Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1154

(04/2013)

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

Безопасные приложения и услуги – Протоколы безопасности

Общая структура комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности

Рекомендация МСЭ-Т X.1154

ITU-T

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
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

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

Рекомендация МСЭ-Т X.1154

Общая структура комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности

Резюме

В последнее время, вследствие роста числа краж идентичности (ID), многим прикладным услугам, особенно финансовым услугам, требуются более надежные или комбинированные методы аутентификации, такие как многофакторная аутентификация. Например, вместо традиционной аутентификации на основе пароля используются аутентификация с помощью одноразового пароля и другие новые методы аутентификации.

Комбинации методов аутентификации предоставляют нескольким поставщикам услуг определения идентичности (IdSP) возможность повысить гарантию аутентификации. В Рекомендации МСЭ-Т X.1154 приводится общая структура комбинированной аутентификации в среде с несколькими IdSP применительно к поставщику услуг. В данной Рекомендации рассматриваются три типа методов комбинированной аутентификации: многофакторная аутентификация, аутентификация по нескольким методам и множественная аутентификация.

В структуре, представленной в настоящей Рекомендации, описываются модели, базовые операции и требования к безопасности для каждого компонента модели и каждого сообщения между компонентами модели, предназначенные для поддержания общего уровня гарантии аутентификации в условиях объединения нескольких IdSP.

Кроме того, в этой структуре описываются также модели, базовые операции и требования к безопасности для обеспечения услуги аутентификации, которая управляет объединением нескольких IdSP.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1154	26.04.2013 г.	17-я

Ключевые слова

Аутентификация объекта, комбинированная аутентификация, многофакторная аутентификация.

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 не получил извещения 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

Введение

В последнее время, вследствие роста числа краж идентичности (ID), многим прикладным услугам, особенно финансовым услугам, требуются более надежные или комбинированные методы аутентификации, такие как многофакторная аутентификация. Например, вместо традиционной аутентификации на основе пароля используются аутентификация с помощью одноразового пароля и другие новые методы аутентификации.

Рекомендации МСЭ-Т, которые касаются аутентификации применительно к безопасной прикладной услуге, см. [b-ITU-T X.509] и [ITU-T X.1141], являются стандартами систем аутентификации. В этих Рекомендациях МСЭ-Т в основном считается, что один поставщик услуг и/или один пользователь принадлежат к одному домену безопасности, обеспечиваемому одним IdSP, даже если поставщик услуг и пользователь принадлежат к разным доменам безопасности. Чтобы добиться улучшенной аутентификации, IdSP требует реализации методов более строгой аутентификации (например, методов, изложенных в [b-ITU-T X.1151], [b-ITU-T X.1084], [b-ITU-T X.1086] и [b-ITU-T X.1089]).

С другой стороны, нередко случается так, что один пользователь получает несколько идентичностей от нескольких IdSP, и один поставщик услуг устанавливает отношения доверия с несколькими IdSP. В этой среде с несколькими IdSP может существовать какой-либо альтернативный способ улучшить аутентификацию, в случае если один поставщик услуг использует нескольких IdSP для аутентификации пользователя.

Кроме того, даже если поставщик услуг реализует более строгую аутентификацию, для объединения нескольких IdSP может использоваться поставщик сопряжения услуг определения идентичности.

Однако, в связи с тем что каждый IdSP находится в ведении разных поставщиков, простое объединение нескольких IdSP может привести к разрушению всего уровня аутентификации.

В связи с этим требуется общая структура для описания моделей, базовых операций и требований к безопасности для каждого компонента модели и каждого сообщения между компонентами модели для обеспечения общего уровня гарантии аутентификации в условиях объединения нескольких IdSP.

Кроме того, требование более строгой/надежной аутентификации повышает сложность реализации системы аутентификации и/или управления этой системой. В связи с этим используется услуга аутентификации, которая управляет объединением нескольких IdSP, для аутентификации пользователя от имени прикладной услуги. Данная услуга аутентификации требуется для управления объединением нескольких IdSP, которые удовлетворяют политике аутентификации каждой прикладной услуги.

Эта структура необходима также для описания моделей, базовых операций и требований к безопасности, обеспечивающих услугу аутентификации.

Рекомендация МСЭ-Т X.1154

Общая структура комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности

1 Сфера применения

В настоящей Рекомендации представлена общая структура комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности (IdSP), предназначенная для поставщика услуг, которая обеспечивает комбинированную аутентификацию, например многофакторную аутентификацию.

В представленной в настоящей Рекомендации структуре описываются модели, базовые операции и требования к безопасности для каждого компонента модели и каждого сообщения между компонентами модели, предназначенные для поддержания общего уровня гарантии аутентификации в условиях объединения нескольких IdSP.

Кроме того, в этой структуре описываются также модели, базовые операции и требования к безопасности для обеспечения услуги аутентификации, которая управляет объединением нескольких IdSP.

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.1141] Рекомендация МСЭ-Т X.1141 (2006 г.), *Язык разметки, предусматривающий защиту данных (SAML 2.0)*.

[ITU-T X.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 утверждение (assertion) [b-ITU-T X.1252]: Заявление, сделанное объектом и не сопровождаемое доказательствами его истинности.

3.1.2 уровень гарантии (assurance level) [b-ITU-T X.1252]: Уровень доверия к связи между объектом и представленной информацией идентичности.

3.1.3 аутентификация (authentication) [b-ITU-T X.1252]: Процесс достижения достаточной меры доверия к связи между объектом и представленной идентичностью.

3.1.4 гарантия аутентификации (authentication assurance) [b-ITU-T X.1252]: Степень доверия, достигаемого в процессе аутентификации, в отношении того, что партнер по связи является тем объектом, которым он утверждает, что является, или которым ожидается, что он является.

ПРИМЕЧАНИЕ. − Доверие основано на степени доверия к связи между осуществляющим связь объектом и представленной идентичностью.

3.1.5 конечный пользователь (end user) [ITU-T X.1141]: Человек, который использует ресурсы для прикладных целей.

3.1.6 идентификатор (identifier) [b-ITU-T X.1252]: Один или несколько атрибутов, используемых для идентификации объекта в том или ином контексте.

3.1.7 идентичность (identity) [b-ITU-T X.1252]: Представление какого-либо объекта в виде одного или нескольких атрибутов, которые позволяют однозначно распознать объекты в каком-либо контексте в той мере, в какой это необходимо. В целях управления определением идентичности (IdM) термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), т. е. разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует.

