МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т X.1122

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(04/2004)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ
И ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ

Безопасность электросвязи

Руководящие указания по созданию безопасных подвижных систем на основе инфраструктуры открытого ключа (PKI)

Рекомендация МСЭ-Т X.1122

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ И ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	
Службы и услуги	X.1–X.19
Интерфейсы	X.20–X.49
Передача, сигнализация и коммутация	X.50–X.89
Сетевые аспекты	X.90–X.149
Техническое обслуживание	X.150–X.179
Административные предписания	X.180–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	
Модель и обозначение	X.200–X.209
Определения служб	X.210–X.219
Спецификации протоколов в режиме с установлением соединений	X.220–X.229
Спецификации протоколов в режиме без установления соединений	X.230–X.239
Проформы PICS	X.240–X.259
Идентификация протоколов	X.260–X.269
Протоколы обеспечения безопасности	X.270–X.279
Управляемые объекты уровня	X.280–X.289
Испытание на соответствие	X.290–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	
Общие положения	X.300–X.349
Спутниковые системы передачи данных	X.350–X.369
IP-сети	X.370–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	
Организация сети	X.600–X.629
Эффективность	X.630–X.639
Качество обслуживания	X.640–X.649
Наименование, адресация и регистрация	X.650–X.679
Абстрактно-синтаксическая нотация 1 (АСН.1)	X.680–X.699
АДМИНИСТРАТИВНОЕ УПРАВЛЕНИЕ ВОС	
Структура и архитектура административного управления системами	X.700–X.709
Служба и протокол связи для административного управления	X.710–X.719
Структура управляющей информации	X.720–X.729
Функции административного управления и функции ODMA	X.730–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	
Фиксация, параллельность и восстановление	X.850–X.859
Обработка транзакций	X.860–X.879
Удаленные операции	X.880–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ЭЛЕКТРОСВЯЗИ	**X.1000–**

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

Рекомендация МСЭ-Т X.1122

Руководящие указания по созданию безопасных подвижных систем на основе инфраструктуры открытого ключа (PKI)

Резюме

Хотя технология использования инфраструктуры открытого ключа (PKI) и является технологией безопасности, весьма пригодной для реализации многих функций обеспечения защиты (шифрования, цифровой подписи, обеспечения целостности данных и так далее) в подвижной передаче данных от конца до конца, все-таки эту технологию следует адаптировать для подвижной передачи данных от конца до конца. Однако метод проектирования безопасных подвижных систем, основанных на использовании технологии PKI, и управления такими системами еще не определен. В настоящей Рекомендации содержатся руководящие указания по созданию мобильных систем защиты на основе использования инфраструктуры открытого ключа (PKI).

Источник

Рекомендация МСЭ-Т X.1122 утверждена 29 апреля 2004 года, 17-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) в соответствии с процедурой Рекомендации МСЭ-Т A.8.

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.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет 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 соответствие 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 то, что практическое применение или реализация этой 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 реализации 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.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1122

Руководящие указания по созданию безопасных подвижных систем на основе инфраструктуры открытого ключа (PKI)

1 Область применения

В настоящей Рекомендации приводятся руководящие указания по созданию безопасных подвижных систем на основе технологии, использующей инфраструктуру открытого ключа (PKI). Область применения настоящей Рекомендации следующая:

- Предмет настоящей Рекомендации – контроль сертификатов подвижной передачи данных от конца до конца.

- Однако из области применения настоящей Рекомендации исключается определение метода организации подвижной связи как модели такой организации.

2 Ссылки

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

– ITU-T Recommendation F.116 (2000), *Service features and operational provisions in IMT-2000*.

– ITU-T Recommendation Q.814 (2000), *Specification of an electronic data interchange interactive agent*.

– ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks*.

– ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000*.

– ITU-T Recommendation Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.

– ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *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.842 (2000) | ISO/IEC TR 14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services*.

– ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

3 Термины и определения

3.1 Определения сертификационной структуры атрибутов и открытого ключа

В Рекомендации МСЭ-Т X.509 | Стандарте ИСО/МЭК 9594-8 определены следующие термины:

a) орган по присвоению атрибутов;

b) сертификат атрибута;

c) сертифицирующий орган (CA);

d) список аннулирования сертификатов (CRL);

e) открытый ключ;

f) сертификат для открытого ключа (Сертификат);

g) инфраструктура открытого ключа (PKI).

3.2 Определения для архитектуры обеспечения защиты согласно эталонной модели ВОС

В Рекомендации МСЭ-Т X.800 | Стандарте ИСО/МЭК 7498-2 определены следующие термины:

a) информация по аутентификации;

b) конфиденциальность;

c) криптография;

d) ключ;

e) пароль.

3.3 Руководящие указания по использованию и управлению для определений услуг доверенной третьей стороны

В Рекомендации МСЭ-Т X.842 | Стандарте ИСО/МЭК TR 14516 определен следующий термин:

a) регистрационный орган.

3.4 Особенности услуг и обеспечение эксплуатации в определениях для международной подвижной связи IMT-2000

В Рекомендации МСЭ-Т F.116 определен следующий термин:

a) модуль идентификации пользователя.

3.5 Дополнительные определения

В настоящей Рекомендации дается определение следующим терминам:

3.5.1 безопасная подвижная система: Система, осуществляющая безопасную подвижную передачу данных от конца до конца между подвижным пользователем и поставщиком ASP или между подвижными пользователями.

3.5.2 хранилище сертификатов: База данных, в которой хранятся сертификаты, список CRL и прочая, связанная с инфраструктурой PKI информация, и которая доступна в диалоговом режиме.

3.5.3 орган проверки достоверности: Орган, предоставляющий услугу проверки достоверности сертификата в диалоговом режиме (on-line). Он устанавливает путь проверки достоверности сертификата от подписанта до пользователя, желающего получить подтверждение достоверности подписи подписанта. Этот источник проверки достоверности также подтверждает, все ли сертификаты, содержащиеся в записи пути проверки достоверности сертификата, являются достоверными или не аннулированными. Он также проверяет, не был ли сертификат аннулирован.

4 Сокращения

В данной Рекомендации используются следующие сокращения:

AA Орган по присвоению атрибутов

ASP Поставщик (провайдер) прикладных услуг

CA Сертифицирующий орган

CMC Управление сертификатами через систему CMS

CMP Протокол управления сертификатами

CRL Список аннулирования сертификатов

ID Идентификатор

PIN Персональный идентификационный номер

PKI Инфраструктура открытого ключа

POP Доказательство обладания

RA Регистрационный орган

RSA Алгоритм шифрования с открытым ключом по алгоритму Ривеста-Шамира-Адлемана

TLS Безопасность транспортного уровня

UIM Модуль идентификации пользователя

VA Орган проверки достоверности

5 Категории, к которым принадлежат технологии PKI

Технология PKI – это технология безопасности, которая применяется к отношению между подвижным терминалом и сервером приложений в общей модели подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP, или к отношению между подвижным терминалом и шлюзом безопасности подвижной связи или между шлюзом безопасности подвижной связи и сервером в модели шлюза подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP.

Технология PKI – это технология безопасности, используемая для реализации следующих функций безопасности:

1) шифрования;
2) обмена ключами;
3) цифровой подписи;
4) управления доступом;
5) целостности данных;
6) обмена данными аутентификации;
7) заверения.

Таблица 1/X.1122 – Функции и места применения технологии PKI

Места применения технологий / Функции, реализованные по технологиям	Подвижный терминал	Сервер приложений/Шлюз безопасности подвижной связи	Отношение между подвижным пользователем и подвижным терминалом	Отношение между подвижным терминалом и сервером приложений или прочие отношения
Шифрование				X
Обмен ключами				X
Цифровая подпись				X
Управление доступом				X
Целостность данных				X
Обмен данными аутентификации				X
Заверение				X

Хотя технология PKI часто используется в открытой сети для реализации упомянутых выше функций безопасности, но для подвижной передачи данных от конца до конца требуется некоторая адаптация технологий PKI из-за характеристик такой связи, особенно из-за низкой производительности и малого размера памяти.

6 Модели безопасных подвижных систем на основе инфраструктуры PKI

Что касается других безопасных подвижных систем, то модели безопасных подвижных систем на основе инфраструктуры PKI классифицируются следующим образом: общая модель безопасных подвижных систем на основе инфраструктуры PKI для связи между подвижным пользователем и поставщиком ASP, и модель шлюза безопасных подвижных систем на основе инфраструктуры PKI для связи между подвижным пользователем и поставщиком ASP.

Однако для работы инфраструктуры PKI (например, управление жизненным циклом сертификата) в модель добавлены некоторые объекты (органы CA, RA, VA, хранилище и так далее).

6.1 Общая модель безопасных подвижных систем на базе инфраструктуры PKI

На рисунке 1 показана общая модель безопасных подвижных систем на базе инфраструктуры PKI для связи между подвижным пользователем и поставщиком ASP.

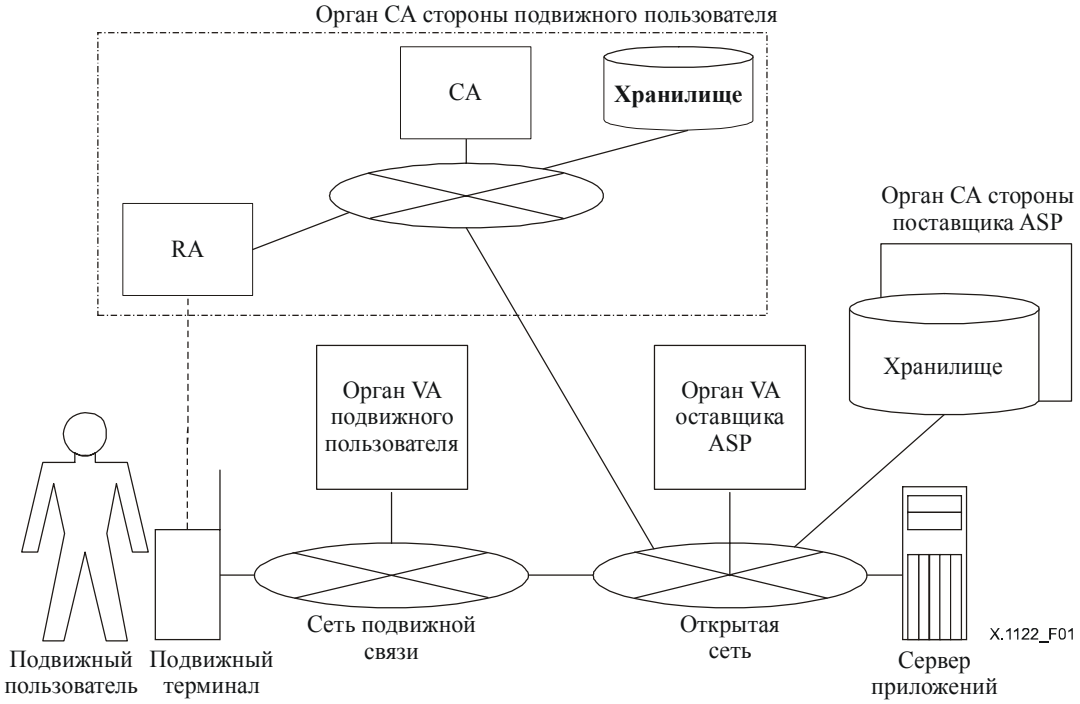

Рисунок 1/X.1122 – Общая модель безопасных подвижных систем на базе инфраструктуры PKI

Эта модель содержит некоторые объекты дополнительно к объектам общей модели безопасной подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP, то есть, орган CA стороны подвижного пользователя (содержит орган RA и хранилище), орган VA подвижного пользователя, орган CA стороны поставщика ASP и орган VA поставщика ASP.

– *Орган CA подвижного пользователя*

  Орган CA стороны подвижного пользователя выдает сертификат подвижного пользователя или сертификат подвижного терминала и управляет им. Он содержит орган RA, который отвечает за идентификацию и аутентификацию подвижного абонента, и хранилище, где хранятся сертификат подвижного пользователя и список CRL.

– *Орган VA подвижного пользователя*

  Орган VA подвижного пользователя предоставляет подвижному пользователю услугу проверки в диалоговом режиме достоверности сертификата, получаемого подвижным пользователем.

– *Орган CA со стороны поставщика ASP*

  Орган CA со стороны поставщика ASP выдает сертификат поставщика ASP или сертификат сервера приложений и управляет ими. Он также содержит орган RA, который отвечает за идентификацию и аутентификацию поставщика ASP, и хранилище, где хранятся сертификат поставщика ASP и список CRL.

