МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

H.235.2

(09/2005)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ
И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных услуг –
Системные аспекты

Безопасность H.323: Профиль защиты цифровой подписи

Рекомендация МСЭ-Т H.235.2

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ H

АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

ХАРАКТЕРИСТИКИ ВИДЕОТЕЛЕФОННЫХ СИСТЕМ	H.100–H.199
ИНФРАСТРУКТУРА АУДИОВИЗУАЛЬНЫХ УСЛУГ	
Общие положения	H.200–H.219
Мультиплексирование и синхронизация при передаче	H.220–H.229
Системные аспекты	**H.230–H.239**
Процедуры связи	H.240–H.259
Кодирование движущихся видеоизображений	H.260–H.279
Сопутствующие системные аспекты	H.280–H.299
Системы и оконечное оборудование для аудиовизуальных услуг	H.300–H.349
Архитектура услуг справочника для аудиовизуальных и мультимедийных услуг	H.350–H.359
Качество архитектуры обслуживания для аудиовизуальных и мультимедийных услуг	H.360–H.369
Дополнительные услуги для мультимедиа	H.450–H.499
ПРОЦЕДУРЫ МОБИЛЬНОСТИ И СОВМЕСТНОЙ РАБОТЫ	
Обзор мобильности и совместной работы, определений, протоколов и процедур	H.500–H.509
Мобильность для мультимедийных систем и услуг серии H	H.510–H.519
Приложения и услуги мобильной мультимедийной совместной работы	H.520–H.529
Защита мобильных мультимедийных систем и услуг	H.530–H.539
Защита приложений и услуг мобильной мультимедийной совместной работы	H.540–H.549
Процедуры мобильного взаимодействия	H.550–H.559
Процедуры взаимодействия мобильной мультимедийной совместной работы	H.560–H.569
ШИРОКОПОЛОСНЫЕ И МУЛЬТИМЕДИЙНЫЕ TRIPLE-PLAY УСЛУГИ	
Предоставление широкополосных мультимедийных услуг по VDSL	H.610–H.619

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т H.235.2

Безопасность H.323: Профиль защиты цифровой подписи

Резюме

В данной Рекомендации описывается дополнительный профиль защиты для использования цифровых подписей для обеспечения защиты сигнализации H.225.0.

В предыдущих версиях Рекомендаций МСЭ-Т подсерии H.235 данный профиль содержался в Приложении E/H.235. В Дополнениях IV, V, VI к Рекомендации МСЭ-Т H.235.0 приводятся полный раздел, рисунок и таблица совместимости версий 3 и 4 Рекомендации МСЭ-Т H.235.

Источник

Рекомендация МСЭ-Т H.235.2 утверждена 13 сентября 2005 года 16-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

Ключевые слова

Аутентификация, сертификат, цифровая подпись, шифрование, целостность, управление ключами, безопасность мультимедиа, профиль защиты.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

© ITU 2007

Все права сохранены. Никакая часть данной публикации не может быть воспроизведена с помощью каких-либо средств без письменного разрешения МСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т H.235.2

Безопасность H.323: Профиль защиты цифровой подписи

1 Сфера применения

В данной Рекомендации описывается дополнительный профиль защиты для использования цифровых подписей для обеспечения защиты сигнализации H.225.0.

2 Справочные документы

2.1 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и других справочных документах содержатся положения, которые посредством ссылок на них в этом тексте составляют основные положения данной Рекомендации. На момент опубликования действовали указанные редакции документов. Все Рекомендации и другие справочные документы являются предметом корректировки, и стороны пришли к договоренности основываться на этой Рекомендации и стараться изыскивать возможность для использования самых последних изданий Рекомендации и справочных документов, перечисленных ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т. Ссылка на документ в рамках этой Рекомендации не дает ему как отдельному документу статуса рекомендации.

– ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

– ITU-T Recommendation H.235 (1998), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.

– ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

– ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.

– ITU-T Recommendation H.235.6 (2005), *H.323 security: Voice encryption profile with native H.235/H.245 key management*.

– ITU-T Recommendation H.245 (2005 г.), *Управляющий протокол для мультимедийной связи*.

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

– ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.

– ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

– ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

– ISO/IEC 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*.

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

2.2 Информативные справочные документы

[ISO/IEC 14888-3] ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms*.

[PKCS] PKCS #1 v2.0: *RSA Cryptography Standard;* RSA Laboratories; October 1, 1998; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[PKCS] PKCS #7: *Cryptographic Message Syntax Standard*, An RSA Laboratories Technical Note, version 1.5, Revised November 1, 1993; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[RFC1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm.*

[RFC3447] IETF RFC 3447 (2003), *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*.

3 Термины и определения

Наряду с определениями, данными в этом пункте, также используются определения, данные в разделах 3/H.323, 3/H.225.0 и 3/H.245. Некоторые из терминов, используемых в данной Рекомендации, также определяются в Рекомендациях МСЭ-Т X.800 | ИСО 7498-2, X.803 | ИСО/МЭК 10745, X.810 | ИСО/МЭК 10181-1 и X.811 | ИСО/МЭК 10181-2.

3.1 органы сертификации: Органы сертификации (CA) в области цифровых подписей заверяют открытые ключи проверки, выдавая "сертификаты".

3.2 хранилища сертификатов: В хранилищах сертификатов (например, каталог X.500) содержатся сертификаты пользователя и списки аннулированных сертификатов (CRL). Их функция состоит в том, чтобы сделать эту информацию доступной, однако они не несут ответственности за содержание или точность информации, получаемой от органов сертификации или органов регистрации.

3.3 цифровая подпись: Представляет собой криптографическое преобразование (с использованием метода ассиметричного шифрования) информационного сообщения, представленное в числовой форме, таким образом, чтобы человек, имеющий подписанное сообщение и соответствующий открытый ключ, мог определить что:

i) преобразование было проведено с использованием частного ключа, соответствующего данному открытому ключу; и

ii) с момента криптографического преобразования в подписанный документ не были внесены изменения.

3.4 поставщики услуг оперативного определения статуса сертификата: Протокол оперативного определения статуса сертификата (OCSP) позволяет прикладным программам определять аннулирование идентифицированного сертификата. Протокол OCSP может быть использован для удовлетворения некоторых текущих потребностей по обеспечению более регулярного обновления информации об аннулировании сертификатов, чем в списках аннулированных сертификатов. Поставщиков услуг оперативного определения статуса сертификата можно рассматривать в качестве альтернативы использованию автономных списков аннулированных сертификатов (CRL).

3.5 модуль-посредник: Модуль-посредник представляет собой промежуточный объект H.323, подобный привратнику. Модуль-посредник может быть отдельным узлом сети, а может работать с функциональными средствами объектов H.323, такими как привратник. Модуль-посредник может выполнять защитные функции, такие, как проверка подписей и сертификатов и контроль доступа.

3.6 регистрационные органы: Регистрационные органы выступают посредниками между пользователями и органами сертификации. Они получают запросы от пользователей и перенаправляют их органам сертификации в соответствующей форме.

3.7 службы отметок времени: Наличие служб отметок времени обязательно для неотказуемости в случае потери ключа или его рассекречивания. На практике они предоставляют встречную подпись любому, в том числе достоверное время, через хэш и идентификатор хэша.

3.8 поставщик услуг доверенной службы: Объект, который может быть использован другими объектами в качестве доверенного посредника в процессе взаимодействия или проверки или в качестве доверенного поставщика услуг информационной службы.

В данной Рекомендации по предоставлению услуг защиты используются следующие термины:

3.9 "**только аутентификация**": Эта служба защиты профиля защиты цифровой подписи обеспечивает аутентификацию пользователя в тех случаях, когда пользователь аутентифицируется, поставив верную цифровую подпись под определенными данными при помощи частного ключа. Заметьте, что данная служба защиты не обеспечивает контрмер против произвольного вырезания и вставки, манипуляций с сообщением или преступных атак. Служба "только аутентификация" может быть полезна для модулей-посредников защиты, которые проверяют аутентичность сообщения (аутентификация происхождения данных) при пересылке этого сообщения на другой адрес (например, привратнику).

ПРИМЕЧАНИЕ. – При пересылке определенные части сообщения обычно претерпевают изменения, поэтому реализация сквозной целостности невозможна.

Тем не менее службу "только аутентификация" можно применять также на основе переход-переход. Применение данной службы защиты для сценария сквозной передачи данных устанавливается в процедуре III, для случаев переход-переход в процедуре II.

