ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 9735-9— 2016

ЭЛЕКТРОННЫЙ ОБМЕН ДАННЫМИ В УПРАВЛЕНИИ, ТОРГОВЛЕ И НА ТРАНСПОРТЕ (EDIFACT)

Синтаксические правила для прикладного уровня (версия 4, редакция 1)

Часть 9

Сообщение системы управления ключами защиты и сертификатами (тип сообщения — KEYMAN)

(ISO 9735-9:2002, IDT)

Издание официальное

Москва
Стандартинформ
2016

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Институт безопасности труда» (АНО «ИБТ») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 55 «Терминология, элементы данных и документация в бизнес-процессах и электронной торговле»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2016 г. № 1901-ст

4 Настоящий стандарт идентичен стандарту ИСО 9735-9:2002 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 9. Сообщение системы управления ключами защиты и сертификатами (тип сообщения — KEYMAN)» [ISO 9735-9:2002 «Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 9: Security key and certificate management message (message type — KEYMAN)», IDT]

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в 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 (www.gost.ru)

Содержание

1 Область применения ... 1
2 Нормативные ссылки ... 1
3 Термины и определения ... 2
4 Соответствие настоящему стандарту ... 2
5 Правила использования ключа защиты и сообщения для управления сертификатами ... 2
5.1 Функциональное назначение ... 2
5.2 Сфера применения ... 2
5.3 Принципы использования управляющего сообщения ... 2
5.4 Определение сообщения ... 3
Приложение А (справочное) Функции сообщения KEYMAN ... 6
Приложение В (справочное) Методы защиты, применимые к сообщениям типа KEYMAN ... 9
Приложение С (справочное) Использование групп сегментов в сообщениях типа KEYMAN ... 10
Приложение D (справочное) Модель для управления ключами ... 12
Приложение Е (справочное) Примеры управления ключами и сертификатами ... 14
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам ... 20
Библиография ... 21

Введение

Настоящий стандарт включает в себя правила прикладного уровня для структурирования данных в рамках обмена электронными сообщениями в открытой среде с учетом требований пакетной обработки. Эти правила утверждены Европейской экономической комиссией ООН (UN/ECE) в качестве синтаксических правил организации электронного обмена данными (Electronic Data Interchange, EDI) в управлении, торговле и на транспорте (EDIFACT) и являются частью Каталога ООН по информационному обмену в сфере торговли (UNTDID), который содержит также рекомендации по разработке сообщений пакетного и интерактивного обмена.

Спецификации и протоколы обмена сообщениями в рамках настоящего стандарта не рассматриваются.

Настоящий стандарт — это новая часть, добавленная в ИСО 9735. Она создает дополнительную возможность управления секретными ключами и сертификатами.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЭЛЕКТРОННЫЙ ОБМЕН ДАННЫМИ В УПРАВЛЕНИИ, ТОРГОВЛЕ И НА ТРАНСПОРТЕ (EDIFACT)

Синтаксические правила для прикладного уровня (версия 4, редакция 1)

Часть 9

Сообщение системы управления ключами защиты и сертификатами (тип сообщения — KEYMAN)

Electronic data interchange for administration, commerce and transport (EDIFACT). Application level syntax rules (Syntax version number 4, Syntax release number 1). Part 9. Security key and certificate management message (message type — KEYMAN)

Дата введения — 2017—09—01

1 Область применения

Настоящим стандартом, который касается обеспечения безопасности пакетного обмена EDIFACT, определяется системное сообщение типа KEYMAN для управления ключами защиты и сертификатами.

2 Нормативные ссылки

Приведенные ниже нормативные документы содержат положения, на которые даются ссылки в настоящем тексте и которые, следовательно, становятся положениями настоящего стандарта. Для датированных ссылок применимо только указываемое издание: никакие его последующие изменения или редакции не применимы. Однако участникам договоров, в которых использован настоящий стандарт, рекомендуется изучить возможность применения самых последних изданий ссылочных документов, указанных ниже. Применительно к недатированным ссылочным документам (с плавающими ссылками) действующим остается самое последнее издание нормативного документа. Членами ИСО и МЭК ведутся реестры действующих международных стандартов.

ISO 9735-1:2002, Electronic data interchange for administration, commerce and transport (EDIFACT). Application level syntax rules (Syntax version number 4, Syntax release number 1). Part 1. Syntax rules common to all parts [Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 1. Синтаксические правила, общие для всех частей]

ISO 9735-2:2002, Electronic data interchange for administration, commerce and transport (EDIFACT). Application level syntax rules (Syntax version number 4, Syntax release number 1). Part 2. Syntax rules specific to batch EDI [Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 2. Специфика синтаксических правил для пакетного EDI]

ISO 9735-5:2002, Electronic data interchange for administration, commerce and transport (EDIFACT). Application level syntax rules (Syntax version number 4, Syntax release number 1). Part 5. Security rules for batch EDI (authenticity, integrity and non-repudiation of origin) [Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 5. Правила безопасности для пакетного EDI (подлинность, целостность и невозможность отказа отправителя от авторства сообщения]

ISO 9735-10:2002, Electronic data interchange for administration, commerce and transport (EDIFACT). Application level syntax rules (Syntax version number 4, Syntax release number 2). Part 10: Syntax service directories [Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 10. Каталоги синтаксической службы]

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины и определения, приведенные в ИСО 9735-1.

4 Соответствие настоящему стандарту

Для соответствия обмена требованиям настоящего стандарта в его обязательном элементе 0002 (номер версии синтаксических правил) следует использовать номер версии «4», а в условно-обязательном элементе данных 0076 (номер редакции синтаксических правил) — номер редакции «01», причем каждый из этих номеров появляется в сегменте UNB (заголовок обмена); однако в обменах, где продолжает использоваться синтаксис, определенный в более ранних версиях, для различения соответствующих синтаксических правил друг от друга и от правил, определенных в настоящем стандарте, должны использовать следующие номера версий:

- ИСО 9735:1988 — номер версии синтаксических правил: 1,
- ИСО 9735:1988 (перепечатанный с изменениями в 1990 г.) — номер версии синтаксических правил: 2;
- ИСО 9735:1988 и его Изменение 1:1992 — номер версии синтаксических правил: 3;
- ИСО 9735:1998 — номер версии синтаксических правил: 4.

Соответствие стандарту означает, что соблюдены все его требования, включая все возможные опции. Если поддерживаются не все опции, то в любом заявлении о соответствии должно содержаться положение, идентифицирующее опции, по которым декларируется соответствие.

Данные, используемые в обмене, признаются соответствующими, если их структура и представление отвечают синтаксическим правилам, определенным в настоящем стандарте.

Устройства, поддерживающие настоящий стандарт, признаются соответствующими ему, если эти устройства способны формировать и/или интерпретировать данные, структурированные и представленные в соответствии с требованиями настоящего стандарта.

Соответствие требованиям настоящего стандарта предполагает обязательное соответствие частям 1, 2, 5 и 10 ИСО 9735.

Положения смежных стандартов, на которые делается ссылка в настоящем стандарте, являются составными элементами критериев соответствия.

