Международный союз электросвязи

МСЭ-Т X.1341

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2015)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги – Рекомендации, связанные с PKI

Протоколы пересылки сертифицированной электронной почты и сертифицированного почтового отделения

Рекомендация МСЭ-Т X.1341

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	**X.1340–X.1349**
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

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

Рекомендация МСЭ-Т X.1341

Протоколы пересылки сертифицированной электронной почты и сертифицированного почтового отделения

Резюме

В Рекомендации МСЭ-Т X.1341 определены протокол пересылки сертифицированной электронной почты (CMTP) и протокол сертифицированного почтового отделения (CPOP) в целях содействия защищенному обмену сообщениями электронной сертифицированной почты в мире благодаря обеспечению конфиденциальности, идентификации корреспондентов, целостности и предотвращению отказа от авторства.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1341	17.09.2015 г.	17-я	11.1002/1000/12352

Ключевые слова

Протокол пересылки сертифицированной электронной почты, протокол сертифицированного почтового отделения, CMTP, конфиденциальность, CPOP, целостность, фиксация авторства, POP, протокол почтового отделения, безопасность, простой протокол пересылки электронной почты, SMTP.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). 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 осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное 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/.

СОДЕРЖАНИЕ

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	2
3.1	Термины, определенные в других документах	2
3.2	Термины, определенные в настоящей Рекомендации	2
4	Сокращения и акронимы	3
5	Условные обозначения	4
6	Базовые понятия сертифицированной почты	4
7	Типы команд сертифицированной почты	4
7.1	Типы команд CMTP	5
7.2	Типы команд CPOP	6
8	Подробная спецификация CMTP	7
8.1	CELO – запрос списка типов доставки	7
8.2	Список типов доставки	7
8.3	Выбранный тип доставки	8
8.4	Подтверждение типа доставки	8
8.5	Адрес электронной почты отправителя	8
8.6	Подтверждение адреса электронной почты отправителя	8
8.7	Запрос на отправку электронной почты получателю	8
8.8	Проверка адреса электронной почты получателя удаленным сервером Cmail	8
8.9	Подтверждение адреса электронной почты получателя	9
8.10	Подтверждение электронной почты получателя	9
8.11	Запрос на отправку конверта	10
8.12	Готовность к приему конверта	10
8.13	Конверт (ENVELOPE)	10
8.14	Подписанное сервером уведомление о помещении в почтовый ящик	10
8.15	Подписанное отправителем и сервером уведомление о помещении в почтовый ящик	10
8.16	Пересылка конверта между серверами Cmail	11
8.17	Подписанное уведомление о транзите между серверами Cmail	11
8.18	Подписанное уведомление о транзите	12
9	Протокол сертифицированного почтового отделения (CPOP)	12
9.1	Запрос ожидающих сообщений	12
9.2	Запрос уведомления о приеме, подписанного получателем и сервером	12
9.3	Ответ на запрос и уведомление о приеме, подписанное получателем и сервером	13
9.4	Конверт	14
9.5	Подписанное получателем и сервером уведомление о приеме при передаче между серверами Cmail (факультативно)	14
9.6	Подписанное получателем и сервером уведомление о приеме	14

Стр.

Приложение A – Уведомления в формате определения схемы XML (XSD) 15
A.1 Обзор XSD 15
A.2 Формальная спецификация уведомлений в формате XSD 18
Приложение B – Уведомления в формате ASN.1 21
Приложение C – Требования к компонентам инфраструктуры открытых ключей 25
C.1 Введение 25
C.2 Сертификаты открытых ключей конечного объекта сервера Cmail 25
C.3 Сертификаты открытых ключей конечного объекта клиента Cmail 25
C.4 Требования к проверке информации 26
Приложение D – Требования к безопасности транспортного уровня (TLS) 27
Приложение E – Идентификаторы объектов, определенные в настоящей Рекомендации 28
Дополнение I – Формат конверта и уведомлений 29
I.1 Уведомление о помещении в почтовый ящик 29
I.2 Уведомление о приеме 29
I.3 Уведомление о транзите 30
I.4 Конверт (ENVELOPE) 31
Библиография 32

Введение

Настоящая Рекомендация расширяет возможности простого протокола пересылки электронной почты (SMTP) и протокола почтового отделения версии 3 (POP3), добавляя в них поддержку аутентификации, безопасности и предотвращения отказа от авторства.

Для этих целей определены два протокола:

– протокол пересылки сертифицированной электронной почты (CMTP), являющийся расширением простого протокола пересылки электронной почты (SMTP), – протокол связи между отправителем электронной почты и почтовым сервером, называемым сервером сертифицированной почты (Cmail);

– протокол сертифицированного почтового отделения (CPOP), являющийся расширением протокола почтового отделения версии 3 (POP3), – протокол связи между получателем электронной почты и сервером Cmail.

В протоколах SMTP и POP3 тип сообщения определяется командой, то есть ключевым словом в начале сообщения. Для протоколов CMTP и CPOP были определены новые команды и расширена функциональность некоторых команд SMTP и POP3. В частности, в некоторые команды добавлена доставка уведомлений (электронных документов), позволяющих документировать и верифицировать различные этапы связи от отправителя к получателю.

Протоколы CMTP и CPOP также вводят понятие сервера Cmail, который является активным участником связи между отправителем и получателем и позволяет удостоверить тот факт, что обмен между двумя сторонами действительно состоялся.

Использование сертифицированной почты предполагает существование действующей инфраструктуры отрытых ключей (PKI).

Приложение A, которое является неотъемлемой частью настоящей Рекомендации, содержит формальную спецификацию уведомлений с использованием метода нотации определения схемы XML (XSD).

Приложение B, которое является неотъемлемой частью настоящей Рекомендации, содержит формальную спецификацию уведомлений с использованием абстрактной синтаксической нотации версии 1 (ASN.1).

Приложение C, которое является неотъемлемой частью настоящей Рекомендации, содержит описание требований к сертификатам открытых ключей, выдаваемым клиентам (отправитель и получатель электронной почты) и серверам Cmail.

Приложение D, которое является неотъемлемой частью настоящей Рекомендации, содержит описание требований к использованию спецификации безопасности транспортного уровня (TLS).

Приложение E, которое является неотъемлемой частью настоящей Рекомендации, содержит описание идентификаторов объектов, определенных для серверов Cmail.

Рекомендация МСЭ-Т X.1341

Протоколы пересылки сертифицированной электронной почты и сертифицированного почтового отделения

1 Сфера применения

В настоящей Рекомендации определено, как сделать отправляемые по электронной почте сообщения надежными в аспекте идентификации и конфиденциальности.

Протокол пересылки сертифицированной электронной почты/протокол сертифицированного почтового отделения (CMTP/CPOP) обеспечивает возможность:

– решения вопросов отказа от авторства путем использования электронной подписи;

– решения вопросов конфиденциальности путем использования шифрования;

– формирования надежных уведомлений о помещении сообщения в почтовый ящик, транзите этого сообщения и его приеме;

– использования сервера сертифицированной почты (Cmail) для отслеживания сертифицированной почты в целях предотвращения ее потери в ходе процесса;

– использования при соединениях механизм безопасности транспортного уровня (TLS) для обеспечения более надежной идентификации; такой более надежный уровень идентификации является требованием сервера Cmail.

Соответствие настоящей Рекомендации не следует рассматривать в качестве какого-либо доказательства заявленного соблюдения любых национальных или региональных законов, норм или политики. Описанные в настоящей Рекомендации технические, организационные и процедурные средства ни в коей мере не гарантируют создания какого-либо уровня безопасности, который может налагаться на определенную корреспонденцию в соответствии с конкретным национальным или региональным законом, нормой или политикой.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.520] Рекомендация МСЭ-Т X.520 (2012 г.) | ISO/IEC 9594-6:2014, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Избранные типы атрибутов.*

[ITU-T X.680] Рекомендация МСЭ-Т X.680 (2008 г.) | ISO/IEC 8824-1:2008, *Информационная технология – Абстрактная синтаксическая нотация № 1: спецификация базовой нотации.*

[ITU-T X.690] Рекомендация МСЭ-Т X.690 (2008 г.) | ISO/IEC 8825-1:2008, *Информационная технология – Правила кодирования ASN.1: спецификация базовых правил кодирования (BER), канонических правил кодирования (CER) и отличительных правил кодирования (DER).*

[ITU-T X.693] Рекомендация МСЭ-Т X.693 (2008 г.) | ISO/IEC 8825-4:2008, *Информационная технология – Правила кодирования ASN.1: правила кодирования языка XML (XER).*

[ISO 3166-1] ISO 3166-1:2013, *Коды для представления названий стран и единиц их административно-территориального деления. Часть 1. Коды стран*.

[IETF RFC 822] IETF RFC 822 (1982), *Standard for the format of ARPA Internet text messages.*

[IETF RFC 1939] IETF RFC 1939 (1996), *Post office protocol – Version 3*.

[IETF RFC 2045] IETF RFC 2045 (1996), *Multipurpose internet mail extensions (MIME) – Part One: Format of internet message bodies*.

[IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) Protocol – Version 1.2*.

[IETF RFC 5321] IETF RFC 5321 (2008), *Simple mail transfer protocol*.

[XML] W3C Recommendation XML1.0 (2008), *Extensible markup language (XML) 1.0 (fifth edition).*

[XSD] W3C Recommendation XML Schema (2012), *XML schema Part 1: Structures*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 орган сертификации (certification authority) (CA) [b-ITU-T X.509]: Орган, которому одним или несколькими пользователями доверено создание и присвоение сертификатов открытых ключей. Дополнительно орган сертификации может создавать ключи пользователя.

3.1.2 проверка сертификата (certificate validation) [b-ITU-T X.509]: Процесс проверки того, что сертификат был действителен на заданный момент времени, возможно включающий создание и обработку тракта сертификации и проверку того, что все сертификаты в данном тракте были действительны (то есть не были просрочены или аннулированы) на тот заданный момент времени.

3.1.3 хэш-функция (hash function) [b-ITU-T X.509]: (Математическая) функция, отображающая значения из большой (возможно очень большой) области в меньший диапазон значений. Хэш-функция считается "хорошей", если результаты ее применения к (большому) множеству значений в области будут равномерно (и, очевидно, случайным образом) распределены по диапазону.

3.1.4 частный ключ (private key) [b-ITU-T X.509]: (В криптосистеме с открытыми ключами) тот ключ пары ключей объекта, который известен только данному объекту.

3.1.5 открытый ключ (public key) [b-ITU-T X.509]: (В криптосистеме с открытыми ключами) тот ключ пары ключей пользователя, который общеизвестен.