ПРИМЕЧАНИЕ. – Каждый объект представлен одной целостной идентичностью, которая включает все возможные элементы информации, характеризующие такой объект (атрибуты). Вместе с тем такая целостная идентичность является теоретическим понятием и не может быть описана и практически использована, поскольку число всех возможных атрибутов бесконечно.

3.1.8 поставщик сопряжения услуг определения идентичности (identity service bridge provider) [b-ITU-T X.1252]: Поставщик услуг определения идентичности, выступающий в качестве доверенного посредника между другими поставщиками услуг определения идентичности.

3.1.9 поставщик услуг определения идентичности (identity service provider) (IdSP) [b-ITU-T X.1252]: Объект, который проверяет, поддерживает информацию об идентичности других объектов, управляет ею и может ее создавать и назначать.

3.1.10 полагающаяся сторона (relying party) [ITU-T X.1141]: Объект системы, который принимает решение о выполнении действий на основе информации от другого объекта системы. Например, полагающаяся сторона SAML зависит от принимаемых утверждений о субъекте от подтверждающей стороны (ответственного органа SAML).

3.1.11 поставщик услуг (service provider) [ITU-T X.1141]: Роль, выполняемая объектом системы, когда объект системы предоставляет услуги клиентам и/или другим объектам системы.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 фактор аутентификации (authentication factor): Тип регистрационных данных; существует три типа факторов аутентификации: фактор владения, фактор знания и биометрический фактор.

3.2.2 биометрический фактор (biometric factor): Фактор аутентификации, обеспечивающий проверку чего-либо, чем является пользователь или что делает пользователь.

3.2.3 комбинированная аутентификация (combined authentication): Аутентификация, при которой используется несколько типов регистрационных данных.

3.2.4 существующий уровень гарантии (current assurance level): Уровень гарантии аутентификации какого-либо конкретного объекта в данный момент времени.

3.2.5 фактор знания (knowledge factor): Фактор аутентификации, обеспечивающий проверку чего-либо, что знает пользователь.

3.2.6 многофакторная аутентификация (multifactor authentication): Аутентификация, при которой используется несколько типов регистрационных данных, относящихся к двум или более из трех категорий факторов аутентификации.

3.2.7 аутентификация по нескольким методам (multi-method authentication): Аутентификация, при которой используется несколько типов регистрационных данных, относящихся к разным методам аутентификации.

3.2.8 множественная аутентификация (multiple authentication): Аутентификация, при которой используется несколько типов регистрационных данных, относящейся к одним и тем же методам аутентификации.

3.2.9 фактор принадлежности (ownership factor): Фактор аутентификации, обеспечивающий проверку чего-либо, что имеет пользователь.

3.2.10 обеспечиваемый уровень гарантии (provided assurance level): Уровень гарантии, который обеспечивается конкретными поставщиками услуг определения идентичности при аутентификации пользователя, осуществляемой IdSP.

3.2.11 требуемый уровень гарантии (required assurance level): Уровень гарантии, который требует обеспечить какой-либо конкретный поставщик услуг для предоставления своей услуги.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ID	Identity	Идентичность
IdM	Identity Management	Управление определением идентичности
IdSP	Identity Service Provider	Поставщик услуг определения идентичности
PKI	Public Key Infrastructure	Инфраструктура открытых ключей
SAML	Security Assertion Markup Language	Язык разметки утверждений безопасности
SP	Service Provider	Поставщик услуг

5 Условные обозначения

В данной Рекомендации:

Слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этой Рекомендации.

Слова "рекомендуется, чтобы" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии это требование не является обязательным.

Слова "запрещается" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этой Рекомендации.

Ключевые слова "может быть дополнительно" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Этот термин не означает, что вариант реализации поставщика должен обеспечивать выполнение этой функции, и что функция может быть активирована по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может дополнительно предоставить эту функцию и по-прежнему заявлять о соответствии этой Рекомендации.

6 Типы комбинированной аутентификации

В настоящей Рекомендации рассматриваются следующие три типа методов комбинированной аутентификации:

- Многофакторная аутентификация, при которой используется несколько типов регистрационных данных, относящихся к двум или более из трех категорий факторов аутентификации. Примерами многофакторной аутентификации являются, например, (1) аутентификация с использованием сертификата открытого ключа, хранящегося в смарт-карте; (2) аутентификация с помощью одноразового пароля, который используется аппаратным устройством; и (3) аутентификация посредством комбинирования аутентификации по одноразовому паролю и биометрической аутентификации.
- Аутентификация по нескольким методам, при которой используется несколько типов регистрационных данных, относящихся к разным методам аутентификации. Примерами аутентификации по нескольким методам являются, например, (1) аутентификация посредством комбинирования аутентификации по одноразовому паролю и аутентификации по кодовой фразе; и (2) аутентификация посредством комбинирования аутентификации по отпечатку пальца и аутентификации по кровеносным сосудам пальца.

− Множественная аутентификация, при которой используется несколько типов регистрационных данных, относящихся к одним и тем же методам аутентификации. Примерами множественной аутентификации являются, например, (1) аутентификация по двойному паролю; и (2) аутентификация по отпечатку пальца с использованием нескольких отпечатков пальцев.

Различие между указанными выше тремя методами аутентификации состоит в комбинации типов регистрационных данных. Кроме того, "фактор аутентификации" обеспечивает разделение регистрационных данных по группам. При этом существует три типа факторов аутентификации: фактор принадлежности, фактор знания и биометрический фактор.

− Фактор принадлежности − это фактор аутентификации, обеспечивающий проверку чего-либо, что имеет пользователь. К числу примеров относятся смарт-карта, метка безопасности, программная метка, телефоны фиксированной связи и мобильные телефоны.

− Фактор знания − это фактор аутентификации, обеспечивающий проверку чего-либо, что знает пользователь. К числу примеров относятся пароль, кодовая фраза и персональный идентификационный номер (PIN).

− Биометрический фактор − это фактор аутентификации, обеспечивающий проверку чего-либо, чем является пользователь или что делает пользователь. К числу примеров относятся отпечатки пальцев, кровеносные сосуды пальцев и радужная оболочка глаза.

7 Модели аутентификации в среде с несколькими IdSP

7.1 Базовые модели относительно поставщика услуг

При рассмотрении модели аутентификации с точки зрения поставщика в моделях аутентификации, в которых пользователь получает прикладную услугу, должны учитываться следующие факторы:

− Метод аутентификации, обеспечиваемый IdSP, является методом однофакторной аутентификации или комбинированной аутентификации.