5 Правила использования ключа защиты и сообщения для управления сертификатами

5.1 Функциональное назначение

Сообщение типа KEYMAN обеспечивает возможность управления ключом защиты и сертификатом. Ключ защиты может быть секретным, использующим симметричные алгоритмы, или открытым либо закрытым, основанным на использовании асимметричных алгоритмов.

5.2 Сфера применения

Сообщение для управления ключами защиты и сертификатами (KEYMAN) может быть использовано в рамках как национальной, так и международной торговли. Структура этого управляющего сообщения определена сложившейся практикой административных, торговых и транспортных операций и не зависит от типа хозяйственной деятельности или отрасли промышленности.

5.3 Принципы использования управляющего сообщения

Управляющее сообщение может быть использовано для запроса или предоставления ключей защиты, сертификатов или маршрутов сертификации (в том числе для запрашивания различных операций управления ключами и сертификатами — например, операций обновления, замены или аннулирования сертификатов, а также предоставления дополнительной информации — к примеру, о статусе сертификата); это сообщение может быть использовано и для представления перечней сертификатов (например, с целью указания тех из них, которые признаны недействительными). Сообщение типа KEYMAN может быть защищено посредством использования групп сегментов заголовка и концевика защиты. Структурные схемы таких групп сегментов определены в ИСО 9735-5.

Сообщение для управления ключами защиты и сертификатами может быть использовано для следующих целей:

a) запрашивания операций, связанных с обработкой ключей и сертификатов;

b) предоставления ключей, сертификатов и относящейся к ним информации.

5.4 Определение сообщения

5.4.1 Детализация сегмента данных

0010 Сегмент UNH — заголовок сообщения

Служебный сегмент в начале сообщения, однозначно идентифицирующий его.

Код типа сообщения для управления закрытыми ключами и сертификатами — KEYMAN.

Для того чтобы соответствовать настоящему стандарту, сообщения для управления закрытыми ключами и сертификатами должны содержать следующие данные в сегменте UNH составного сообщения S009:

элемент данных	0065	KEYMAN
	0052	4
	0054	1
	0051	UN

0020 Группа сегментов 1 — USE-USX- SG2

Группа сегментов, которая содержит всю информацию, необходимую для пересылки или выполнения запросов ключа, сертификата, маршрута сертификации и уведомлений.

0030 Сегмент USE — связь по сообщениям защиты

Сегмент, идентифицирующий связь с предыдущим сообщением: например, с запросным сообщением типа KEYMAN.

0040 Сегмент USX — ссылка, указывающая службу защиты

Сегмент, идентифицирующий ссылку на предшествующее сообщение: например, на запрос. Составной элемент данных «дата и время защиты» может содержать исходную дату и время генерации запрашиваемого сообщения.

0050 Группа сегментов 2 — USF-USA-SG3

Группа сегментов, содержащая единственный ключ и единственный сертификат или группу сертификатов, образующую маршрут сертификации.

0060 Сегмент USF — функция управления ключами

Сегмент, идентифицирующий функцию переключаемой им группы: запрос или представление. В случае использования этого сегмента для показа элементов маршрутов сертификации порядковый номер должен указывать положение очередного сертификата в маршруте. Этот сегмент может использоваться и сам по себе для извлечения списковой информации, даже при отсутствии сертификата. В рамках одного и того же сообщения могут существовать несколько различных сегментов USF, когда производится обработка двух и более ключей и сертификатов. Однако при этом недопустимо одновременное присутствие функции запроса и функции доставки. В сегменте USF может быть также определена функция фильтра, применяемая к двоичным полям сегмента USA, который следует непосредственно за сегментом USF.

0070 Сегмент USA — алгоритм защиты

Сегмент, идентифицирующий алгоритм шифрования и механизм его реализации и содержащий необходимые для этого технические параметры (определенные в ИСО 9735-5). Этот сегмент должен фигурировать в запросах на генерирование, прекращение действия или отправку симметричных ключей. Он может также использоваться для запроса пары асимметричных ключей.

0080 Группа сегментов 3 — USC-USA-USR

Группа сегментов, содержащая все данные, которые необходимы для контроля подлинности методов защиты сообщений/пакетов в случае применения асимметричных алгоритмов (как это определено в ИСО 9735-5). Данная группа должна использоваться при запросе или отправке ключей и сертификатов.

Для однозначной идентификации пары используемых асимметричных ключей необходимо присутствие в сегменте USC либо полной группы сегментов сертификата (включая сегмент USR), либо только элементов данных. Присутствия полного сертификата можно избежать,

если обмен сертификатами между двумя сторонами уже состоялся или если сертификат может быть извлечен из базы данных.

В случаях принятия решения использовать сертификат, не относящийся к типу EDIFACT (например, X.509), синтаксис и версия такого сертификата подлежат идентификации в элементе данных 0545 сегмента USC. Подобные сертификаты могут пересылаться в составе пакета EDIFACT.

0090 Сегмент сертификата USC

Сегмент, который содержит мандат владельца сертификата и идентифицирует сертификационный орган (центр сертификации), выпустивший данный сертификат (как определено в ИСО 9735-5). Этот сегмент подлежит использованию в запросах, касающихся сертификатов (например, для их обновления) или асимметричных ключей, как в случае прекращения действия или при пересылке сертификата.

0100 Сегмент USA — алгоритм защиты

Сегмент, идентифицирующий алгоритм обеспечения безопасности и его техническую реализацию и содержащий необходимые для этого технические параметры защиты (определенные в ИСО 9735-5). Данный сегмент должен использоваться при запросе сертификата (например, для регистрации мандата владельца) и в случаях представления сертификата.

0110 Сегмент USR — результат защиты

Сегмент, содержащий результат применения функций защиты сертификата сертификационным органом (как определено в ИСО 9735-5). Этот сегмент должен использоваться для проверки подлинности сертификата или в случаях представления сертификата.

0120 Группа сегментов 4 — USL-SG5

Группа сегментов, содержащая списки сертификатов или открытых ключей. Эта группа должна использоваться для группирования сертификатов с одинаковым статусом — то есть тех, которые все еще сохраняют достоверность, и тех, которые по той или иной причине могут быть недостоверными.

0130 Сегмент USL — статус списков защиты

Сегмент, идентифицирующий достоверные, недействительные, неизвестные или аннулированные элементы. Такими элементами могут оказаться сертификаты (например, достоверные, недействительные) или открытые ключи (например, действующие или аннулированные). Если предоставление сертификатов или открытых ключей предусматривает использование двух и более списков, то в рамках одного сообщения могут присутствовать несколько разных сегментов USL. Различные списки могут определяться перечнем параметров.

0140 Группа сегментов 5 — USC-USA-USR

Группа сегментов, содержащая данные, которые необходимы для контроля подлинности методов защиты сообщений/пакетов в случае применения асимметричных алгоритмов (как определено в ИСО 9735-5). Эта группа подлежит использованию в тех случаях, когда предоставляются списки ключей или сертификатов с одинаковым статусом.