3.10 аутентификация и целостность: Это комбинированная служба защиты, которая поддерживает целостность сообщения совместно с аутентификацией пользователя. Аутентификация пользователя происходит, если пользователь поставил верную цифровую подпись под определенными данными с помощью частного ключа. Кроме того, сообщение защищено от несанкционированного использования. Обе службы защиты обеспечиваются одним и тем же алгоритмом защиты. Совмещение аутентификации и целостности возможно только на основе переходов. Эта служба защиты описывается в процедуре II.

ПРИМЕЧАНИЕ. – При использовании цифровых подписей может поддерживаться служба защиты неотказуемости, это также зависит от установки битов использования ключа подписанного ключа в сертификате (см. также RFC 3280).

4 Символы и сокращения

В данной Рекомендации используются следующие сокращения:

ARQ	Admission Request	Запрос допуска	
ASN.1	Abstract Syntax Notation One	Абстрактно-синтаксическая нотация версии 1	
CA	Certification Authority	Органы сертификации	
CRL	Certificate Revocation List	Список аннулированных сертификатов	
DH	Diffie-Hellman	Алгоритм Диффи-Хеллмана	
DNS	Domain Name Service	Служба доменных имен	
EP	Endpoint	Конечная точка	
EPID	Endpoint Identifier	Идентификатор конечной точки	
GK	Gatekeeper	Привратник	
GKID	Gatekeeper Identifier	Идентификатор привратника	
GRQ	Gatekeeper Request	Запрос привратника	
ICV	Integrity Check Value	Значение проверки целостности	
IP	Internet Protocol	Протокол Интернет	
ITU	International Telecommunication Union	Международный союз электросвязи	МСЭ

LDAP	Light-weight Directory Access Protocol	Облегченный протокол доступа к каталогам
LRQ	Location Request	Запрос местонахождения
MCU	Multipoint Control Unit	Узел контроля многоточечной связи
MD5	Message Digest 5	Алгоритм профиля сообщения версии 5, хэш-функция MD5
NAT	Network Address Translation	Трансляция сетевых адресов
OID	Object Identifier	Идентификатор объекта
OCSP	Online Certificate Status Protocol	Протокол оперативного определения статуса сертификата
PKCS	Public-Key Crypto System	Система шифрования открытым ключом,
RA	Registration Authority	Орган регистрации
RAS	Registration, Admission and Status	Регистрация, допуск, статус
RSA	Rivest, Shamir, Adleman	Алгоритм шифрования Райвеста-Шамира-Адлемана
RTP	Real-Time Protocol	Протокол режима реального времени
SHA	Secure Hash Algorithm	Надежный алгоритм хэширования
URL	Uniform Resource Locator	Унифицированный указатель ресурса, URL-адрес

5 Соглашения по терминам

В данной Рекомендации используются следующие соглашения:

– "должен/необходимо" означает обязательное требование,

– "следует" указывает на предполагающийся, но не обязательный образ действия,

– "может" означает скорее необязательный образ действий, чем указание на то, что должно быть сделано.

При необходимости профиль защиты цифровой подписи может использовать **профиль защиты шифрования голоса** H.235.1 для достижения конфиденциальности голоса.

В процедурах II и III описывается применение служб защиты для различных сценариев, как, например, сквозной и переход-переход с различными алгоритмами защиты, такими, как метод ассиметричного шифрования (цифровая подпись).

Служба целостности сообщения всегда обеспечивает аутентификацию сообщения, обратное не всегда верно. В режиме "только аутентификация" гарантированная целостность охватывает только определенное подмножество полей сообщения. Данное утверждение справедливо и для служб целостности, реализуемых ассиметричными средствами (например, цифровые подписи). Таким образом, на практике, комбинированная служба аутентификации и целостности использует один и тот же материал ключа с сохранением защиты.

Более того, вся информация по защите переход-переход помещается в элемент **CryptoSignedToken**. Эта информация повторно рассчитывается при каждом переходе согласно процедуре II.

С другой стороны информация по сквозной защите (возможная только при использовании модуля-посредника H.323 и процедуры III), в основном вычисляет информацию, аналогичную информации, помещенной в **CryptoSignedToken**, но хранит эту информацию в отдельном **CryptoToken** всего сообщения. Эта информация не меняется при пересылке. Отдельный идентификатор объектов позволяет различать **CryptoToken** для случаев переход-переход и сквозного.

Ассиметричные методы шифрования, использующиеся в цифровых подписях, могут применяться на основе переходов и/или сквозной основе.

6 Общие положения

В данной Рекомендации описывается дополнительный профиль защиты для использования цифровых подписей для обеспечения сигнализации защиты H.225.0. Объекты защиты H.323 (оконечные устройства, привратники, шлюзы, узлы контроля многоточечной связи (MCU) и т. д.) могут приводить в исполнение данный профиль защиты цифровой подписи для усовершенствования защиты или по требованию.

Профиль защиты цифровой подписи санкционирует использование модели, маршрутизируемой привратником, и основывается на методах туннелирования H.245, поддержка моделей, не маршрутизируемых привратником, является материалом для дальнейшего изучения.

Профиль защиты цифровых подписей применим для масштабируемой "глобальной" IP-телефонии; данный профиль защиты преодолевает ограничения простого, базового профиля защиты H.235.1. Например, профиль защиты цифровой подписи не зависит от администрирования общих паролей переходов в различных доменах. Он обеспечивает туннелирование сообщений H.245 для сохранения целостности сообщений H.245, а также обеспечивает неотказуемость сообщений. Профиль защиты цифровой подписи поддерживает защиту переход-переход, а также верную сквозную аутентификацию с одновременным использованием модулей-посредников H.235 или промежуточных привратников.

Возможности, предоставляемые данными профилями, включают в себя, для сообщений RAS, H.225.0 и H.245:

- Аутентификация пользователя по эталонному объекту, независимо от количества переходов прикладного уровня, которые проходит сообщение.

  ПРИМЕЧАНИЕ 1. – "Переход" в данном случае понимается как доверенный элемент сети H.235 (например, привратник, шлюз, узел MCU, модуль-посредник, брандмауэр). Таким образом, защита переход-переход прикладного уровня при использовании симметричных методов не обеспечивает истинную сквозную защиту между оконечными устройствами.
- Целостность всех необходимых частей (полей) сообщений, приходящих на объект независимо от количества переходов прикладного уровня, которые проходят сообщения. Также дополнительной является возможность обеспечения целостности самого сообщения с использованием порожденного случайного числа.
- Аутентификация, целостность и неотказуемость сообщения переход-переход прикладного уровня предоставляют эти услуги защиты всему сообщению.
- Также может быть обеспечена неотказуемость сообщений, которыми обмениваются два объекта, независимо от количества переходов прикладного уровня, которые проходят сообщения. В частности, обеспечивается неотказуемость необходимых частей (полей) сообщения. Например, в случае, когда конечная точка (EP) посылает сообщение SETUP на привратник (GK), а EP и GK отделены друг от друга одним или более модулями-посредниками.

Используя вышеперечисленные службы защиты соответствующим образом, можно предотвратить некоторые виды атак. Среди них:

- Атаки типа "отказ в обслуживании": такие атаки можно предотвратить с помощью быстрой проверки подлинности цифровых подписей.
- Атака через посредника: от подобных атак защищает последовательная аутентификация сообщения уровня приложений, если недоброжелатель, скажем, враждебный роутер, находится между переходами прикладного уровня. Если недоброжелатель является объектом прикладного уровня, его атаки можно предотвратить при наличии сквозной аутентификации пользователя и целостности для отдельных частей сообщения.
- Атака замещением оригинала: такие атаки предотвращаются с помощью использования отметок времени и порядковых номеров.
- Имитация соединения (спуфинг): такие атаки отражает использование аутентификации пользователя.
- Захват соединения: такие атаки предотвращает аутентификация/целостность для каждого сигнального сообщения.

Данный профиль защиты применим в сетевом окружении с потенциально большим числом оконечных устройств, где использование пароля/присвоение симметричного кода не приемлемо, например, в сценариях большого или глобального масштаба. Профиль защиты цифровой подписи обеспечивает дополнительную службу защиты для неотказуемости при помощи использования цифровых подписей и сертификатов. Цифровые подписи могут использовать хэш-функции SHA1 или MD5 и обеспечивать аутентификацию и/или целостность (см. процедуры II и III).

Объекты H.323, использующие аутентификацию и целостность, "или только аутентификацию" на основе переход-переход, должны использовать процедуру II. Объекты H.323, использующие "только аутентификацию", не реализуют целостности. Объекты H.323, использующие "только аутентификацию", должны использовать процедуру III для истинной сквозной аутентификации.