3.1.6 сертификат открытого ключа (public-key certificat) (PKC) [b-ITU-T X.509]: Открытый ключ пользователя в совокупности с некоторой дополнительной информацией, воспроизводимой, без возможности фальсификации, при помощи цифровой подписи с открытым ключом выдавшего его CA.

3.1.7 инфраструктура открытых ключей (public-key infrastructure) (PKI) [b-ITU-T X.509]: Инфраструктура, способная поддерживать управление открытыми ключами для обеспечения услуг аутентификации, шифрования, целостности или фиксации авторства.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 сертифицированная почта (certified mail): Электронная почта, передаваемая с использованием протокола пересылки сертифицированной электронной почты (CMTP) и протокола сертифицированного почтового отделения (CPOP).

3.2.2 протокол пересылки сертифицированной электронной почты (certified mail transfer protocol) (CMTP): Протокол прикладного уровня, работающий поверх соединения протокола управления передачей/протокола Интернет (TCP/IP), который основан на простом протоколе пересылки электронной почты (SMTP) и используется для отправки сертифицированной почты.

3.2.3 протокол сертифицированного почтового отделения (certified post office protocol) (CPOP): Протокол прикладного уровня, работающий поверх соединения протокола управления передачей/протокола Интернет (TCP/IP), который основан на протоколе почтового отделения версии 3 (POP3) и используется для приема сертифицированной почты.

3.2.4 сервер Cmail (Cmail server): Доверенный объект, задействованный в транзакциях с сертифицированной почтой.

3.2.5 уведомление о помещении в почтовый ящик (notice of deposit): Электронный документ, подписанный отправителем и сервером Cmail и содержащий информацию, которая позволяет удостоверить факт помещения сертифицированной почты в почтовый ящик.

3.2.6 уведомление о приеме (notice of reception): Электронный документ, подписанный получателем и сервером Cmail и содержащий информацию, которая позволяет удостоверить факт получения адресатом сертифицированной почты.

3.2.7 уведомление о транзите (notice of transit): Электронный документ, подписанный участвующими в транзакции серверами Cmail и содержащий информацию, которая позволяет удостоверить факт передачи сертифицированной почты серверу Cmail.

3.2.8 протокол почтового отделения версии 3 (post office protocol v3) (POP3): Протокол прикладного уровня, работающий поверх соединения протокола управления передачей/протокола Интернет (TCP/IP), который используется для приема электронной почты.

3.2.9 простой протокол пересылки электронной почты (simple mail transfer protocol) (SMTP): Протокол прикладного уровня, работающий поверх соединения протокола управления передачей/протокола Интернет (TCP/IP), который используется для отправки электронной почты.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AES	Advanced Encryption Standard	Усовершенствованный стандарт шифрования
ASN.1	Abstract Syntax Notation One	Абстрактная синтаксическая нотация версии 1
CA	Certification Authority	Орган сертификации
CBC	Cipher Block Chaining	Сцепление блоков шифротекста
Cmail	Certified Mail	Сертифицированная почта
CMTP	Certified Mail Transfer Protocol	Протокол пересылки сертифицированной электронной почты
CPOP	Certified Post Office Protocol	Протокол сертифицированного почтового отделения
DER	Distinguished Encoding Rules	Отличительные правила кодирования
DNS	Domain Name System	Система наименований доменов
id	Identity	Идентичность
MIME	Multipurpose Internet Mail Extensions	Многоцелевые расширения электронной почты интернета
PKI	Public-Key Infrastructure	Инфраструктура открытых ключей
POP3	Post Office Protocol version 3	Протокол почтового отделения версии 3
RSA	Rivest, Shamir and Adleman algorithm	Алгоритм Ривеста, Шамира и Адлемана
RSCK	Random Symmetric Cypher Key	Случайный симметричный криптографический ключ
S/MIME	Secure/Multipurpose Internet Mail Extensions	Защищенные многоцелевые расширения электронной почты интернета

SMTP	Simple Mail Transfer Protocol	Простой протокол пересылки электронной почты
TCP/IP	Transmission Control Protocol/Internet Protocol	Протокол управления передачей/протокол Интернет
TLS	Transport Layer Security	Безопасность транспортного уровня
UTF-8	Universal Character Set Transformation Format-8	Формат преобразования универсального набора символов, 8-битовая форма
XER	XML Encoding Rules	Правила кодирования XML
XML	eXtensible Markup Language	Расширяемый язык разметки
XSD	XML Schema Definition	Определение схемы XML

5 Условные обозначения

Отсутствуют.

6 Базовые понятия сертифицированной почты

При традиционном обмене электронной почтой с использованием простого протокола пересылки электронной почты (SMTP) и протокола почтового отделения версии 3 (POP3) получатель электронной почты может отрицать факт получения почты. Это возможно даже в том случае, когда к стеку протоколов добавляются защищенные многоцелевые расширения электронной почты интернета (S/MIME). Расширения S/MIME обеспечивают шифрование сообщений и аутентификацию отправителя, но не обеспечивают доказательства доставки.

В настоящей Рекомендации определяется стек протоколов, называемый сертифицированной почтой, который включает протокол пересылки сертифицированной электронной почты (CMTP) и протокол сертифицированного почтового отделения (CPOP).

При обмене с использованием SMTP и POP3 почтовый сервер не является активным участником обмена, он осуществляет пересылку сообщений без изменений при регистрации пользователя на почтовом сервере. Это справедливо и в случае использования S/MIME.

В системе сертифицированной почты почтовый сервер является активным участником обмена между отправителем и получателем таким образом, который позволяет серверу Cmail верифицировать факт согласия получателя принять почтовое сообщение. Почтовые сообщения отправляются в зашифрованном виде, что не позволяет серверу Cmail читать содержимое электронной почты. Общее описание процедуры изложено ниже, а подробная спецификация приведена в разделе 8.

Описание взаимодействия отправителя и сервера Cmail приведено в разделе 8.

Описание взаимодействия получателя и сервера Cmail приведено в разделе 9.

7 Типы команд сертифицированной почты

В системе сертифицированной почты используется сочетание команд текущих реализаций протоколов SMTP и POP3, некоторых расширенных команд SMTP и POP3, а также ряда специальных команд сертифицированной почты. Команды, которые не имеют эквивалентов в протоколах SMTP/POP3, отмечены в таблицах 1 и 2 как "дополнительные". Команды, являющиеся расширенными версиями команд протоколов SMTP/POP3, отмечены как "измененные". Команды протоколов SMTP/POP3, которые используются без изменений, отмечены как "неизмененные".

Тип команды задается в виде ключевого слова, написанного заглавными буквами, которое определяет тип конкретного сообщения наряду с некоторыми дополнительными характеристиками данного типа сообщения.

7.1 Типы команд CMTP

Таблица 1 − Команды CMTP

Команда	Функция команды
CELO Дополнительная	Разрешает серверу определить свой процесс обработки команд CMTP
DELV Дополнительная	Определяет режим доставки certifiedMail
MAIL FROM Измененная	Указывает отправителя сообщения; используется в формате MAIL FROM. Если на сервере существует учетная запись, сервер в ответ отправляет сертификат открытого ключа известного отправителя в кодировке base64
RCPT TO Измененная	Указывает получателей сообщения; используется в формате RCPT TO. Если на сервере существует учетная запись, сервер в ответ отправляет сертификат открытого ключа известного отправителя в кодировке base64. Если учетная запись существует на другом сервере CMTP, с которым был произведен обмен ключами, то сервер опрашивает этот другой сервер и отправляет ему сертификат открытого ключа в кодировке base64, принадлежащего известному получателю, с помощью команды CHCK RCPT
CHCK RCPT Дополнительная	Направляется только в том случае, когда получатель и отправитель зарегистрированы на разных серверах Cmail
DATA Измененная	Направляется клиентом для инициирования передачи содержимого сообщения. Сервер возвращает уведомление о помещении письма в почтовый ящик, которое подписано сервером и должно быть подписано отправителем
DEPO Дополнительная	Направляется клиентом для инициирования передачи содержимого подписанного сервером уведомления о помещении письма в ящик, которое было подписано также отправителем
SEND EVLP Дополнительная	Осуществляет пересылку конверта от одного сервера Cmail к другому
HELP Неизмененная	Возвращает список команд, поддерживаемых сервером CMTP
QUIT Неизмененная	Завершает сеанс связи

7.2 Типы команд CPOP

Таблица 2 − Команды CPOP

Команда	Функция команды
USER Неизмененная	Используется для указания имени пользователя, осуществляющего регистрацию в системе
PASS Неизмененная	Пароль пользователя, осуществляющего регистрацию в системе
LIST Измененная	Используется для отображения списка сообщений и их совокупного размера. Например, вызов команды LIST без параметров вернет +OK 2 сообщения (320 октетов) и список сообщений: идентификатор (id), длина и режим доставки (если указан), например CertifiedMail
RETR Измененная	Здесь *N* – число от 1 до последнего числа из списка, возвращенного командой LIST. Данная команда не может использоваться для получения сообщения, помеченного как удаленное. Если тип доставки не указан, сервер отправляет электронную почту, используя кодировку многоцелевых расширений электронной почты интернета (MIME). Если режим доставки определен, сервер обрабатывает сообщение соответствующим образом. Например, в случае режима доставки CertifiedMail сервер проверяет получателя до отправки конверта, используя команду RCPT
CHLG RESP Дополнительная	Направляется клиентом для выдачи уведомления о приеме сообщения и выдачи ответа на секретный вопрос. Если дан верный ответ, сервер направляет в ответ конверт MIME
SEND NORP Дополнительная	Направляет подписанное уведомление о приеме сообщения
HELP Неизмененная	Возвращает список команд, поддерживаемых сервером CPOP
QUIT Неизмененная	Завершает сеанс связи