0150 Сегмент сертификата USC

Сегмент, который содержит мандат владельца сертификата и идентифицирует сертификационный орган, выдавший этот сертификат (как определено в ИСО 9735-5). Этот сегмент должен либо использоваться применительно к полному сертификату — и тогда необходимо присутствие дополнительных сегментов USA и USR, либо он может указывать ссылочный номер сертификата или имя ключа; в последнем случае сообщение должно быть подписано с использованием групп сегментов заголовка и концевика защиты.

0160 Сегмент USA — алгоритм защиты

Сегмент, идентифицирующий алгоритм обеспечения безопасности и его техническую реализацию и содержащий необходимые для этого технические параметры защиты (как определено в ИСО 9735-5). Этот сегмент подлежит использованию в том случае, если требуется указание алгоритмов защиты сертификата.

0170 Сегмент USR — результат защиты

Сегмент, содержащий результат применения функций защиты сертификата сертификационным органом (как определено в ИСО 9735-5). Этот сегмент подлежит использованию в том случае, когда требуется подпись в сертификате.

0180 Сегмент UNT — концевик сообщения

Завершающий сообщение служебный сегмент, указывающий общее число сегментов и контрольную сумму сообщения.

5.4.2 Указатель сегментов данных

Тег	Имя
UNH	Заголовок сообщения
UNT	Концевик сообщения
USA	Алгоритм защиты
USC	Сертификат
USE	Связь по сообщениям защиты
USF	Функция управления ключами
USL	Статус списка защиты
USR	Результат защиты
USX	Ссылочные номера защиты

Таблица 1 — Перечень сегментов

ПОЗ.	ТЕГ	Имя	S	R
0010	UNH	Заголовок сообщения	M	1
0020	-----	Группа сегментов 1 ----------		
------ C	999	--------+		
0030	USE	Связь по сообщениям защиты		
M 1				
0040	USX	Ссылочные номера защиты	C	1
	|		
0050	-----	Группа сегментов 2 ----------		
------ M	9	----+ |		
0060	USF	Функция управления ключами		
M 1				
0070	USA	Алгоритм защиты	C	1
| |				
0080	-----	Группа сегментов 3 ----------		
------ C	1	-+ | |		
0090	USC	Сертификат	M	1 |
|				
0100	USA	Алгоритм защиты	C	3 |
| |				
0110	USR	Результат защиты	C	1
--------+				
0120	-----	Группа сегментов 4 ----------		
------ C	99	--------+		
0130	USL	Статус списков защиты	M	1
	|		
0140	-----	Группа сегментов 5 ----------		
------ M	9999	----+ |		
0150	USC	Сертификат	M	1 |
|				
0160	USA	Алгоритм защиты	C	3
| |				
0170	USR	Результат защиты	C	1
--------+				
0180	UNT	Концевик сообщения	M	1

Приложение А
(справочное)

Функции сообщения KEYMAN

А.1 Введение

В данном приложении описаны различные функции, обеспечиваемые сообщением KEYMAN. При этом под мандатом понимается только информация, относящаяся к одной конкретной стороне взаимодействия, а не открытый ключ и не отметки времени. Поэтому сертификат считается состоящим из следующих компонентов:

- мандат;
- открытый ключ;
- отметки времени;
- цифровая подпись.

Определенные функции рассматривают как реализуемые вне процедур информационного обмена, то есть с использованием внешнего канала взаимодействия. В частности, это относится к секретному ключу пользователя, если такой ключ он формирует самостоятельно.

А.2 Регистрационные функции управления ключами

А.2.1 Предъявление к регистрации

Цель этой функции состоит в представлении для регистрации полного или частичного контента сертификата.

Хотя обычно эту функцию следует реализовывать внешним по отношению к каналу связи способом (например, путем доставки нужной информации или простановки заверяющей подписи вручную), для регистрационного органа (которому один или несколько пользователей доверили процедуру их регистрации) более продуктивным может стать достоверность. По этой причине само сообщение не нуждается в защите, но контроль его целостности с применением определенного в ИСО 9735-5 стандартного метода заголовка и концевика может оказаться полезным в случае дальнейшей защиты информации во внешних каналах.

А.2.2 Запрос пары асимметричных ключей

Цель этой процедуры заключается в том, чтобы направить доверенной стороне запрос на генерирование пары асимметричных ключей. Последующее транспортирование секретного ключа должно быть осуществлено с использованием внешнего канала взаимодействия.

А.3 Сертификационные функции управления ключами

А.3.1 Запрос сертификата

Целью данной процедуры является запрос сертификации мандата и открытого ключа.

Это может быть просто запрос, осуществляемый до передачи информации по внешнему каналу взаимодействия, и тогда в ответ на указанный запрос информация пересылаться не будет. Так как зарегистрированных ключей еще может не быть, сообщение при этом считается не защищенным. Однако в случае передачи нужной информации в рамках сообщения она потребует раздельной аутентификации. Если же зарегистрированный ключ уже существует, то он может быть использован для обеспечения невозможности отказа от авторства сообщения, передаваемого с применением нового ключа и сертификата.

Тем не менее, если сообщение использовано источником для пересылки своего открытого ключа, у него должна существовать возможность подписи сообщения соответствующим секретным ключом даже в том случае, когда еще нет метки для открытого ключа. Такая ситуация называется самосертификация; она требует использования групп сегментов заголовка и концевика системы защиты. Для указания на самосертифицированный ключ определенная в ИСО 9735-5 группа сегментов заголовка защиты должна содержать сертификат, созданный пользователем для своего закрытого ключа. Хотя самосертифицированный открытый ключ не является для принимающей стороны доказательством подлинности его пользователя, для сертификационного органа он свидетельствует о том, что владелец открытого ключа располагает надлежащим закрытым ключом.

А.3.2 Запрос на обновление сертификата

Цель запроса — продление (или обновление) имеющегося сертификата.

Это делается для увеличения периода использования текущего действующего ключа, срок сертификата которого в скором времени истекает. Запрос на обновление должен быть подписан закрытым ключом с сертификатом, подлежащим обновлению, с использованием групп сегментов заголовка и концевика защиты в рамках обмена EDIFACT, описанного в ИСО 9735-5.

А.3.3 Запрос на замену сертификата

Цель запроса состоит в замене имеющегося сертификата на новый, с другим открытым ключом и при необходимости — с дополнительными информационными возможностями. Запрос должен быть подписан в соответствии с действующей политикой управления ключами и с использованием определенных в ИСО 9735-5 групп сегментов заголовка и концевика защиты в рамках обмена EDIFACT.

Замена сертификата отличается от его обновления тем, что старый сертификат, как правило, аннулируется, а не продлевается по истечении срока действия. Новый сертификат всегда имеет новый регистрационный номер, тогда как у продленного сертификата этот номер не меняется.

А.3.4 Запрос сертификата или маршрута сертификации

Цель запроса — отправка существующего сертификата (действующего либо аннулируемого) или продлеваемого сертификата. К этой же процедуре относится случай, когда ответное сообщение содержит маршрут сертификации, а не только сам сертификат, поскольку запрашивающая сторона обычно не располагает такими детализированными данными.