– *Орган VA поставщик ASP*

  Орган VA поставщика ASP предоставляет услугу проверки в диалоговом режиме достоверности сертификата, полученного провайдером ASP.

6.2 Модель со шлюзом для безопасных подвижных систем на основе инфраструктуры PKI

На рисунке 2 показана модель со шлюзом для безопасных подвижных систем на базе инфраструктуры PKI для связи между подвижным пользователем и поставщиком ASP.

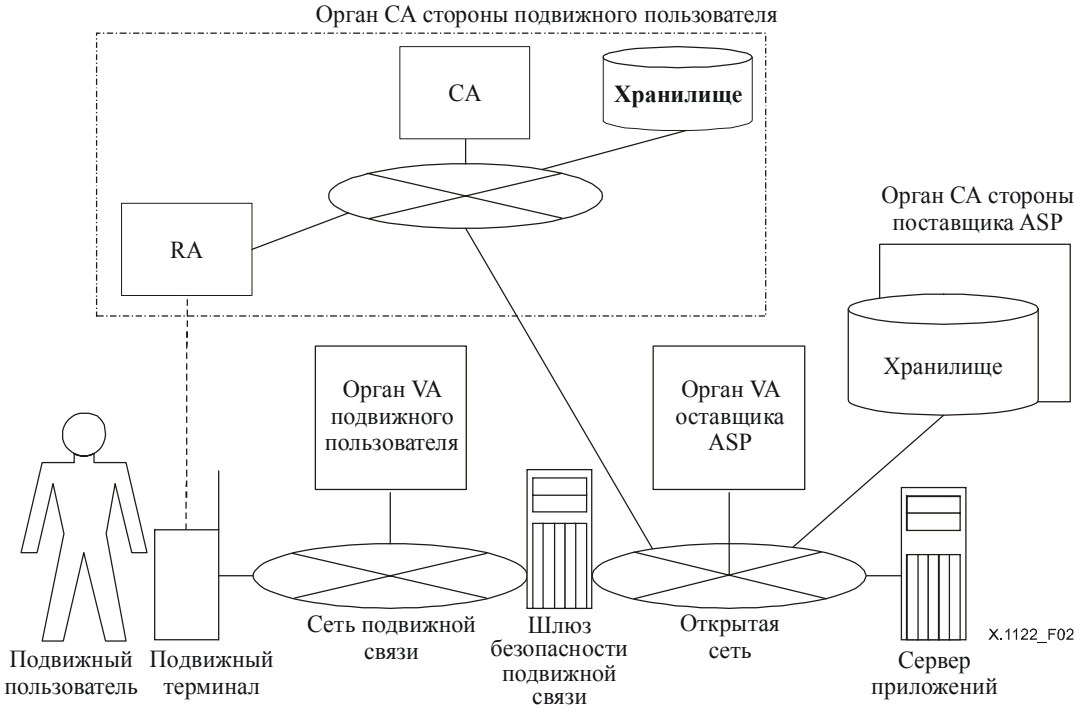

Рисунок 2/X.1122 – Модель со шлюзом для безопасных подвижных систем на базе инфраструктуры PKI

Данная модель, подобно общей модели безопасных подвижных систем на базе инфраструктуры PKI для связи между подвижным пользователем и поставщиком ASP, содержит ряд объектов дополнительно к объектам модели со шлюзом для подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP; то есть, орган CA стороны подвижного пользователя (содержит орган RA и хранилище), орган VA подвижного пользователя, орган CA стороны поставщика ASP и орган VA.

7 Операции инфраструктуры PKI для подвижной передачи данных от конца до конца

7.1 Операции инфраструктуры PKI, связанные с жизненным циклом сертификата

Общий жизненный цикл сертификата определяют следующие операции:

1) генерирование пары ключей, состоящей из частного ключа и открытого ключа;
2) заявка на сертификат, выдача и активирование сертификата;
3) использование сертификата;
4) аннулирование сертификата; и
5) обновление сертификата.

7.1.1 Генерирование пары ключей, состоящей из частного ключа и открытого ключа

Для генерирования пары ключей, состоящей из частного ключа и открытого ключа, существуют разные модели в зависимости от того, кто генерирует ключ или где генерируется ключ.

7.1.1.1 Объект, генерирующий ключи

Хотя с точки зрения безопасности желательно иметь модель, согласно которой подвижный пользователь генерирует ключи, может иметься модель, согласно которой вместо подвижного пользователя ключи генерирует орган CA, а также модель, в которой ключи генерирует третья сторона.

Что касается моделей, согласно которым ключи генерирует третья сторона, то существует модель, где пользователь приобретает устройство, в котором установлены ключи. (Это устройство может быть самим подвижным терминалом или может быть блоком, присоединенным к этому подвижному терминалу.) В этом случае производитель устройства является изготовителем ключа.

7.1.1.2 Место генерирования ключей

Могут быть модели, согласно которым ключи генерируются в устройстве, и модели, согласно которым ключи генерируются вне устройства и устанавливаются в устройстве.

7.1.2 Заявка на сертификат, выдача и активирование сертификата

Что касается заявки на сертификат, выдачи и активирования сертификата, то существуют различные модели в зависимости от того, делаются ли заявка, выдача и активирование в диалоговом режиме или в автономном режиме на каждом шаге.

Имеются случаи, когда, как оказывается, сертификат активируется при выдаче.

Модель, которую следует выбрать, зависит от лица, которому выдан сертификат (подвижный пользователь), от выдающего сертификат (орган CA), от того, кто дает гарантии на сертификат; от цели использования сертификата и так далее.

Кроме того, модели в условиях подвижной среды отличаются друг от друга в зависимости от связи между временными характеристиками таких функций, как:

a) генерирование ключей;

b) выдача сертификата;

c) активирование сертификата; и

d) получение устройства.

7.1.2.1 Модель, согласно которой устройство получено после того, как сертификат был активирован (модель, в которой порядок следования приведенных выше пунктов таков: (a)→(b)→(c)→(d))

Эта модель соответствует случаю, когда подвижный пользователь приобретает устройство, в котором ранее были установлены ключи и сертификат. Согласно этой модели можно продать устройство с заранее установленным сертификатом, имеющим субъект, который не связан с подвижным пользователем (например, когда это устройство – подвижный терминал, то телефонный номер или некоторый электронный серийный номер могут быть использованы как этот субъект), или установить сертификат в кассе–автомате магазина во время покупки устройства (например, сертификат вырабатывается и устанавливается на основе информации заявки во время выполнения заявки на устройство). В этом случае необходимо, чтобы события (b), (c) и (d) происходили одновременно.

7.1.2.2 Модель, согласно которой пользователь получает устройство, в котором сертификат уже был выдан (модель, в которой порядок следования таков: (a)→(b)→(d)→(c))

Это, в основном, та же модель, что и упомянутая выше, но процедура активирования сертификата необходима после получения устройства. Желательно между событиями (b) и (d) иметь короткий интервал времени.

7.1.2.3 Модель, согласно которой пользователь получает устройство, в котором хранятся только ключи (модель, в которой порядок следования таков: (a)→(d)→(b)→(c))

Эта модель соответствует случаю, когда пользователь подает заявку на сертификат в диалоговом режиме после того, как приобрел устройство с установленными ключами.

7.1.2.4 Модель, согласно которой пользователь получает устройство, в котором не установлены какие-либо ключи и сертификаты (модель, в которой порядок следования таков: (d)→(a)→(b)→(c))

Согласно этой модели пользователь генерирует ключи и делает заявку на сертификат после приобретения устройства. Эта модель обеспечивает секретность частного ключа подвижного терминала. Но для выработки ключей в этом устройстве требуется иметь повышенную вычислительную мощность, больший объем памяти и большее время обработки.

7.1.3 Использование сертификата

7.1.3.1 Лицо, подписывающее сертификат

Лицо, подписывающее сертификат, присоединяет этот сертификат к подписанному сообщению и посылает его верификатору. Имеются разные модели, зависящие от метода присоединения сертификата (такие как присоединение сертификата к сообщению и присоединение места хранилища).

7.1.3.2 Верификатор

При проверке аутентичности сообщения, принятого от подписывающего сертификат лица, требуется выполнить следующие процессы:

1) *Проверка подлинности сертификата*

   Это делается для проверки аутентичности сертификата от лица, подписывающего сертификаты. Конкретно, это определение пути аутентификации сертификата и проверка подлинности каждого сертификата на пути аутентификации.

   В зависимости от метода проверки подлинности возможны две следующие модели:

   a) *Модель, согласно которой верификатор сам осуществляет проверку подлинности*

      Во время проверки подлинности сертификата верификатор определяет путь аутентификации и проверяет подлинность каждого сертификата на пути аутентификации.

      Для проверки каждого сертификата, то верификатор проверяет подлинность сертификата путем получения списка CRL из хранилища органа CA или путем запроса органа CA, который предоставляет информацию о состояниях сертификатов в диалоговом режиме либо иным способом.

      Следует заметить, что частость получения списка CRL или запросов к органу CA зависят от использования и важности сертификата (в принципе, это необходимо всякий раз при проверке сертификата).

   b) *Модель, согласно которой используется надежный орган проверки достоверности (VA)*

      К органу VA посылается запрос о том, является ли подлинным сертификат, связанный с сообщением, а процесс фактической проверки подлинности (определение пути аутентификации и проверка подлинности каждого сертификата) выполняется органом VA.

      Сертификат с малым жизненным циклом или по другим причинам может миновать этот процесс.

2) *Проверка подписи, поставленной под сообщением*

   Это проверка того, является ли аутентичной подпись, поставленная под сообщением.

   Часто бывает так, что верификатор сам(а) устанавливает аутентичность подписи, используя открытый ключ сертификата, но есть модели, согласно которым это делает орган VA.

7.1.4 Аннулирование сертификата

После заявки на аннулирование сертификата, направленной органу CA, сертификат аннулируется. В зависимости от вида заявки имеются две модели аннулирования сертификата, а именно: модель, согласно которой заявка на аннулирование выполняется в диалоговом режиме, и модель, в которой заявка на аннулирование выполняется в автономном режиме.

7.1.5 Обновление сертификата

Обновление сертификата предполагает аннулирование существующего сертификата, генерирование новой пары ключей и получение нового сертификата, выдаваемого органом CA. В основном, заявка на аннулирование и выдача сертификата осуществляются последовательно, но модели отличаются друг от друга в зависимости от порядка следования процессов и от того, используется ли или не используется существующий сертификат (информация о существующем сертификате) в заявке на новый сертификат.

8 Модель использования уровней в услугах электросвязи

В данном разделе рассматриваются модели использования уровней, которые становятся доступными при использовании инфраструктуры PKI.

Имеются два типа моделей использования уровней: модель использования надсеансового уровня и модель использования прикладного уровня. Модель использования надсеансового уровня – это модель, согласно которой в эталонной модели ВОС на надсеансовом уровне предоставляются функции зашифрованной связи, аутентификации и целостности данных (такие как функции TLS). Модель использования прикладного уровня – это модель, предоставляющая функции обеспечения целостности и конфиденциальности на прикладном уровне.

Многие существующие реализации модели использования надсеансового уровня (наиболее известны реализации этой модели для функций TLS) предназначены для обеспечения безопасной транспортировки от конца до конца и для предоставления защищенного туннеля между сервером и клиентом. Поэтому клиент и сервер могут предоставлять друг другу полномочия и их аутентификация может быть реализована при использовании инфраструктуры PKI.

В основу модели использования надсеансового уровня входят следующие функции безопасности:

- аутентификация сервера;
- аутентификация клиента;
- целостность и засекречивание тракта связи.

В основу модели использования прикладного уровня входят следующие функции безопасности:

- функция цифровой подписи на прикладном уровне (для обеспечения целостности и аутентификации);
- функция шифрования данных на прикладном уровне (для конфиденциальности).

Кроме упомянутых выше моделей, также возможно применение модели использования сетевого уровня.

8.1 Функции, подлежащие реализации в модели использования надсеансового уровня

Модель использования надсеансового уровня предоставляет следующие функции: функцию аутентификации сервера, функцию аутентификации клиента и функцию обеспечения целостности и засекречивания тракта связи (фактически, она будет реализована путем сочетания функции аутентификации сервера и функции обеспечения целостности и засекречивания тракта связи или путем сочетания функции аутентификации сервера, функции аутентификации клиента и функции обеспечения целостности и засекречивания тракта связи). Реализации этой модели использования уровня (такие, как TLS) могут быть применены в подвижной передаче данных от конца до конца для обеспечения аутентификации как подвижного терминала, так и сервера приложений, а также для образования защищенного туннеля между двумя конечными пунктами. Сертификат играет в этой модели использования уровня очень важную роль. Поэтому важно точное определение процедуры выдачи, аннулирования или приостановки действия сертификата, а также описание метода аутентификации для пользователя и сервера.

