписанный и зашифрованный инфо-набор SOAP сообщений инфо-набора SOAP сообщений из A.1.4, где SOAP тело было подписано, а затем содержимое SOAP тела было зашифровано, представлен в приложении C.

A.3.2 Формирование подписанного и зашифрованного инфо-набора SOAP сообщений

A.3.2.1 Сначала инфо-набор SOAP сообщений подписывается, как описано в A.2.2, затем формируется зашифрованный инфо-набор SOAP сообщений (см. приложение C) путем добавления и замены информационных элементов подписанного инфо-набора SOAP сообщений (см. приложение B).

A.3.2.2 Процесс шифрования указан в W3C XML шифрование, 4.1. Ниже следует описание этого процесса применительно к подписанному инфо-набору SOAP сообщений.

A.3.2.3 Шифрующее приложение выбирает один или несколько элементов данных для шифрования и для каждого элемента данных: выбирает алгоритм для шифрования элемента данных; шифрует элемент данных; формирует информацию зашифрованного типа, инкапсулирующую результат шифрования элемента данных (зашифрованных данных) и заменяет элемент данных на информацию зашифрованного типа.

A.3.2.4 Шифрующее приложение выбирают единственный элемент данных для шифрования — информационный элемент **n:payment element** (и содержимое) инфо-набора SOAP сообщений из A.1.4.

A.3.2.5 Шифрующее приложение выбирает алгоритм RSA v1.5 Key Transport (см. [IETF RFC 3447]) для шифрования транспортировки ключа и выбирает ключ, что был использован для подписи информации (см. A.2.2.13), как ключ для шифрования элемента данных. Это приводит к появлению элементов информации **xenc:EncryptionMethod**, **ds:KeyInfo** и **xenc:CipherData element**, связанных с зашифрованной ключевой информацией (см. информационный элемент **xenc:EncryptionMethod element**).

A.3.2.6 Шифрующее приложение выбирает тройной DES алгоритм (см. [ANSI X9.52]) для шифрования информационного элемента **n:payment element** (и содержимого). Это приводит к появлению информационного элемента **xenc:EncryptionMethod element**, связанного с информацией зашифрованного типа (см. информационный элемент **xenc:EncryptedData element**).

A.3.2.7 Шифрующее приложение шифрует информационный элемент **n:payment element** (и содержимое) следующим образом:

a) информационный элемент **n:payment element** должен быть преобразован в полный XML инфо-набор (см. 8.1.3, a));

b) этот XML инфо-набор должен быть сериализован в документ быстрого инфо-набора (см. 8.1.3, b));

c) октеты этого документа быстрого инфо-набора шифруются для получения зашифрованной последовательности октетов (см. 8.1.3, c)).

A.3.2.8 Шифрующее приложение формирует информацию зашифрованного типа. Это приводит к появлению информационного элемента **xenc:EncryptedData element**, который имеет:

a) элемент информации **wsu:Id attribute** со свойством **[normalized value]** «**EncryptedBodyContents**», то есть идентификатор зашифрованных данных;

b) элемент информации **Type attribute** со свойством **[normalized value]** «**urn:fastinfoset:element**», который идентифицирует элемент зашифрованных данных, как документ быстрого инфо-набора, полученный из элемента информации **element** (см. 8.1.4);

c) дочерний элемент информации **xenc:EncryptedKey element**, сформированный в A.3.2.6;

d) дочерний элемент информации **xenc:CipherData element**, имеющий дочерний элемент информации **xenc:CipherValue element**, содержащий символы зашифрованной последовательности октетов в base64 кодировании (см. [IETF RFC 2045]), сформированной в A.3.2.7, c).

A.3.2.9 Шифрующее приложение формирует зашифрованную ключевую информацию. Это приводит к появлению информационного элемента **xenc:EncryptedData element**, который имеет:

a) дочерние элементы информации **xenc:EncryptionMethod**, **ds:KeyInfo** и **xenc:CipherData element**, сформированные в A.3.2.5;

b) дочерний элемент информации **xenc:ReferenceList element**, который имеет дочерний элемент информации **wsse:Reference element** с элементом информации **URI attribute**, чье свойство **[normalized value]** является URI «**#EncryptedBodyContents**», которое ссылается на информационный элемент **xenc:EncryptedKey element**.