8 Подробная спецификация CMTP

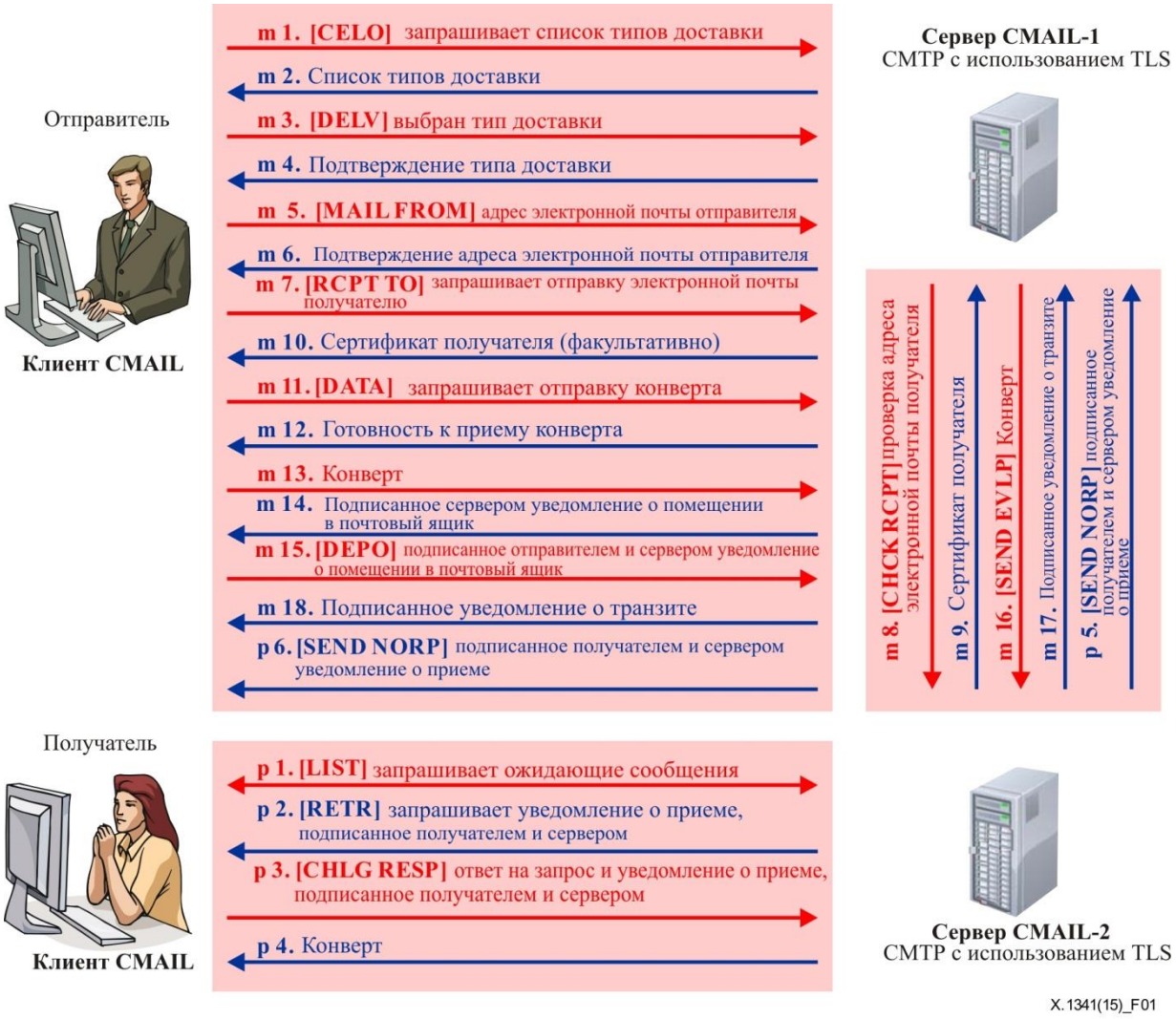

Рисунок 1 – Общая схема обмена данными

Команды с префиксом "m" используются в протоколе CMTP, а команды с префиксом "p" – в протоколе CPOP. В пунктах 8.1–8.18 приведено подробное описание обмена по командам m 1 – m 18 на рисунке 1, а в пункте 9 – по командам p 1 – p 6.

8.1 CELO – запрос списка типов доставки

Тип команды направляется как сообщение SMTP аналогично команде HELO, за которым следует полностью определенное наименование домена. Команда предназначена для получения списка типов доставки.

8.2 Список типов доставки

Список типов доставки выдается в ответ на команду CELO. Список выдается в формате SMTP и имеет следующее содержимое (без учета регистра):

250-<полностью определенное наименование домена сервера Cmail>

250-8BITMIME

250-Delivery-Types CertifiedMail <прочие типы доставки>

250 OK

Настоящая Рекомендация содержит спецификацию только для CertifiedMail. Дальнейшие издания могут включать спецификации и для других типов доставки.

8.3 Выбранный тип доставки

Это сообщение определяет тип доставки из перечисленных в списке типов доставки. Сообщение имеет следующий формат (SMTP):

DELV <тип доставки>

8.4 Подтверждение типа доставки

В том случае, если выбранный тип доставки допустим, это сообщение имеет следующий формат SMPT (без учета регистра):

250 Delivery-Type <тип доставки>OK

В случае если в сообщении о выбранном типе доставки допущена синтаксическая ошибка, поступает следующий ответ:

501 Syntax: DELV <тип доставки>

В случае нарушения установленной последовательности при выдаче сообщения о выбранном типе доставки поступает следующий ответ:

501 Syntax: сначала используйте команду CELO

В случае направления в сообщении неизвестного типа доставки поступает следующий ответ:

501 Unknown Delivery-Type: <тип доставки>

8.5 Адрес электронной почты отправителя

Это сообщение направляется серверу Cmail для запроса отправки сертифицированной почты и, факультативно, для запроса у сервера Cmail сертификата открытого ключа отправителя:

MAIL FROM <адрес электронной почты отправителя> [CertificateRequested]

8.6 Подтверждение адреса электронной почты отправителя

Это сообщение отправляется для подтверждения наличия адреса электронной почты отправителя в базе данных сервера Cmail. Если отправитель запрашивает свой сертификат открытого ключа, то в сообщение включается сертификат открытого ключа отправителя:

[250 User-Certificate: <сертификат открытого ключа в кодировке Base64>]

250 OK

8.7 Запрос на отправку электронной почты получателю

Это сообщение направляется серверу Cmail для запроса отправки получателю одного сообщения сертифицированной электронной почты и, факультативно, для запроса у сервера Cmail сертификата открытого ключа получателя:

RCPT TO <адрес электронной почты получателя> [CertificateRequested]

Эта команда может использоваться столько раз, сколько необходимо для добавления каждого получателя в случае нескольких получателей. Информация о том, указан ли тип получатель как "To" (кому) или "CC" (копия), содержится в заголовке конверта [IETF RFC 5321]. Указание типа получателей "BCC" не допускается.

8.8 Проверка адреса электронной почты получателя удаленным сервером Cmail

Это сообщение направляется только в том случае, когда получатель и отправитель зарегистрированы на разных серверах Cmail. Сообщение отправляется с сервера Cmail отправителя серверу Cmail получателя в целях проверки достоверности адреса электронной почты и, факультативно, для запроса сертификата открытого ключа получателя:

CHCK RCPT <адрес электронной почты получателя> [CertificateRequested]

8.9 Подтверждение адреса электронной почты получателя

Это сообщение направляется в ответ на сообщение "Проверка адреса электронной почты получателя удаленным сервером Cmail".

Следующее сообщение подтверждает адрес электронной почты и содержит сертификат открытого ключа получателя, если он был запрошен:

[250 User-Certificate: <сертификат открытого ключа в кодировке Base64>]

250 OK

Если адрес электронной почты не может быть подтвержден, то возможна отправка следующих сообщений об ошибке:

503 Sender already specified (отправитель уже определен)

должно быть отправлено, если это ответ на дублированный запрос.

501 Syntax: CHCK RCPT <адрес>

должно быть отправлено, если в адресе электронной почты получателя допущена синтаксическая ошибка.

501 Syntax: CHCK RCPT <адрес> Error in parameters (ошибка в параметрах) <параметр>

должно быть отправлено, если параметр после адреса электронной почты не был распознан.

553 <адрес электронной почты> Invalid email address (неверный адрес электронной почты)

должно быть отправлено, если указанный адрес электронной почты не существует на удаленном сервере Cmail.

8.10 Подтверждение электронной почты получателя

Это сообщение отправляется для подтверждения существования адреса электронной почты получателя. Если отправитель запрашивает сертификат открытого ключа получателя, то в сообщение включается сертификат открытого ключа получателя.

Следующее сообщение подтверждает адрес электронной почты и содержит сертификат открытого ключа получателя, если он был запрошен:

[250 User-Certificate: <сертификат открытого ключа в кодировке Base64>]

250 OK

Если адрес электронной почты не может быть подтвержден, то возможна отправка следующих сообщений об ошибке:

503 Error: need MAIL FROM command (требуется команда MAIL FROM)

должно быть отправлено, если сообщение направлено с нарушением установленной последовательности.

452 Error: too many recipients (слишком много получателей)

должно быть отправлено, если указано слишком много получателей.

501-6.1.1 Syntax: RCPT TO <адрес>

должно быть отправлено, если в адресе электронной почты получателя допущена синтаксическая ошибка.

501-6.1.2 Syntax: RCPT TO <адрес> Error in parameters (ошибка в параметрах): <параметры>

должно быть отправлено, если параметр после адреса электронной почты не был распознан.

550-5.1.1 <адрес электронной почты> Invalid email address (неверный адрес электронной почты)

должно быть отправлено, если указанный адрес электронной почты не существует.

8.11 Запрос на отправку конверта

Для запроса у сервера Cmail разрешения на отправку данных отправитель использует следующий формат:

DATA

8.12 Готовность к приему конверта

В случае готовности сервера Cmail к приему данных направляется следующее сообщение:

354 Smart mail input (начать ввод почты); end input (завершить) <CRLF>.<CRLF>

Если не была отправлена команда MAIL FROM, направляется следующее сообщение:

503 Error: need MAIL FROM command (требуется команда MAIL FROM)

Если не была отправлена команда RCPT TO, направляется следующее сообщение:

503 Error: need RCPT TO command (требуется команда RCPT TO)

Если не была отправлена команда DELV, направляется следующее сообщение:

503 Error: need DELV command (требуется команда DELV)

8.13 Конверт (ENVELOPE)

Клиент должен:

1) сгенерировать случайный симметричный криптографический ключ (RSCK), например, используя усовершенствованный стандарт шифрования (AES) 256;
2) используя этот ключ, зашифровать тело сообщения и вложения, если таковые имеются;
3) сформировать сообщение в формате MIME, содержащее часть, называемую конвертом (ENVELOPE), и включающую в себя зашифрованное сообщение (см. [IETF RFC 2045]);
4) завершить сообщение последовательностью <CR><LF>.<CR><LF>; и
5) отправить сообщение MIME.

8.14 Подписанное сервером уведомление о помещении в почтовый ящик

250 Notice-of-deposit:

<уведомление о помещении в почтовый ящик, подписанное сервером Cmail и закодированное в кодировке base64>

250 OK

Сервер формирует уведомление о помещении в почтовый ящик, содержащее информацию о конверте (идентификатор конверта, тип доставки и хэш MIME) и подписывает его, используя свой частный ключ.