В данной Рекомендации может применяться защита целостности сообщения, которая охватывает все сообщение целиком. Для RAS H.225.0 защита целостности охватывает все сообщение RAS; для сигнализации вызова защита целостности охватывает все сообщение сигнализации вызова H.225.0, включая заголовки Q.931.

Профиль защиты цифровой подписи позволяет безопасно туннелировать модули данных протокола (PDU) контроля вызова H.245 в сообщения facility H.225.0. Туннелирование, полезное, например, при очень продолжительных вызовах, требуется для алгоритмов синхронизации и обновления кодов H.245.

ПРИМЕЧАНИЕ 2. – Обновление кодов для кодирования голоса G.711 должно происходить не позднее пересылки 2^{30} 64-битовых блоков, т. е. не более 12 дней с момента текущего разговора.

Участок с вертикальной штриховкой (в электронной версии – участок голубого цвета) в таблице 1 обозначает сферу применения профиля защиты цифровых подписей. Исключая целостность, обозначенную в таблице горизонтальной штриховкой (в электронной версии – участок зеленого цвета), получаем профиль защиты "только аутентификация". Дополнительной возможностью профиля защиты цифровой подписи является возможность выбора между алгоритмами шифрования RSA-SHA1 и RSA-MD5. Вместе с профилем защиты цифровой подписи можно дополнительно использовать профиль защиты шифрования голоса H.235.6 (см. 6.1/H.235.6).

Таблица 1/H.235.2 – Профиль защиты цифровой подписи

Службы защиты	**Функции вызова**			
	RAS	**H.225.0**	**H.245 (Примечание)**	**RTP**
Аутентификация	**SHA1/ MD5** **цифровая подпись**	**SHA1/ MD5** **цифровая подпись**	**SHA1/ MD5** **цифровая подпись**	
Неотказуемость	**SHA1/ MD5** **цифровая подпись**	**SHA1/ MD5** **цифровая подпись**	**SHA1/ MD5** **цифровая подпись**	
Целостность	**SHA1/ MD5** **цифровая подпись**	**SHA1/ MD5** **цифровая подпись**	**SHA1/ MD5** **цифровая подпись**	
Конфиденциальность				
Контроль доступа				
Управление ключом	**распределение сертификата**	**распределение сертификата**		
ПРИМЕЧАНИЕ. – Сообщение H.245, туннелированное или инкапсулированное в сообщение быстрого соединения H.225.0.				

ПРИМЕЧАНИЕ 3. – Необходимо, чтобы профиль защиты цифровой подписи поддерживался другими объектами H.235 (например, привратниками, шлюзами и модулями-посредниками H.235).

ПРИМЕЧАНИЕ 4. – Доступные биты использования кодов в сертификате также могут определять службу защиты, предоставляемую оконечным устройством (например, утвержденная неотказуемость).

Для аутентификации пользователю следует использовать схему цифровой подписи открытого/частного ключа. Такая схема обычно обеспечивает лучшую целостность и неотказуемость вызова.

В данной Рекомендации **не** описываются процедуры для:

- регистрации, сертификации, и предоставления сертификатов от доверенного центра и назначения частного/открытого ключа, службы каталогов, специальных (особых) параметров CA, аннулирования сертификата, обновления/восстановления криптографической пары и других процедур по работе и управлению сертификатами таких, как сертификат или частный/открытый ключ и поставки и инсталляции сертификатов в оконечные устройства.

Такие процедуры могут осуществляться средствами, которые не являются частью данной Рекомендации.

Объекты связи, участвующие в процессе, могут в неявном виде определять использование базовых профилей защиты H.235.1 или данного профиля защиты цифровой подписи, оценивая сигнализированные идентификаторы объектов защиты в сообщениях (метка **tokenOID** и алгоритм **algorithmOID**; см. также пункт 20).

Для использования данного профиля описываются следующие процедуры:

Процедура II основывается на цифровых подписях, использующих криптографическую пару частного/открытого ключей для обеспечения аутентификации, целостности и неотказуемости сообщений RAS, Q.931 и H.245. Оконечные устройства могут использовать данный метод, если требуется неотказуемость и сложная целостность.

В зависимости от политики защиты аутентификация может быть односторонней или двусторонней, применяющей аутентификацию/целостность в обратном направлении и таким образом обеспечивающей более высокий уровень защиты. Политика защиты оконечного устройства может разрешать "только аутентификацию" без вычисления криптографической целостности (см. пункт 9).

Привратники, обнаружившие отказ в аутентификации и/или неудовлетворительную проверку целостности данных в сообщении RAS/сообщении сигнального вызова, полученном от оконечного устройства/другого привратника, отвечают соответствующим сообщением отказа, указывающим на отказ защиты, устанавливая **securityDenial** или другой подходящий код ошибки защиты в качестве причины отказа согласно 11.1/H.235.0. В зависимости от способности распознать атаку и наиболее подходящего способа реагирования на нее, привратнику, получившему защищенное сообщение **xRQ** с неопределенными идентификаторами объекта (**tokenOID**, **algorithmOID**), следует ответить незащищенным сообщением **xRJ**, или удалить это сообщение. Данное событие следует занести в журнал регистрации. В ответ конечная точка должна удалить полученное незащищенное сообщение, сделать паузу и попытаться снова, выбрав другие идентификаторы объектов. Так же привратнику, получившему защищенное сообщение SETUP H.225.0 с неопределенными идентификаторами объекта (**tokenOID**, **algorithmOID**) следует ответить незащищенным сообщением RELEASE COMPLETE, установить причину в **securityDenied**, или удалить это сообщение. Данное событие также следует занести в журнал регистрации.

Существует неявная сигнализация H.235 для обозначения использования процедуры II и применяемого алгоритма защиты, основывающаяся на значении идентификаторов объекта (см. также пункт 20) и заполненных полей сообщения. В данном тексте идентификаторы объекта символически обозначаются буквами (например, "A").

Данный профиль не использует поля значения проверки целостности (ICV) H.235. Скорее криптографические значения проверки целостности вносятся в поле **signature token** в **cryptoSignedToken**.

6.1 Требования H.323

Предполагается, что объекты H. 323, которые применяют данный профиль защиты цифровой подписи, поддерживают следующие характеристики H.323:

- Быстрое соединение;
- Модель, маршрутизируемая привратником.

7 Цифровые подписи с элементами криптографической пары частный/открытый ключ (процедура II)

Если для обеспечения последовательной защиты используется процедура II, необходимо соблюдать следующие процедуры:

- Для генерирования цифровой подписи наряду с алгоритмом RSA следует использовать алгоритмы SHA1 или MD5. В этом отношении совместное функционирование сетей облегчается при использовании PKCS #1 и PKCS #7.

  Поле **CryptoH323Token** в каждом сообщении RAS/H.225.0 должно содержать следующие поля:

  – **nestedCryptoToken**, содержащее **CryptoToken**, которое содержит **cryptoSignedToken**, содержащее следующие поля:

    - **tokenOID** устанавливается в:
      – "A", указывающее, что вычисление аутентификации/целостности включает в себя все поля в сообщении RAS H.225.0 или в сигнальном сообщении вызова (см. пункт 11);
      – "B", указывающее, что вычисление аутентификации/целостности включает в себя только подмножество полей (см. пункт 10) сообщения RAS/H.225.0 для режима "только аутентификация".
    - **token**, содержащее поля**:**
      – **toBeSigned**, содержащее **EncodedGeneralToken**, которое на самом деле является **ClearToken** со следующими значениями полей:
        - **tokenOID** устанавливается в "S", указывающее, что **ClearToken** используется для аутентификации/целостности/неотказуемости сообщения;
        - **timeStamp** содержит отметку времени;
        - **random** содержит монотонно возрастающий порядковый номер;
        - **generalID** содержит идентификатор получателя (только в случае одноадресного сообщения);
        - **sendersID** содержит идентификатор отправителя;
        - **dhkey**, используемый для прохождения параметров Диффи-Хеллмана, как описано в данной Рекомендации во время установки связи **Setup** to **Connect**:
          – **halfkey** содержит случайный открытый ключ одной из сторон;
          – **modsize** содержит основную часть DH (см. таблицу 4/H.235.6);
          – **generator** содержит группу Диффи-Хеллмана (см. таблицу 4/H.235.6).