8.1.1 Аутентификация сервера в модели использования надсеансового уровня

Поскольку, как упомянуто в разделе 6, имеются две модели для безопасных подвижных систем на базе инфраструктуры PKI, то в настоящей модели использования имеются два типа аутентификации сервера; один тип – это аутентификация сервера в общей модели, а второй тип – это аутентификация сервера в модели со шлюзом.

При аутентификации сервера в общей модели подвижный терминал проверяет сервер приложений путем проверки сертификата, представленного сервером приложений, и цифровой подписи в принимаемом сообщении во время процедуры установления связи.

При аутентификации сервера в общей модели будут применяться следующие процедуры:

- Сервер приложений посылает подвижному терминалу свой сертификат и соответствующую информацию аутентификации.
- Подвижный терминал проверяет, выдан ли сертификат органом CA, которому "доверяет" подвижный терминал.

- Подвижный терминал проверяет подлинность принятой информации аутентификации, используя открытый ключ в сертификате сервера приложений.
- В то же время подвижный терминал определяет, является ли сервер приложений, к которому он хочет получить доступ, определенно правильным.

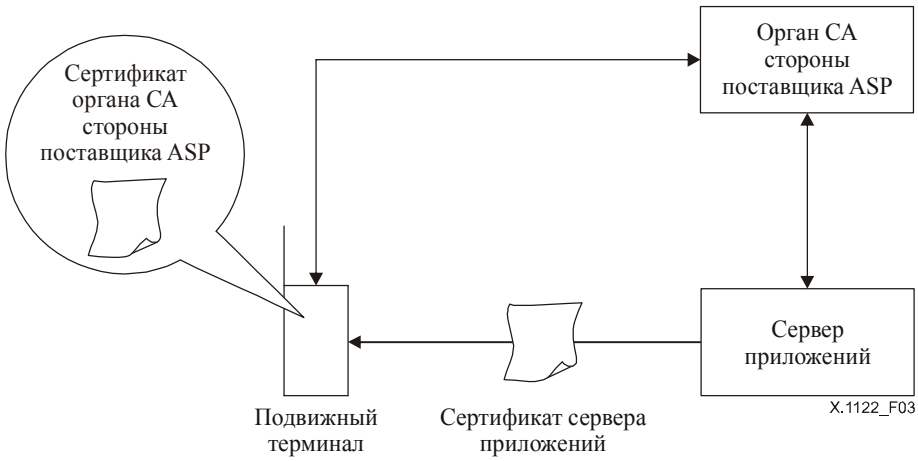

Рисунок 3/X.1122 – Аутентификация сервера в общей модели

При аутентификации сервера в модели со шлюзом выполняется двухфазная аутентификация между подвижным терминалом и шлюзом безопасности подвижной связи и между шлюзом безопасности подвижной связи и сервером приложений.

Двухфазная аутентификация сервера выполняется в соответствии со следующими процедурами:

- Во-первых, между подвижным терминалом и шлюзом безопасности подвижной связи устанавливается защищенный сеанс связи путем использования сертификата шлюза безопасности подвижной связи.
- Затем между шлюзом безопасности подвижной связи и сервером приложений также устанавливается защищенный сеанс связи.

Таким образом, при двухфазной аутентификации сервера шлюз безопасности подвижной связи должен быть способен преобразовать защищенный сеанс связи между подвижным терминалом и шлюзом безопасности подвижной связи соответственно в один защищенный сеанс связи между шлюзом безопасности подвижной связи и сервером приложений.

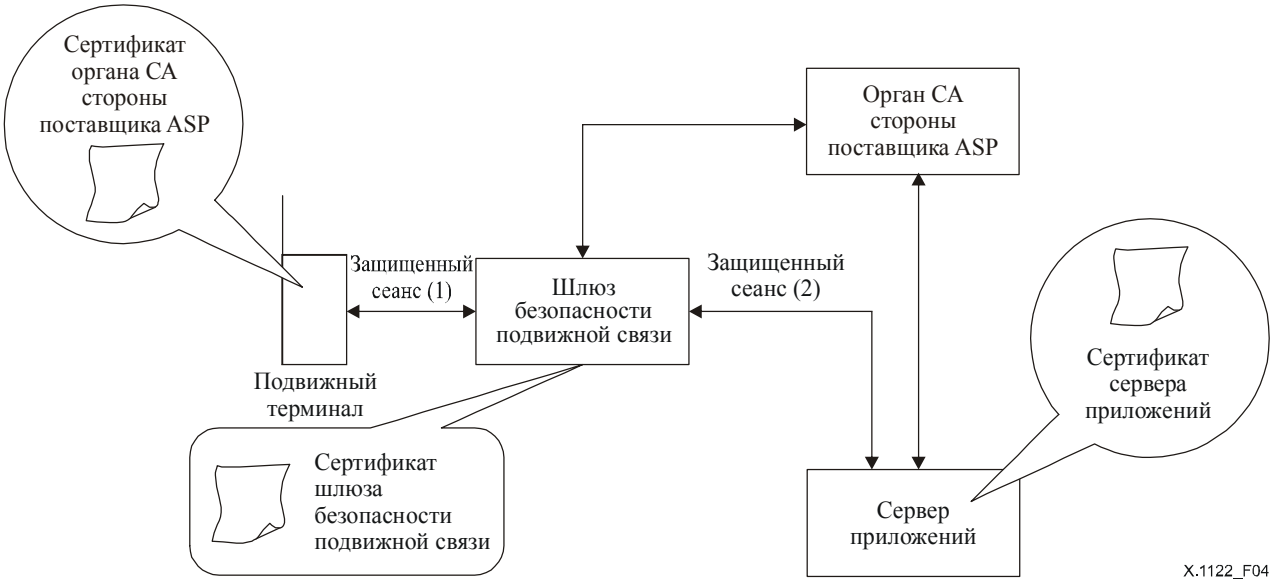

Рисунок 4/X.1122 – Аутентификация сервера в модели со шлюзом

8.1.2 Аутентификация клиента в модели использования надсеансового уровня

При аутентификации клиента в модели использования надсеансового уровня подвижный терминал представляет серверу приложений, отвечая на запрос этого сервера, сертификат и соответствующую информацию по аутентификации, а сервер приложений выполняет аутентификацию клиента.

Аутентификация клиента в этой модели использования уровня выполняется в соответствии со следующими процедурами:

- Подвижный терминал посылает сертификат серверу приложений.
- В то же самое время подвижный терминал посылает серверу приложений подписанное сообщение проверки подлинности (образованное по частному ключу клиента).
- Сервер приложений проверяет подлинность сертификата подвижного терминала.
- Кроме того, сервер приложений дешифрирует и проверяет сообщение проверки подлинности сертификата с открытым ключом в сертификате.

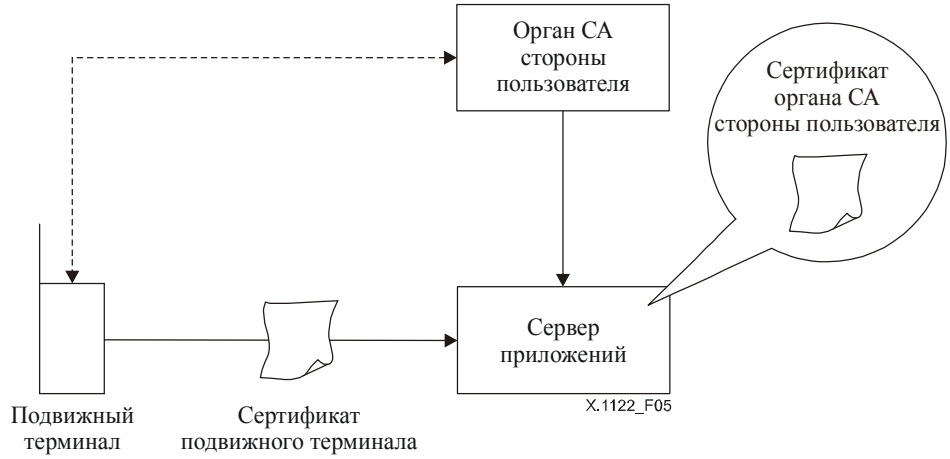

Рисунок 5/X.1122 – Аутентификация клиента в модели использования надсеансового уровня

Из-за характеристик подвижной передачи данных от конца до конца процедура в ряде реализаций модифицируется следующим образом:

- Подвижный терминал посылает органу CA стороны пользователя (или его агенту) запрос сертификата.
- Орган CA выполняет аутентификацию подвижного терминала.
- Орган CA генерирует сертификат подвижного терминала и посылает информацию о местонахождении сертификата (информацию, такую как URL) подвижному терминалу.
- Орган CA заносит сертификат подвижного терминала в область памяти.
- Далее, подвижный терминал ставит подпись под данными, подлежащими подписи, и посылает серверу приложений подписанные данные, подпись и информацию о местонахождении сертификата.
- Сервер приложений получает из хранилища сертификат подвижного терминала, используя информацию о местонахождении сертификата.
- Сервер приложений проверяет подлинность сертификата подвижного терминала (если необходимо), проверяет подлинность подписи по ее открытому ключу в сертификате подвижного терминала и аутентифицирует подвижный терминал путем использования сертификата подвижного терминала.
- Между подвижным терминалом и сервером приложений устанавливается защищенный сеанс связи.

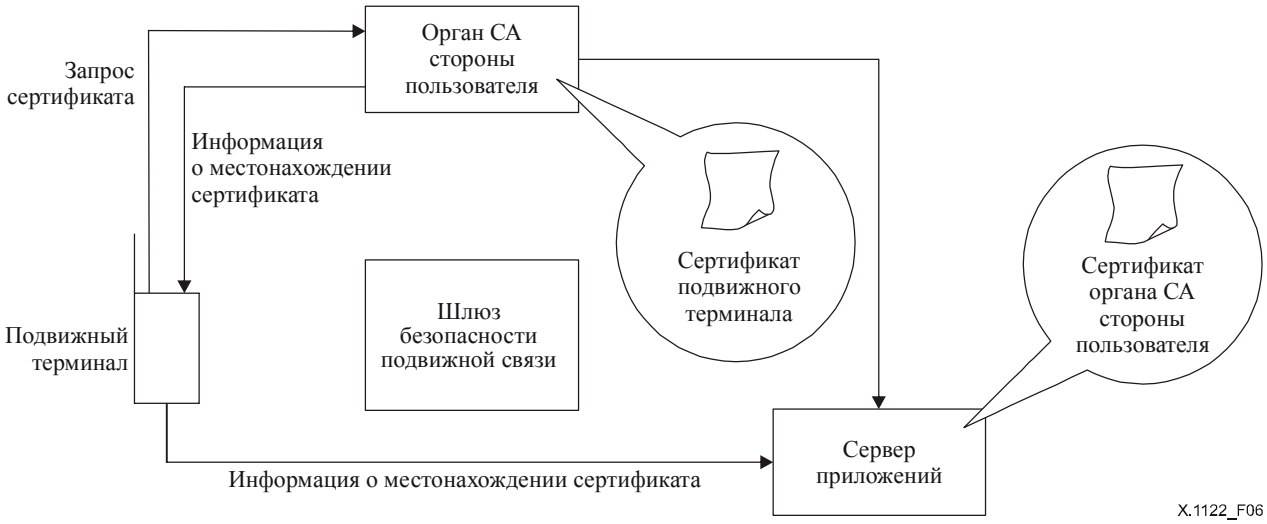

Рисунок 6/X.1122 – Аутентификация клиента в модели использования надсеансового уровня

8.1.3 Обеспечение целостности и засекречивания тракта связи в модели использования сеансового уровня

При обеспечении целостности и шифрования тракта связи в модели использования надсеансового уровня выполняются следующие процедуры:

- Подвижный терминал передает серверу приложений набор используемых криптографических алгоритмов и очередность приоритетов.
- Сервер приложений выбирает конкретный криптографический алгоритм наивысшего ранга из криптографических алгоритмов с общим ключом, который может быть использован обеими сторонами.
- Для предотвращения подлогов со стороны сервера приложений выполняется аутентификация сервера.
- Подвижный терминал генерирует случайное число в качестве генератора ключа сеанса и зашифровывает открытым ключом сервера приложений в сертификате сервера приложений в

случае использования метода обмена ключами по алгоритму RSA и посылает зашифрованный генератор сеансового ключа серверу приложений. Как сервер приложений, так и подвижный терминал могут использовать общий сеансовый ключ из генератора для последующей связи.