8.15 Подписанное отправителем и сервером уведомление о помещении в почтовый ящик

Отправитель должен:

1) расшифровать полученное уведомление о помещении в почтовый ящик;
2) сформировать запрос для каждого получателя;
3) подписать подписанное сервером уведомление о помещении в почтовый ящик, используя свой собственный частный ключ;
4) зашифровать результат в кодировке base64; и
5) передать его серверу Cmail, используя команду

DEPO <уведомление о помещении в почтовый ящик в кодировке base64>

Запрос определен на рисунке A.6.

Запрос содержит секретный вопрос (**`SecretQuestion`**), криптографический ключ конверта (**`CipherEnvelopeKey`**) и сертификат открытого ключа получателя.

SecretQuestion включает в себя запрос (**Request**) и ответ (**Response**).

Запрос может содержать случайное число (**RandomNumber**). Ответ содержит идентификатор алгоритма (**AlgorithmIdentifier**), который отправитель должен пересчитать, для того чтобы получить конверт (ENVELOPE). Значение этого **AlgorithmIdentifier** определяет, какой алгоритм использован для вычисления хэша. Процедура запроса включает, во-первых, восстановление криптографического ключа RSCK, зашифрованного с помощью открытого ключа получателя, далее сцепление **RandomNumber** и RSCK и вычисление хэша для формирования ответа.

Пример построения запроса на языке XML:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1"
Encoding="base64">5mYZWhtl0yxBa/wl7VLiiQ=</response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

ПРИМЕЧАНИЕ 1. − Для данного запроса могут использоваться отличительные правила кодирования (DER) с абстрактной синтаксической нотацией версии 1 (ASN.1).

ПРИМЕЧАНИЕ 2. − Сервер не сможет выполнить пересчет хэша, поскольку ему неизвестен ключ шифрования. Однако только серверу известен ожидаемый результат вычисления хэша.

ПРИМЕЧАНИЕ 3. − В процессе опроса получателя сервер направляет только секретный вопрос и ожидает ответа получателя.

8.16 Пересылка конверта между серверами Cmail

Сообщение, описанное в п. 8.13, пересылается другому серверу Cmail только в том случае, если получатель и отправитель зарегистрированы на разных серверах Cmail (см. пункт m 16, рисунок 1):

SEND EVLP <сообщение в формате MIME>

8.17 Подписанное уведомление о транзите между серверами Cmail

Должен использоваться следующий формат:

250 Notice-of-transit:

<уведомление о транзите в кодировке base64>

При получении сервером Cmail уведомления о транзите отправляется следующее сообщение:

250 OK

При получении сервером Cmail неправильного уведомления о транзите отправляется следующее сообщение:

503 Error: incorrect Notice-of-transit

Уведомление о транзите формируется сервером Cmail, который получил конверт.

Этот сервер формирует уведомление о помещении в почтовый ящик, содержащее информацию о конверте (идентификатор конверта, тип доставки и хэш MIME), и подписывает его, используя свой частный ключ. Это уведомление аналогично уведомлению о помещении в почтовый ящик.

8.18 Подписанное уведомление о транзите

Сервер Cmail отправителя должен:

1) расшифровать полученное уведомление о транзите;
2) подписать подписанное сервером уведомление о транзите, используя свой собственный частный ключ;
3) зашифровать результат в кодировке base64; и
4) передать его серверу Cmail, используя команды:

   250 Signed-notice-of-transit:

   <подписанное уведомление о транзите в кодировке base64>

   250 Signed-notice-of-deposit:

   <подписанное уведомление о помещении в почтовый ящик в кодировке base64>

   250 OK

9 Протокол сертифицированного почтового отделения (CPOP)

В пунктах 9.1–9.6 приведено объяснение действий, выполняемых в пунктах p 1 – p 6, рисунок 1.

9.1 Запрос ожидающих сообщений

Информация об ожидающих сообщениях предоставляется с использованием процедуры, приведенной в описании команды LIST в разделе 5 [IETF RFC 1939], с включением дополнительного параметра. К каждой строке с информацией об ожидающем почтовом сообщении добавляется дополнительный параметр, указывающий тип доставки, если это не стандартная электронная почта (см. пункт p 1, рисунок 1). Пример:

C: LIST

S: +OK 2 messages (320 octets)

S: 1 120

S: 2 200 CertifiedMail

S: .

Данная процедура также выполняет извлечение всех стандартных сообщений электронной почты, оставляя только сообщения, имеющие на сервере Cmail метку с указанием типа доставки.

9.2 Запрос уведомления о приеме, подписанного получателем и сервером

Если сообщения имеют метку с указанием типа доставки, то команда RETR не извлекает сообщение, а извлекает запрос и подписанное сервером уведомление о приеме в кодировке base64. Клиент проверяет цифровую подпись и сертификат отправителя, содержащиеся в уведомлении о приеме.

Пример:

C: RETR 2

Если сервер Cmail отправляет уведомление о приеме, направляется следующее сообщение:

S: +OK 200 octets

S: <сервер Cmail отправляет уведомление о приеме, включая запрос>

S: .

Если сервер Cmail не может отправить уведомление о приеме, направляется следующее сообщение:

503 Error: impossible to send Notice-of-reception

В уведомлении о помещении в почтовый ящик сервер Cmail выполняет поиск узла **`Entity`**, связанного с отправителем. Затем сервер Cmail копирует этот узел в уведомление о приеме и удаляет содержимое узла **`Response`**, включенное в узел **`Entity`.**

Пример – узел в уведомлении о помещении в почтовый ящик:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1"
Encoding="base64">5mYZWhtl0yxBa/wl7VLiiQ=</response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

ПРИМЕЧАНИЕ 1. – В этом запросе может использоваться кодировка DER с ASN.1.

Тот же узел, скопированный в уведомление о приеме:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64" />
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

ПРИМЕЧАНИЕ 2. – В этом запросе может использоваться кодировка DER с ASN.1.

9.3 Ответ на запрос и уведомление о приеме, подписанное получателем и сервером

Получатель должен:

1) расшифровать полученное уведомление о приеме;
2) извлечь RSCK;
3) вычислить ответ на запрос;
4) подписать подписанное сервером уведомление о приеме, используя свой собственный частный ключ;
5) зашифровать результат в кодировке base64; и
6) передать его серверу Cmail, используя команду:

   CHLG RESP <ответ на запрос и уведомление о приеме, подписанное получателем и сервером>

Получатель расшифровывает следующее сообщение:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1"
Encoding="base64"></response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

ПРИМЕЧАНИЕ. – В этом запросе может использоваться кодировка DER с ASN.1.

Используя свой частный ключ, получатель восстанавливает RSCK, расшифровывая содержимое узла **`CipherEnvelopeKey`**. Затем получатель сцепляет **`RandomNumber`** и RSCK, хэширует результат, используя указанный **`AlgorithmIdentifier`**, и получает результат **`SecretQuestion`**.

Получатель копирует этот результат в подписанное уведомление о приеме, ставит свою подпись и отправляет его серверу Cmail.

9.4 Конверт

Если запрос завершен удачно (OK), сервер Cmail отправляет конверт таким же образом, как и результат команды RETR. После этого у получателя окажется сообщение и ключ для его открытия.

Если сервер не может отправить конверт, направляется следующее сообщение:

503 Error: impossible to send ENVELOPE

9.5 Подписанное получателем и сервером уведомление о приеме при передаче между серверами Cmail (факультативно)

Это сообщение направляется только в том случае, если отправитель и получатель зарегистрированы на разных серверах Cmail:

SEND NORP <подписанное получателем и сервером уведомление о приеме в кодировке base64>

9.6 Подписанное получателем и сервером уведомление о приеме

Это сообщение направляется только в том случае, если отправитель и получатель зарегистрированы на разных серверах Cmail:

SEND NORP <подписанное получателем и сервером уведомление о приеме в кодировке base64>

Приложение A

Уведомления в формате определения схемы XML (XSD)

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

В настоящем Приложении определены уведомления с использованием формата определения схемы XML (XSD), соответствующего [XSD]. Экземпляр связи кодируется с использованием XML, соответствующего [XML], и должен соответствовать спецификациям XSD, приведенным в настоящем Приложении.

A.1 Обзор XSD

См. рисунки A.1–A.10.