Если регистрационный номер сертификата задан, то нет необходимости в использовании защиты, поскольку сертификаты носят открытый характер.

А.3.5 Предоставление сертификата

Цель этой процедуры состоит в отправке существующего или продленного сертификата по предварительному запросу или без такового.

Передачу открытого ключа от сертификационного органа (CA) следует при нормальных условиях осуществлять по внешним каналам взаимодействия. Однако для обеспечения большего удобства замены ключей может потребоваться формирование сообщения, защищенного ради сохранения целостности группами сегментов заголовка и концевика системы безопасности, с раздельной аутентификацией. Наличие подобной защиты может стать поводом для игнорирования пользователями необходимости контроля параметров, полученных по внешним каналам взаимодействия, что неминуемо приведет к существенному снижению уровня безопасности. В данном случае могут потребоваться службы защиты наподобие обеспечения невозможности отказа отправителя от авторства сообщения.

А.3.6 Запрос статуса сертификата

Цель — получение сведений о текущем статусе конкретного сертификата.

А.3.7 Уведомление о статусе сертификата

Цель — предоставление информации о статусе конкретного сертификата запрашивающей стороне.

Возможные состояния: «неизвестен», «действителен», «аннулирован». Это уведомление может пересылаться без предварительного запроса и обычно должно снабжаться защитой, обеспечивающей невозможность отказа источника от авторства сообщения.

А.3.8 Запрос на проверку подлинности сертификата

Этот запрос должен пересылаться в сертификационный орган для осуществления контроля подлинности существующего сертификата.

Запрос касается сертификатов, относящихся к другим сферам безопасности (то есть выпускаемых иными CA), которые могут быть недоступны для контроля пользователем.

А.3.9 Уведомление о проверке подлинности сертификата

Это ответ на запрос проверки подлинности сертификата. Рекомендуется защищать данное уведомление посредством обеспечения невозможности отказа источника от авторства сообщения.

А.4 Ликвидационные функции управления ключами

А.4.1 Запрос на аннулирование

Цель состоит в запросе аннулирования (изменения статуса «действительный» на «недействительный») сертификата запрашивающей стороны: например, из-за компрометации закрытого ключа; смены CA пользователя; замены исходного сертификата; прекращения использования сертификата (например, вследствие увольнения пользователя из компании) или по иной причине. При этом, по возможности, следует использовать процедуру аутентификации. Рассматриваемая функция может требовать отдельного канала связи и охватывать случаи потери пользователем своего закрытого ключа.

А.4.2 Подтверждение аннулирования

Цель этого сообщения — подтверждение факта аннулирования запрошенного сертификата.

Рекомендуется защищать данное уведомление посредством обеспечения невозможности отказа источника от авторства сообщения.

А.4.3 Запрос списка аннулирования

Цель — получение полного или частичного списка аннулированных сертификатов.

А.4.4 Предоставление списка аннулирования

Цель этого сообщения состоит в информировании взаимодействующих сторон обо всех (или определенных) сертификатах, аннулированных на данный момент в сфере ответственности данного органа сертификации.

Это сообщение похоже на групповое статусное уведомление, но распространяется только на аннулированные сертификаты. Хотя для этого можно было бы иметь отдельный тип черного списка, все же удобнее работать с единственным списком, в котором определен текущий статус сертификатов. Данное уведомление должно быть защищено посредством обеспечения невозможности отказа источника от авторства сообщения.

А.5 Запрос предупреждения

Цель этого запроса состоит в активизации тревожного сигнала относительно сертификата одной из сторон взаимодействия.

В данном случае сертификат не аннулируется (запрос в адрес CA отсутствует), но другие пользователи предупреждаются о том, что подлинность конкретного сертификата вызывает сомнения. Такой способ уведомления можно использовать в тех ситуациях, когда у пользователя нет подходящих средств аутентификации для защиты ликвидационного запроса: например, он не располагает для этого вторым, действительным, ключом и сертификатом.

А.6 Предоставление маршрута сертификации

Целью данного сообщения является предоставление существующего маршрута сертификации по предварительному запросу или без такового.

А.7 Генерирование и транспортирование симметричных ключей

А.7.1 Запрос симметричного ключа

Цель запроса состоит в получении симметричных ключей для шифрования данных или ключей шифрования ключей. Поскольку предоставление таких ключей требует предварительного установления связи между двумя взаимодействующими сторонами, в том случае, когда методы открытых ключей не применяются, необходима аутентификация инициатора запроса с помощью ключа шифрования ключей (KEK — key encrypting key); данный ключ используют для обеспечения конфиденциальности другого ключа.

А.7.2 Доставка симметричных ключей

Цель данного сообщения — предоставление симметричных ключей по предварительному запросу или без такового.

Если используют только симметричные алгоритмы, то следует иметь в виду, что до передачи симметричных ключей по каналу связи должна быть осуществлена передача KEK по внешнему каналу взаимодействия. В данном случае параметр алгоритма в сегменте USA должен будет содержать в себе зашифрованный ключ.

А.8 Прекращение действия ключа

А.8.1 Запрос на прекращение действия симметричного или асимметричного ключа

Цель состоит в прекращении действия существующего симметричного или асимметричного ключа (если сертификаты не используют), например вследствие его компрометации, замены исходного ключа, смены сертификационного органа пользователя; прекращения использования ключа (например, из-за увольнения пользователя из компании) или по иной причине. Рекомендуется обезопасить рассматриваемый запрос, используя для аутентификации существующие ключи.

А.8.2 Подтверждение прекращения действия ключа

Цель состоит в уведомлении пользователей о том, что некоторые конкретные ключи признаны недействительными.

Примечание — Ниже перечислены функции, которые не поддерживаются сообщением типа KEYMAN:

- автономные функции генерирования временных меток (для них требуется отдельное сообщение, например типа AUTACK);
- функции квитирования сообщений и уведомления об ошибках, относящиеся к принятым сообщениям типа KEYMAN; в данном случае требуется использование других типов сообщений (например, AUTACK или CONTRL).

Приложение В
(справочное)

Методы защиты, применимые к сообщениям типа KEYMAN

Настоящее приложение содержит рекомендации по минимальной и максимальной степеням защиты сообщений с помощью сегментов заголовка/концевика (H/T) службы защиты, как описано в ИСО 9735-5, для использования применительно к каждой функции управления ключами (KEYMAN).

Таблица В.1 — Уровни обеспечения безопасности с помощью сегментов служб защиты

Функция	Служба защиты		Примечания
	мин	макс.	
Представление к регистрации		INT	AUT по внешнему каналу взаимодействия (Out of band)
Запрос пары асимметричных ключей			
Запрос сертификата		NRO	AUT по внешнему каналу взаимодействия (Out of band)
Запрос на обновление сертификата	NRO		
Запрос на замену сертификата	NRO		
Запрос сертификата или маршрута сертификации		NRO	
Представление сертификата			
Запрос статуса сертификата		NRO	
Уведомление о статусе сертификата		NRO	
Запрос на проверку подлинности сертификата			
Уведомление о проверке подлинности сертификата	NRO		
Запрос на аннулирование	NRO		
Подтверждение аннулирования	NRO		
Запрос списка аннулирования			
Представление списка аннулирования	NRO		
Запрос предупреждения		NRO	
Предоставление маршрута сертификации			
Запрос симметричного ключа			
Представление симметричного ключа	CON		Возможно использование KEK
Запрос на прекращение действия симметричного или асимметричного ключа	AUT	NRO	
Квитирование прекращения действия	AUT	NRO	

AUT — аутентификация.
CON — конфиденциальность.
INT — целостность.
KEK — ключ шифрования ключей.
NRO — невозможность отказа отправителя от авторства сообщения.
Out of band — использование внешнего канала взаимодействия.