- Засекреченная связь вводится в действие.

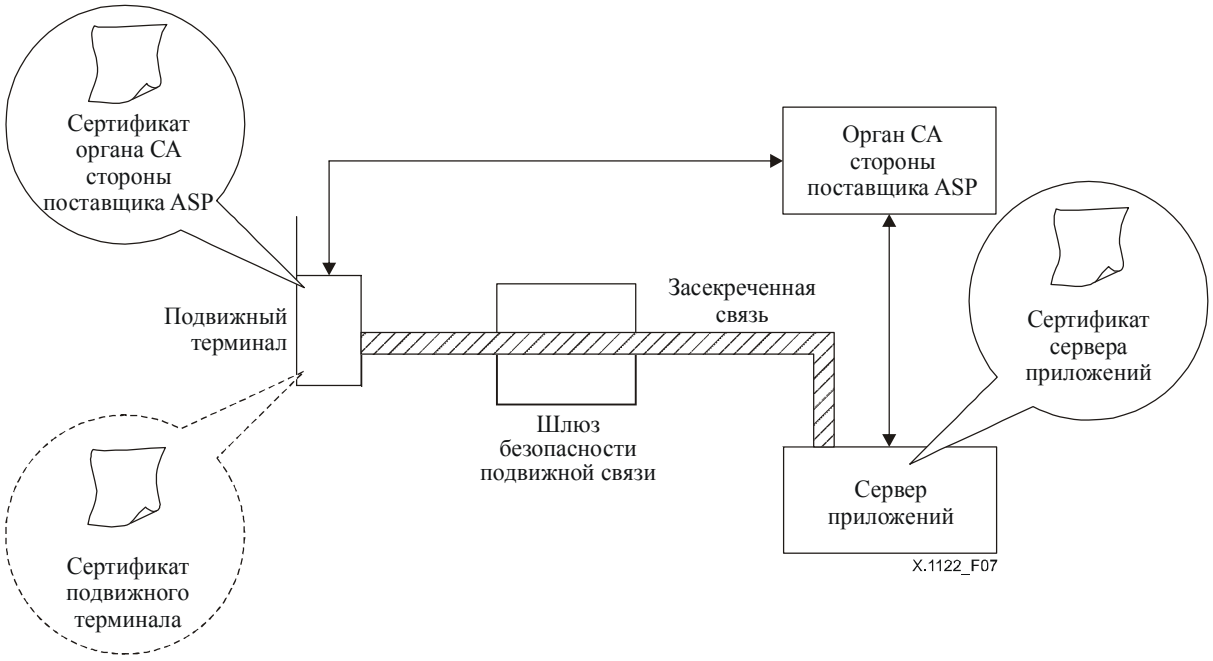

Рисунок 7/X.1122 – Засекречивание тракта связи в модели использования надсеансового уровня

8.2 Модель использования уровней на прикладном уровне

Инфраструктура PKI может быть использована для функции шифрования, характерной для приложения; функции цифровой подписи и для сочетания этих обеих функций, что требует идентификации и обеспечения секретности самих данных и что не может быть полностью обеспечено только средствами безопасности тракта связи на надсеансовом уровне, такими как аутентификация и шифрование. Примерами реализаций такой модели служат зашифрованные почтовые отправления и использование учета и взаиморасчетов для электронной коммерции.

8.2.1 Функция подписи на прикладном уровне

Эта функция гарантирует целостность данных и образует цифровую подпись над хэшированным значением данных, передаваемых с подвижного терминала, чтобы гарантировать тот факт, что данные исходили от лица, ставящего подпись. Функцию подписи на прикладном уровне реализуют следующие операции:

- Ввод или выбор данных, подлежащих подписи.
- Обработка цифровой подписи над хэшированным значением данных при использовании частного ключа, хранящегося в подвижном терминале или устройстве защиты, которое присоединено к подвижному терминалу.
- Представление подлежащих подписи данных, цифровой подписи и сертификата, включая открытый ключ, соответствующий частному ключу.
- Проверка получателем подлинности сертификата и цифровой подписи с помощью открытого ключа в сертификате.

Эта функция может быть использована для аутентификации типа "запрос–ответ" путем использования запроса (такого, как случайные числа) от сервера данных, подлежащих подписи.

8.2.2 Функция шифрования на прикладном уровне

Предоставление функции шифрования на прикладном уровне позволяет обеспечить секретность данных, если шифрование в тракте связи оказывается недостаточным. Функцию шифрования на прикладном уровне реализуют следующие операции:

- Генерирование случайного числа в качестве общего ключа.
- Шифрование данных по общему ключу при использовании симметричного криптографического алгоритма.
- Получение сертификата лица, к которому осуществляется передача.
- Шифрование общего ключа по открытому ключу в сертификате.
- Передача зашифрованных данных и зашифрованного общего ключа.
- Дешифрирование получателем зашифрованного общего ключа собственным частным ключом.
- Дешифрирование зашифрованных данных общим ключом.

9 Примеры конфигураций систем

9.1 Примеры конфигураций системы управления сертификатами

На рисунке 8 представлен пример системы, в которой оператор связи выдает сертификат для своего пользователя. Для выдачи/аннулирования сертификата используется автономная обработка, а для проверки подлинности сертификата используется орган VA.

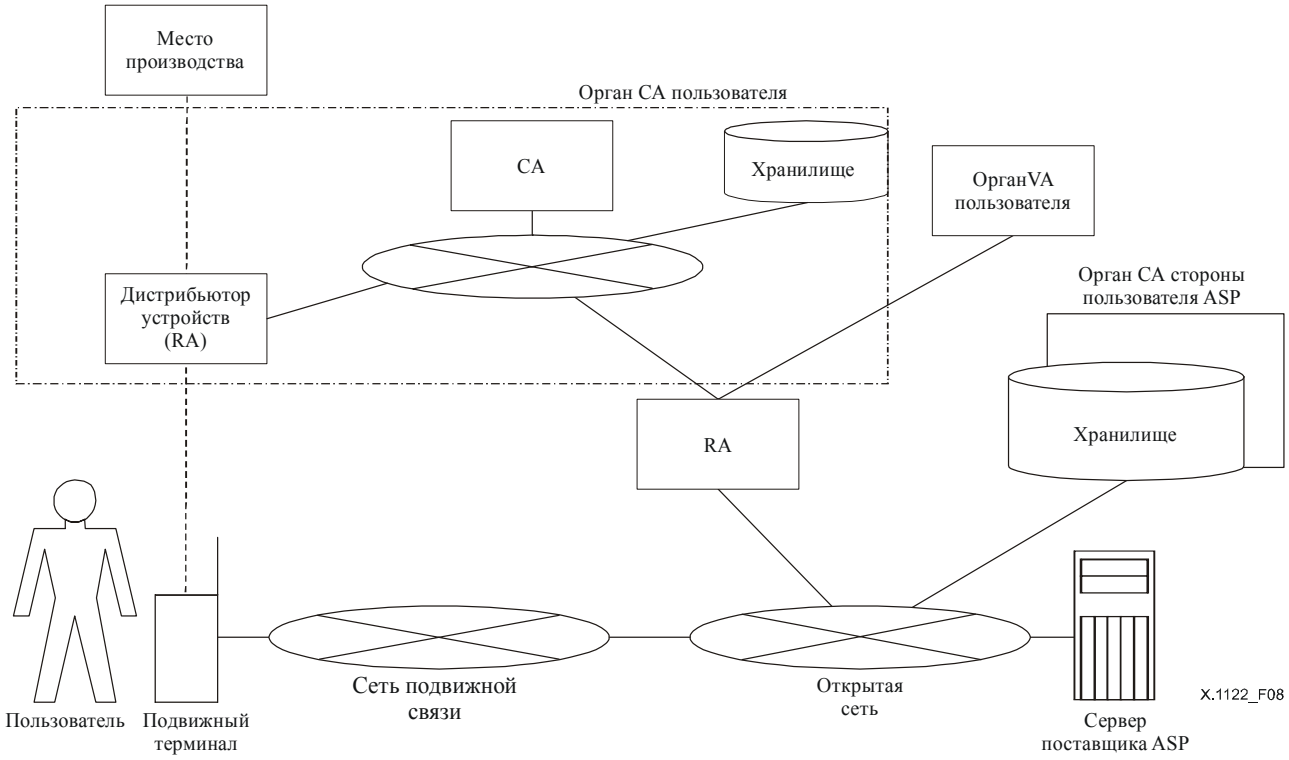

Рисунок 8/X.1122 – Пример системы, в которой оператор связи выдает сертификат для своего пользователя

9.1.1 Пример выдачи сертификата

Существуют два примера выдачи сертификата в зависимости от того места, где генерируется ключ: один пример – это метод, когда ключ генерируется на месте производства, а другой пример – это метод, когда ключ генерируется в подвижном терминале или в защищенном от подделки устройстве идентификации (подобно модулю UIM) после того, как пользователь приобретает подвижный терминал и хочет выдать сертификат.

Для применения сертификата очень важно свидетельство того, что в нем содержится частный ключ. Протокол доказательства обладания (POP) ключом дает возможность органу CA/RA проверить подлинность связи между конечным объектом и парой ключей. Необходимо, чтобы органы CA/RA обязательно требовали "соблюдения" соответствующего сертификата. Конкретный протокол POP может выполняться по-разному в зависимости от типа ключа, для которого запрошен сертификат.

На рисунке 9 приведен пример системы, в которой оператор связи выдает сертификат для своего пользователя. Этот ключ устанавливается в устройство, когда оно транспортируется от места производства. На этот сертификат делается заявка, когда пользователь приобретает это устройство у дистрибьютора, и сертификат устанавливается дистрибьютором. Это имеет место, когда выполняется протокол POP.

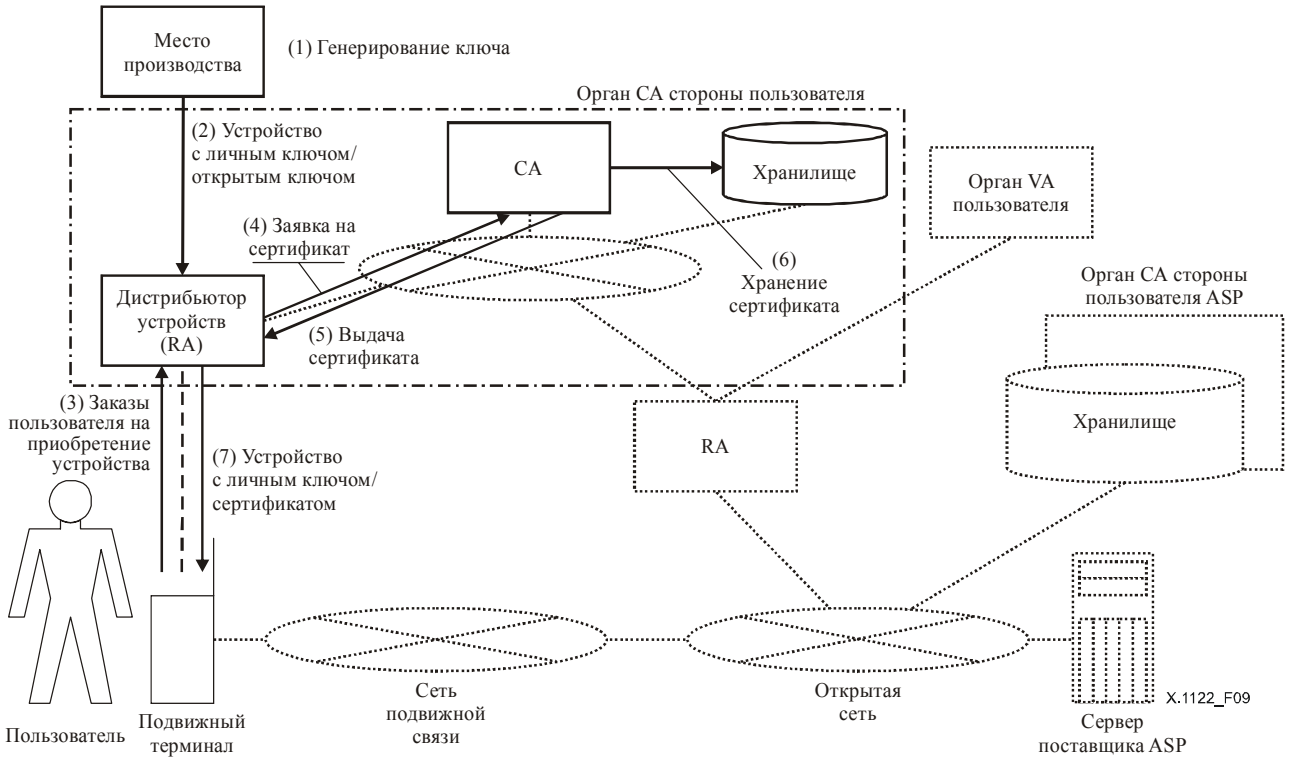

Рисунок 9/X.1122 – Пример выдачи сертификата (1)

На рисунке 10 представлен пример системы, в которой клиент генерирует ключ и сам выдает запрос на сертификат. На этот сертификат делается заявка, когда пользователь хочет получить его от органа CA, а частный ключ может оставаться секретным в подвижном терминале. Предполагается, что до выполнения описанного выше протокола как подвижному терминалу, так и органу CA следует сохранять общую секретную информацию для обеспечения целостности и аутентичности сообщения при обмене. Этот метод может защитить секретность частного ключа подвижного терминала.