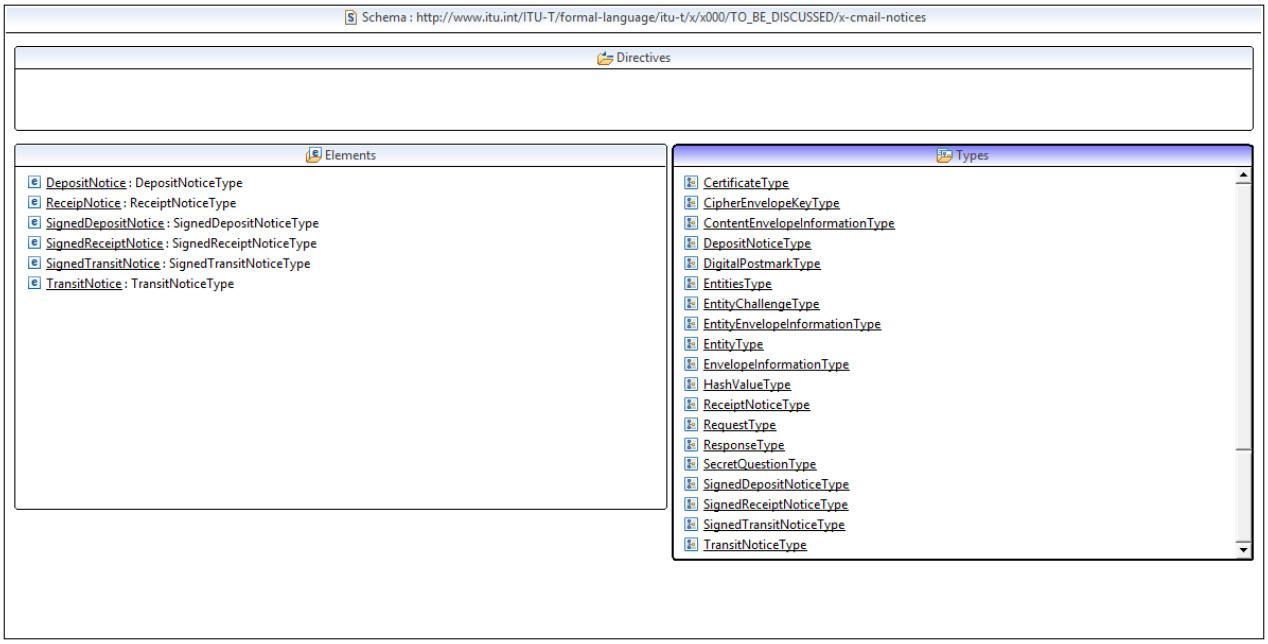

Рисунок A.1 − Список элементов и типов

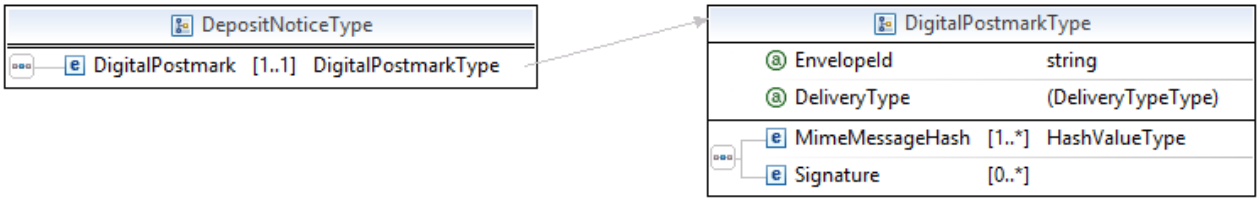

Рисунок A.2 − Уведомление о помещении в почтовый ящик

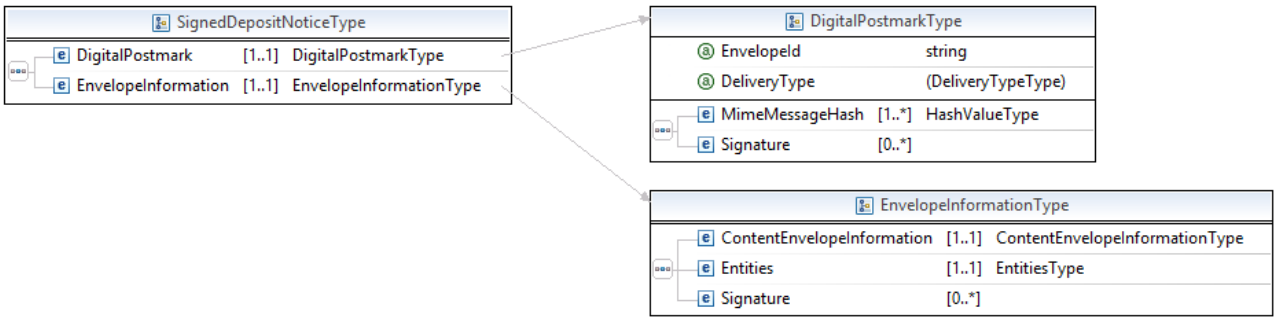

Рисунок A.3 – Подписанное уведомление о помещении в почтовый ящик

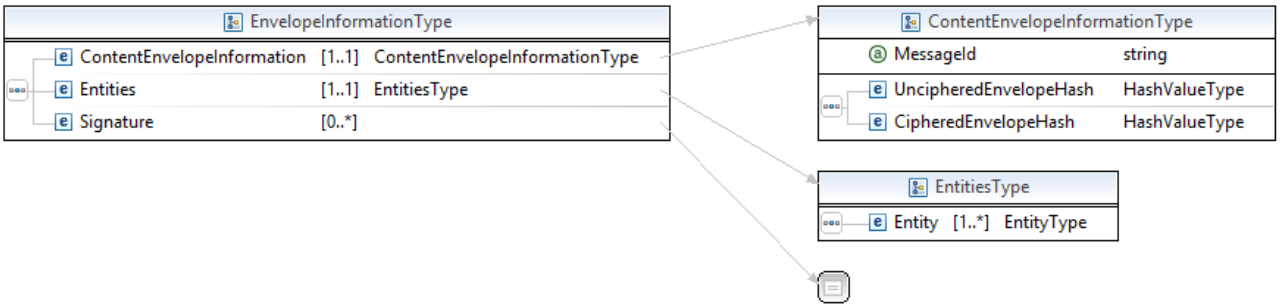

Рисунок A.4 – Тип информации о конверте

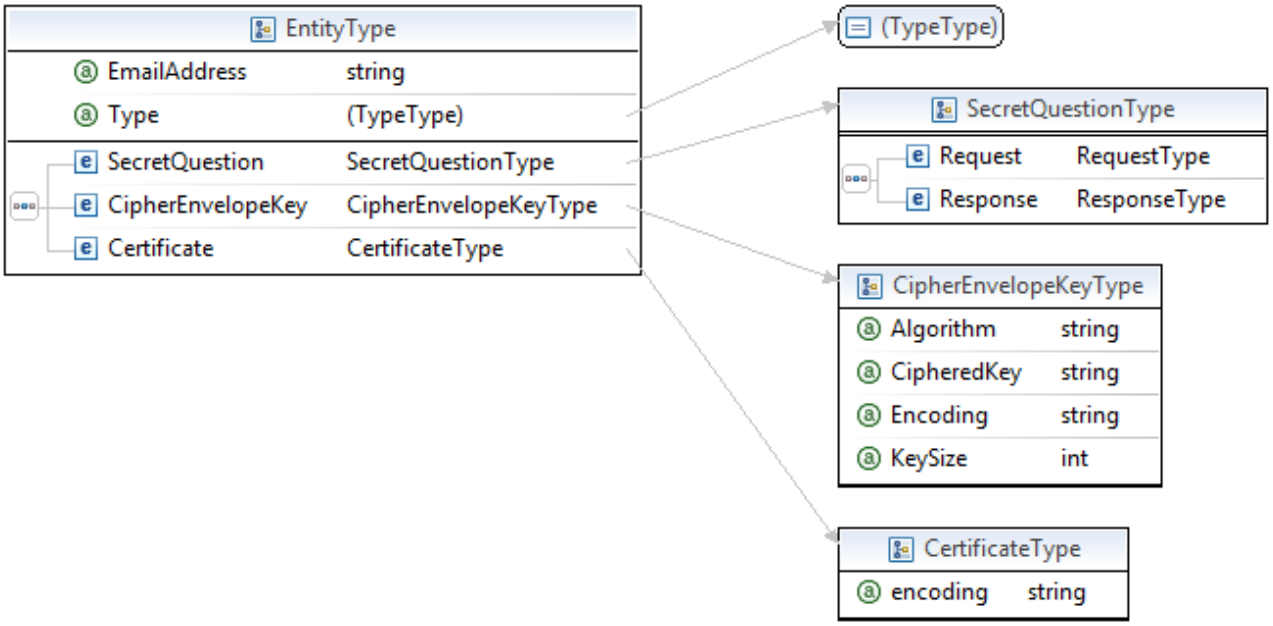

Рисунок A.5 – Тип объекта

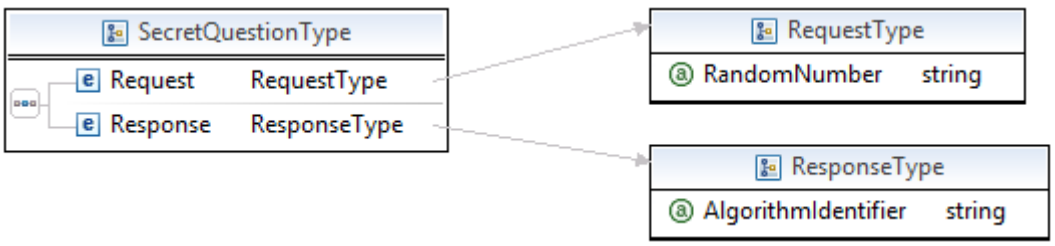

Рисунок A.6 – Запрос

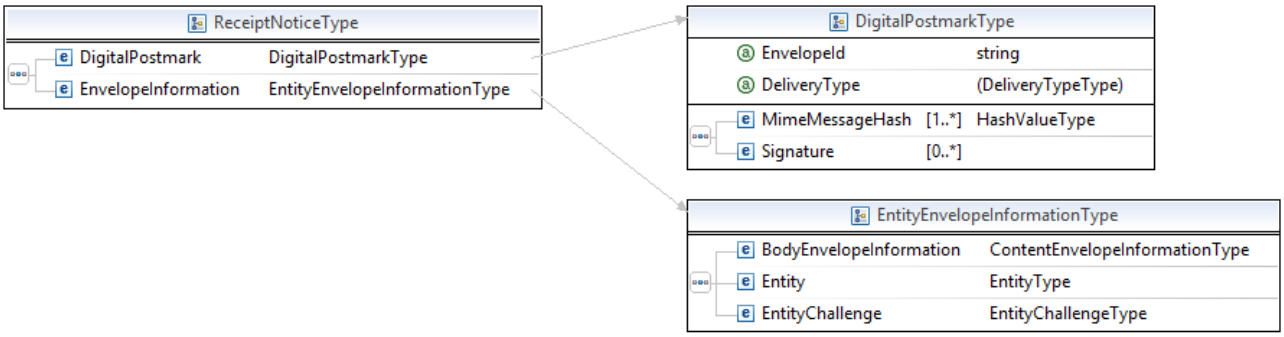

Рисунок A.7 – Уведомление о приеме

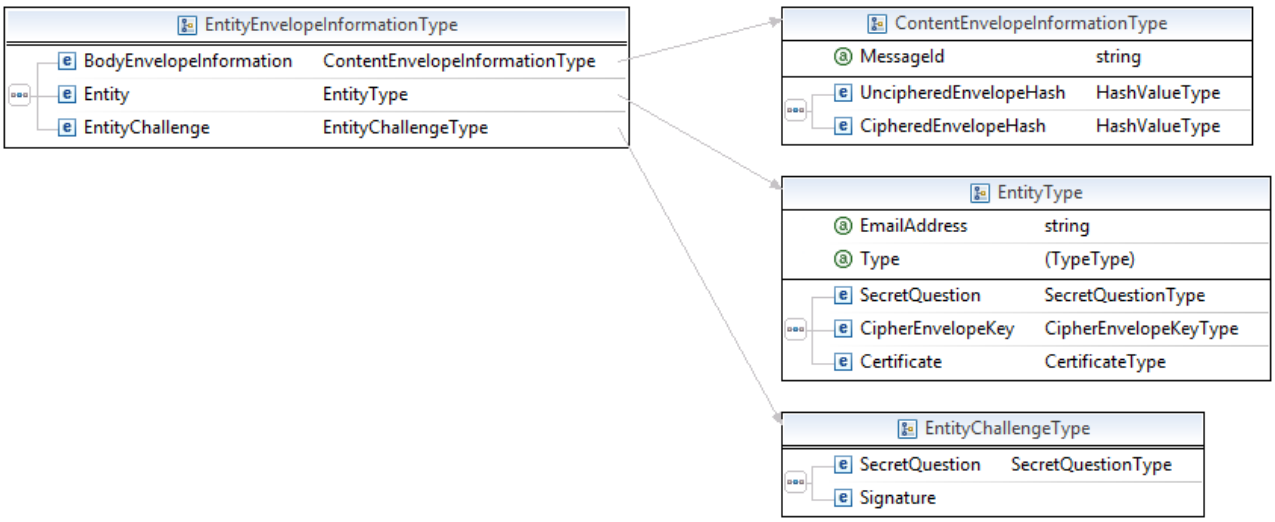

Рисунок A.8 – Ответ получателя на запрос

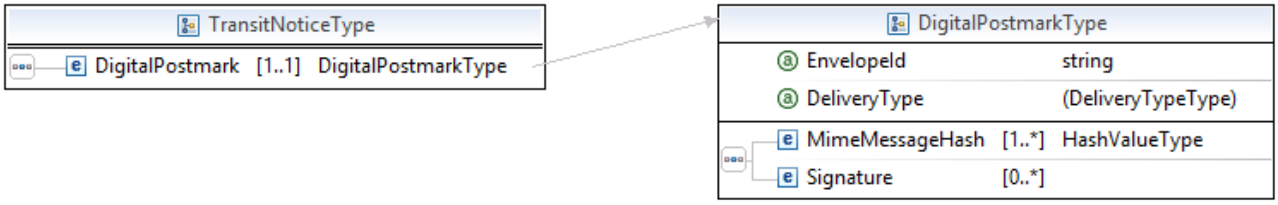

Рисунок A.9 – Уведомление о транзите

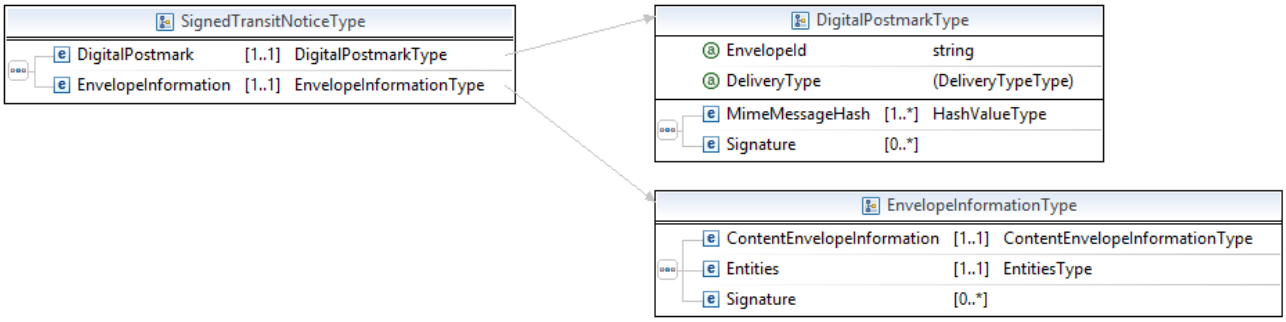

Рисунок A.10 – Подписанное уведомление о транзите

A.2 Формальная спецификация уведомлений в формате XSD

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices"
     elementFormDefault="qualified" xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  <import namespace="http://www.w3.org/2009/xmldsig11#"
    schemaLocation="http://www.w3.org/TR/xmldsig-core1/xmldsig11-schema.xsd" />
  <import namespace="http://www.w3.org/2009/xmldsig-properties"
    schemaLocation="http://www.w3.org/TR/xmldsig-properties/xmldsig-properties.xsd" />

  <import namespace=http://www.w3.org/2000/09/xmldsig#
    schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd" />

  <element name="DepositNotice" type="tns:DepositNoticeType"></element>
  <element name="SignedDepositNotice" type="tns:SignedDepositNoticeType"></element>
  <element name="TransitNotice" type="tns:TransitNoticeType"></element>
  <element name="SignedTransitNotice" type="tns:SignedTransitNoticeType"></element>
  <element name="ReceipNotice" type="tns:ReceiptNoticeType"></element>
  <element name="SignedReceiptNotice" type="tns:SignedReceiptNoticeType"></element>

  <complexType name="DigitalPostmarkType">
    <sequence>
      <element name="MimeMessageHash" type="tns:HashValueType"
        maxOccurs="unbounded" minOccurs="1">
      </element>
      <element name="Signature" type="ds:SignatureType"
        maxOccurs="unbounded" minOccurs="0">
      </element>
    </sequence>
    <attribute name="EnvelopeId" type="string" use="required"></attribute>
    <attribute name="DeliveryType" use="required">
      <simpleType>
        <restriction base="string">
          <enumeration value="CertifiedMail"></enumeration>
        </restriction>
      </simpleType>
    </attribute>
  </complexType>

  <complexType name="EnvelopeInformationType">
    <sequence>
      <element name="ContentEnvelopeInformation"
        type="tns:ContentEnvelopeInformationType" maxOccurs="1" minOccurs="1">
      </element>
      <element name="Entities" type="tns:EntitiesType"
        maxOccurs="1" minOccurs="1">
      </element>
      <element name="Signature" type="ds:SignatureType"
        maxOccurs="unbounded" minOccurs="0">
      </element>
    </sequence>
  </complexType>

  <complexType name="ContentEnvelopeInformationType">
    <sequence>
      <element name="UncipheredEnvelopeHash" type="tns:HashValueType"></element>
      <element name="CipheredEnvelopeHash" type="tns:HashValueType"></element>
    </sequence>
    <attribute name="MessageId" type="string"></attribute>
  </complexType>

  <complexType name="SecretQuestionType">
    <sequence>
      <element name="Request" type="tns:RequestType"></element>
      <element name="Response" type="tns:ResponseType"></element>
    </sequence>
  </complexType>
```

```
<complexType name="EntityType">
  <sequence>
    <element name="SecretQuestion" type="tns:SecretQuestionType"></element>
    <element name="CipherEnvelopeKey"
      type="tns:CipherEnvelopeKeyType">
    </element>
    <element name="Certificate" type="tns:CertificateType"></element>
  </sequence>
  <attribute name="EmailAddress" type="string" use="required">
    <annotation>
      <documentation>Email address has to be in RFC 822format</documentation>
    </annotation></attribute>