Приложение С
(справочное)

Использование групп сегментов в сообщениях типа KEYMAN

В данном приложении описаны группы сегментов, используемые для реализации определенных функций управления ключами (KEYMAN).

Таблица С.1 — Группы сегментов для формирования запросов

Функция	Используемые сегменты	Комментарии
Представление к регистрации	USE-USF-USC-USA	
Запрос пары асимметричных ключей	USE-USF-USA	
Запрос сертификата	USE-USF-USC-USA	Группа идентифицирует сертификат и открытый ключ
Запрос на обновление сертификата	USE-USF-USC	Группа идентифицирует сертификат и определяет новый период действия
Запрос на замену сертификата	USE-USF-USC-USA	В группе dayf ссылка на сертификат, подлежащий аннулированию
Запрос сертификата или маршрута сертификации	USE-USF-USC	С помощью сегмента USF в группу включается запрос на извлечение списка сертификатов
Запрос статуса сертификата	USE-USF-USC	
Запрос на проверку подлинности сертификата	USE-USF-USC-USA(3)-USR	
Запрос на аннулирование	USE-USF-USC	Использован также внешний канал взаимодействия (Out of band)
Запрос списка аннулирования	USE-USF	
Запрос предупреждения	USE-USF-USC	
Запрос симметричного ключа	USE-USF-USA	Касается только симметричных ключей. Сегмент USA определен при необходимости имя ключа
Запрос на прекращение действия симметричного или асимметричного ключа	USE-USF-USA/USC	Охватывает симметричные и асимметричные ключи. Группа идентифицирует ключи
Out of band — Использование внешнего канала взаимодействия.		

Таблица С.2 — Группы сегментов для функций доставки или уведомления

Функция	Используемые сегменты	Комментарии
Предоставление сертификата	USE-USX-USF-USC-USA(3)-USR	
Уведомление о статусе сертификата	USE-USX-USF-USC-USA(3)-USR	Может быть аналогом предоставления сертификата или маршрута сертификации, когда к указанию нормального сертификата добавляется указание причины аннулирования и/или статус определяется в сегменте USF
Запрос на проверку подлинности сертификата	USE-USX-USF-USC-USA(3)-USR	Аналог уведомления о статусе сертификата с защитой посредством NRO
Подтверждение аннулирования	USE-USX-USF-USC	Аналог уведомления о статусе сертификата. Подлежит защите посредством NRO

Окончание таблицы С.2

Функция	Используемые сегменты	Комментарии
Запрос списка аннулирования	USL-USC	Аналог группового уведомления о статусе сертификатов, но касается только аннулированных сертификатов
Запрос маршрута сертификации	USE-USX-USF-USC-USA(3)-USR	Для указания маршрутов используются повторные вхождения сегмента USF
Предоставление симметричного ключа	USE-USX-USF-USA	Касается только симметричных ключей. Требует предварительной передачи KEK по внешнему каналу взаимодействия (Out of band)
Квитирование прекращения действия	USE-USX-USF-USA/USC	Охватывает симметричные и асимметричные ключи. Аналог уведомления о статусе сертификата. Подлежит защите посредством аутентификации/NRO

KEK — ключ шифрования ключей.
NRO — невозможность отказа отправителя от авторства сообщения.
Out of band — использование внешнего канала взаимодействия.

Приложение D
(справочное)

Модель для управления ключами

D.1 Введение

В открытой и защищенной информационной среде системы управления ключами осуществлены функции генерирования, распределения, сертификации, проверки достоверности и аннулирования криптографических ключей. Модель, рассматриваемая здесь, отображена в схематическом виде на рисунке D.1, где выделены пять логических блоков в соответствии с их функциональным назначением.

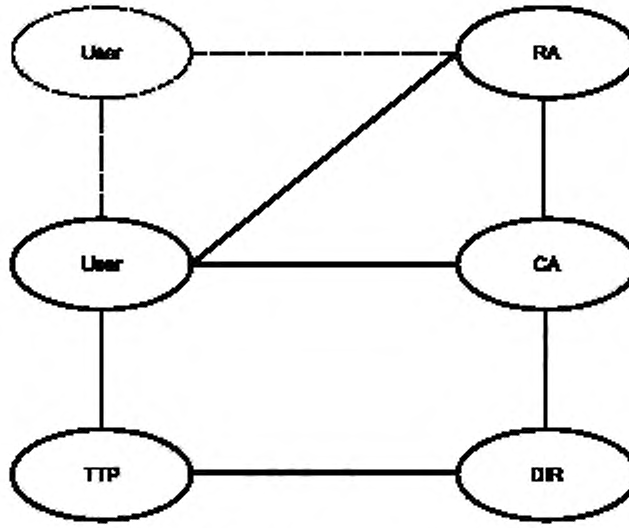

Рисунок D.1 — Модель управления ключами

Основные условия данной модели — обеспечение безопасности посредством использования методов защиты с открытыми ключами и соответствие архитектуры базовому стандарту ITU/TS X.509.

Область защиты определена «юрисдикцией» пары открытых ключей, которые использованы сертификационным органом CA для выпуска сертификатов. Таким образом, в рамках конкретной сферы обеспечения безопасности существует единственный CA, и область защиты характеризуется тем фактом, что все ее пользователи сертифицированы с применением одного и того же ключа, контролируемого CA.

Сертификационный орган соединен по защищенным каналам связи с целым рядом регистрационных органов (RA), доступных любому регистрирующемуся пользователю. Факт регистрации подтвержден сертификатом, выпущенным CA по запросу того или иного RA. После такого подтверждения информация о пользователях (их сертификаты) становится доступной в каталоге (DIR). Кроме того, возможна регистрация многочисленных доверенных третьих сторон (TTP) и пользователей, предлагающих специальные услуги.

D.2 Конечный пользователь U

Пользователь представлен в системе уникальным идентификатором, зафиксированным в его мандате. Реальный пользователь может обладать несколькими идентификаторами. Идентификатор может принадлежать юридическому лицу, фактическому (физическому) лицу или системному устройству.

D.3 Регистрационный орган RA

Для незарегистрированного пользователя защищенный канал электронного обмена данными с системой не предоставляется. Регистрационный орган использован в качестве точки входа для пользователей, которые устанавливают связь с системой с помощью тех или иных существующих доверительных средств, таких как заказное письмо или регистрационная ведомость. Такой тип регистрации при необходимости тоже создает юридическую основу для применения пользователями электронных подписей, хотя сам по себе и не образует систему управления ключами. Как только регистрация осуществлена, мандат пользователя и его открытый ключ передаются посредством запроса сертификации в сертификационный орган.