          ПРИМЕЧАНИЕ 1. – Когда профиль защиты цифровой подписи используется без профиля защиты шифрования голоса, не следует отправлять параметры Диффи-Хеллмана, **dhkey** должно отсутствовать; значения **halfkey**, **modsize** и **generator** могут быть установлены в {'0'B,'0'B,'0'B}.
        - **certificate** содержит цифровой сертификат отправителя, где в **type** указывается тип сертификата ("V" для сертификатов MD5-RSA или "W" для сертификатов SHA1-RSA), а **certificate** содержит действительный сертификат (см. пункт 14)
        - **algorithmOID** устанавливается в:
          – "V", указывающее использование алгоритма MD5-RSA;
          – "W", указывающее использование алгоритма SHA1-RSA.
        - **params** со значением NULL.
        - **signature**, содержащее подпись, вычисленную с использованием алгоритмов SHA1 или MD5 RSA для всех полей (если значение **tokenOID** – "A", см. пункт 11) или определенных необходимых полей (если значение **tokenOID** – "B", см. пункт 10) сообщения RAS H.225.0 или сообщения сигнализации вызова.

Когда для защиты туннелированных сообщений H323-UU-PDU, включая все содержание сообщения H.245, используется значение "A" **tokenOID**, вычисление подписи должно происходить по всему сообщению сигнализации вызова H.225.0, все поля должны быть заполнены согласно процедуре, описанной в пункте 11. В случае, когда используется значение "B" **tokenOID**, при применении процедуры III достигается аутентификация – только **CryptoToken** (см. пункт 10).

- Объект (который может находиться через один или более переходов), для которого предназначена подпись, проверяет ее.

ПРИМЕЧАНИЕ 2. – Получатель может определить использование процедуры II, оценив значение **algorithmOID** в **cryptoSignedToken** (значения "V" или "W").

8 Процедуры многоточечных конференций

Узел контроля многоточечной связи (MCU) должен поддерживать защищенное распределение сертификатов по запросу оконечных устройств при помощи туннелированных команд H.245 **ConferenceRequest** и **ConferenceResponse**, как описано в 8.8.1/H.235.6. Это позволяет оконечным устройствам запрашивать сертификаты у других оконечных устройств многоточечной конференции и таким образом получать достоверные сведения о подлинности других участников конференции.

Команда **ConferenceRequest** содержит **requestTerminalCertificate**, в котором заданы следующие поля:

- **terminalLabel**: используется в качестве средства адресации удаленного оконечного устройства через MCU;
- **certSelectionCriteria**: отправитель может запрашивать сертификаты только определенных типов;
- **sRandom**: случайный запрос, генерируемый отправителем.

Команда **ConferenceResponse** содержит **terminalCertificateResponse**, в котором заданы следующие поля:

- **terminalLabel**: разрешает соединение возвращаемого сертификата с оконечным устройством.
- **CertificateResponse**: выдает ответ от MCU, в котором установлены следующие поля:
  - **terminalLabel**: идентификация удаленного оконечного устройства;
  - **certificateResponse**: в действительности представляет собой байтовую строку на языке ASN.1 зашифрованную из **EncodedReturnSig** как:
    - **generalID**: идентификация оконечного устройства назначения;
    - **responseRandom**: произвольное значение запроса, сгенерированное MCU;
    - **requestRandom**: воспроизводится **sRandom**;
    - **certificate**: содержит возвращаемый сертификат, где в **type** указывается тип сертификата как идентификатор объекта, а **certificate** содержит цифровой сертификат (см. пункт 14).

9 Сквозная аутентификация (процедура III)

На рисунке 1 показан сценарий, в котором привратники (GK) и конечные точки (EP) отделены друг от друга модулями-посредниками (PXY). Для сквозной аутентификации и аутентификации переход-переход и/или целостности переход-переход используются два различных маркера **CryptoToken**. **CryptoToken** для аутентификации переход-переход применяется только к участку между двумя объектами, и его вычисляют заново на каждом новом участке. С другой стороны, при сквозной аутентификации отсылающая конечная точка генерирует **CryptoToken** только один раз и оно не меняется при прохождении промежуточных узлов сети. Промежуточные узлы сети могут подтверждать правильность цифровых подписей и сертификатов, передаваемых сквозными маркерами **CryptoToken**, и должны пересылать транзитом **CryptoToken**.

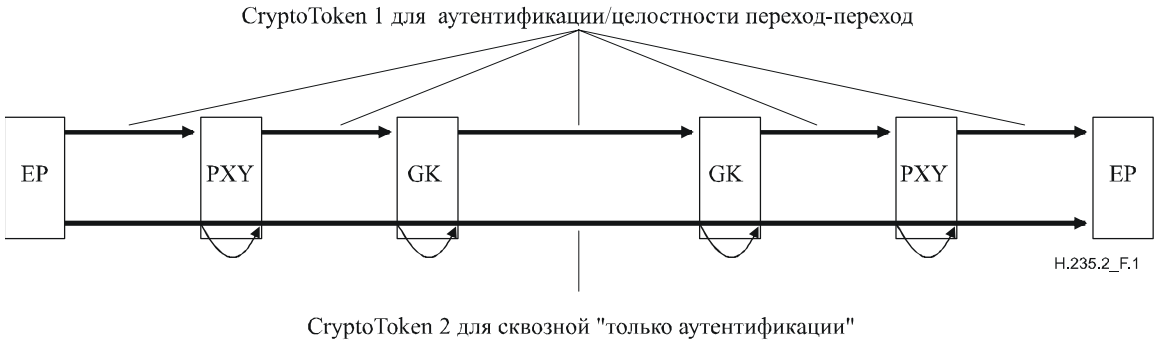

Рисунок 1/H.235.2 – Одновременное использование защиты переход-переход и сквозной аутентификации

ПРИМЕЧАНИЕ 1. – Модуль-посредник может быть отдельным узлом сети, как показано на рисунке 1, или может состоять в функциональной зависимости с другим объектом H.323, например, являться частью привратника.

ПРИМЕЧАНИЕ 2. – В зависимости от **tokenOID**, о котором сообщают, модуль-посредник может определять, предназначено ли полученный **CryptoToken** для модуля-посредника ("S") или для другого получателя ("R").

ПРИМЕЧАНИЕ 3. – Поскольку промежуточные объекты изменяют содержание сообщения сигнализации на каждом участке сети, сквозная целостность невозможна.

Для правильной сквозной аутентификации посредством модулей-посредников H.323 или промежуточных элементов сети, отсылающая конечная точка/оконечное устройство должны вычислять цифровую подпись следующим образом.

Поле **CryptoH323Token** в каждом сообщении RAS/H.225.0 должно содержать следующие поля:

- **nestedCryptoToken**, содержащее **CryptoToken**, которое должно содержать **cryptoSignedToken**, содержащее следующие поля:
  - **tokenOID** устанавливается в:
    - "A", указывающее, что вычисление последовательной аутентификации/целостности включает все поля сообщения RAS/H.225.0 (см. пункт 11);
    - "B", указывающее, что вычисление аутентификации включает только подмножество полей (см. пункт 10) в сообщении RAS H.225.0 или сообщении сигнального вызова для режима "только аутентификация".
- **token**, содержащее поля:
  - **toBeSigned**, содержащее поле **ClearToken**, использованное со следующими полями:
    - **tokenOID**, устанавливается в "R", указывающее на то, что **ClearToken** используется для "только аутентификации"/неотказуемости на сквозной основе;

      ПРИМЕЧАНИЕ 4. – То, какая служба защиты задействована на самом деле, также зависит от битов использования кодов в сертификате.
    - **random** содержит монотонно возрастающее порядковое число;
    - **timeStamp** дополнительно для повышения защиты, только, когда конечные объекты сети синхронизированы по времени;
    - **generalID** содержит идентификатор конечной точки отправителя (только в случае одноадресной передачи). В случае последовательного подтверждения – это идентификатор следующего перехода; в случае сквозной передачи – это идентификатор удаленной конечной точки сети;
    - **sendersID** содержит конечную точку отправителя;
    - **certificate** содержит цифровой сертификат отправителя, где в **type** обозначается тип сертификата ("V" для сертификатов MD5-RSA или"W" для сертификатов SHA1-RSA), а **certificate** содержит действительный сертификат (см. пункт 14);

- **dhkey** используется для прохождения параметров Диффи-Хеллмана, как описано в данной Рекомендации во время установления связи **Setup** to **Connect**:
  - **halfkey** содержит произвольный открытый ключ одной из сторон;
  - **modsize** содержит основную часть DH (см. таблицу 4/H.235.6);

    generator содержит группу Диффи-Хеллмана (см. таблицу 4/H.235.6).