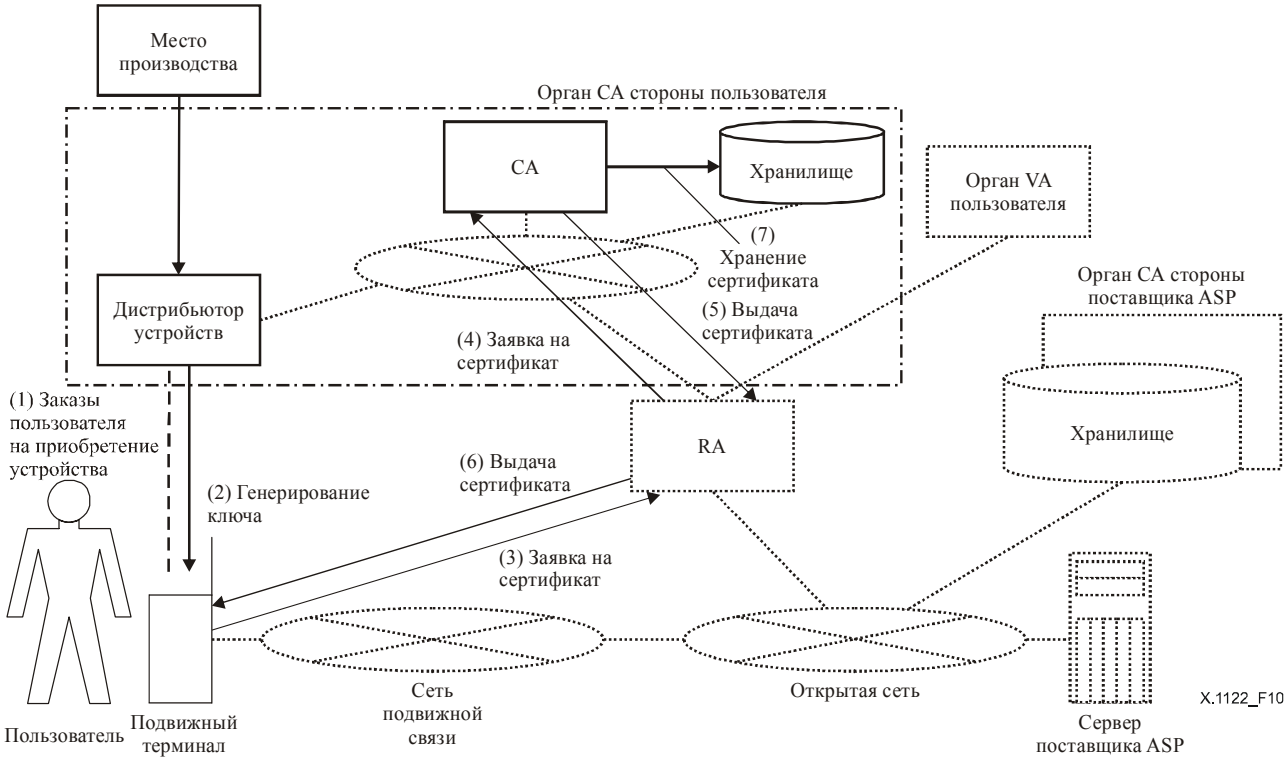

Рисунок 10/X.1122 – Пример выдачи сертификата (2)

9.1.2 Пример проверки сертификата

Вообще, мобильный терминал обладает ограниченной вычислительной мощностью и ограниченным объемом памяти. Поэтому схема проверки сертификата, основанная на списке CRL, трудна для реализации на подвижном терминале. Для подвижного терминала предпочтительна схема проверки сертификата в диалоговом режиме, когда используется орган VA. На рисунке 11 приведен пример проверки сертификата в диалоговом режиме.

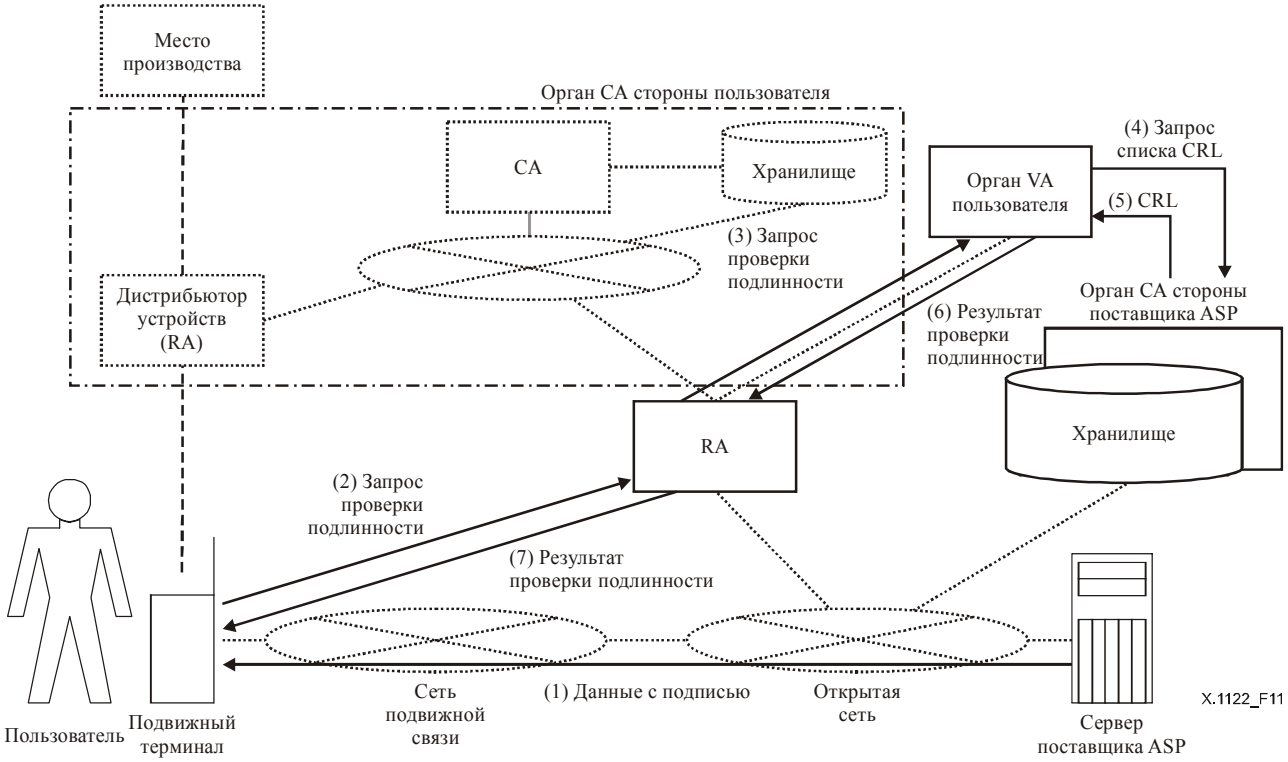

Рисунок 11/X.1122 – Пример проверки сертификата

Для проверки данных, полученных от поставщика ASP, пользователь посылает через орган RA запрос к органу VA, является ли сертификат поставщика ASP подлинным. Орган VA проверяет подлинность сертификата путем получения списка CRL от органа CA стороны поставщика ASP. Результат проверки возвращается к пользователю через орган RA. Существенно, чтобы подвижный пользователь имел возможность проверить результат проверки (см. подраздел 10.2.3.2).

9.1.3 Пример аннулирования сертификата

Чтобы аннулировать сертификат, пользователь обращается к дистрибьютору для выполнения процедуры аннулирования. Однако в случае аварийной ситуации в сети предоставляется услуга приостановки действия сертификата. Для приостановки действия сертификата органу CA через орган RA посылается соответствующая заявка. Аннулирование сертификата завершается в результате передачи органу CA подписанной заявки через орган RA. В случае потери или кражи подвижного терминала потребуются альтернативные методы приостановки действия сертификата. Например, пользователь может приостановить действие сертификата путем непосредственного обращения к дистрибьютору устройств, чтобы запросить приостановку. На рисунке 12 показан пример аннулирования сертификата.

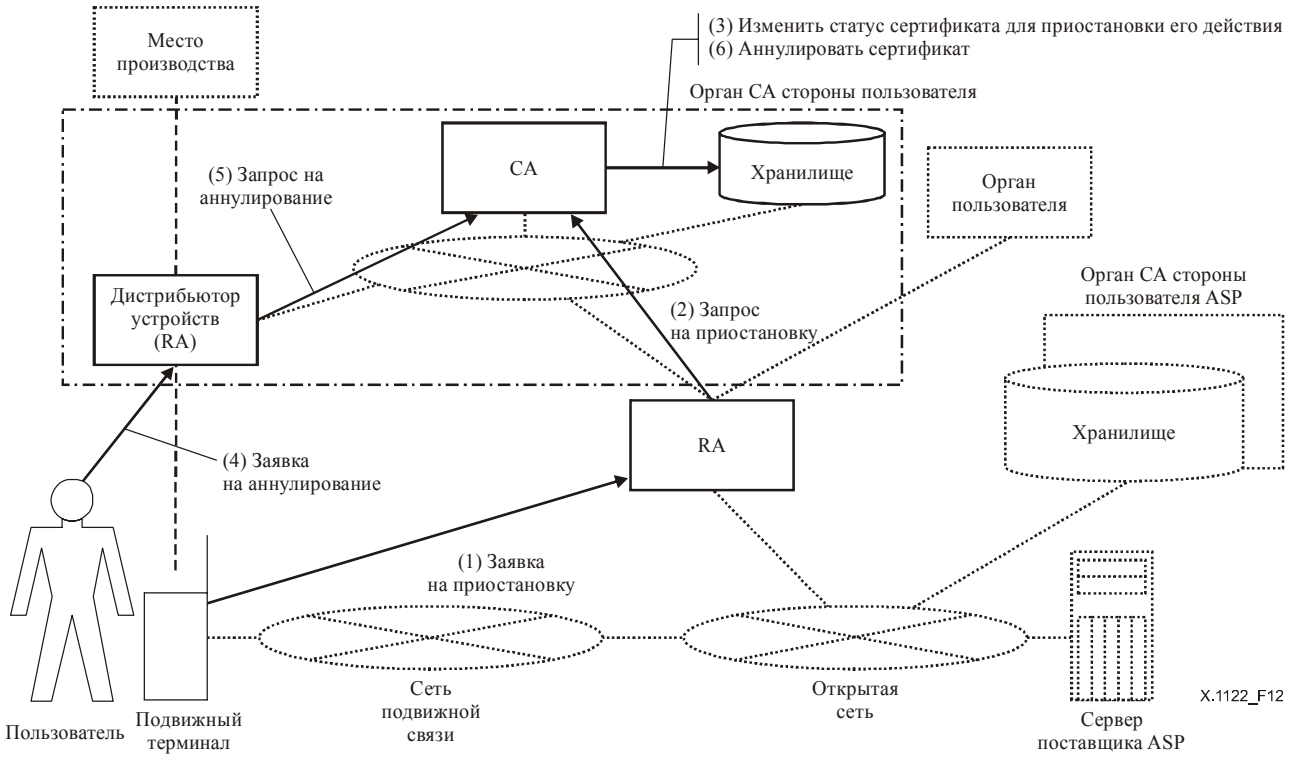

Рисунок 12/X.1122 – Пример аннулирования сертификата

9.2 Пример модели аутентификации с использованием сертификата

Ниже приводится пример модели аутентификации, когда используется сертификат.