− Модель включает одного IdSP или несколько IdSP; эти IdSP обеспечивают один и тот же метод или разные методы. Если множество IdSP обеспечивают разные методы, то эти методы связаны с разными факторами или одним и тем же фактором.

  Следовательно, существует восемь типов функциональных моделей в соответствии с числом поставщиков услуг и IdSP, а также один тип комбинированной аутентификации, позволяющих добиться комбинированной аутентификации (таблица 1). Кроме того, если имеется несколько пользователей в среде с несколькими IdSP, то какой-либо один пользователь может и не иметь отношений доверия со всеми IdSP. Другими словами, IdSP могут быть сгруппированы с точки зрения совокупности пользователей, у которых имеются отношения доверия с ними (рисунок 1). В этом случае учитывается также следующий фактор.

− IdSP отнесены к одной группе или нескольким группам с точки зрения отношений доверия с пользователями.

Если IdSP отнесены к одной группе, то можно применять модели T-3−T-8 из таблицы 1.

Если IdSP отнесены более чем к двум группам, то можно учитывать модели T-9−T-14 (см. таблицу 2).

Таблица 1 − Базовые модели аутентификации (если IdSP отнесены к одной группе)

	Кол-во IdSP	**Кол-во типов методов аутентификации**	**Тип метода аутентификации, обеспечиваемого одним IdSP**	**Кол-во групп IdSP**	**Метод аутентификации, обеспечиваемый путем комбинации IdSP**
T-1	Один	Один	Однофакторный	Одна	Отсутствует
T-2			Комбинированный	Одна	Комбинированный (Примечание 1)
T-3	Несколько	Один	Однофакторный	Одна	Множественный
T-4			Комбинированный	Одна	Комбинированный (Примечание 1)
T-5		Несколько (разные методы)	Однофакторный	Одна	Множественный, по нескольким методам (Примечание 2)
T-6			Комбинированный (множественный или по нескольким методам)	Одна	Множественный, по нескольким методам (Примечание 3)
T-7		Несколько (разные факторы)	Однофакторный	Одна	Множественный, по нескольким методам, многофакторный (Примечание 2)
T-8			Комбинированный	Одна	Комбинированный (Примечание 3)

ПРИМЕЧАНИЕ 1. − Могут быть обеспечены все три типа комбинированной аутентификации. Однако обеспечиваемый метод аутентификации зависит от типа аутентификации, обеспечиваемой IdSP.

ПРИМЕЧАНИЕ 2. − Могут быть обеспечены все три типа комбинированной аутентификации. Однако обеспечиваемый метод аутентификации зависит от выбранных IdSP.

ПРИМЕЧАНИЕ 3. − Могут быть обеспечены все три типа комбинированной аутентификации. Однако обеспечиваемый метод аутентификации зависит не только от типа аутентификации, обеспечиваемой IdSP, но и от выбранных IdSP.

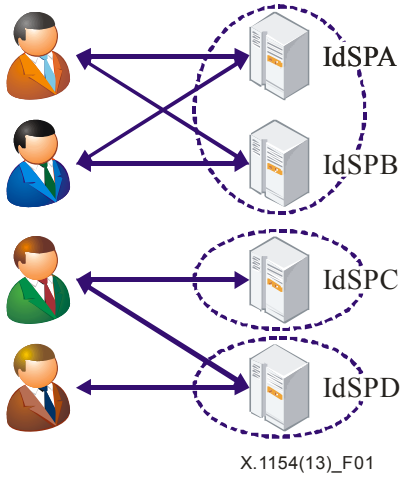

Рисунок 1 − Пример образования нескольких групп IdSP с точки зрения отношений доверия с пользователями

Таблица 2 − Базовые модели аутентификации (если IdSP отнесены к нескольким группам)

	Кол-во IdSP	Кол-во типов методов аутентификации	Тип метода аутентификации, обеспечиваемого одним IdSP	Кол-во групп IdSP	Метод аутентификации, обеспечиваемый путем комбинации IdSP
T-9	Несколько	Один	Однофакторный	Несколько	Множественный
T-10			Комбинированный	Несколько	Комбинированный (Примечание 1)
T-11		Несколько (разные методы)	Однофакторный	Несколько	Множественный, по нескольким методам (Примечание 2)
T-12			Комбинированный (множественный или по нескольким методам)	Одна	Множественный, по нескольким методам (Примечание 3)
T-13		Несколько (разные факторы)	Однофакторный	Несколько	Множественный, по нескольким методам, многофакторный (Примечание 2)
T-14			Комбинированный	Несколько	Комбинированный (Примечание 3)
ПРИМЕЧАНИЕ 1. − Могут быть обеспечены все три типа комбинированной аутентификации. Однако обеспечиваемый метод аутентификации зависит от типа аутентификации, обеспечиваемой IdSP. ПРИМЕЧАНИЕ 2. − Могут быть обеспечены все три типа комбинированной аутентификации. Однако обеспечиваемый метод аутентификации зависит от выбранных IdSP. ПРИМЕЧАНИЕ 3. − Могут быть обеспечены все три типа комбинированной аутентификации. Однако обеспечиваемый метод аутентификации зависит не только от типа аутентификации, обеспечиваемой IdSP, но и от выбранных IdSP.					

7.1.1 Модель T-1

Модель T-1 является моделью, в которой один IdSP обеспечивает однофакторную аутентификацию, и в которой IdSP, поставщик услуг и один или несколько терминалов соединены друг с другом по сети.

Когда поставщик услуг получает от терминала запрос на обслуживание, поставщик услуг просит IdSP аутентифицировать пользователя. IdSP, который получает запрос на аутентификацию от поставщика услуг, аутентифицирует пользователя с использованием метода однофакторной аутентификации. Если результаты аутентификации, полученные от IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет свою услугу терминалу.

Эта модель не способна обеспечить комбинированную аутентификацию, поэтому она не входит в сферу применения настоящей Рекомендации.

7.1.2 Модель T-2

Модель T-2 является моделью, в которой один IdSP обеспечивает комбинированную аутентификацию (множественную, по нескольким методам или многофакторную аутентификацию), и в которой IdSP, поставщик услуг и один или несколько терминалов соединены друг с другом по сети.

Когда поставщик услуг получает от терминала запрос на обслуживание, поставщик услуг просит IdSP аутентифицировать пользователя. IdSP, который получает запрос на аутентификацию от поставщика услуг, аутентифицирует пользователя с использованием метода комбинированной аутентификации. Если результаты аутентификации, полученные от IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет свою услугу терминалу.

Эта модель способна обеспечить любой тип метода комбинированной аутентификации, однако она зависит от типа метода аутентификации, обеспечиваемого IdSP.