ПРИМЕЧАНИЕ 5. – Когда профиль защиты цифровой подписи используется без профиля защиты шифрования голоса, не следует отправлять параметры Диффи-Хеллмана, и **dhkey** должно отсутствовать; значения **halfkey**, **modsize** и **generator** могут быть установлены в {'0'B,'0'B,'0'B}

- **algorithmOID** устанавливается в:
  - "V", указывающее на использование алгоритма MD5-RSA;
  - "W", указывающее на использование алгоритма SHA1-RSA.
- **params** со значением NULL.
- **signature** содержащее подпись, вычисленную с использованием алгоритмов SHA1 или MD5 RSA во всех полях (если значение **tokenOID** – "A", см. пункт 11) или определенных необходимых полях (если значение **tokenOID** – "B", см. пункт 10) сообщения RAS H.225.0 или сообщения сигнализации вызова.

Модуль-посредник может проверить любую полученную цифровую подпись и/или сертификат и может удалить сообщение, если оно не будет удовлетворять требованиям локальной политики, или модуль-посредник направит полученное **CryptoToken** далее. Для обеспечения защиты переход-переход модуль-посредник должен генерировать новые сигнальные элементы информации H.235 согласно процедурам II и III.

Объект на конце участка (это может быть оконечное устройство) проверяет информацию, полученную в **CryptoToken**, и, в зависимости от наличия сквозных элементов защиты, может дополнительно оценить информацию сквозного **CryptoToken**. Детали процедуры проверки на оконечном устройстве или промежуточном объекте H.323 могут варьироваться в зависимости от локальной политики.

10 Только аутентификация

Оконечные устройства могут применять только аутентификацию (используя OID "B"). В этом случае, аутентификация вычисляется только по подмножеству (**ClearToken** внутри **CryptoToken**) сообщения RAS/H.225.0. Режим "только аутентификация" может быть полезен для правильной сквозной аутентификации (см. пункт 9). В качестве подмножества в структуре **ClearToken** используются следующие поля:

- **tokenOID**: Для применения "только аутентификации" существует отдельный идентификатор объекта (tokenOID "B").
- **random**: монотонно возрастающее порядковое число.
- **timeStamp**: отметка времени.
- **generalID**: идентификатор получателя (только в случае одноадресной передачи). В случае переход - переход – это идентификатор следующего перехода; в случае сквозной передачи – это идентификатор удаленной конечной точки сети.
- **sendersID**: идентификатор отправителя.
- **dhkey**: параметры Диффи-Хеллмана. Это поле и подполя используются во время сообщений установления связи **Setup** to **Connect**.

Аутентификации вычисляется по **ClearToken** внутри **EncodedGeneralToken** (т. е. **ClearToken**) **token cryptoSignedToken**. Цифровая подпись должна вычисляться по битовой строке **ClearToken**, зашифрованной в ASN.1. Перед вычислением цифровой подписи значение **tokenOID** в **ClearToken** должно быть установлено в {0 0}.

11 Аутентификация и целостность

Для обеспечения аутентификации и целостности во всех полях сообщения, зашифрованных языком ASN.1 (с использованием OID "A"), выполняется следующая последовательность действий.

Отправитель сообщения должен вычислять цифровую подпись следующим образом:

1) Занести значение цифровой подписи в специальный заданный по умолчанию шаблон битов фиксированной длины (например, 1024 бита). Это действие зарезервирует место для цифровой подписи максимальной длины, что возможно при данном сертификате. Точная последовательность битов здесь не имеет значения, однако хорошим вариантом является уникальная последовательность, которая не встречается в остальной части сообщения.
2) Зашифровать все сообщение на языке ASN.1; для RAS будет зашифровано все сообщение RAS H.225.0, для сигнализации вызова шифрование будет включать все сообщение сигнализации вызова H.225.0.
3) Разместить заданный по умолчанию шаблон в шифруемом сообщении; перезаписать всю найденную комбинацию битов нулевыми битами.

   ПРИМЕЧАНИЕ 1. – Это не относится к действиям методом проб и ошибок в редких случаях, когда заданная по умолчанию последовательность битов появляется в сообщении более одного раза.
4) Вычислить цифровую подпись для сообщения, зашифрованного на ASN.1, используя метод, указанный в **algorithmOID** как "V" или "W" (см. пункт 12).
5) Подставить вычисленное значение цифровой подписи вместо заданного по умолчанию шаблона в шифруемом сообщении. В случае если цифровая подпись окажется короче, чем зарезервированное место, впереди наиболее важных битов значения цифровой подписи будут поставлены лидирующие нули.

Получатель получает сообщение и действует следующим образом:

1) Декодирует сообщение ASN.1.
2) Извлекает значение полученной цифровой подписи и сохраняет его в качестве локальной переменной SV.
3) Находит значение цифровой подписи в полученном зашифрованном сообщении.

   ПРИМЕЧАНИЕ 2. – В редких случаях, когда подстрока значения цифровой подписи может появляться в сообщении несколько раз, появляется необходимость повторять пункты 3–6, начиная с различных позиций поиска.
4) Перезаписывает нулями шаблон битов в зашифрованном сообщении.
5) Вычисляет цифровую подпись закодированного сообщения, используя метод, указанный в **algorithmOID** как "V" или "W" (см. пункт 12).
6) Сравнивает значения SV с вычисленным значением цифровой подписи. Сообщение считается неискаженным и аутентичным, только если оба значения цифровой подписи равны; в этом случае аутентификация считается успешной и процедура прерывается.
7) В противном случае, пункты 3–7 повторяются, восстанавливается первоначальное значение SV, и ищется другая пара. Если ни одна из пар не дает верного сравнения значений цифровой подписи, аутентификация считается неудавшейся, это означает, что во время передачи в сообщение были внесены изменения (случайно или намеренно), или по другой причине.

12 Вычисление цифровой подписи

Входными данными в процессе генерирования цифровой подписи является битовая строка, зашифрованная на ASN.1, она включает в себя результат процесса вычисления профиля сообщения и частный ключ подписавшегося. Детали генерирования цифровой подписи зависят от используемого алгоритма цифровой подписи; алгоритм цифровой подписи определяется сертификатом; если в сертификате присутствует расширение использования ключа, для того чтобы ключ был подходящим для подписи, должен быть установлен бит **digitalSignature**. Значение цифровой подписи, генерируемое подписавшимся, шифруется в битовой строке и размещается в поле **signature**.

Для вычисления цифровой подписи на основе алгоритма RSA необходимо использовать метод, описанный в [PKCS #1, секция E.8.1.1] с приложением (RSASSA-PKCS1-v1_5-SIGN), а также процедуры OS2IP, RSASP1, I2OSP и метод EMSA-PKCS1-v1_5-ENCODE.

13 Проверка цифровой подписи

В процессе проверки цифровой подписи, входными данными является результат процесса вычисления профиля сообщения и открытый ключ отправителя. Получатель может получить верный открытый ключ любыми способами, но предпочтительным является метод, при котором сертификат извлекается из поля **certificate**, а затем подтверждается при помощи хэш-функции сертификата подписавшегося. Подтверждение открытого ключа отправителя может основываться на обработке пути сертификации (RFC 3280). Детали проверки цифровой подписи зависят от используемого алгоритма цифровой подписи.

Для проверки цифровой подписи на основе алгоритма RSA необходимо использовать метод, описанный в [PKCS #1, секция E.8.1.2] с приложением (RSASSA-PKCS1-v1_5- VERIFY), а также процедуры OS2IP, RSASP1, I2OSP и метод EMSA-PKCS1-v1_5-ENCODE.

14 Управление сертификатами

Для проверки цифровой подписи, получающий объект должен иметь доступ к сертификату отправителя, который подписан признанными органами сертификации (CA). У получателя существует несколько возможностей для получения доступа к сертификату отправителя:

- Сертификат включен в обмен сообщениями, как описано в процедурах II и III; в данном случае, в **certificate** содержится действительный сертификат, а в **type** – OID "V" или OID "W".
- Получатель знает сертификат, возможно сохранившийся от предыдущего обмена сообщениями.
- Вместо того чтобы включать в сообщение сертификат, отправитель высылает URL, где можно найти сертификат. В таком случае, в **certificate** содержится URL, а в **type** стоит OID "P".
- Получатель получает сертификат средствами, не входящими в сферу применения данной Рекомендации (например, при поиске в каталоге LDAP).