9.2.1 Пример модели аутентификации для пользователей, операторов связи и поставщиков прикладных услуг (ASP)

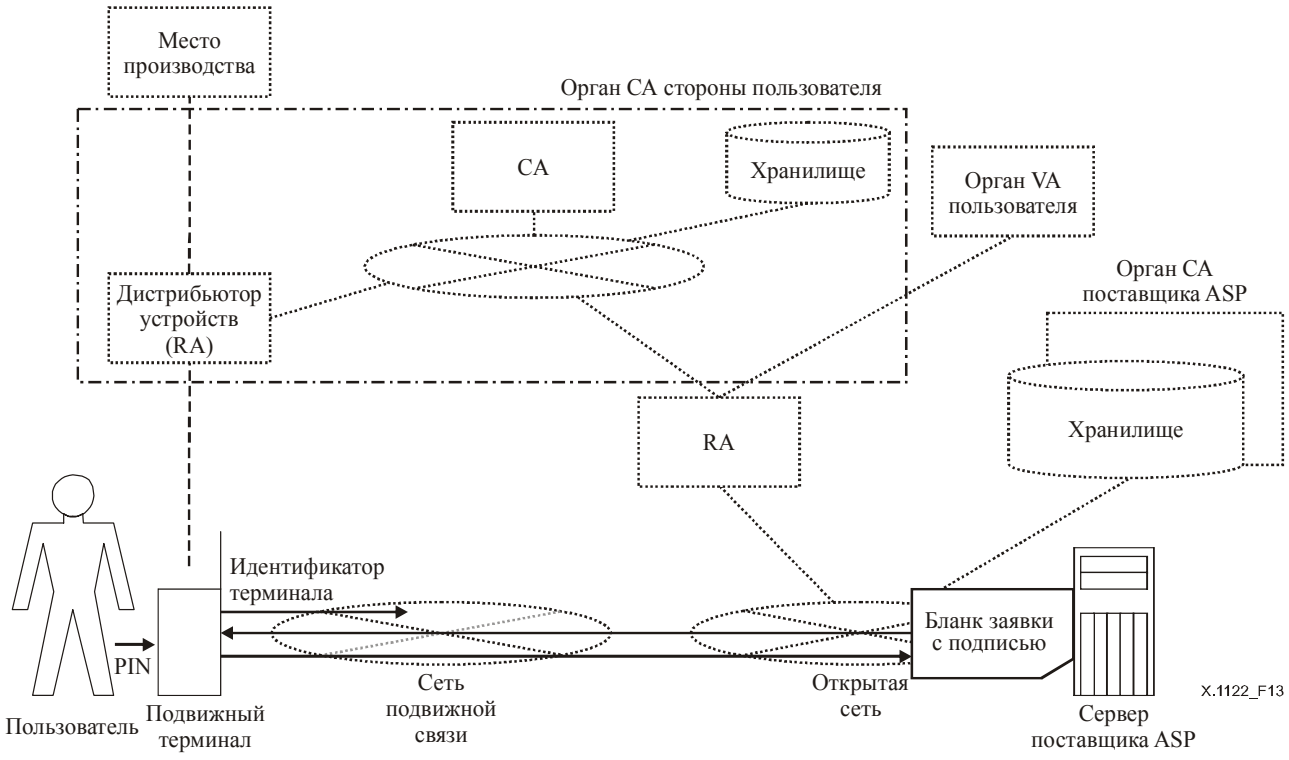

Рисунок 13/X.1122 – Пример модели аутентификации для пользователей, операторов связи и поставщиков ASP

9.2.1.1 Аутентификация пользователя подвижного терминала оператором связи

Подвижный терминал идентифицируется как легальный абонент путем представления оператору связи идентификатора терминала для данного подвижного терминала.

9.2.1.2 Аутентификация поставщика ASP пользователем подвижного терминала

Чтобы проверить, является ли поставщик ASP надежным поставщиком, проверяется сертификат этого поставщика. При этой проверке пользователь может получить сертификат самого поставщика ASP и соответствующие данные аутентификации, такие как цифровая подпись, код аутентификации сообщения и зашифрованные данные, используя частный ключ поставщика ASP, чтобы проверить его в подвижном терминале пользователя. Пользователь также может запросить орган VA проверить полученный сертификат через орган RA. Пользователь также может задать информацию URL для сертификата вместо самого сертификата. При аутентификации пользователь проверяет соответствующие данные аутентификации, используя открытый ключ, соответствующий открытому ключу в сертификате.

9.2.1.3 Аутентификация подвижного пользователя подвижным терминалом (право пользователя карточки)

Чтобы избежать незаконного использования подвижного терминала третьей стороной при использовании информации на микросхеме, такой как смарт-карточка (такой как модуль UIM), хранящейся в подвижном терминале, должна выполняться аутентификация пользователя по персональному идентификационному номеру (PIN). Может быть использована и другая схема аутентификации пользователя, подобно отпечатку пальцев.

Кроме того, для блокировки использования смарт-карточки, если устройство потеряно или украдено, следует обеспечить механизм блокировки.

9.2.1.4 Аутентификация подвижного терминала (или подвижного пользователя) поставщиком ASP

Пользователь получает сертификат на стороне поставщика ASP. Подобно аутентификации поставщика ASP подвижным терминалом, поставщик ASP может получить сертификат самого подвижного терминала (или сертификат подвижного пользователя) и соответствующие данные аутентификации, такие как цифровая подпись, код аутентификации сообщения и зашифрованные данные, используя частный ключ пользователя, чтобы проверить его у поставщика ASP. Поставщик ASP может также запросить орган VA проверить полученный сертификат. Поставщик ASP может также точно определить информацию о местонахождении сертификата вместо определения самого сертификата. При аутентификации поставщик ASP проверяет соответствующие данные аутентификации, используя открытый ключ, соответствующий открытому ключу в сертификате.

9.2.1.5 Законность заявки

Для проверки того, в действительности ли заявка исходила от подвижного терминала, который был аутентифицирован согласно алгоритму в подразделе 9.2.1.4, поставщик ASP проверяет цифровую подпись, поставленную под этой заявкой. Может быть использована функция подписи на прикладном уровне. Бланк заявки также может быть зашифрован в целях защиты от разглашения тайны.

9.2.2 Пример модели аутентификации, использующей финансовое учреждение

На рисунке 14 представлена также возможная модель аутентификации, использующая информацию о кредитной карточке или другие существующие инфраструктуры.

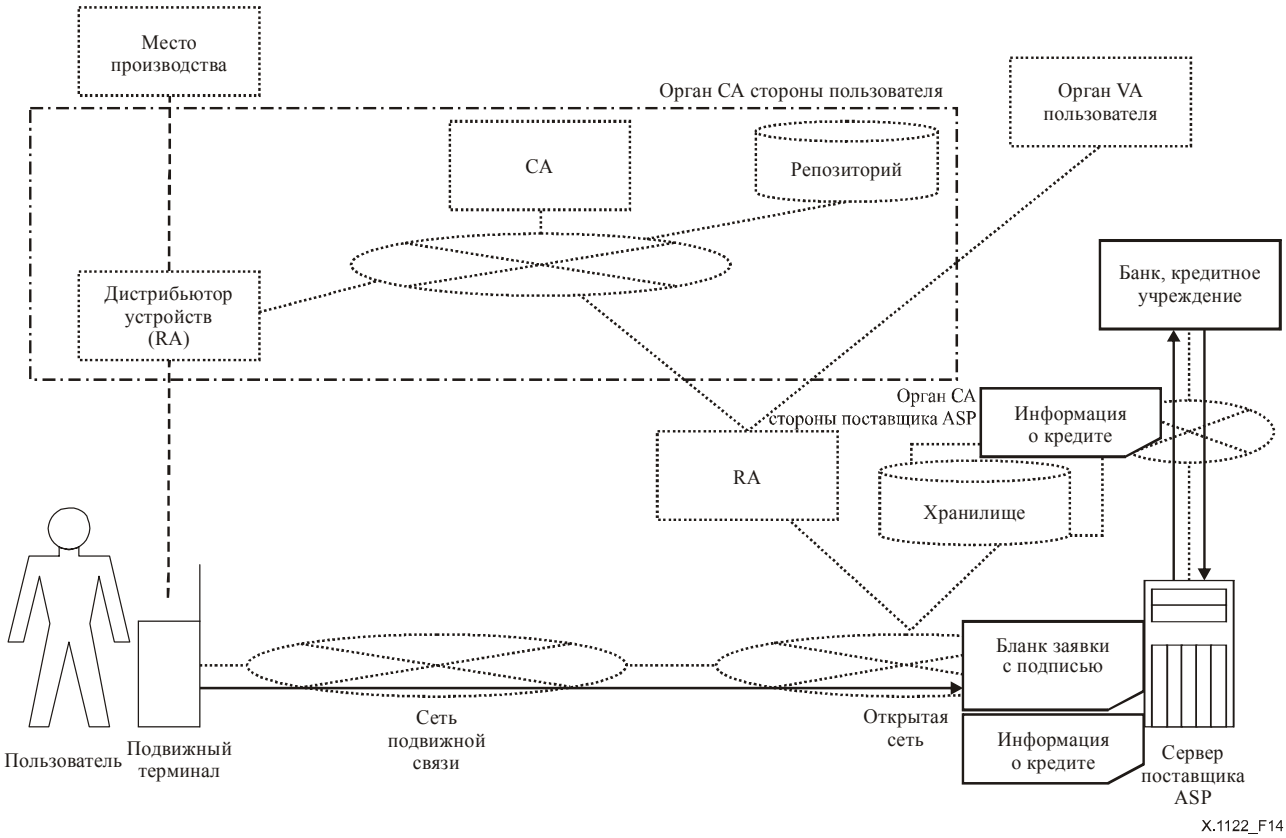

Рисунок 14/X.1122 – Пример модели аутентификации, использующей финансовое учреждение

9.2.2.1 Аутентификация пользователя банком или кредитным учреждением

Банк или кредитное учреждение получает от пользователя финансовую информацию (номер счета, номер кредитной карточки и прочее) для аутентификации этого пользователя как законного обладателя кредитной карточки.

Номер кредитной карточки и дата истечения срока пользования, хранящиеся в микросхеме смарт-карточки (в модуле UIM), используются на стороне пользователя, так что их не требуется вводить при каждой аутентификации. При аутентификации пользователя требуется информация, подобная номеру PIN, когда эта информация используется в подвижном терминале, чтобы определить законного пользователя, имеющего право доступа к этому подвижному терминалу.

Финансовая информация может быть также использована как сертификат атрибута.

При передаче информации финансового учреждения эту информацию следует зашифровать по случайному сеансовому ключу, который зашифрован открытым ключом финансового учреждения субъекта, но не открытым ключом поставщика ASP.

Результат аутентификации возвращается от финансового учреждения поставщику ASP.

9.2.2.2 Аутентификация поставщика ASP банком или кредитным учреждением

Когда вместо существующей сети с системой электронных платежей используется открытая сеть, тогда поставщик ASP должен быть аутентифицирован как официальный, наделенный соответствующими полномочиями, дистрибьютор путем представления сертификата и соответствующей информации по аутентификации, которая указывает на то, что это – официальный, наделенный соответствующими полномочиями, дистрибьютор от банка или кредитного учреждения.

9.2.2.3 Аутентификация поставщика ASP пользователем

Поставщик ASP должен быть аутентифицирован как официальный, наделенный соответствующими полномочиями, дистрибьютор путем представления пользователю сертификата и соответствующей информации по аутентификации, которая указывает на то, что это – официальный, наделенный соответствующими полномочиями, дистрибьютор от банка или кредитного учреждения. Например, сертификат атрибута, выданный банком, может быть использован для аттестации официального дистрибьютора.

10 Рассмотрение использования инфраструктуры PKI для подвижной передачи данных от конца до конца

10.1 Рассмотрение взаимодействия с существующей системой

При адаптации существующей системы, базирующейся на инфраструктуре PKI и разработанной для открытой сети, к подвижной среде сертификаты для поставщика ASP или других пользователей в открытой сети будут выдаваться и использоваться у поставщика ASP (и кроме него).

В таких случаях подвижный терминал должен уметь проверять подлинность существующих сертификатов.

Кроме того, если формат сертификата, используемого в мобильной среде, отличается от формата сертификата поставщика ASP из-за ограничений по пропускной способности или по емкости памяти, то требуется, чтобы существующая система для поставщиков ASP была модифицирована так, чтобы поставщик ASP мог проверять истинность сертификатов для подвижных терминалов.

Кроме того, если у подвижного терминала нет достаточного пространства памяти для хранения сертификата пользователя подвижного терминала, то подвижный терминал может хранить информацию URL о сертификате вместо самого сертификата, и посылать поставщику ASP информацию о местонахождении сертификата (URL). Поставщику ASP необходимо произвести выборку сертификата, используя эту информацию (URL).