7.1.3 Модель T-3

Модель T-3 является моделью, в которой несколько IdSP обеспечивают один и тот же метод однофакторной аутентификации и в которой несколько IdSP, поставщик услуг и один или несколько терминалов соединены друг с другом по сети. Как правило, в модели T-3 все пользователи имеют отношения доверия со всеми IdSP.

Когда поставщик услуг получает от терминала запрос на обслуживание, поставщик услуг выбирает несколько IdSP, удовлетворяющих требуемому уровню гарантии аутентификации, и просит выбранные IdSP аутентифицировать пользователя. Если все результаты аутентификации, полученные от этих IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет свою услугу терминалу.

Эта модель способна обеспечить метод множественной аутентификации.

Следует отметить, что эта модель способна обеспечить однофакторную аутентификацию, если метод аутентификации, обеспечиваемый одним IdSP, удовлетворяет требуемому уровню гарантии аутентификации. Однако однофакторная аутентификации, используемая в этой модели, не входит в сферу применения настоящей Рекомендации.

7.1.4 Модель T-4

Модель T-4 является моделью, в которой несколько IdSP обеспечивают один и тот же метод комбинированной аутентификации и в которой несколько IdSP, поставщик услуг и один или несколько терминалов соединены друг с другом по сети. Как правило, в модели T-4 все пользователи имеют отношения доверия со всеми IdSP.

Когда поставщик услуг получает от терминала запрос на обслуживание, поставщик услуг выбирает один или несколько IdSP, удовлетворяющих требуемому уровню гарантии аутентификации, и просит выбранный(е) IdSP аутентифицировать пользователя. Если все результаты аутентификации, полученные от этого(их) IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет свою услугу терминалу.

Эта модель способна обеспечить любой тип комбинированной аутентификации, однако она зависит от типа комбинированной аутентификации, обеспечиваемой одним IdSP и/или выбранными IdSP. (Может быть выполнена множественная многофакторная аутентификация и множественная аутентификация по нескольким методам).

7.1.5 Модель T-5

Модель T-5 является моделью, в которой несколько IdSP обеспечивают методы однофакторной аутентификации, относящиеся к разным типам, но использующие один и тот же фактор, и в которой несколько IdSP, поставщик услуг и один или несколько терминалов соединены друг с другом по сети. Как правило, в модели T-5 все пользователи имеют отношения доверия со всеми IdSP.

Когда поставщик услуг получает от терминала запрос на обслуживание, поставщик услуг выбирает несколько IdSP, удовлетворяющих требуемому уровню гарантии аутентификации, и просит выбранные IdSP аутентифицировать пользователя. Если все результаты аутентификации, полученные от этих IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет свою услугу терминалу.

Эта модель способна обеспечить множественную аутентификацию или аутентификацию по нескольким методам. Следует отметить, что метод выполняемой аутентификации зависит от комбинации IdSP.

Эта модель способна также обеспечить однофакторную аутентификацию, если метод аутентификации, обеспечиваемый одним IdSP, удовлетворяет требуемому уровню гарантии аутентификации. Однако однофакторная аутентификации, используемая в этой модели, не входит в сферу применения настоящей Рекомендации.

7.1.6 Модель T-6

Модель T-6 является моделью, в которой несколько поставщиков IdSP предоставляют методы комбинированной аутентификации, относящиеся к разным типам, но использующие один и тот же фактор (то есть обеспечиваются методы множественной аутентификации или аутентификации по нескольким методам), и в которой поставщики IdSP, поставщик услуг и один или более терминалов соединены друг с другом по сети. Как правило, в модели T-6 все пользователи имеют отношения доверия со всеми IdSP.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг для обеспечения требуемого уровня гарантии аутентификации выбирает одного или нескольких IdSP и просит выбранного(ых) IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщика(ов) IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечивать множественную аутентификацию или аутентификацию по нескольким методам, однако это зависит от выбора или комбинации поставщиков IdSP.

7.1.7 Модель T-7

Модель T-7 является моделью, в которой несколько поставщиков IdSP предоставляют методы однофакторной аутентификации, использующие разные факторы, и в которой несколько IdSP, поставщик услуг и один или более терминалов соединены друг с другом по сети. Как правило, в модели T-7 все пользователя имеют отношения доверия со всеми IdSP.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг для обеспечения требуемого уровня гарантии аутентификации выбирает нескольких IdSP и просит выбранных IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщика(ов) IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечить любой тип комбинированной аутентификации. Следует заметить, что применяемый метод аутентификации зависит от выбора поставщиков IdSP.

Данная модель способна также обеспечить однофакторную аутентификацию, если метод аутентификации, обеспечиваемый одним IdSP, удовлетворяет требуемому уровню гарантии аутентификации. Однако однофакторная аутентификация, используемая в этой модели, не входит в сферу применения настоящей Рекомендации.

7.1.8 Модель T-8

Модель T-8 является моделью, в которой несколько поставщиков IdSP предоставляют методы комбинированной аутентификации, использующие разные факторы, и в которой несколько IdSP, поставщик услуг и один или более терминалов соединены друг с другом по сети. Как правило, в модели T-8 все пользователя имеют отношения доверия со всеми IdSP.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг выбирает для обеспечения требуемого уровня гарантии аутентификации одного или нескольких IdSP и просит выбранного(ых) IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщика(ов) IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечить любой тип комбинированной аутентификации.

7.1.9 Модель T-9

Модель T-9 является моделью, в которой несколько поставщиков IdSP предоставляют тот же метод однофакторной аутентификации, и в которой несколько IdSP, поставщик услуг и несколько терминалов соединены друг с другом по сети. Как правило, в модели T-9 один или несколько пользователей не имеют отношений доверия со всеми IdSP.

ПРИМЕЧАНИЕ. − Данная модель может существовать с IdSP, который не имеет отношений доверия с любым пользователем. Однако модель, содержащая такого IdSP, не входит в сферу применения настоящей Рекомендации.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг для обеспечения требуемого уровня гарантии аутентификации выбирает нескольких IdSP из группы IdSP, имеющих отношения доверия с пользователем, и просит выбранных IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщиков IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечить метод множественной аутентификации.

Следует заметить, что данная модель способна также обеспечить однофакторную аутентификацию, если метод аутентификации, обеспечиваемый одним IdSP, удовлетворяет требуемому уровню гарантии аутентификации. Однако однофакторная аутентификация, используемая в этой модели, не входит в сферу применения настоящей Рекомендации.