Всякий раз когда цифровой сертификат помещается в сообщение, получающий объект (привратник, конечная точка) должны проверить подлинность отправителя (привратника, конечной точки) и подлинность сертификата во избежание атак через посредника.

В случае если сообщения с цифровой подписью посылаются от привратника к конечной точке, для проверки подлинности привратника у конечной точки существует несколько возможностей:

– Если имя хоста доступно, например, в атрибуте общего имени поля subject или поля subjectAltName сертификата, конечная точка может проверить данное имя хоста в отношении к идентификатору привратника. Кроме того, конечная точка может использовать службу DNS, чтобы запросить прикрепленный IP адрес и проверить его в отношении к IP адресу привратника, представленного в ответном подписанном сообщении привратника.

– Например, идентификатор объекта может быть создан на основе IP адреса (представленного в виде 4-х байтового значения в сетевой байтовой системе), связанного с другой идентифицирующей информацией идентификатора привратника, округленного до максимальной длины поля ID отправителя, где располагается идентифицирующая информация привратника. Конечная точка может дополнительно проверить IP адрес, принадлежащий имени хоста в отношении к IP адресу, представленному в заголовке IP ответа привратника.

  ПРИМЕЧАНИЕ. – Данный метод не будет работать должным образом, если в процессе участвуют устройства Network address translation (NAT).

– Если имя хоста в сертификате недоступно, для проведения проверок, описанных выше, необходимо непосредственно брать IP адрес, который будет являться частью сертификата (*iPAddress subjectAltName*).

Чтобы определить, соответствует ли представленный привратником сертификат ожиданиям пользователей, им следует тщательно изучить его. Если конечная точка располагает внешней информацией касательно ожидаемой идентификационной информации привратника, проверку имени хоста можно пропустить. Например, конечная точка связывается с привратником, который имеет динамический адрес и имя хоста, но конечной точке известен сертификат, который будет представлен привратником. В таких случаях важно сократить число разрешенных сертификатов до минимума, чтобы предотвратить атаки через посредника. В особых случаях, для конечной точки было бы удобнее просто игнорировать идентификационную информацию привратника, однако, следует помнить, что это делает соединение уязвимым для активных атак.

Если имя хоста не совпадает с идентификационной информацией в сертификате, конечные точки, ориентированные на пользователя, должны либо уведомить пользователя (в любом случае, конечные точки могут дать пользователю возможность продолжить соединение), или прервать соединение с выводом ошибки сертификата. Автоматизированные конечные точки должны занести ошибку в соответствующий контрольный журнал и прервать соединение (в случае уведомления об ошибке сертификата).

Автоматизированные конечные точки могут обеспечивать настройку конфигурации, которая отключает данную проверку, но должны также обеспечивать настройку, которая включает ее.

Также рекомендуется, чтобы привратник производил проверку идентификации любых сообщений с цифровой подписью, отправленных ему конечной точкой. То, как именно привратник будет выполнять такую проверку, оставляется на усмотрение локальной администрации, и должно быть реализацией политики защиты привратника. Например, имя пользователя, являющееся частью сертификата, может также быть частью идентификатора H.323. Более того, привратник может выполнять перекрестную проверку такой идентификационной информации в отношении к данным по пользователям, администрируемым/конфигурируемым локально, и может основывать свое решение на них.

Если привратник располагает внешней информацией касательно ожидаемой идентификационной информации конечной точки, проверку имени хоста можно пропустить. Например, привратник может связываться с конечной точкой, которая имеет динамический адрес и имя хоста, но привратнику известен сертификат, который будет представлен конечной точкой. В таких случаях важно сократить число разрешенных сертификатов до минимума, чтобы предотвратить атаки – подставы (атаки с человеком посередине). В особых случаях, для привратника было бы удобнее просто игнорировать идентификационную информацию конечной точки, однако, следует помнить, что это делает соединение уязвимым для активных атак.

Если имя хоста не совпадает с идентификационной информацией в сертификате, привратник должен занести ошибку в соответствующий контрольный журнал (если соединение разрешено) и прервать соединение (в случае уведомления об ошибке сертификата).

Если присутствует расширение subjectAltName типа dNSName, можно использовать в качестве идентификационной информации его. В других случаях необходимо использовать особое поле Common Name в поле Subject сертификата. Хотя использование Common Name является существующей практикой, органам сертификации рекомендуется использовать вместо него dNSName.

Сопоставление должно производиться согласно правилам сопоставления, описанным в документе RFC 3280. Если в сертификате присутствует более одной идентификационной информации данного типа (например, более одного имени dNSName), совпадение с одним из них считается допустимым. Имена могут содержать символ обобщения *, для подстановки вместо любого отдельного компонента или фрагмента доменного имени. Например, *.a.com соответствует foo.a.com, но не bar.foo.a.com. f*.com соответствует foo.com но не bar.com.

В процедурах II и III описываются средства для передачи электронного сертификата. Для повышения эффективности работы, необходимо передавать электронные сертификаты объектов не более одного раза, если они еще не доступны посредством других средств, не описанных в данной Рекомендации. Таким образом, обмен сертификатами следует производить только в начале установления соединения: для RAS это происходит либо во время обнаружения привратника либо, если данный этап отсутствует, во время регистрации привратника. В случае быстрого соединения, поскольку.

сертификат может быть включен в первоначальные сообщения сигнализации вызова, его можно благополучно пропустить в последующих сообщениях сигнализации вызова.

Для данного профиля защиты необходимо использовать формат сертификата X.509v3 (1997 г.). Другие форматы сертификатов являются объектом для дальнейшего изучения.

15 Пример использования процедуры II

Рассмотрим случай, представленный на рисунке 2, где каждый объект обладает своей собственной криптографической парой (частный/открытый ключ)/сертификатом. Объект может также обладать многочисленными криптографическими парами. На рисунке конечная точка EP1 отделена от привратника GK1 модулем-посредником H.323.

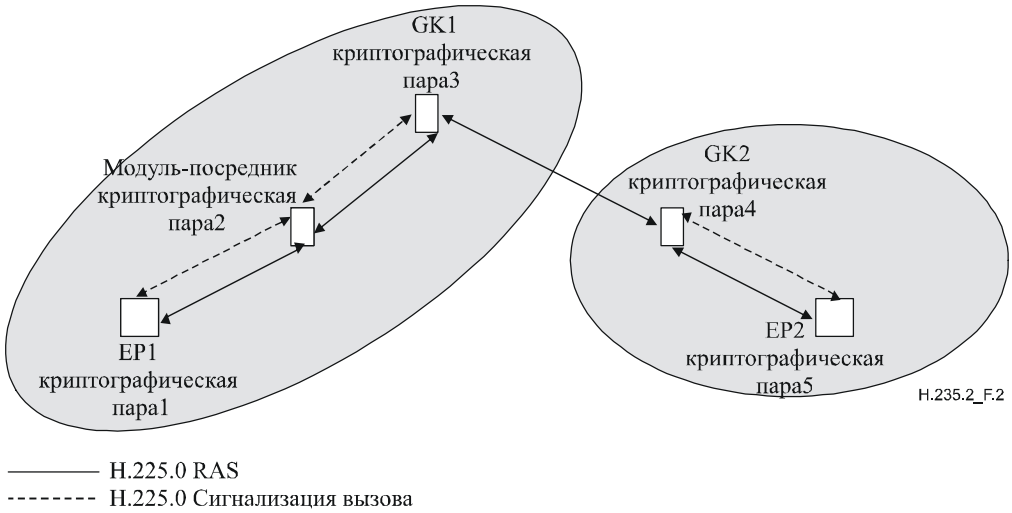

Рисунок 2/H.235.2 – Иллюстрация использования открытого ключа в модели GK-GK

Режим работы модуля-посредника H.323 имеет двойственный характер. С одной стороны, модуль-посредник завершает аутентификацию и целостность на каждом участке сети. Модуль-посредник активно включает недавно вычисленную информацию по аутентификации/целостности в исходящие сообщения RAS таким же образом, как описано в процедуре I H.235.1. С другой стороны, модуль-посредник пропускает сквозную информацию по защите без изменений. Однако модуль-посредник может проверить полученные сертификаты и/или цифровые подписи при передаче.

Ниже мы рассматриваем детали аутентификации, целостности и неотказуемости для сообщений RAS, H.225.0 сигнализации вызова и H.245.