  <attribute name="Type" use="required">
    <simpleType>
      <restriction base="string">
        <enumeration value="from"></enumeration>
        <enumeration value="to"></enumeration>
        <enumeration value="cc"></enumeration>
        <enumeration value="transit"></enumeration>
      </restriction>
    </simpleType>
  </attribute>
</complexType>

<complexType name="CipherEnvelopeKeyType">
  <attribute name="Algorithm" type="string"></attribute>
  <attribute name="CipheredKey" type="string"></attribute>
  <attribute name="Encoding" type="string"></attribute>
  <attribute name="KeySize" type="int"></attribute>
</complexType>

<complexType name="CertificateType">
  <attribute name="encoding" type="string"></attribute>
</complexType>

<complexType name="EntitiesType">
  <sequence>
    <element name="Entity" type="tns:EntityType"
      maxOccurs="unbounded" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="SignedDepositNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
    <element name="EnvelopeInformation"
      type="tns:EnvelopeInformationType" maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="DepositNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="TransitNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="SignedTransitNoticeType">
```

```
    <sequence>
      <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
        maxOccurs="1" minOccurs="1">
      </element>
      <element name="EnvelopeInformation"
        type="tns:EnvelopeInformationType" maxOccurs="1" minOccurs="1">
      </element>
    </sequence>
  </complexType>

  <complexType name="ReceiptNoticeType">
    <sequence>
      <element name="DigitalPostmark"
        type="tns:DigitalPostmarkType">
      </element>
      <element name="EnvelopeInformation"
        type="tns:EntityEnvelopeInformationType">
      </element>
    </sequence>
  </complexType>

  <complexType name="SignedReceiptNoticeType">
    <sequence>
      <element name="DigitalPostmark"
        type="tns:DigitalPostmarkType">
      </element>
      <element name="EnvelopeInformation"
        type="tns:EntityEnvelopeInformationType">
      </element>
    </sequence>
  </complexType>

  <complexType name="HashValueType">
    <attribute name="AlgorithmOID">
      <simpleType>
        <restriction base="string">
          <enumeration value="1.3.14.3.2.26"></enumeration>
          <enumeration value="2.16.840.1.101.3.4.2.1"></enumeration>
        </restriction>
      </simpleType>
    </attribute>
  </complexType>

  <complexType name="EntityEnvelopeInformationType">
    <sequence>
      <element name="BodyEnvelopeInformation" type="tns:ContentEnvelopeInformationType">
      </element>
      <element name="Entity" type="tns:EntityType"></element>
      <element name="EntityChallenge" type="tns:EntityChallengeType"></element>
    </sequence>
  </complexType>

  <complexType name="EntityChallengeType">
    <sequence>
      <element name="SecretQuestion" type="tns:SecretQuestionType"></element>
      <element name="Signature" type="ds:SignatureType"></element>
    </sequence>
  </complexType>

  <complexType name="RequestType">
    <attribute name="RandomNumber" type="string"></attribute>
  </complexType>

  <complexType name="ResponseType">
    <attribute name="AlgorithmIdentifier" type="string"></attribute>
  </complexType>

</schema>
```

Приложение B

Уведомления в формате ASN.1

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

В настоящем Приложении представлена спецификация уведомлений с использованием абстрактной синтаксической нотации версии 1 (ASN.1), соответствующей [ITU-T X.680]. Уведомления могут кодироваться с использованием отличительных правил кодирования (DER) с абстрактной синтаксической нотацией версии 1 (ASN.1), определенных в [ITU-T X.690], либо с использованием расширенных правил кодирования XML (EXTENDED-XER), определенных в [ITU-T X.693]. В последнем случае получаемый в результате кодирования XML будет идентичен XML, созданному в соответствии со спецификациями XSD, приведенными в Приложении A.