В настоящее время протоколы SSL/TLS широко используются как протоколы защиты сообщений (и протоколы аутентификации) для передачи данных от конца до конца.

Однако криптографический алгоритм и/или формат сертификата, которые могут быть использованы для протокола TLS, могут оказаться непригодными для режима обработки в подвижном терминале.

Например, во многих существующих системах, использующих инфраструктуру PKI, криптографический алгоритм RSA широко используется как алгоритм электронной подписи. Однако этот алгоритм может потребовать большей вычислительной мощности, чем та, которую имеет подвижный терминал. Желательно, чтобы для условий подвижной среды использовался криптографический алгоритм, требующий меньшей вычислительной мощности и меньшего объема памяти. Одной из альтернатив алгоритму RSA является алгоритм эллиптической кривой. Криптографический алгоритм эллиптической кривой более быстр, чем алгоритм RSA, и подвижный терминал может проводить обработку по этому алгоритму за практически приемлемый период времени. Однако криптографический алгоритм эллиптической кривой еще не нашел места в спецификациях протокола TLS и прочее. Кроме того, при использовании криптографии с эллиптической кривой длина битов хэширования может превышать длину ключа, что может потребовать много времени для криптографической обработки.

Хотя предоставление органа VA с функцией проверки подписи является одним из методов разрешения упомянутой выше проблемы, другой вопрос состоит в том, как защитить связь между подвижным терминалом и органом VA.

Поскольку криптографический алгоритм с общим ключом является более быстрым, чем криптографический алгоритм с открытым ключом, то с этим алгоритмом не возникнут проблемы в техническом смысле, даже если он используется для подвижного терминала.

Кроме того, поскольку на стадии инициализации протоколы SSL/TLS обмениваются своими сертификатами, то это может потребовать большей области памяти для хранения, чем имеет мобильный терминал.

Хотя и был предложен метод преобразования протокола, использующий шлюз безопасности подвижной связи, как было упомянуто ранее, но может оказаться необходимым протокол аутентификации между поставщиком ASP и пользователем, используемый на более высоком уровне.

10.2 Вопросы использования инфраструктуры PKI в подвижной среде

10.2.1 Вопросы генерирования ключей

10.2.1.1 Генератор ключей

При использовании модели, когда пользователь генерирует пару ключей, хотя требуется, чтобы функцией генерирования ключей обладало устройство (то есть, модель, при которой ключ генерируется в устройстве, используется как место, где генерируется ключ), объем памяти и производительность обработки вызовут, вероятно, проблемы в подвижном терминале.

При использовании модели, в которой орган CA или третья сторона генерируют пару ключей, требуется рассмотрение вопросов функционирования и механизма предотвращения раскрытия ключа.

10.2.1.2 Место генерирования ключа

По причинам безопасности желательно генерировать личный ключ в устройстве, а производительность обработки будет другой возможной проблемой.

При использовании модели, в которой генерируемый вовне ключ устанавливается в устройстве, требуется механизм предотвращения раскрытия ключа.

10.2.1.3 Место хранения ключа/сертификата

Вообще, никто не может удалить личный ключ из устройства. Личный ключ должен храниться в защищенной области. Имеются два типа защищенных областей:

– Физически защищенная область: Личный ключ записывается в физически защищенную область, такую как память, доступную только для чтения (ROM), в подвижном терминале или во внешних устройствах, подобных смарт-картам.

– Область, защищенная программными средствами: Личный ключ хранится в области, защищенной программными средствами, в подвижном терминале.

Следует отметить, что защищенная программными средствами область должна быть безопасной областью, так чтобы только действительный пользователь мог повторно записать личный ключ или иметь к нему доступ: путем управления доступом и/или криптографической защиты. Типичная криптографическая защита такой информации состоит в использовании схемы шифрования на основе паролей.

Кроме того, предпочтительным является хранение открытого ключа (сертификата) пользователя и сертификата корневого органа CA в защищенной области в устройстве.

10.2.2 Вопросы заявки на сертификат и выдачи сертификата

10.2.2.1 Предварительная установка сертификата в устройстве

В моделях, при которых подвижный пользователь приобретает устройство с заранее установленным сертификатом, трудно обновить ключ и сертификат.

Кроме того, в том случае, когда сертификат не связан с подвижным пользователем, в зависимости от использования может потребоваться выдать сертификат атрибута, описывающий связь сертификата с подвижным пользователем.

10.2.2.2 Предварительная установка ключа в устройстве

Поскольку обновление ключа является трудным, то при аннулировании сертификата устройство перестает использоваться.

10.2.3 Вопросы использования сертификата

10.2.3.1 В подвижном терминале ставится цифровая подпись

В случае использования протокола TLS метод присоединения сертификатов (всех сертификатов, начиная от сертификата корневого органа CA и заканчивая сертификатом подписывающего лица) к сообщению используется как метод связи сертификата корневого органа CA с сертификатом подписывающего лица.

Однако, если к сообщению присоединяются все сертификаты от сертификата корневого органа CA до сертификата лица, ставящего подпись, то когда присоединяется подпись, это может привести к тяжелой нагрузке для подвижного терминала из-за таких ограничений, как емкость памяти подвижного терминала.

И хотя также доступны средства присоединения к сообщению информации URL, описывающей местонахождение хранящегося сертификата, эти средства еще не поддерживаются протоколом TLS.

10.2.3.2 Проверка подписи подвижным терминалом

Модели, согласно которым подлинность сертификата проверяется самим верификатором, могут оказаться непригодными для подвижных терминалов из-за множества ограничений, связанных с вычислительной мощностью и объемом памяти для хранения.

В моделях, использующих орган VA, заявка, использующая сертификат, должна иметь информацию о том органе VA, на который ее помещают. Кроме того, при связи с органом VA должна быть возможной гарантия подлинности органа VA.

В примере, приведенном в подразделе 9.1.2, подвижный терминал имеет доступ к органу VA через орган RA. В этом случае подвижному терминалу требуется функция распознавания органа RA, на который это возлагается, а также функция, удостоверяющая (выполняющая аутентификацию) тот факт, что орган RA функционирует правильно при связи с органом VA. Для органа RA требуется функция идентификации органа VA, которому "доверяет" подвижный терминал, и функция, удостоверяющая, что орган VA является подлинным, когда с ним осуществляется связь.

10.2.4 Вопросы, касающиеся органа CA

В существующих системах, использующих инфраструктуру PKI, между различными областями сертификации устанавливаются надежные связи путем построения иерархии с множеством органов CA и установления перекрестной сертификации.

Однако при проверке подлинности сертификатов каждого органа CA с целью проверки подписей возможно возникновение трудностей, связанных с вычислительной мощностью подвижного терминала.

Когда орган VA не используется, желательно создание простой структуры органов CA.

10.3 Общие вопросы, касающиеся инфраструктуры PKI

10.3.1 Вопросы генерирования ключей

10.3.1.1 Генератор ключей

В моделях, где пользователь генерирует ключи, возможно, что одно лицо сможет осуществлять поиск ключей другого лица путем перебора сертификатов, которые соответствуют сгенерированному открытому ключу, и выдавать себя за владельца этого сертификата.

Поэтому для моделей, где пользователь генерирует ключи, требуется применять ключ достаточной длины для предполагаемого числа пользователей.

Кроме того, для предотвращения легкого получения сертификата другого лица могут потребоваться определенные методы.

10.3.2 Вопросы, касающиеся заявки на сертификат/выдачи/активирования сертификата

10.3.2.1 Процедура активирования сертификата

Когда пользователь явным образом выполняет процедуру активирования сертификата, требуется механизм гарантирования того, что эта процедура выполняется самым пользователем.

Когда сертификат активируется в диалоговом режиме, пользователь ставит подпись под данными заявки на активирование и передает их в орган RA и так далее. В случае автономной обработки может быть использован такой же механизм, как и в кредитной карточке (включая обращение к оператору с запросом об активировании).

10.3.2.2 Заявка на сертификат в диалоговом режиме

Требуется механизм гарантирования целостности и аутентичности при подаче заявки. В действительности требуются проверка органа CA, проверка заявителя, защита тракта связи и прочее.

10.3.3 Вопросы, касающиеся аннулирования сертификата

Для использования модели с аннулированием в диалоговом режиме требуется механизм проверки того, что заявителем является пользователь. Особенно в случае, когда сертификат аннулирован из-за потери личного ключа, идентификация заявителя по цифровой подписи не может быть использована. Поэтому должен быть предоставлен другой метод (такой, как идентификация по номеру PIN).

Для использования модели с аннулированием в автономном режиме может потребоваться в экстренном случае предоставление механизма "приостановки" действия сертификата в диалоговом режиме.

10.3.4 Вопросы обновления сертификата

В дополнение к вопросам, связанным с заявкой на сертификат и аннулированием сертификата, как единственной в своем роде проблеме по обновлению сертификата, с точки зрения доступности системы требуется решение по предотвращению отмены обновления сертификата.

10.3.5 Проблема с описанием сертификата

Информация, содержащаяся в сертификате, должна быть тщательно проверена ввиду возможности того, что сертификат будет широко распространяться без ведома выдающего сертификата.

Добавление I

Примеры моделей сервисных средств

В данном добавлении приводится описание моделей сервисных средств инфраструктуры PKI для подвижной связи.

I.1 Модели сервисных средств управления сертификатами

В разделе 9 дан пример автономного использования системы, в которой сертификаты выдает оператор связи. В данном добавлении содержатся другие модели сервисных средств управления сертификатами.

I.1.1 Пример системы, в которой поставщик ASP выдает сертификаты

На примерах на рисунках I.1 и I.2 представлены два вида сертификатов: первый сертификат предоставляется органом CA 1-го сегмента (см. рисунок I.1), являющимся органом CA оператора связи, предоставляющего сертификат подвижному терминалу, который используется при безопасной транспортировке сеанса. Второй сертификат предоставляется органом CA 2-го сегмента (см. рисунок I.2), являющимся органом CA поставщика ASP, предоставляющего сертификат подвижному терминалу, для использования при всех применениях подвижного терминала. Поставщик ASP использует сертификат органа CA, выданный оператором связи для выдачи своего собственного сертификата. Для выдачи/аннулирования сертификата система на стороне оператора связи (орган CA 1-го сегмента) использует автономную обработку, а система на стороне поставщика ASP (орган CA 2-го сегмента) использует обработку в диалоговом режиме. Между тем при подаче заявки на сертификат система на стороне поставщика ASP (орган CA 2-го сегмента) использует сертификат, выданный оператором связи (орган CA 1-го сегмента) в качестве защиты тракта связи и аутентификации заявителя и принимает заявку в диалоговом режиме.