7.1.10 Модель T-10

Модель T-10 является моделью, в которой несколько поставщиков IdSP предоставляют тот же метод комбинированной аутентификации, и в которой несколько IdSP, поставщик услуг и несколько терминалов соединены друг с другом по сети. Как правило, в модели T-10 один или несколько пользователей не имеют отношений доверия со всеми IdSP.

ПРИМЕЧАНИЕ. − Модель T-10 существует, когда IdSP не имеет отношений доверия с любым пользователем. Однако модель, содержащая такого IdSP, не входит в сферу применения настоящей Рекомендации.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг выбирает одного или нескольких IdSP, которые удовлетворяют требуемому уровню гарантии аутентификации и просит выбранного(ых) IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщика(ов) IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечить любой тип комбинированной аутентификации, однако это зависит от типа комбинированной аутентификации, обеспечиваемой IdSP, и/или от выбора IdSP. Может выполняться множественная многофакторная аутентификация и множественная аутентификация по многим методам.

7.1.11 Модель T-11

Модель T-11 является моделью, в которой несколько поставщиков IdSP предоставляют методы одинофакторной аутентификации, относящиеся к разным типам, но использующие один и тот же фактор, и в которой поставщики IdSP, поставщик услуг и несколько терминалов соединены друг с другом по сети. Как правило, в модели T-11 один или несколько пользователей не имеют отношений доверия со всеми IdSP.

ПРИМЕЧАНИЕ. − Модель T-11 существует, когда IdSP не имеет отношений доверия с любым пользователем. Однако модель, содержащая такого IdSP, не входит в сферу применения настоящей Рекомендации.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг для обеспечения требуемого уровня гарантии аутентификации выбирает нескольких IdSP из группы IdSP, имеющих отношения доверия с пользователем, и просит выбранных IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщиков IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечивать множественную аутентификацию или аутентификацию по нескольким методам. Следует заметить, что применяемый метод аутентификации зависит от комбинации поставщиков IdSP.

Данная модель способна также обеспечить однофакторную аутентификацию, если метод аутентификации, обеспечиваемый одним IdSP, удовлетворяет требуемому уровню гарантии аутентификации. Однако однофакторная аутентификация, используемая в этой модели, не входит в сферу применения настоящей Рекомендации.

7.1.12 Модель T-12

Модель T-12 является моделью, в которой несколько поставщиков IdSP предоставляют методы комбинированной аутентификации, относящиеся к разным типам, но использующие один и тот же фактор (то есть обеспечиваются методы множественной аутентификации или аутентификации по нескольким методам), и в которой поставщики IdSP, поставщик услуг и один или более терминалов соединены друг с другом по сети. Как правило, в модели T-12 один или несколько пользователей не имеют отношений доверия со всеми IdSP.

ПРИМЕЧАНИЕ. − Модель T-12 существует, когда IdSP не имеет отношений доверия с любым пользователем. Однако модель, содержащая такого IdSP, не входит в сферу применения настоящей Рекомендации.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг для обеспечения требуемого уровня гарантии аутентификации выбирает одного или нескольких IdSP из группы IdSP, имеющих отношения доверия с пользователем, и просит выбранного(ых) IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщика(ов) IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечить множественную аутентификацию или аутентификацию по нескольким методам, однако это зависит от выбора и комбинации поставщиков IdSP.

7.1.13 Модель T-13

Модель T-13 является моделью, в которой несколько IdSP предоставляют методы однофакторной аутентификации, в которых используются разные факторы, и в которой несколько IdSP, поставщик услуг и несколько терминалов соединены друг с другом по сети. Как правило, в модели T-13 один или несколько пользователей не имеют отношений доверия со всеми IdSP.

ПРИМЕЧАНИЕ. − Модель T-13 существует, когда IdSP не имеет отношений доверия с любым пользователем. Однако модель, содержащая такого IdSP, не входит в сферу применения настоящей Рекомендации.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг для обеспечения требуемого уровня гарантии аутентификации выбирает нескольких IdSP из группы IdSP, имеющих отношения доверия с пользователем, и просит выбранных IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщиков IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечить любой тип множественной аутентификации. Следует заметить, что применяемый метод аутентификации зависит от выбора поставщиков IdSP.

Данная модель способна также обеспечить однофакторную аутентификацию, если метод аутентификации, обеспечиваемый одним IdSP, удовлетворяет требуемому уровню гарантии аутентификации. Однако однофакторная аутентификация, используемая в этой модели, не входит в сферу применения настоящей Рекомендации.

7.1.14 Модель T-14

Модель T-14 является моделью, в которой несколько поставщиков IdSP предоставляют методы комбинированной аутентификации, использующие разные факторы, и в которой несколько IdSP, поставщик услуг и несколько терминалов соединены друг с другом по сети. Как правило, в модели T-14 один или более пользователей не имеют отношений доверия со всеми IdSP.

ПРИМЕЧАНИЕ. − Модель T-14 существует, когда IdSP не имеет отношений доверия с любым пользователем. Однако модель, содержащая такого IdSP, не входит в сферу применения настоящей Рекомендации.

Когда поставщик услуг принимает от терминала запрос на обслуживание, поставщик услуг для обеспечения требуемого уровня гарантии аутентификации выбирает одного или нескольких IdSP из группы IdSP, имеющих отношения доверия с пользователем, и просит выбранного(ых) IdSP провести аутентификацию пользователя соответствующим образом. Если все результаты аутентификации, полученные от поставщика(ов) IdSP, указывают на то, что пользователь был успешно аутентифицирован, поставщик услуг предоставляет терминалу свою услугу.

Эта модель может обеспечить любой тип методов комбинированной аутентификации.

7.2 Модель жизненного цикла аутентификации объекта

Модель жизненного цикла аутентификации объекта − это модель перехода состояний на этапе аутентификации объекта, который определен в [ITU-T X.1254].

Существуют два типа моделей: модель жизненного цикла с точки зрения пользователя и модель жизненного цикла с точки зрения поставщика услуг.

7.2.1 Модель жизненного цикла с точки зрения пользователя

На протяжении процесса аутентификации модели жизненного цикла с точки зрения пользователя статус аутентификации состоит из четырех экземпляров: "аутентификация отсутствует", "идентифицирован", "верифицирован" и "зарегистрирован выход" (рисунок 2).

Исходный статус аутентификации − "аутентификация отсутствует".

Когда пользователь направляет запрос на аутентификацию и идентифицирован поставщиком IdSP, статус "аутентификация отсутствует" изменяется на статус "идентифицирован".

После того как пользователь аутентифицирован поставщиком IdSP, статус "идентифицирован" изменяется на статус "верифицирован".