15.1 Аутентификация, целостность и неотказуемость сообщений RAS

Рассмотрим случай связи переход-переход, где конечная точка EP1 желает отправить привратнику GK1 сообщение RAS, скажем сообщение **ARQ**. EP1 генерирует отметку времени и порядковый номер и помещает их в поля **timeStamp** и **random** соответственно, наряду с псевдонимом модуля-посредника в поля **generalID** и **sendersID** EP1. Эти поля присутствуют в поле **ClearToken EncodedGeneralTokens**, в **token cryptoSignedToken CryptoToken** поля **cryptoH323Token** сообщения **ARQ**. **CryptoH323Token** является одним из по крайней мере нескольких маркеров в последовательности **cryptoTokens**. **TokenOID** внутри **cryptoSignedToken** установлено в "A", что означает, что все поля сообщения **ARQ** имеют цифровую подпись. **algorithmOID token** в **cryptoSignedToken** установлен в "V", что указывает на использование алгоритмов шифрования MD5-RSA, или в "W", что указывает на использование алгоритмов SHA1-RSA, в **params** указано значение NULL. Затем EP1 вычисляет цифровую подпись на основе заданного алгоритма вычисления цифровой подписи, используя свой частный ключ. Когда **tokenOID** установлен в "A", подпись вычисляется по всем полям сообщения **ARQ**. Конечная точка EP1 включает вычисленную цифровую подпись в **signature** поля **token** поля **cryptoSignedToken CryptoToken**, присутствующего в **cryptoH323Token** сообщения **ARQ**, и включает его сертификат в поле **certificate**.

Таким же образом для сквозного взаимодействия через модуль-посредник конечная точка EP1 генерирует другой **CryptoToken**, содержащий цифровую подпись, которая охватывает определенные важные поля (см. пункт 9) в **ClearToken** сообщения **ARQ**. **TokenOID** в **CryptoSignedToken** установлен в "B", что указывает на "только аутентификацию" этого **ClearToken**. Затем конечная точка устанавливает **tokenOID** в **ClearToken** в "R", что указывает на сквозную аутентификацию. Также **timeStamp**, **random**, **sendersID**, **generalID** и, в случае **SETUP/CONNECT**, также **dhkey**, устанавливают в **token** заносятся следующие поля: **algorithmOID** в "V" или "W", указывающее алгоритм подписи, **params** в NULL, и **signature** в вычисленное значение цифровой подписи через поля **ClearToken**. **Certificate** несет цифровой сертификат EP1. Затем сообщение **ARQ** посылается модулю-посреднику.

После получения сообщения **ARQ** модуль-посредник проверяет адресованные ему цифровые подписи (в данном случае, скажем, с меткой **tokenOID** "A"). Это основывается на нескольких критериях, среди которых:

- живучесть отметки времени, уникальность **random**;
- идентичность **generalID** и собственного идентификатора;
- разрешение на доступ для **sendersID**;
- сопоставление подписи в сообщении **ARQ** и подписи, вычисленной привратником GK1;
- проверка параметров Диффи-Хеллмана, например, проверка 1024-битового простого числа и генератора на правильность. Тестирование параметров Диффи-Хеллмана на защищенность занимает много времени и может проводиться только по требованию местной администрации;
- проверка полученного сертификата.

Если проверка подписи проходит успешно, модуль-посредник вычисляет новую подпись для того, чтобы вставить ее в сообщение **ARQ** перед тем, как направить его привратнику GK1 следующим образом. Модуль-посредник заменяет поля **timeStamp**, **random**, **sendersID** и **generalID** в поле **ClearToken** (**toBeSigned**), используя значения, существенные для участка модуль-посредник – GK1. Поле **timestamp** содержит текущую отметку времени, поле **random** содержит следующее монотонно возрастающее порядковое число для участка модуль-посредник – GK1, модуля-посредника **sendersID** и поле **generalID** содержат псевдоним GK1. Затем модуль-посредник вычисляет новую цифровую подпись для сообщения **ARQ**, используя секретный ключ и алгоритм подписи, вставляет новую подпись в **signature** внутри **token** и добавляет свой **certificate**. В новое исходящее сообщение модуль-посредник также включает полученное сквозное **CryptoToken** с его **ClearToken** и пересылает сообщение **ARQ** привратнику GK1. Подпись, вычисленная EP1 на основе избранных полей сообщения **ARQ** (метка **tokenOID** – "B") и не предназначенная для модуля-посредника, передается GK1 в сообщении **ARQ** без изменений.

После получения сообщения **ARQ**, GK1 проверяет подписи, вычисляет новую подпись и, после внесения соответствующих изменений в поля **ClearToken** в **toBeSigned**, вставляет ее в поле **signature**, добавляет свой **certificate**, и пересылает сообщение **Setup** конечной точке EP2. И снова GK1 должен передать любую сквозную информацию, полученную в отдельном **CryptoTokens** привратнику GK2, включив эту информацию в отдельное **CryptoToken** без изменений.

15.2 "Только аутентификация" RAS

Рассмотрим случай связи переход-переход, где конечная точка EP1 желает отправить привратнику GK1 сообщение RAS, скажем сообщение **ARQ**. EP1 генерирует отметку времени и порядковый номер и включает их в поля **timeStamp** и **random** соответственно, в поле **generalID** вносится псевдоним EP1, а в **sendersID** – идентификатор EP1. Данные поля присутствуют в поле **ClearToken toBeSigned**, присутствующего в **token** в **cryptoSignedToken CryptoToken** поля **cryptoH323Token** сообщения **ARQ**. **TokenOID** в **cryptoSignedToken** установлен в "B", что указывает, что только некоторое подмножество полей в **ClearToken** имеет цифровую подпись. **AlgorithmOID token** в **cryptoSignedToken** установлен в "V", что указывает на использование алгоритмов MD5-RSA, или в "W", что указывает на использование алгоритмов SHA1-RSA, значение **params** установлено в NULL. Затем EP1 вычисляет цифровую подпись на основе алгоритма вычисления цифровой подписи, используя свой секретный ключ. Цифровая подпись высчитывается для определенных полей **ClearToken** сообщения **ARQ**. EP1 включает вычисленную цифровую подпись в **signature** поля **token**

поля **cryptoSignedToken CryptoToken**, присутствующего в **cryptoH323Token** сообщения **ARQ**, и добавляет свой **certificate**.

Таким же образом EP1 генерирует другую цифровую подпись для сквозной аутентификации, охватывающей определенные поля **ClearToken** в отдельном **CryptoToken** сообщения **ARQ**. Также включается эта цифровая подпись (идентифицируемая значениями **tokenOID** "V" или "W"). Затем сообщение **ARQ** посылается модулю-посреднику.

После получения сообщения **ARQ**, модуль-посредник проверяет цифровую подпись адресованных ему (в данном случае, скажем, значением "B" **tokenOID**). Данный процесс основывается на нескольких критериях, среди которых:

- живучесть отметки времени, уникальность **random**;
- идентичность **generalID** и собственного идентификатора;
- разрешение на доступ для **sendersID**;
- сопоставление подписи в сообщении **ARQ** и подписи, вычисленной привратником GK1;
- проверка полученного сертификата.

Если проверка цифровой подписи прошла успешно, модуль-посредник вычисляет новую подпись для вставки в сообщение **ARQ** перед тем, как переслать ее GK1 следующим образом. Модуль-посредник заполняет поля **timeStamp**, **random**, **sendersID** и **generalID** в поле **ClearToken toBeSigned**, используя значения, существенные для участка модуль-посредник – GK1. Поле **timestamp** содержит текущую отметку времени, поле **random** содержит следующее монотонно возрастающее порядковое число для участка модуль-посредник – GK1, а поле **generalID** содержит псевдоним GK1. Затем модуль-посредник вычисляет новую цифровую подпись для **ClearToken**, используя секретный ключ или алгоритмы цифровой подписи MD5-RSA или SHA1-RSA (**algorithmOID** ="V" или "W"), вставляет ее в **signature token cryptoSignedToken**, добавляет свой **certificate** и пересылает сообщение **ARQ** привратнику GK1. Цифровая подпись, вычисленная EP1 на основе избранных полей **ClearToken** сообщения **ARQ** (значение **tokenOID** – "B") и не предназначенная для модуля-посредника, также передается GK1 в сообщении **ARQ** без изменений.

После получения сообщения **ARQ**, GK1 проверяет подпись, вычисляет новую подпись после внесения соответствующих изменений в поля **ClearToken** в **toBeSigned**, вставляет ее в **по**ле **signature** и передает сообщение **Setup** EP2. Сквозная информация от EP1 включается в сообщение **Setup** без изменений.