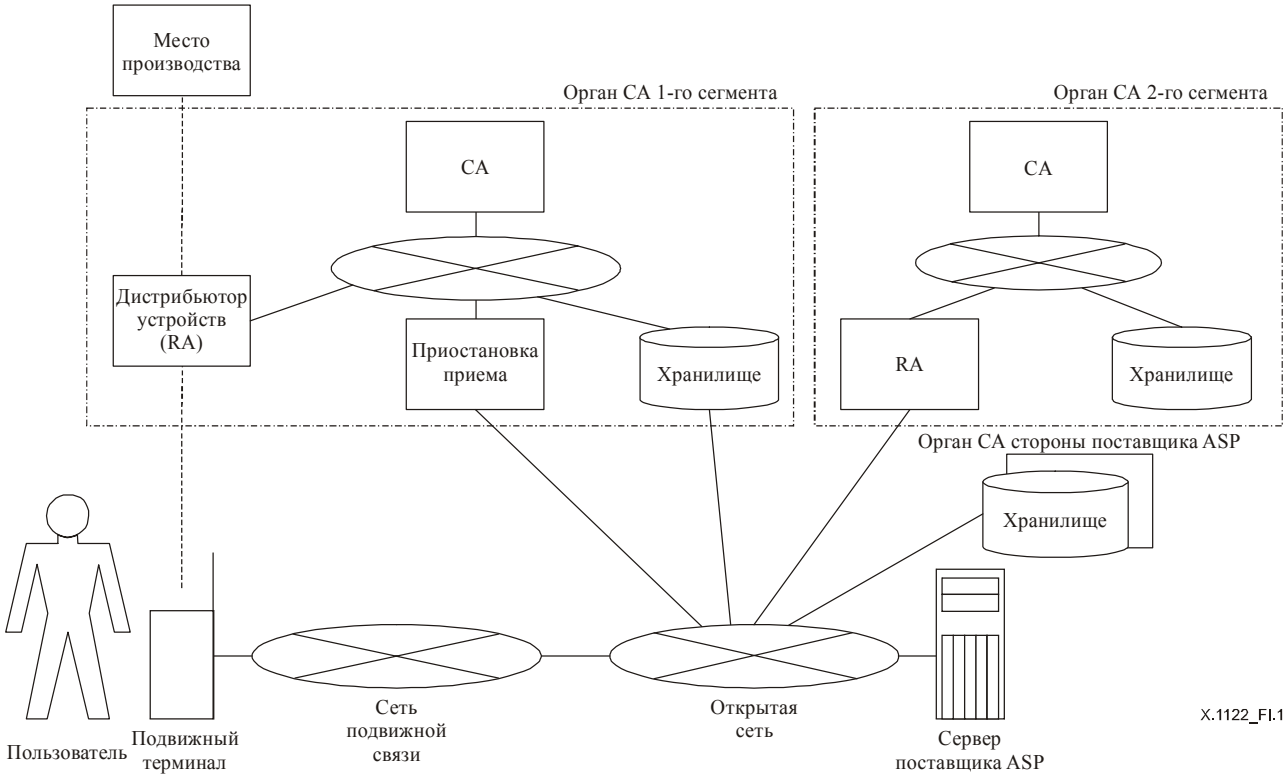

Рисунок I.1/X.1122 – Пример системы, в которой поставщик ASP выдает сертификаты

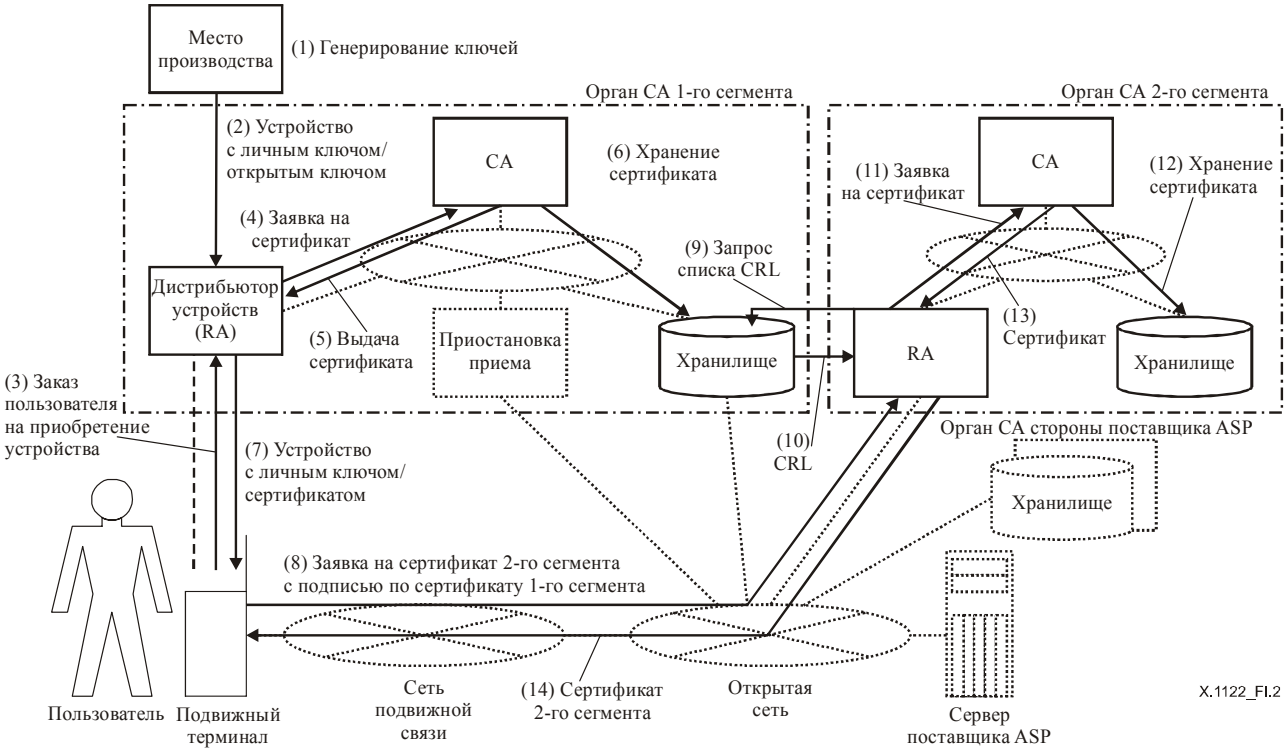

Рисунок I.2/X.1122 – Пример выдачи сертификатов 2-го сегмента

Для аннулирования сертификата, выданного органом CA 2-го сегмента, пользователь использует доступ к органу RA через сеть и выполняет процедуру аннулирования.

I.1.2 Пример системы, в которой используется сертификат атрибута

В данном примере (см. рисунок I.3) предполагается, что поставщик ASP использует сертификат, выданный оператором связи для идентификации заявителя и так далее, и использует сертификат атрибута, например, для более сложного управления доступом. Хотя орган AA пользователя используется для выдачи пользователю сертификата атрибута, орган CA используется для выдачи пользователю сертификата.

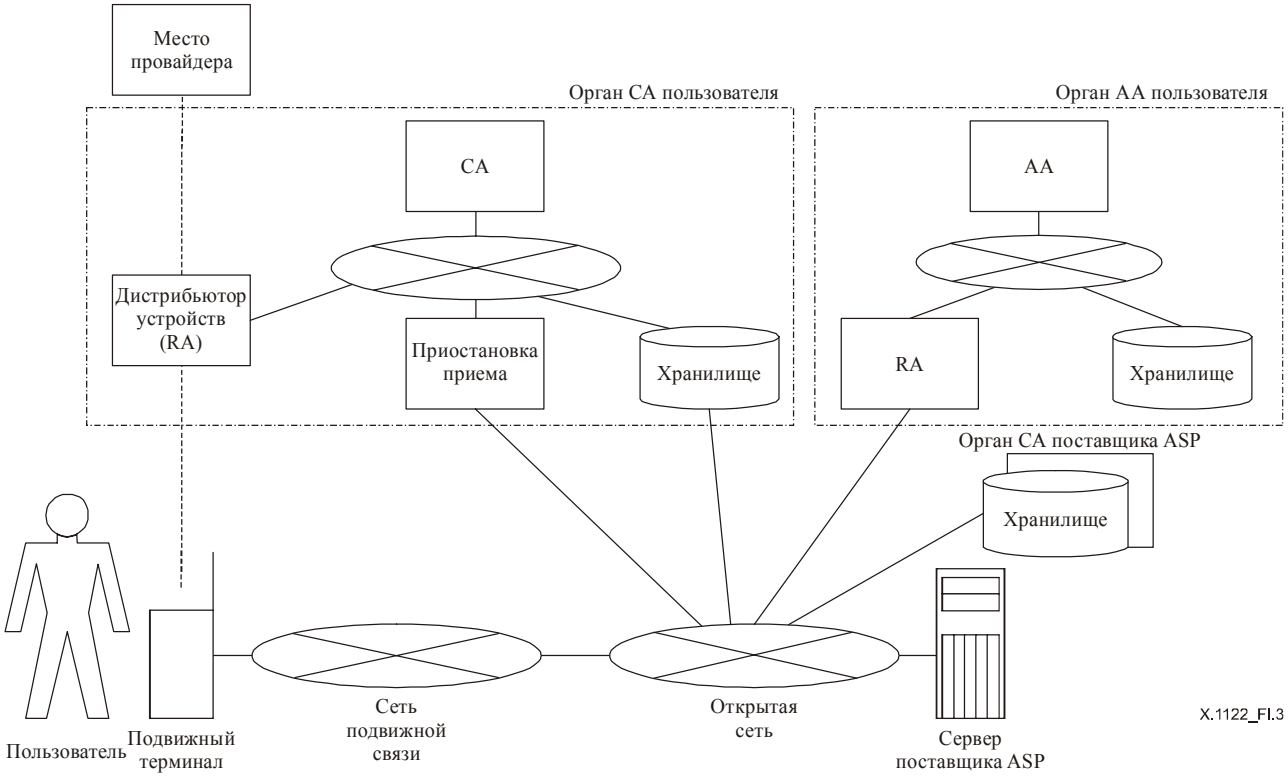

Рисунок I.3/X.1122 – Пример системы, в которой используется сертификат атрибута

В системе на стороне оператора связи (орган CA пользователя) используется обработка в автономном режиме при выдаче и аннулировании сертификата и используется орган VA для проверки сертификата.

Система на стороне поставщика ASP (орган AA пользователя) принимает в диалоговом режиме заявку от пользователя, генерирует сертификат атрибута на основе правил подачи заявки и затем связывает его с сертификатом, выданным оператором связи. Сертификат атрибута хранится в хранилище в органе AA. (Также возможна модель, в которой сертификат атрибута передается пользователю).

Если поставщик ASP получил данные с подписью от своего пользователя, он сначала получает список CRL из хранилища органа CA стороны оператора связи для проверки подлинности сертификата. (В месте продажи также проверяется подпись под данными, переданными от пользователя). Затем поставщик ASP получает сертификат атрибута от органа AA стороны поставщика ASP для проверки, имеет ли пользователь право на использование сервисных средств (см. рисунок I.4).

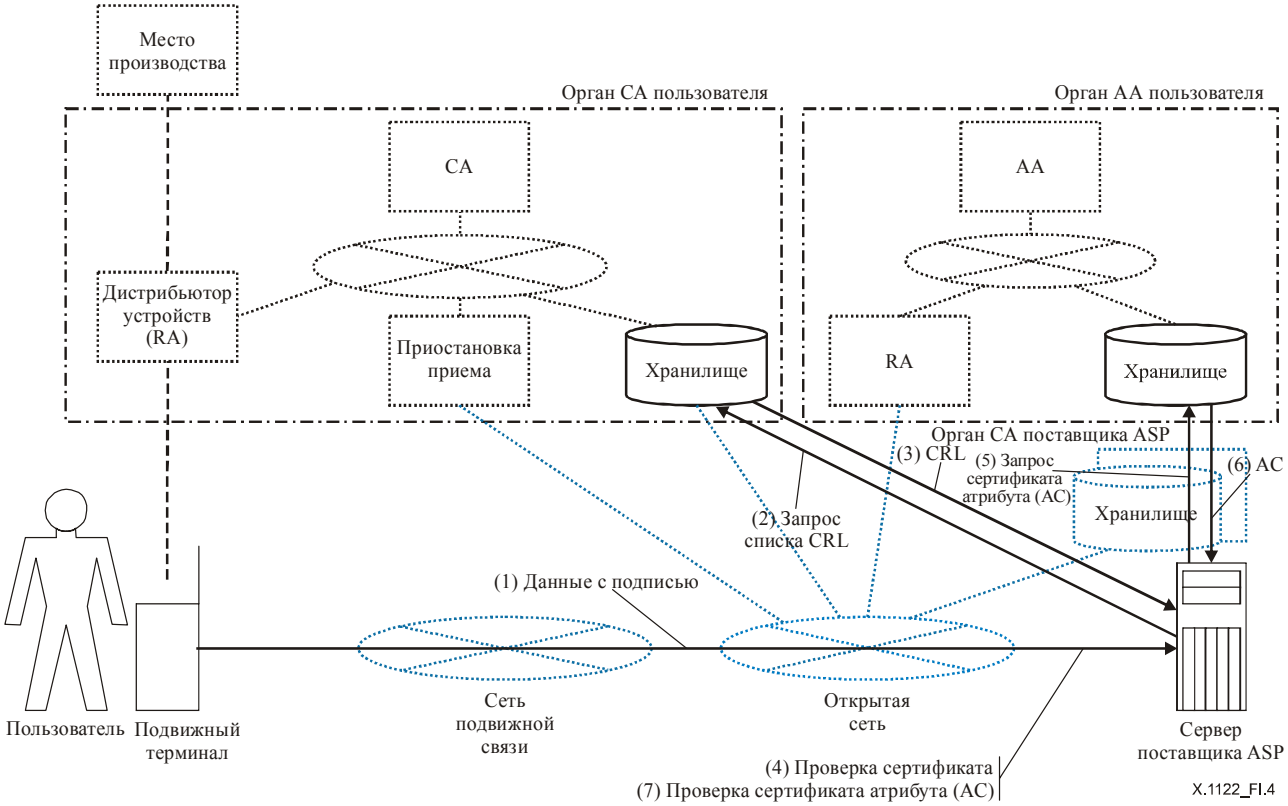

Рисунок I.4/X.1122 – Пример модели аутентификации, использующей сертификат атрибута

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
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	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
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 и взаимосвязь открытых систем**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола (IP) и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2005 г.