ЕВРАЗИЙСКИЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(EACC)
EURO-ASIAN COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(EASC)

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

Зарегистрирован
№ 8805
19 ноября 2013 г.

Минск
Евразийский совет по стандартизации, метрологии и сертификации

Предисловие

Евразийский совет по стандартизации, метрологии и сертификации (ЕАСС) представляет собой региональное объединение национальных органов по стандартизации государств, входящих в Содружество Независимых Государств. В дальнейшем возможно вступление в ЕАСС национальных органов по стандартизации других государств.

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0—92 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2009 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, применения, обновления и отмены».

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием Государственный научно-исследовательский и конструкторско-технологический институт «ТЕСТ» (ФГУП ГосНИИ «ТЕСТ»)

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии Российской Федерации

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

За принятие стандарта 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
Кыргызстан	KG	Кыргызстандарт
Российская Федерация	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт

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

Степень соответствия – идентичная (IDT).

Сведения о соответствии межгосударственных стандартов ссылочным международным стандартам приведены в дополнительном приложении ДА.

Официальные экземпляры международного стандарта, на основе которого подготовлен настоящий межгосударственный стандарт, и международных стандартов, на которые даны ссылки, имеются в национальных органах по стандартизации.

Степень соответствия - идентичная (IDT)

5 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных (государственных) стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных (государственных) органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация также будет опубликована в сети Интернет на сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

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 —

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 ссылок применяют последнее издание ссылочного документа (включая все его изменения).

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

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))

[1)] Отменен. Действует ISO/IEC 10646:2012.

- 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), http://www.w3.org/TR/2001/REC-xml-c14n-20010315 (Канонический 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) http://www.w3.org/TR/2001/REC-xml-c14n-20010315)

- 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), http://www.w3.org/TR/2002/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) http://www.w3.org/TR/2002/REC-xmlenc-core-20021210)

- 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), http://www.w3.org/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), http://www.w3.org/TR/2004/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) http://www.w3.org/TR/2004/REC-xml-infoset-20040204)

- 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), http://www.w3.org/TR/2002/REC-xmldsig-core-20020212 (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) http://www.w3.org/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), http://www.w3.org/TR/1999/REC-xpath-19991116 (XPath: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) http://www.w3.org/TR/1999/REC-xpath-19991116)

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).