15.3 Аутентификация, целостность и неотказуемость сообщений H.225.0

Процедура для сообщений H.225.0 аналогична процедуре для сообщений RAS. Разница лишь в том, что, когда значение в **tokenOID** установлено в "B", подмножество полей для цифровой подписи идентифицируется для каждого сообщения сигнализации вызова H.225.0.

15.4 Аутентификация и целостность сообщений H.245

Рассмотрим случай, где EP1 желает послать EP2 сообщение H.245, скажем сообщение **TerminalCapabilitySet**. EP1 проверяет, необходимо ли посылать модулю-посреднику сообщение H.225.0. Если да, то сообщение H.245 туннелируется в сообщение H.225.0. Поля сообщения H.225.0 заполняются, как было описано ранее для передачи сообщения H.225.0. Поскольку сообщение H.245 туннелируется, поля **h323-uu-pdu** в сообщении **h323-UserInformation** заполняются следующим образом:

- в поле **h323-message-body** указывается тип передаваемого сообщения H.225.0.
- **h245Tunnelling** установлено в TRUE.
- **h245Control** содержит байтовую строку H.245 PDU.

Однако, если передачи сообщения H.225.0 не ожидается, сообщение H.245 туннелируется в специальное сообщение **facility** H.225.0. Поля **h323-uu-pdu** в сообщении **h323-UserInformation** заполняются следующим образом:

- поле **h323-message-body** установлено в **facility**, которое содержит:
  - **reason** установлено в **undefinedReason**;
  - **tokens** и **cryptoTokens**, установлены также как для любого сообщения H.225.0.
- **h245Tunnelling** установлено в TRUE.
- **h245Control** содержит байтовую строку H.245 PDU.

Затем сообщение **facility** передается конечной точкой EP1 модулю-посреднику.

В обоих случаях (когда ожидается передача сообщения H.225.0 или используется специальное сообщение **facility** H.225.0) после получения сообщения модуль-посредник проверяет предназначенную для него цифровую подпись (в данном случае, описываемую значением "A" **tokenOID**). Затем, если для участка модуль-посредник – GK1 ожидается передача сообщения H.225.0, сообщение H.245 туннелируется в данное сообщение; в противном случае сообщение туннелируется в специальное сообщение **facility** H.225.0. Как и в случае передачи любого сообщения сигнализации вызова H.225.0, вычисление новой цифровой подписи для сообщения H.225.0 происходит раньше передачи этого сообщения от модуля-посредника GK1. Подпись, отправленная EP1 модулю-посреднику и не предназначенная для него, передается модулем-посредником на GK1 без изменений.

В данном пункте резюмируется то, как и какими средствами профиль цифровой подписи обеспечивает защиту различных сигнальных сообщений H.323.

16 Совместимость с H.235 версии 1

Хотя данные профили защиты разрабатывались на основе Рекомендации H.235 версии 2 (Рек. МСЭ-Т H.235v2), возможно применение данных профилей защиты для Рекомендации H.235 версии 1 (Рек. МСЭ-Т H.235v1) с небольшими изменениями. Получатель может распознать присутствие версии протокола H.235 отправителя, оценив идентификаторы объекта профиля защиты (см. пункт 20).

Реализация Рекомендации H.235 версия 1 (Рек. МСЭ-Т H.235v1):

- значения в **sendersID ClearToken** не устанавливаются или не оцениваются.

17 Многоадресный режим

Многоадресные сообщения H.225.0 такие, как **GRQ** или **LRQ**, должны включать **CryptoToken** согласно процедурам II и III, где значение **generalID** не установлено. Если такие сообщения участвуют в одноадресной передаче, данное сообщение должно включать **CryptoToken**.

18 Список защищенных сообщений сигнализации

18.1 Сообщения RAS H.225.0

Сообщения RAS H.225.0	Сигнальные поля H.235	Только аутентификация	Аутентификация и целостность	Неотказуемость
Любое	cryptoTokens	Процедура II/III	Процедура II/III	Процедура II/III

ПРИМЕЧАНИЕ. – При одноадресной передаче процедуры II или III нужно применять с использованием полей защиты в **CryptoToken**.

18.2 Сообщения сигнализации вызова H.225.0

H.225.0 сообщение сигнализации вызова	Сигнальные поля H.235	Только аутентификация	Аутентификация и целостность	Неотказуемость
Alerting-UUIE, CallProceeding-UUIE, Connect-UUIE, Setup-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	cryptoTokens	Процедура II/III	Процедура II/III	Процедура II/III

19 Использование sendersID и generalID

ClearToken содержит поля **sendersID** и **generalID**. Если идентификационная информация доступна, в **sendersID** должно быть установлено в значение идентификатора привратника (GKID) для сообщения, исходящего от привратника, и значение идентификатора конечной точки (EPID) для сообщения, исходящего от конечной точки. Если идентификационная информация доступна, в **generalID** должно быть установлено в значение GKID для сообщений, исходящих от конечной точки, и EPID для сообщений, исходящих от привратника. Если идентификационная информация недоступна, или в случае неоднозначности широковещательной/многоадресной рассылки, данное поле пропускается или должно содержать нулевую строку. В таблице 2 суммируется вышесказанное:

Таблица 2/H.235.2 – Использование sendersID и GeneralID

Сообщение	sendersID	generalID
Одноадресное **GRQ**	**EPID**, если доступна, иначе **NULL**	**GKID**
Многоадресное **GRQ**	**EPID**, если доступна, иначе **NULL**	
GCF, **GRJ**	**GKID**	**EPID**, если доступна, иначе **NULL**
Первоначальное **RRQ**		**GKID**
RCF	**GKID**	**EPID**
RRJ	**GKID**	
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (EP-to-GK)	**EPID**	**GKID**
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (GK-to-EP)	**GKID**	**EPID**
ARQ, IRQ, RAI	**EPID**	**GKID**
ACF, ARJ, BCF, LCF, LRJ, IRR, IRQ, RAC, LCF, LRJ, IACK, INAK	**GKID**	**EPID**

Таблица 2/H.235.2 – Использование sendersID и GeneralID

Сообщение	sendersID	generalID
Одноадресное **LRQ** (EP-to-GK)	**EPID**	**GKID**
Одноадресное **LRQ** (GK-to-GK)	**GKID**	**GKID**
Многоадресное **LRQ**	**EPID**	
ПРИМЕЧАНИЕ. – GKID обозначает идентификатор привратника, EPID обозначает идентификатор конечной точки. Пустое место обозначает пропуск или нулевую строку идентификации.		

20 Список идентификаторов объекта

В таблице 3 приводится список всех идентификаторов OID, рассмотренных в данной рекомендации (см. также [OIW] и [WEBOIDs]). Здесь приводятся идентификаторы объекта для Рекомендаций H.235v1 и H.235v2.

Таблица 3/H.235.2 – Идентификаторы объекта

Обозначение идентификатора объекта	Значение(я) идентификатора объекта	Описание
"A"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 1} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 1}	Используется в процедуре II для **CryptoToken**-tokenOID, указывает, что подпись включает **все** поля сообщения RAS H.225.0 или сообщения сигнализации вызова (аутентификация и целостность).
"B"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 2} {itu-t (0) recommendation (0) h (8) 235 version (0) 2 2} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 2}	Используется в процедуре II для **CryptoToken**-tokenOID, указывает, что подпись включает **подмножество** полей в сообщении RAS/H.225.0 (ClearToken) для оконечных устройств "только аутентификация", без целостности. Используется в процедуре IA H.235.1 для CryptoToken-tokenOID, указывает, что хэш-функция включает подмножество полей в сообщении RAS/H.225.0 (ClearToken) для оконечных устройств "только аутентификация" без целостности.
"P"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 4} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 4}	Используется в процедурах II или III для обозначения, что **certificate** передает URL.
"R"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 3} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 3}	Используется в процедуре II для ClearToken-tokenOID, указывает, что ClearToken используется для сквозной аутентификации/целостности.

Таблица 3/H.235.2 – Идентификаторы объекта

Обозначение идентификатора объекта	Значение(я) идентификатора объекта	Описание
"S"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 7} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 7}	В процедуре II эта метка OID указывает аутентификацию, целостность и неотказуемость сообщения.
"V"	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}	Используется в процедуре II или процедуре III в качестве алгоритма OID, указывающего использование цифровой подписи MD5 RSA.
"W"	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}	Используется в процедуре II или процедуре III в качестве алгоритма OID, указывающего использование цифровой подписи SHA1 RSA.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	**Аудиовизуальные и мультимедийные системы**
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2007 г.