```
CMAIL {itu-t(0) recommendation(0) x(24) cmail(1341) asn1Module(1) cmail(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS String
     FROM XSDv2 {joint-iso-itu-t asn1(1) specification(0) modules(0)
          xsd-module(2) version2(2)};

DepositNotice        ::= DepositNoticeType

SignedDepositNotice  ::= SignedDepositNoticeType

TransitNotice        ::= TransitNoticeType

SignedTransitNotice  ::= SignedTransitNoticeType

ReceiptNotice        ::= ReceiptNoticeType

SignedReceiptNotice  ::= SignedReceiptNoticeType

DigitalPostmarkType  ::= SEQUENCE {
     mimeMessageHash SEQUENCE (SIZE(1..MAX)) OF
          mimeMessageHash HashValueType,
     signature  SEQUENCE (SIZE(0..MAX)) OF
          signature  SignatureType,
     envelopeId String,
     deliveryType    ENUMERATED {
          certifiedMail,
          ...
          }
     }

EnvelopeInformationType    ::= SEQUENCE {
     contentEnvelopeInformation ContentEnvelopeInformationType,
     entities              EntitiesType,
     signature       SEQUENCE (SIZE(0..MAX)) OF
          signature SignatureType
     }

ContentEnvelopeInformationType  ::= SEQUENCE {
     uncipheredEnvelopeHash    HashValueType,
     cipheredEnvelopeHash HashValueType,
     messageId       String
     }

SecretQuestionType    ::= SEQUENCE {
     request         RequestType,
     response   ResponseType
     }

EntityType ::= SEQUENCE {
     secretQuestion       SecretQuestionType,
     cipheredEnvelopeKey  CipheredEnvelopeKeyType,
```

```
      certificate          CertificateType,
      emailAddress         String
           (CONSTRAINED BY
           {-- "Email address has to be in IETF RFC 822 format --}),
      type ENUMERATED {
           from,
           to,
           cc,
           transit
           }
      }

CipheredEnvelopeKeyType    ::= SEQUENCE {
      algorithm  String,
      cipherededKey   String,
      encoding   String,
      keySize          String
      }

CertificateType ::= SEQUENCE {
      encoding   String
      }

EntitiesType     ::= SEQUENCE {
      entity           SEQUENCE(SIZE(1..MAX)) OF entity EntityType
      }

SignedDepositNoticeType    ::= SEQUENCE {
      digitalPostmark      DigitalPostmarkType,
      envelopeInformation  EnvelopeInformationType
      }

DepositNoticeType     ::= SEQUENCE {
      digitalPostmark      DigitalPostmarkType
      }

TransitNoticeType     ::= SEQUENCE {
      digitalPostmark      DigitalPostmarkType
      }

SignedTransitNoticeType    ::= SEQUENCE {
      digitalPostmark      DigitalPostmarkType,
      envelopeInformation  EnvelopeInformationType
      }

ReceiptNoticeType     ::= SEQUENCE {
      operatorPostmark     DigitalPostmarkType
      }

SignedReceiptNoticeType    ::= SEQUENCE {
      operatorPostmark     DigitalPostmarkType,
      envelopeInformation  EntityEnvelopeInformationType
      }

HashValueType    ::= SEQUENCE {
      algorithmOID    ENUMERATED {
           sha-1,
           sha-256
           }
      }

EntityEnvelopeInformationType   ::= SEQUENCE {
      bodyEnvelopeInformation    ContentEnvelopeInformationType,
      entity               EntityType,
      entityChallenge      EntityChallengeType
      }

EntityChallengeType  ::= SEQUENCE {
      secretQuestion _SecretQuestionType,
      signature  SignatureType
      }
```

```
RequestType     ::= SEQUENCE {
     randomNumer     String
     }

ResponseType    ::= SEQUENCE {
     algorithmIdentifier  String
     }

SignatureType   ::= String

ENCODING-CONTROL XER
     GLOBAL-DEFAULTS MODIFIED-ENCODINGS
     [NAME AS CAPITALIZED] DigitalPostmarkType.mimeMessageHash
     [UNTAGGED] DigitalPostmarkType.mimeMessageHash
     [NAME AS CAPITALIZED] DigitalPostmarkType.signature.*
     [UNTAGGED] DigitalPostmarkType.signature
     [NAME AS CAPITALIZED] DigitalPostmarkType.envelopeId
     [ATTRIBUTE] DigitalPostmarkType.envelopeId
     [NAME AS CAPITALIZED] DigitalPostmarkType.deliveryType
     [ATTRIBUTE] DigitalPostmarkType.deliveryType
     [TEXT AS CAPITALIZED] DigitalPostmarkType.delivetyType:certifiedMail
     [NAME AS CAPITALIZED] EnvelopeInformationType.contentEnvelopeInformation
     [NAME AS CAPITALIZED] EnvelopeInformationType.entities
     [NAME AS CAPITALIZED] EnvelopeInformationType.signature
     [UNTAGGED] EnvelopeInformationType.signature
     [NAME AS CAPITALIZED]
          ContentEnvelopeInformationType.uncipheredEnvelopeHash
     [NAME AS CAPITALIZED]
          ContentEnvelopeInformationType.cipheredEnvelopeHash
     [NAME AS CAPITALIZED] ContentEnvelopeInformationType.messageId
     [ATTRIBUTE] ContentEnvelopeInformationType.messageId
     [NAME AS CAPITALIZED] SecretQuestionType.request
     [NAME AS CAPITALIZED] SecretQuestionType.response
     [NAME AS CAPITALIZED] EntityType.secretQuestion
     [NAME AS CAPITALIZED] EntityType.cipheredEnvelopeKey
     [NAME AS CAPITALIZED] EntityType.certificate
     [NAME AS CAPITALIZED] EntityType.emailAddress
     [ATTRIBUTE] EntityType.emailAddress
     [NAME AS CAPITALIZED] EntityType.type
     [ATTRIBUTE] EntityType.type
     [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.algorithm
     [ATTRIBUTE] CipheredEnvelopeKeyType.algorithm
     [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.cipheredKey
     [ATTRIBUTE] CipheredEnvelopeKeyType.cipheredKey
     [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.encoding
     [ATTRIBUTE] CipheredEnvelopeKeyType.encoding
     [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.keysize
     [ATTRIBUTE] CipheredEnvelopeKeyType.keysize
     [NAME AS CAPITALIZED] CertificateType.encoding
     [ATTRIBUTE] CertificateType.encoding
     [UNTAGGED] EntitiesType.entity
     [NAME AS CAPITALIZED] EntitiesType.entity.*
     [NAME AS CAPITALIZED] SignedDepositNoticeType.digitalPostmark
     [NAME AS CAPITALIZED] SignedDepositNoticeType.envelopeInformation
     [NAME AS CAPITALIZED] DepositNoticeType.digitalPostmark
     [NAME AS CAPITALIZED] TransitNoticeType.digitalPostmark
     [NAME AS CAPITALIZED] SignedTransitNoticeType.digitalPostmark
     [NAME AS CAPITALIZED] SignedTransitNoticeType.envelopeInformation
     [NAME AS CAPITALIZED] ReceiptNoticeType.digitalPostmark
     [NAME AS CAPITALIZED] SignedReceiptNoticeType.digitalPostmark
     [NAME AS CAPITALIZED] SignedReceiptNoticeType.envelopeInformation
     [NAME AS CAPITALIZED] HashValueType.algorithmOID
     [ATTRIBUTE] HashValueType.algorithmOID
     [TEXT AS "1.3.14.3.2.26"] HashValueType.algorithmOID:sha-1
     [TEXT AS "2.16.840.1.101.3.4.2.1"] HashValueType.algorithmOID:sha-256
     [NAME AS CAPITALIZED]
          EntityEnvelopeInformationType.BodyEnvelopeInformation
     [NAME AS CAPITALIZED]
          EntityEnvelopeInformationType.entityChallenge
     [NAME AS CAPITALIZED] EntityChallengeType.secretQuestion
```

```
      [NAME AS CAPITALIZED] EntityChallengeType.signature
      [NAME AS CAPITALIZED] RequestType.randomNumber
      [ATTRIBUTE] RequestType.randomNumber
      [NAME AS CAPITALIZED] ResponseType.algorithmIdentifier
      [ATTRIBUTE] ResponseType.algorithmIdentifier