Кроме того, если пользователь направляет запрос на выход или если проходит определенное время после аутентификации пользователя и установления статуса "верифицирован", статус "верифицирован" изменяется на статус "зарегистрирован выход".

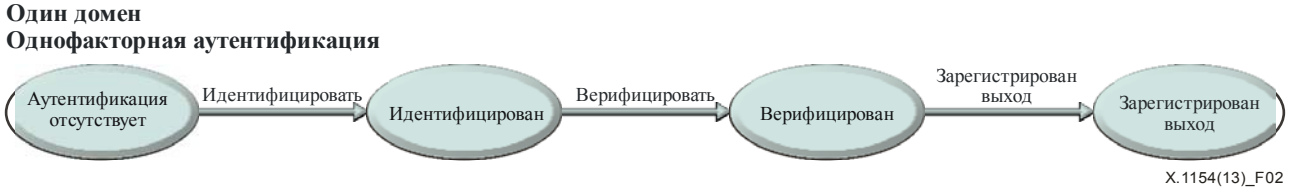

Рисунок 2 − Переход состояний однофакторной аутентификации

В случае комбинированной аутентификации переход состояний с "идентифицирован" на "верифицирован" отличается (рисунок 3).

На протяжении процесса комбинированной аутентификации существующим уровнем гарантии аутентификации пользователя управляет IdSP или поставщик услуг.

После того как пользователь успешно аутентифицирован путем однофакторной аутентификации, существующий уровень гарантии аутентификации обновляется и оценивается на предмет соответствия требуемому уровню гарантии аутентификации.

Если существующий уровень гарантии аутентификации соответствует требуемому уровню гарантии аутентификации, статус "идентифицирован" изменяется на статус "верифицирован".

Кроме того, если пользователь направляет запрос на выход или если проходит определенное время после аутентификации пользователя и установления статуса "верифицировн", статус "верифицирован" изменяется на статус "зарегистрирован выход".

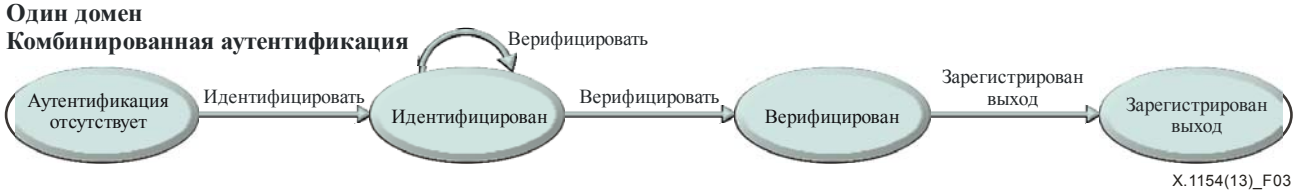

Рисунок 3 − Переход состояний комбинированной аутентификации в одном домене

На рисунке 4 показан переход состояний в случае комбинированной аутентификации в нескольких доменах, в которых действуют различные требования к уровню гарантии аутентификации в моделях T-4, T-6 и T-8.

Притом что переход состояний в первом домене тот же, что и показанный на рисунке 3, переход состояний в других доменах отличается.

Когда в первом домене установлен статус "верифицирован для 1-го домена" и пользователь направляет запрос на аутентификацию во второй домен, статус во втором домене изменяется на статус "недостаточно для 2-го домена", если пользователь идентифицирован во втором домене. Если существующий уровень гарантии аутентификации пользователя соответствует требуемой гарантии аутентификации во втором домене, статус "недостаточно для 2-го домена" изменяется на статус "верифицирован для 2-го домена".

В противном случае, пользователь аутентифицируется поставщиком IdSP (или поставщиком услуг) и существующий уровень гарантии аутентификации обновляется и оценивается на предмет соответствия требуемому уровню гарантии аутентификации. Кроме того, если пользователь направляет запрос на выход в любой домен, статус "верифицирован" во всех доменах изменяется на статус "зарегистрирован выход".

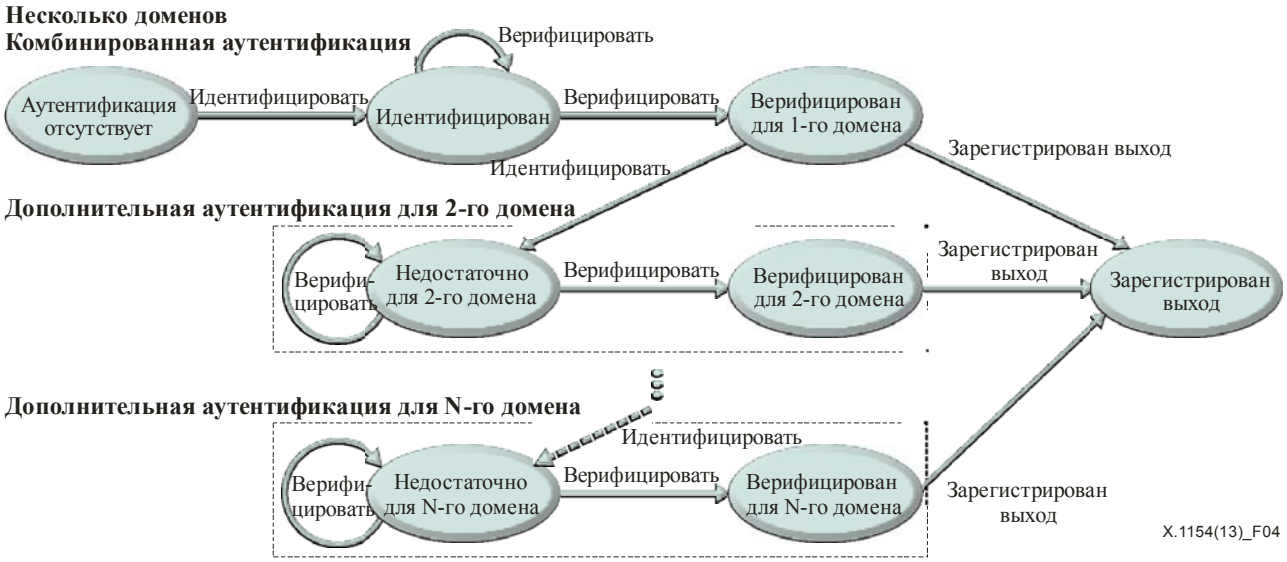

Рисунок 4 − Переход состояний комбинированной аутентификации в нескольких доменах с разными требованиями к гарантии аутентификации

На рисунке 5 показан переход состояний в случае комбинированной аутентификации в нескольких доменах с федерацией. Это аналогично случаю комбинированной аутентификации в нескольких доменах, в которых действуют различные требования к гарантии аутентификации в моделях T-4, T-6 и T-8.