А.3.2.10 Наконец, шифрующее приложение заменяет элемент информации **n:payment element** (и содержимое) на полученный элемент информации **xenc:EncryptedData element**, как указано в 8.1.5, и элемент информации **xenc:EncryptedKey element** добавляется в качестве дочернего элемента информации **wsse:Security element**, и этот дочерний элемент появляется до элемента информации **ds:Signature element**.

Примечание — Последовательность **xenc:EncryptedData** и **ds:Signature** соответствует последовательности, в которой выполняются шифрование и подписание.

А.3.3 Проверка и дешифровка подписанного и зашифрованного инфо-набора SOAP сообщений

А.3.3.1 Процесс дешифровки указан в W3C XML шифрование, 4.2. Ниже представлено описание этого процесса применительно к зашифрованному и подписанному инфо-набору SOAP сообщений.

А.3.3.2 Сначала дешифрующее приложение обрабатывает зашифрованную ключевую информацию, представленную элементом информации **xenc:EncryptedKey element**, чтобы получить ключ для дешифровки и данные, которые были зашифрованы с использованием этого ключа.

А.3.3.3 Дешифрующее приложение использует алгоритм RSA v1.5 Key Transport (см. [IETF RFC 3447]) для зашифрованной ключевой транспортировки и использует тот же ключ для дешифровки данных, что и для проверки информации о подписи (см. А.2.3.14).

А.3.3.4 Дешифрующее приложение определяет, что данные, которые должны быть дешифрованы, являются элементом информации **xenc:EncryptedData element** (на это ссылается зашифрованная ключевая информация).

А.3.3.5 Дешифрующее приложение расшифровывает последовательность октетов, представленную в виде декодирования символов base64 (см. [IETF RFC 2045]) элемента информации **xenc:CipherValue element**, для получения открытой последовательности октетов.

А.3.3.6 Типом открытой последовательности октетов является документ быстрого инфо-набора, полученный из информационного элемента **element**, представленного элементом информации **Type attribute** со свойством **[normalized value]** «**urn:fastinfoset:element**» (см. 8.3, a)).

А.3.3.7 Дешифрующее приложение получает элемент информации **element** из документа быстрого инфо-набора и заменяет элемент информации **xenc:EncryptedData element** на этот информационный элемент **element** (см. 8.3, b) и c)).

А.3.3.8 Наконец, подписанный и дешифрованный инфо-набор SOAP сообщений проверяется, как описано в А.2.3.

Приложение В
(справочное)

Подписанный инфо-набор SOAP сообщений

```
<soap:Envelope xmlns:soap=«...» xmlns:wsse=«...» xmlns:wsu=«...» xmlns:ds=«...»>
    <soap:Header>
        <wsse:Security>
            <wsse:BinarySecurityToken wsu:Id=«X509Token»
        ValueType=«...#X509v3»>
        ...
            </wsse:BinarySecurityToken>
            <ds:Signature>
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod
                            Algorithm=«urn:fastinfoset:c14n:exclusive»>
                        <c14n:InclusiveNamespaces PrefixList='wsse soap' xmlns:c14n=«...»/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod
                            Algorithm=«gost.e-ecolog.ru
                    <ds:Reference URI=«#TheBody»>
                        <ds:Transforms>
                            <ds:Transform
                                Algorithm=«urn:fastinfoset:c14n:exclusive»>
                            <c14n:InclusiveNamespaces PrefixList='' xmlns:c14n=«...»/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod
                            Algorithm=«gost.e-ecolog.ru                    >
                        <ds:DigestValue>...</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>...</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference>
                        <wsse:Reference URI=«#X509Token»/>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
        </wsse:Security>
    </soap:Header>
    <soap:Body wsu:Id=«TheBody»>
        <n:payment xmlns:n=«...»>1000</n:payment>
    </soap:Body>
</soap:Envelope>
```

Приложение С
(справочное)