D.4 Сертификационный орган CA

Сертификационный орган является центральной частью системы обеспечения безопасности. Он предоставляет пользователям сертификаты, позволяющие установить на их основе доверительные отношения между различными пользователями и регистрационными органами. Эти сертификаты становятся после регистрации доступными в одном или нескольких каталогах для всех пользователей.

Довольно часто возникает недопонимание того факта, что выпуск сертификата осуществляется с целью уведомления о надежности действующего открытого ключа. Если же открытый ключ позже аннулируют, то его сертификат становится недействительным. Вместо оповещения об этом факте CA просто выпускает аннулированный сертификат, который заносится в каталог взамен исходного сертификата. Поэтому пользователи должны периодически обращаться к каталогу сертификатов для проверки надежности даже действительных сертификатов. Выбор частоты таких просмотров основан на пользовательской оценке допустимой степени риска.

D.5 Каталог DIR

Открытый каталог DIR, играющий роль своеобразной общедоступной телефонной книги, хранит все действующие и аннулированные сертификаты для обеспечения возможности оперативной проверки всеми пользователями. Важно, чтобы канал информационного обмена между каталогом и пользователями был защищен — для гарантии того, что извлеченная из каталога информация всегда актуальна и достоверна.

В действительности CA должен постоянно удостоверять статус сертификатов в каталоге с использованием собственного секретного ключа. Для этого, в частности, требуется, чтобы каталог DIR был зарегистрирован в CA как пользователь с открытым ключом.

D.6 Услуги доверительных третьих сторон DIR

Доверительная третья сторона TTP может предоставлять целый ряд дополнительных услуг, например формирование отметок времени. Применительно к электронному обмену данными это могут быть следующие службы:

- независимое штемпелевание;
- сертификация характеристик;
- нотариальные действия;
- репозиторий документов;
- обеспечение невозможности отказа отправителя от авторства сообщения;
- перевод сертификатов с заверением.

Приложение Е
(справочное)

Примеры управления ключами и сертификатами

Для иллюстрирования различных случаев использования сообщения типа KEYMAN ниже приведены четыре практических примера.

Е.1 Запрос на аннулирование

Е.1.1 Описание ситуации

Сертификат, выпущенный ранее сертификационным органом CA2 для сотрудника E1 учреждения O1, аннулирован этим учреждением по причине увольнения сотрудника 31 декабря 1996 г., в полдень по Гринвичу. Это сообщение организации, адресуемой сертификационному органу, должно быть снабжено электронной подписью, обеспечивающей невозможность отказа источника от авторства сообщения, обычным способом, с использованием групп сегментов заголовка и концевика защиты, как описано в стандарте ИСО 9735-5. В ответ на это сообщение учреждением O1 может быть получено подтверждение аннулирования сертификата от сертификационного органа CA2.

Е.1.2 Детализация системы обеспечения безопасности

СВЯЗЬ ПО СООБЩЕНИЯМ ЗАЩИТЫ	
СВЯЗЬ СООБЩЕНИЯ	'1' — нет связи

ФУНКЦИЯ УПРАВЛЕНИЯ КЛЮЧАМИ	
СПЕЦИФИКАТОР ФУНКЦИИ УПРАВЛЕНИЯ КЛЮЧАМИ	'130' — запрос на аннулирование

СЕРТИФИКАТ	
ССЫЛКА НА СЕРТИФИКАТ	'CA2-O1-E1' — интересующий сертификат
ДЕТАЛИЗАЦИЯ ЗАЩИТЫ Спецификатор стороны защиты Имя ключа Идентификатор стороны защиты Спецификатор реестра кодов стороны защиты Агентство, ответственное за реестр кодов стороны защиты	 '3' — владелец сертификата 'O1-E1' — сотрудник организации 'ZZZ' — по обоюдному согласию '1' — UN/CEFACT
ДЕТАЛИЗАЦИЯ ИДЕНТИФИКАТОРА ЗАЩИТЫ Спецификатор стороны защиты Имя ключа Идентификатор стороны защиты Спецификатор реестра кодов стороны защиты Агентство, ответственное за реестр кодов стороны защиты	 '4' — сторона аутентификации 'CA2' — сертификационный орган 'ZZZ' — по обоюдному согласию '1' — UN/CEFACT
ДАТА И ВРЕМЯ ЗАЩИТЫ Спецификатор даты и времени Дата события Время события Сдвиг времени	'6' — дата и время аннулирования сертификата '19961231' '120000' '0000'
ПРИЧИНА АННУЛИРОВАНИЯ	'3' — владелец перешел в другую компанию

Е.2 Запрос на прекращение действия симметричного ключа

Е.2.1 Описание ситуации

Организация O1 просит организацию O2 остановить использование общего симметричного ключа K1, поскольку он был заменен. Сообщение, соответствующее этому запросу, должно быть обеспечено проверкой подлинности источника обычным способом — с использованием групп сегментов заголовка и концевика защиты, как описано в ИСО 9735-5, с помощью другого предварительно согласованного симметричного ключа. В ответ на это сообщение может последовать подтверждение прекращения действия указанного в запросе ключа от организации O2 организации O1.

Е.2.2 Детализация защиты

СВЯЗЬ ПО СООБЩЕНИЯМ ЗАЩИТЫ	
СВЯЗЬ СООБЩЕНИЯ	'1' — нет связи

ФУНКЦИЯ УПРАВЛЕНИЯ КЛЮЧАМИ	
СПЕЦИФИКАТОР ФУНКЦИИ УПРАВЛЕНИЯ КЛЮЧАМИ	'151' — запрос на прекращение действия ключа

АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '2' — симметричный алгоритм владельца '2' — CBC '1' — DES
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '9' — имя симметричного ключа 'K1'

E.3 Предоставление сертификата или маршрута сертификации

E.3.1 Описание ситуации

Данное сообщение от сертификационного органа CA2 организации O1 направлено в ответ на предварительный запрос маршрута сертификации от этой организации, касающийся сертификата организации O2. В рассматриваемом примере и CA2, и сертификационный орган CA3 организации O2 удостоверяются в двухуровневой иерархии сертификационным органом CA1. Запросное сообщение может присутствовать в явной форме в сегменте USX, размещенном между сегментами USE и USF.

Все метки времени сертификатов указывают полночь по Гринвичу, причем сертификат верхнего уровня сгенерирован 1 декабря 1996 г. на 10-летний срок, начинающийся с 1 января 1997 г., а пользовательский сертификат сгенерирован 1 февраля 1997 г. на двухлетний срок, начинающийся с 1 марта 1997 г. Открытые ключи CA1, CA3 и O2 имеют длину 2048, 1024 и 512 соответственно. Все открытые ключи представляют собой открытую экспоненту 10001_{16}.