Переход состояний в первом домене тот же, что и показанный на рисунках 3 и 4.

Когда в первом домене установлен статус "верифицирован" и пользователь направляет запрос на аутентификацию во второй домен, статус не изменяется, при том что пользователь идентифицирован во втором домене.

Кроме того, если пользователь направляет запрос на выход в любой домен, статус "верифицирован" во всех доменах изменяется на статус "зарегистрирован выход".

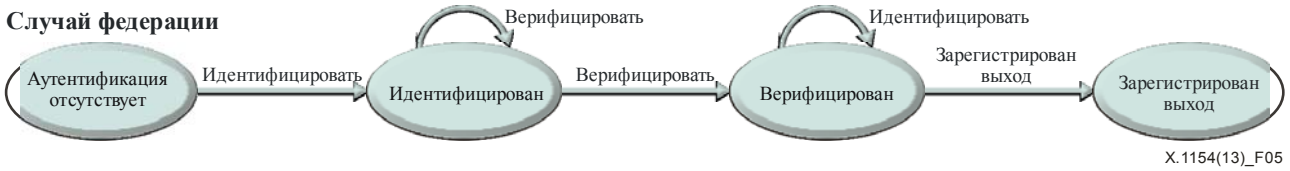

Рисунок 5 − Переход состояний комбинированной аутентификации в нескольких доменах с федерацией

7.2.2 Модель жизненного цикла с точки зрения поставщика услуг

На протяжении процесса аутентификации модели жизненного цикла с точки зрения поставщика услуг статус аутентификации также состоит из четырех экземпляров: "аутентификация отсутствует", "идентифицирован", "верифицирован" и "зарегистрирован выход" (рисунок 6).

Исходный статус аутентификации − "аутентификация отсутствует".

Когда поставщик услуг принимает запрос на аутентификацию и определяет, кем является пользователь, статус "аутентификация отсутствует" изменяется на статус "идентифицирован". После этой стадии статус "идентифицирован" изменяется на статус "верифицирован", если пользователь аутентифицирован поставщиком IdSP.

Кроме того, если поставщик услуг принимает от пользователя запрос на выход или если проходит определенное время после аутентификации пользователя и установления статуса "верифицирован", статус "верифицирован" изменяется на статус "зарегистрирован выход".

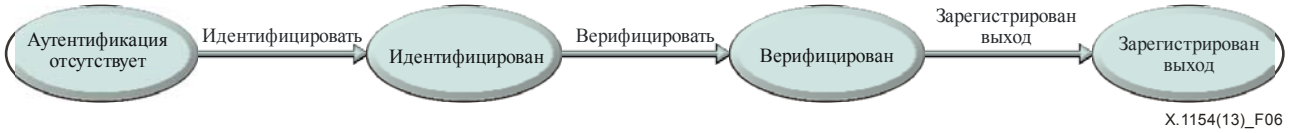

Рисунок 6 − Переход состояний однофакторной аутентификации

В случае комбинированной аутентификации переход состояний с "идентифицирован" на "верифицирован" отличается.

На протяжении процесса комбинированной аутентификации существующим уровнем гарантии аутентификации пользователя управляет IdSP или поставщик услуг.

После того как пользователь успешно аутентифицирован поставщиком IdSP, существующий уровень гарантии аутентификации обновляется и оценивается на предмет соответствия требуемому уровню гарантии аутентификации.

Если существующий уровень гарантии аутентификации соответствует требуемому уровню гарантии аутентификации, статус "идентифицирован" изменяется на статус "верифицирован".

Кроме того, если пользователь направляет запрос на выход или если проходит определенное время после аутентификации пользователя и установления статуса "верифицировн", статус "верифицирован" изменяется на статус "зарегистрирован выход".

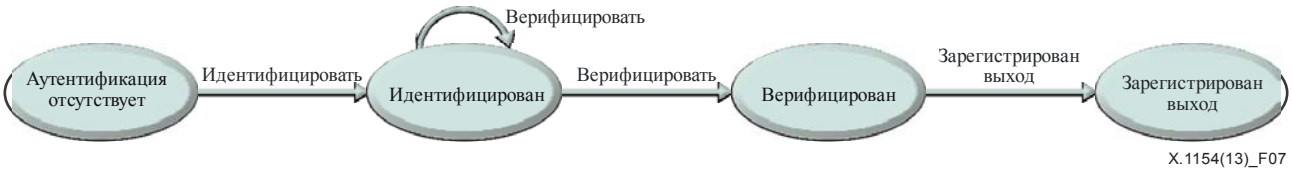

Рисунок 7 − Переход состояний комбинированной аутентификации

С точки зрения поставщика услуг не существует отличий от случая комбинированной аутентификации, даже если пользователь осуществляет доступ в несколько доменов и федеративные домены.

8 Операции в среде с несколькими IdSP

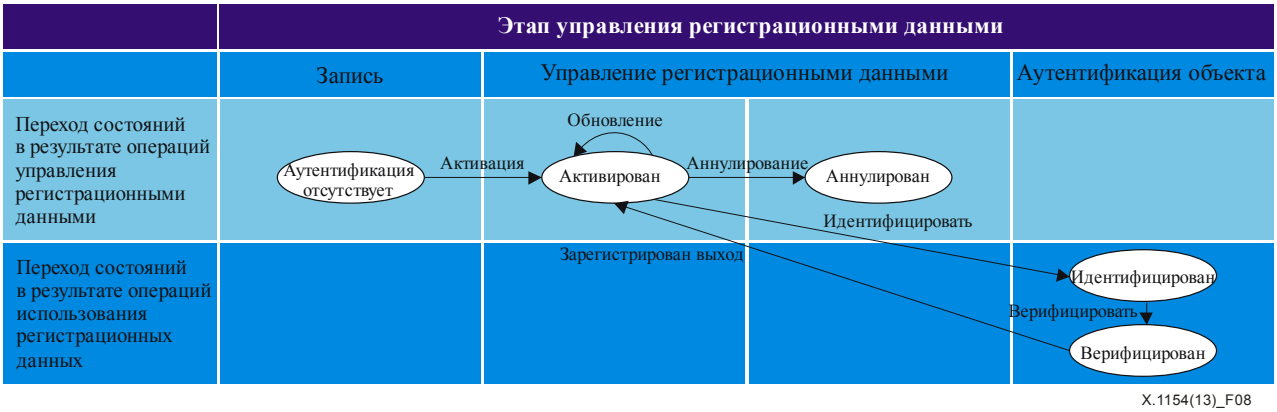

Рисунок 8 − Операции для пользователя

Рисунок 9 − Операции для поставщика услуг

В моделях, представленных в разделе 7, описаны следующие типы операций IdSP:

1) операции управления регистрационными данными (рисунок 8);
2) операции использования регистрационных данных (рисунок 8);
3) операции управления отношениями доверия с поставщиками услуг (рисунок 9).