Подписанный и зашифрованный инфо-набор SOAP сообщений

```
<soap:Envelope xmlns:soap=«...» xmlns:wsse=«...» xmlns:wsu=«...» xmlns:ds=«...» xmlns:xenc=«...»>
  <soap:Header>
    <wsse:Security>
      <wsse:BinarySecurityToken wsu:Id=«X509Token»
        ValueType=«...#X509v3»>
        ...
      </wsse:BinarySecurityToken>
      <xenc:EncryptedKey>
        <xenc:EncryptionMethod
            Algorithm=«gost.e-ecolog.ru                                    >
        <ds:KeyInfo>
          <wsse:SecurityTokenReference>
            <wsse:Reference URI=«#X509Token»/>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>...</xenc:CipherValue>
        </xenc:CipherData>
        <xenc:ReferenceList>
          <xenc:DataReference URI=«#EncryptedBodyContents»/>
        </xenc:ReferenceList>
      </xenc:EncryptedKey>
      <ds:Signature>
        <ds:SignedInfo>
          <ds:CanonicalizationMethod
              Algorithm=«urn:fastinfoset:c14n:exclusive»>
            <c14n:InclusiveNamespaces PrefixList='wsse soap'/ xmlns:c14n=«...»>
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod
              Algorithm=«gost.e-ecolog.ru                                  >
          <ds:Reference URI=«#TheBody»>
            <ds:Transforms>
              <ds:Transform
                Algorithm=«urn:fastinfoset:c14n:exclusive»>
              <c14n:InclusiveNamespaces PrefixList='' xmlns:c14n=«...»/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod
              Algorithm=«gost.e-ecolog.ru                                  >
            <ds:DigestValue>...</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
          <wsse:SecurityTokenReference>
            <wsse:Reference URI=«#X509Token»/>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </soap:Header>
  <soap:Body wsu:Id=«TheBody»>
    <xenc:EncryptedData wsu:Id=«EncryptedBodyContents»
        Type=«urn:fastinfoset:element»>
      <xenc:EncryptionMethod
          Algorithm=«gost.e-ecolog.ru                                    >
```

```
            <xenc:CipherData>
                <xenc:CipherValue>...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </soap:Body>
</soap:Envelope>
```

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам

Таблица ДА.1

Обозначение международного стандарта	Степень соответствия	Обозначение и наименование межгосударственного стандарта
ISO/IEC 24824-1:2007	IDT	ГОСТ ISO/IEC 24824-1—2013 «Информационные технологии. Общие правила применения ASN.1. Быстрые команды. Часть 1»
ISO/IEC 10646:2003	—	*

* Соответствующий межгосударственный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

[ITU-T X.509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks (Рекомендации X.509 (2005) МСЭ-Т | ISO/IEC 9594-8:2005 Информационные технологии. Взаимосвязь открытых систем. Директория. Структура сертификата на общий ключ и атрибуты)

[ANSI X9.52] ANSI X9.52: Triple Data Encryption Algorithm Modes of Operation, 1998. (Режимы работы алгоритма тройного шифрования данных, 1998)

[FIPS 180-2] FIPS PUB 180-2, Secure Hash Standard, U.S. Department of Commerce/National Institute of Standards and Technology, 2002 (Стандарт безопасного хэширования, Департамент коммерции/Национальный Институт стандартов и технологий (США), 2002)

[IETF RFC 2045] IETF RFC 2045 (1996), Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies (Многоцелевые расширения интернет-почты (MIME). Часть 1. Формат текста интернет-сообщения)

[IETF RFC 3447] IETF RFC 3447 (2003), Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 (Криптографические стандарты открытого ключа #1. RSA Криптографические спецификации версии 2.1)

[WSS] OASIS Web Services Security (WSS): SOAP Message Security 1.1 (WS-Security 2004) (Безопасность веб-сервисов. Безопасность SOAP сообщений 1.1)

[WS-I] WS-I Basic Security Profile 1.0 (Организация интероперабельности веб-сервисов (WS-I). Базовый профиль безопасности 1.0)

УДК 681.3:691.39:006.354 МКС 35.100.60 IDT

Ключевые слова: обработка данных, информационный обмен, сетевое взаимодействие, взаимосвязь открытых систем, ASN.1, шифрование, безопасность, быстрый инфо-набор

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 02.10.2018. Подписано в печать 11.10.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31. к. 2.

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

gost.e-ecolog.ru