E.3.2 Детализация защиты

СВЯЗЬ ПО СООБЩЕНИЯМ ЗАЩИТЫ	
СВЯЗЬ СООБЩЕНИЯ	'2' — ответ

ФУНКЦИЯ УПРАВЛЕНИЯ КЛЮЧАМИ	
СПЕЦИФИКАТОР ФУНКЦИИ УПРАВЛЕНИЯ КЛЮЧАМИ	'222' — предоставление маршрута сертификации
ПОРЯДКОВЫЙ НОМЕР СЕРТИФИКАТА	'1' — первый сертификат в маршруте

СЕРТИФИКАТ	
ССЫЛКА НА СЕРТИФИКАТ	'CA1-CA3' — сертификат от CA1 для CA3
ДЕТАЛИЗАЦИЯ ИДЕНТИФИКАТОРА ЗАЩИТЫ Спецификатор стороны защиты Имя ключа Идентификатор стороны защиты Спецификатор реестра кодов стороны защиты Агентство, ответственное за реестр кодов стороны защиты	 '3' — владелец сертификата 'CA3' — сертификационный орган организации O2 'ZZZ' — по обоюдному согласию '1' — UN/CEFACT
ДЕТАЛИЗАЦИЯ ИДЕНТИФИКАТОРА СЛУЖБЫ ЗАЩИТЫ Спецификатор стороны защиты Имя ключа Идентификатор стороны защиты Спецификатор реестра кодов стороны защиты Агентство, ответственное за реестр кодов стороны защиты	 '4' — сторона аутентификации 'CA1' — сертификационный орган верхнего уровня 'ZZZ' — по обоюдному согласию '1' — UN/CEFACT
Синтаксис и версия сертификата	'1' — версия 4
ФУНКЦИЯ ФИЛЬТРАЦИИ	'2' — шестнадцатеричный фильтр
СПОСОБ КОДИРОВАНИЯ БАЗОВОГО НАБОРА СИМВОЛОВ	'1' — 7-битовый код ASCII
ИСХОДНЫЙ НАБОР СИМВОЛОВ СЕРТИФИКАТА	'2' — синтаксис UN/ECE, уровень B

СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '1' — терминатор сегмента '27' — апостроф
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '2' — разделитель элементов составных данных '3A' - двоеточие
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '3' — разделитель элементов данных '2B' — символ знака «плюс»
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '4' — символ разрешения выпуска '3F' — знак вопроса
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '5' — символ повторения '2A' — звездочка
ДАТА И ВРЕМЯ ЗАЩИТЫ Спецификатор даты и времени Дата события Время события Сдвиг времени	 '2' — дата и время генерирования сертификата '19961201' '000000' '0000'
ДАТА И ВРЕМЯ ЗАЩИТЫ Спецификатор даты и времени Дата события Время события Сдвиг времени	 '3' — начало периода действия сертификата '19970101' '000000' '0000'
ДАТА И ВРЕМЯ ЗАЩИТЫ Спецификатор даты и времени Дата события Время события Сдвиг времени	 '4' - начало периода действия сертификата '20070101' '000000' '0000'
СТАТУС ЗАЩИТЫ	'1' — действует
АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '6' — подпись владельца '10' — RSA
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '13' — открытая экспонента '010001'
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '12' — модуль открытый ключ CA3
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '14' — длина модуля '1024'

АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '4' — хэш-функция издателя '42' — HDS2

АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '3' — подпись издателя '10' — RSA

ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '13' — открытая экспонента '010001'
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '12' — модуль открытый ключ CA1
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '14' — длина модуля '2048'

РЕЗУЛЬТАТ ЗАЩИТЫ	Цифровая подпись органа CA1 в сертификате
РЕЗУЛЬТАТ КОНТРОЛЯ Спецификатор контрольного значения Контрольное значение	 '1' — уникальная контрольная величина отфильтрованная цифровая подпись 2048 бит

ФУНКЦИЯ УПРАВЛЕНИЯ КЛЮЧАМИ	
СПЕЦИФИКАТОР ФУНКЦИИ УПРАВЛЕНИЯ КЛЮЧАМИ	'222' — предоставление маршрута сертификации
ПОРЯДКОВЫЙ НОМЕР СЕРТИФИКАТА	'2' — второй сертификат в маршруте

СЕРТИФИКАТ	
ССЫЛКА НА СЕРТИФИКАТ	'CA3-O2' — сертификат от CA3 для организации O2
ДЕТАЛИЗАЦИЯ ИДЕНТИФИКАТОРА СЛУЖБЫ ЗАЩИТЫ Спецификатор стороны защиты Имя ключа Идентификатор стороны защиты Спецификатор реестра кодов стороны защиты Агентство, ответственное за реестр кодов стороны защиты	 '3' — владелец сертификата 'O2' — организация O2 'ZZZ' — по обоюдному согласию '1' — UN/CEFACT
ДЕТАЛИЗАЦИЯ ИДЕНТИФИКАТОРА СЛУЖБЫ ЗАЩИТЫ Спецификатор стороны защиты Имя ключа Идентификатор стороны защиты Спецификатор реестра кодов стороны защиты Агентство, ответственное за реестр кодов стороны защиты	 '3' — владелец сертификата 'O2' — организация O2 'ZZZ' — по обоюдному согласию '1' — UN/CEFACT
Синтаксис и версия сертификата	'1' — версия 4
ФУНКЦИЯ ФИЛЬТРАЦИИ	'2' — шестнадцатеричный фильтр
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА СИМВОЛОВ	'1' — 7-битовый код ASCII
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА СИМВОЛОВ СЕРТИФИКАТА	'2' — синтаксис UN/ECE, уровень B
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '1' — терминатор сегмента '27' — апостроф
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '2' — разделитель элементов составных данных '3A' — двоеточие
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '3' — разделитель элементов данных '2B' — знак «плюс»
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '4' — символ разрешения на передачу '3F' — знак вопроса
СЛУЖЕБНЫЙ СИМВОЛ ДЛЯ ПОДПИСИ Служебный символ спецификатора подписи Служебный символ для подписи	 '5' — разделитель повторений '2A' — звездочка

ДАТА И ВРЕМЯ ЗАЩИТЫ Спецификатор даты и времени Дата события Время события Сдвиг времени	 '2' — дата и время генерирования сертификата '19970201' '000000' '0000'
ДАТА И ВРЕМЯ ЗАЩИТЫ Спецификатор даты и времени Дата события Время события Сдвиг времени	 '3' — начало периода действия сертификата '19970301' '000000' '0000'
ДАТА И ВРЕМЯ ЗАЩИТЫ Спецификатор даты и времени Дата события Время события Сдвиг времени	 '4' — конец периода действия сертификата '19990301' '000000' '0000'
СТАТУС ЗАЩИТЫ	'1' — действует

АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '6' — подписание владельцем '10' — RSA
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '13' — открытая экспонента '010001'
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '12' — модуль открытый ключ организации О2
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '14' — длина модуля '512'

АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '4' — хэш-функция издателя '42' — HDS2

АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '3' — подпись запрашивающей стороны '10' — RSA
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '13' — открытая экспонента '010001'
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '12' — модуль открытый ключ СА3
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '14' — длина модуля '1024'

РЕЗУЛЬТАТ ЗАЩИТЫ	
РЕЗУЛЬТАТ КОНТРОЛЯ Спецификатор контрольного значения Контрольное значение	 '1' — уникальная контрольная величина отфильтрованная цифровая подпись 1024 бита

Е.4 Предоставление симметричного ключа

Е.4.1 Описание ситуации

Организация О2 предоставляет организации О1 симметричный ключ, зашифрованный по предварительному согласию ключом KEK1, в ответ на предшествующий запрос симметричного ключа организацией О1. Запросное сообщение может быть сформировано в явном виде путем вставки сегмента USX между сегментами USE и USF.