END
```

Приложение C

Требования к компонентам инфраструктуры открытых ключей

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

C.1 Введение

В настоящем Приложении представлены требования к сертификатам открытых ключей, выдаваемых клиентам и серверам Cmail.

C.2 Сертификаты открытых ключей конечного объекта сервера Cmail

Сертификат открытого ключа конечного объекта, выданный серверу Cmail, должен иметь следующее содержимое.

a) Должна быть указана версия 3.

b) CA должен создавать непоследовательные порядковые номера.

c) Поле субъекта должно содержать отличительное имя справочника с одним компонентом, в котором используется атрибут **dnsName**, соответствующий определенным в [ITU-T X.520]. Значение должно быть зарегистрированным наименованием из системы наименований доменов (DNS).

d) Должно присутствовать расширение альтернативного имени субъекта с двумя элементами:

- для одного элемента должно быть использовано альтернативное имя **rfc822Name** и оно должно быть адресом электронной почты администратора сервера Cmail;
- для другого элемента должно быть использовано альтернативное имя **directoryName** и оно должно быть отличительным именем, содержащим следующие компоненты:
  - компонент **countryName** должен присутствовать и содержать трехбуквенный код (alpha-3) в соответствии с [ISO 3166-1];
  - компонент **organizationName** должен присутствовать и содержать доверенное название организации, управляющей сервером Cmail;
  - компонент **streetAddress** должен присутствовать и содержать название улицы и номер дома;
  - компонент **localityName** должен присутствовать и содержать название населенного пункта;
  - компонент **stateOrProvinceName** должен присутствовать при необходимости для уникальной идентификации; иначе он должен отсутствовать;
  - компонент **postalCode** должен присутствовать и содержать почтовый индекс местоположения.

e) Должно присутствовать расширение **certificatePolicies** и содержать по крайней мере идентификатор объекта **{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailServer(1)}** для указания на то, что сертификат открытого ключа выдан в соответствии с настоящей Рекомендацией.

C.3 Сертификаты открытых ключей конечного объекта клиента Cmail

Сертификат открытого ключа конечного объекта, выданный клиенту Cmail, должен иметь следующее содержимое.

a) Должна быть указана версия 3.

b) CA должен создавать непоследовательные порядковые номера.

c) Поле субъекта должно содержать отличительное имя справочника со следующими компонентами:

- компонент **surname** должен присутствовать в том случае, если клиентом является физическое лицо, и отсутствовать – если клиентом является организация;

– компонент **givenName** должен присутствовать, если присутствует компонент **surname**; иначе он должен отсутствовать;

– компонент **initials** может присутствовать, если присутствует компонент **surname**, **иначе** он должен отсутствовать;

– компонент **generationQualifier** может присутствовать, если присутствует компонент **surname**, **иначе** он должен отсутствовать;

– компонент **organizationName** должен присутствовать, если клиент не является физическим лицом; иначе он должен отсутствовать. Если этот компонент присутствует, он должен содержать доверенное название организации, к которой принадлежит клиент;

– компонент **streetAddress** должен присутствовать и содержать название улицы и номер дома;

– компонент **localityName** должен присутствовать и содержать название населенного пункта;

– компонент **stateOrProvinceName** должен присутствовать при необходимости для уникальной идентификации; иначе он должен отсутствовать;

– компонент **postalCode** должен присутствовать и содержать почтовый индекс местоположения;

– компонент **countryCode3c** должен присутствовать и содержать трехбуквенный код (alpha-3) в соответствии с [ISO 3166-1].

d) Должно присутствовать расширение **subjectAltName**. Это расширение должно содержать один указанный ниже элемент:

– элемент **rfc822Name** должен содержать адрес электронной почты администратора сервера Cmail.

e) Должно присутствовать расширение **certificatePolicies** и содержать по крайней мере идентификатор объекта **{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailClient(2)}** для указания на то, что сертификат открытого ключа выдан в соответствии с настоящей Рекомендацией.

C.4 Требования к проверке информации

Перед выдачей сертификата открытого ключа выдающая сторона должна проверить:

a) что субъект (заявитель) является зарегистрированным владельцем наименования домена, указываемого в сертификате открытого ключа;

b) физическое существование субъекта;

c) коммерческое существование (деловую активность) субъекта;

d) что субъект является доверенным объектом;

e) название и адрес, указываемые в сертификате открытого ключа;

f) что названием, указываемое в поле **organizationName** сертификата открытого ключа, является доверенным и признанным названием, идентифицирующим субъект.

Приложение D

Требования к безопасности транспортного уровня (TLS)

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Должна поддерживаться спецификация [IETF RFC 5246] или ее более поздняя версия.

В процессе согласования ни сервер Cmail, ни клиент не должны принимать соединение, если предпринимается попытка согласовать использование версии TLS ниже TLS 1.2.

Реализация должна поддерживать следующий набор шифров:

TLS_DH_RSA_WITH_AES_256_CBC_SHA256

Приложение E

Идентификаторы объектов, определенные в настоящей Рекомендации

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

В настоящей Рекомендации определены следующие идентификаторы объектов:

a) идентификатор объекта, связанный с модулем ASN.1:
{itu-t recommendation(0) x(24) cmail(1341) asn1module(0) cmail(1)}

b) идентификатор объекта, используемый расширением certificatePolicies сервера Cmail:
{itu-t recommendation(0) x(24) cmail(1341) certificateProfile(2) cmailServer(1)}

c) идентификатор объекта, используемый расширением certificatePolicies клиента Cmail:
{itu-t recommendation(0) x(24) cmail(1341) certificateProfile(2) cmailClient(2)}

Дополнение I

Формат конверта и уведомлений

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем Дополнении приведены примеры кодирования уведомлений.

I.1 Уведомление о помещении в почтовый ящик

Уведомление о помещении в почтовый ящик содержит информацию об отправителе, конверт и имеет подписи сервера Cmail и отправителя.

Это уведомление служит для отправителя доказательством помещения в почтовый ящик, и он может использовать его в судебных спорах.

Формальная спецификация уведомления о помещении в почтовый ящик приведена в Приложении A.

Пример – файл "1373360283931.deposit.notice ".

```
Received: from localhost ([127.0.0.1])
        by begmeil
        with SMTP (SubEthaSMTP null) id HIWV8HF9
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 10:58:14 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=depositNotice.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
bG9wZWQtc2lnbmF0dXJlIi8+CiAgICA8L1lyYW5zZm9ybXM+CiAgICA8RGln
...
ICAgPFJTQUtleVZhbHVlPgogICAgICAgICA8TW9kdWx1cz5tMkFSUURXUGJBMmgvMzJEQWs4
ICAgICAgICAgIDxFeHBvbmVudD5BUUFCPC9FeHBvbmVudD4KICAgICAgICAgIDwvUlNBS2V5VmFs
dWU+CiAgICAgICAgPC9LZXlWYWx1ZT4KICAgICAgICA8ZT4KICAgICAgICAgIDxmZvPgogICAgPC9TaWduYXR1cmU+
CiAgPC9lbnZlbG9wSW5mb3JtYXRpb24+CjwvbGV0dGVyRGVwb3NpdFBvc3RtYXJrPgo=
```

I.2 Уведомление о приеме

Уведомление о приеме содержит информацию об отправителе, конверт, запрос открытия конверта и имеет подписи сервера Cmail и получателя.

Это уведомление служит для отправителя доказательством приема, и он может использовать его в судебных спорах.

Формальная спецификация уведомления о приеме приведена в Приложении A.

Пример – файл "1373360283931.laura.prin@legalbox.com.receipt.notice".

```
Received: from begmeil get hostname ([127.0.0.1])
        by localhost
        with SMTP (LegalBox POP Server v1.0) id HIWX27L5
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 11:49:01 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=receiptNotice.xml
```


```
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
PjEzNzMzNjAyODM5MzE8L2VudmVsb3BJZD4KICAgIDxkZWxpdmVyeU1vZGU+Y2VydGlmaWVkTGV0
dGVyPC9kZWxpdmVyeU1vZGU+CiAgICA8bWltZU1lc3NhZ2VIYXNoPgogICAgICA8c2hhMT5hNTVk
ZDhmYWU0Mzg2M2VmYWRmMWY3ZjM3MmEwYmU1MmEwMGRhYTFkPC9zaGExPgogICAgPC9taW1lTWVz
...
MDkwSDl0NFVkTTdWVU92bjY3WlU2aTJvVSt3b3lGR2tYMDJ3YkVMM2pDYmpJCm5VR1BwUGpoT3Zo
dzNPTy9mYmhKVk13dkM2NXB1MTl1cnA2M05kS0tHNlBuNjZtQkVnUldxZ2cvTVBITmZmWkhrOXFs
WExSSXhETi8Kb0ZnS285RmI0NExlSzBnZ3Vyb1Y2azNicm1TeGM1UnpYVWNxTzdwbldUN0FoNFl6
WXJJUHdYL1hjS1VqbXYxZi9JZjQ5VHVnWGtLcgpodklyOG9qUkdQcEdPdlB4cWR5QWNQR1BOUVRY
NFJrc29kSEVwdz09PC9Nb2R1bHVzPgogICAgICAgICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l
bnQ+CiAgICAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICAgIDwvS2V5VmFsdWU+CiAgICAgIDwv
S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogIDwvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy
RGVwb3NpdFBvc3RtYXJrPgo=
```


I.3 Уведомление о транзите

Уведомление о транзите содержит информацию об отправителе, конверт, запрос открытия конверта и имеет подписи серверов Cmail.

Это уведомление служит для отправителя доказательством транзита, и он может использовать его в судебных спорах.

Формальная спецификация уведомления о транзите приведена в Приложении A.

Пример – файл "1373360283931.laura.prin@legalbox.com.receipt.notice".

```
Received: from begmeil get hostname ([127.0.0.1])
        by localhost
        with SMTP (LegalBox POP Server v1.0) id HIWX27L5
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 11:49:01 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=receiptNotice.xml
```


```
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
PjEzNzMzNjAyODM5MzE8L2VudmVsb3BJZD4KICAgIDxkZWxpdmVyeU1vZGU+Y2VydGlmaWVkTGV0
dGVyPC9kZWxpdmVyeU1vZGU+CiAgICA8bWltZU1lc3NhZ2VIYXNoPgogICAgICA8c2hhMT5hNTVk
ZDhmYWU0Mzg2M2VmYWRmMWY3ZjM3MmEwYmU1MmEwMGRhYTFkPC9zaGExPgogICAgPC9taW1lTWVz
...
MDkwSDl0NFVkTTdWVU92bjY3WlU2aTJvVSt3b3lGR2tYMDJ3YkVMM2pDYmpJCm5VR1BwUGpoT3Zo
dzNPTy9mYmhKVk13dkM2NXB1MTl1cnA2M05kS0tHNlBuNjZtQkVnUldxZ2cvTVBITmZmWkhrOXFs
WExSSXhETi8Kb0ZnS285RmI0NExlSzBnZ3Vyb1Y2azNicm1TeGM1UnpYVWNxTzdwbldUN0FoNFl6
WXJJUHdYL1hjS1VqbXYxZi9JZjQ5VHVnWGtLcgpodklyOG9qUkdQcEdPdlB4cWR5QWNQR1BOUVRY
NFJrc29kSEVwdz09PC9Nb2R1bHVzPgogICAgICAgICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l
bnQ+CiAgICAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICAgIDwvS2V5VmFsdWU+CiAgICAgIDwv
S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogIDwvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy
RGVwb3NpdFBvc3RtYXJrPgo=
```

I.4 Конверт (ENVELOPE)

Конверт представляет собой сообщение в формате MIME, в котором находится содержимое электронной почты, зашифрованное с помощью AES.

Пример – файл "1373360283931.certifiedLetter.msg".

```
Received: from localhost ([127.0.0.1])
        by begmeil
        with SMTP (SubEthaSMTP null) id HIWV8HF9
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 10:58:03 +0200 (CEST)
Date: Tue, 9 Jul 2013 10:57:51 +0200 (CEST)
From: david.keller@legalbox.com
To: laura.prin@legalbox.com
Message-ID: proto_cmtp_1373360269856
Subject: =?UTF-8?Q?Bienvenue_=C3=A0_CMTP!?=
MIME-Version: 1.0
Content-Type: multipart/mixed;
       boundary="----=_Part_1_1013939722.1373360271613"

------=_Part_1_1013939722.1373360271613
Content-Type: multipart/mixed;
       boundary="----=_Part_0_2062834323.1373360271584"

------=_Part_0_2062834323.1373360271584
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=envelop

RG44gUlyr1A/L+ps0R+yKMUpgPcJACmcRQdLZSMoLnm07gtRataSAWkG5qnc/f5Q

------=_Part_0_2062834323.1373360271584--

------=_Part_1_1013939722.1373360271613--
```

Библиография

[b-ITU-T X.509] Рекомендация МСЭ-Т X.509 (2012 г.) | ISO/IEC 9594-8:2014, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Структура сертификатов открытых ключей и атрибутов*.

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	Оконечное оборудование, субъективные и объективные методы оценки
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 протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2016 г.