Е.4.2 Детализация защиты

СВЯЗЬ ПО СООБЩЕНИЯМ ЗАЩИТЫ	
СВЯЗЬ СООБЩЕНИЯ	'2' — ответ

ФУНКЦИЯ УПРАВЛЕНИЯ КЛЮЧАМИ	
СПЕЦИФИКАТОР ФУНКЦИИ УПРАВЛЕНИЯ КЛЮЧАМИ	'251' — предоставление симметричного ключа
ФУНКЦИЯ ФИЛЬТРАЦИИ	'2' — шестнадцатеричный фильтр

АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Криптографический режим работы Алгоритм	 '5' — шифрование владельцем '2' — CBC '1' — DES
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '5' — симметричный ключ, зашифрованный симметричным ключом отфильтрованное значение зашифрованного ключа: '3A94BACCF7DE11A5BEAD5320A2F493'
ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 '10' — имя ключа шифрования ключей 'KEK1'

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 9735-1	IDT	ГОСТ Р ИСО 9735-1—2012 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 1. Синтаксические правила, общие для всех частей»
ISO 9735-2	IDT	ГОСТ Р ИСО 9735-2—2012 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 2. Синтаксические правила, специфичные для пакетного ЭОД»
ISO 9735-5	IDT	ГОСТ Р ИСО 9735-5—2012 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 5. Правила безопасности для пакетного EDI (подлинность, целостность и невозможность отказа отправителя от авторства сообщения»
ISO 9735-10	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

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

- IDT — идентичные стандарты.

Библиография

[1] ISO 639 (all parts), Code for the representation of names of langua
Коды для представления названий языков (все части ISO 639)

[2] ISO/IEC 646, Information technology; ISO 7-bit coded character set for information interchange (Информационные технологии. 7-битный набор кодированных символов ISO для обмена информацией)

[3] ISO/IEC 2022, Information technology — Character code structure and extension techniques (Информационные технологии. Структура кода символов и методы расширения)

[4] ISO/IEC 2375, Information technology — Procedure for registration of escape sequences and coded character sets (Информационные технологии. Процедура регистрации управляющей последовательности и наборов кодированных знаков)

[5] ISO/IEC 6523 (all parts), Information technology — Structure for the identification of organizations and organization parts (Информационные технологии. Структура идентификации организаций и их подразделений (все части ISO/IEC 6523)

[6] ISO 8372[1)], Information processing; Modes of operation for a 64-bit block cipher algorithm (Обработка информации. Режимы работы алгоритма 64-битового блочного шифрования)

[7] ISO 8601, Data elements and interchange formats; information interchange; representation of dates and times (Элементы данных и форматы информационного обмена. Обмен информацией. Представление дат и времени)

[8] ISO 8731-1[1)], Banking; Approved algorithms for message authentication; Part 1 : DEA (Банковское дело. Утвержденные алгоритмы для аутентификации сообщений. Часть 1. Алгоритмы кодирования данных (DEA)

[9] ISO 8731-2[1)], Banking; approved algorithms for message authentication; Part 2: message authenticator algorithm (Банковское дело. Утвержденные алгоритмы для аутентификации сообщений. Часть 2. Алгоритм аутентификации сообщений)

[10] ISO/IEC 8859 (all parts), Information technology — 8-bit single-byte coded graphic character sets (Информационные технологии. 8-битные однобайтовые наборы кодированных графических знаков (все части ISO/IEC 8859)

[11] ISO/IEC 9594-8, Information technology. Open Systems Interconnection. The Directory. Part 8: Public-key and attribute certificate frameworks (Информационные технологии. Взаимосвязь открытых систем. Директория. Часть 8. Системы сертификатов открытого ключа и атрибутов)

[12] ISO 9735:1988, Electronic data interchange for administration, commerce and transport (EDIFACT); application level syntax rules (Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня)

[13] ISO 9735:1988/Amd 1:1992, Electronic data interchange for administration, commerce and transport (EDIFACT); application level syntax rules; amendment 1 (Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня. Изменение 1)

[14] ISO 9735 (all parts):1998[1)], Electronic data interchange for administration, commerce and transport (EDIFACT); application level syntax rules [Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4) (все части ISO 9735)]

[15] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature schemes giving message recovery Информационные технологии. Методы защиты. Схемы цифровой подписи, обеспечивающие восстановление сообщений (все части ISO/IEC 9796)

[16] ISO/IEC 9797, Information technology; security techniques; data integrity mechanism using a cryptographic check function employing a block cipher algorithm (Информационные технологии. Методы защиты. Коды аутентификации сообщений (MAC)

[17] ISO/IEC 10116, Information technology; modes of operation for an n-bit block cipher algorithm (Информационные технологии. Методы защиты. Режимы работы для n-битовых блочных шифров)

[18] ISO/IEC 10118-1, Information technology — Security techniques — Hash-functions — Part 1. General (Информационные технологии. Методы защиты. Хэш-функции. Часть 1. Общие положения)

[19] ISO/IEC 10118-3, Information technology — Security techniques - Hash-functions — Part 3: Dedicated hash-functions (Информационные технологии. Методы защиты. Хэш-функции. Часть 3: Специализированные хэш-функции)

[20] ISO 10126-1[1)], Banking; procedures for message encipherment (wholesale); Part 1. General principles (Банковское дело. Процедуры кодирования сообщений (оптовая торговля). Часть 1. Общие принципы)

[21] ISO/IEC 10646, Information technology — Universal Coded Character Set (UCS) (Информационные технологии. Универсальный набор кодированных знаков (UCS)

[22] ISO 11166-2[1)], Banking — Key management by means of asymmetric algorithms — Part 2: Approved algorithms using RSA cryptosystem (Банковское дело. Управление ключами с помощью асимметричных алгоритмов. Часть 2. Утвержденные алгоритмы с использованием криптосистемы RSA)

[23] ISO/IEC 12042, Information technology; data compression for information interchange; binary arithmetic coding algorithm (Информационные технологии. Уплотнение данных для обмена информацией. Алгоритм двоичного арифметического кодирования)

[1)] Изъят из обращения.

УДК 006.354 ОКС 35.240.60

Ключевые слова: атрибут, сертификат, кодовый список, справочник составных элементов, управляющий знак, криптография, дешифрация

Редактор *Я.В. Кожаринова*
Технический редактор *В.Ю. Фотиева*
Корректор *Е.Ю. Митрофанова*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 23.11.2016. Подписано в печать 27.12.2016. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,93. Тираж 27 экз. Зак. 3287.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер , 4.
www.gostinfo.ru info@gostinfo.ru