8.1 Операции управления регистрационными данными

Операции управления регистрационными данными − это следующие, предназначенные для пользователя операции по управлению жизненным циклом его регистрационных данных:

1) Активация
   Операция активации осуществляет процесс активации регистрационных данных, который описан в [ITU-T X.1254], с тем чтобы определить регистрационные данные пользователя.
2) Обновление
   Операция обновления осуществляет процесс обновления регистрационных данных, который описан в [ITU-T X.1254], с тем чтобы определить регистрационные данные пользователя.
3) Аннулирование
   Операция аннулирования обрабатывает процесс аннулирования регистрационных данных, который описан в [ITU-T X.1254], с тем чтобы определить регистрационные данные пользователя.

8.2 Операции использования регистрационных данных

Если регистрационные данные активированы, возможно выполнение операций использования. Операции использования регистрационных данных − это операции, предназначенные для идентификации/верификации пользователя, а также для прекращения действия утверждения, которое первоначально было создано операцией для верификации пользователя.

1) Идентификация
   Операция идентификации осуществляет идентификацию пользователя.
   Эта операция используется на этапе аутентификации объекта.

2) Верификация
   Операция верификации выполняет проверку того, является ли равноправный участник связи пользователем, заявленным согласно представленным регистрационным данным. После проверки участника связи для этого участника связи создается утверждение.
   Эта операция используется на этапе аутентификации объекта.

3) Зарегистрирован выход
   Срок действия утверждения истекает после операции выхода из системы.
   Эта операция применяется на этапе использования.

8.3 Операции управления отношениями доверия с поставщиками услуг

Операции управления отношениями доверия с поставщиками услуг − это предназначенные для поставщиков услуг операции создания и удаления отношений доверия с поставщиками услуг.

1) Установление
   Операция установления создает новые отношения доверия с определенным поставщиком услуг.
   Эта операция используется на этапе записи отношений доверия.

2) Обновление
   Операция обновления обновляет существующие отношения доверия с определенным поставщиком услуг.
   Эта операция используется на этапе управления отношениями доверия.

3) Завершение
   Операция завершения уничтожает указанные отношения доверия с определенным поставщиком услуг.
   Эта операция используется на этапе управления отношениями доверия.

9 Общая структура комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности

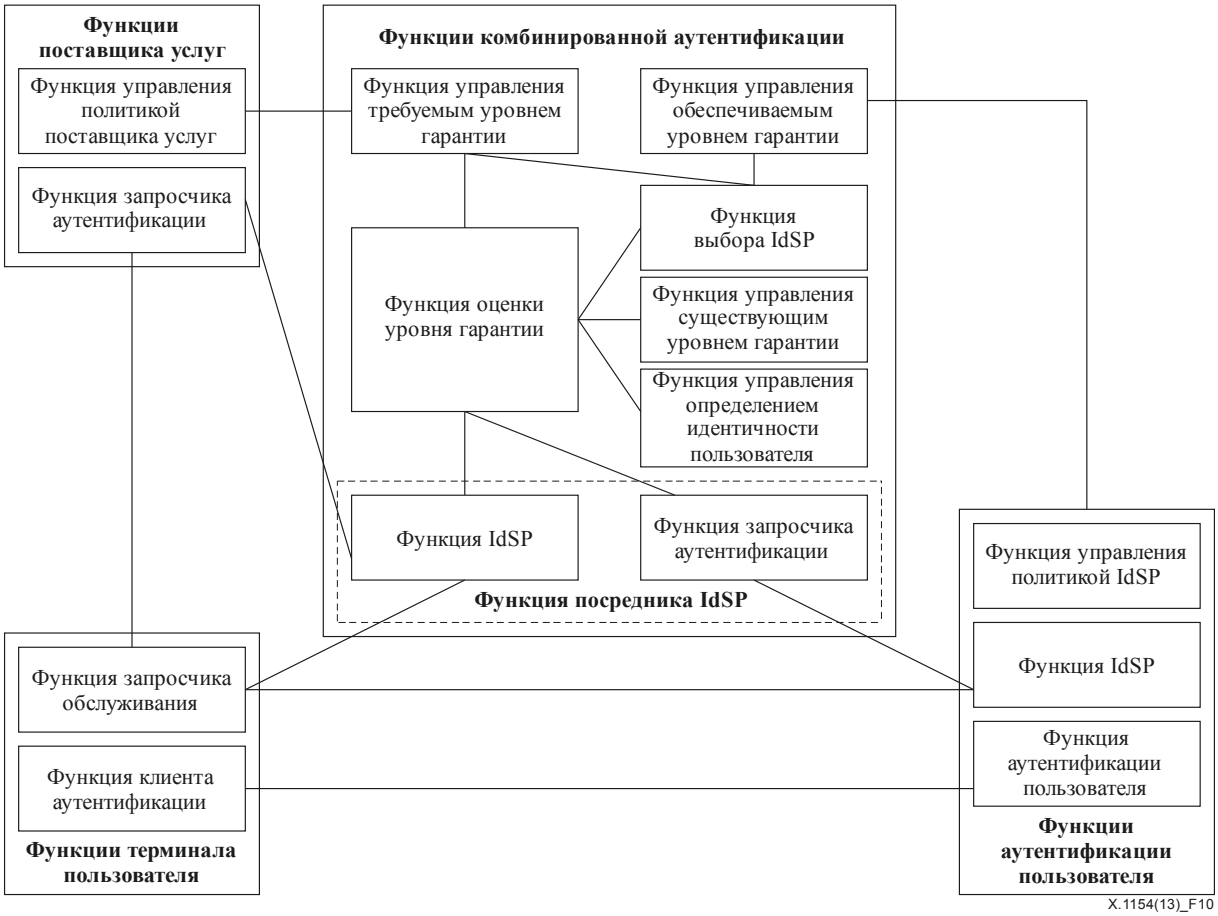

Рисунок 10 − Модель общей структуры комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности

Представленная на рисунке 10 структура комбинированной аутентификации состоит из четырех логических функциональных блоков: функции аутентификации пользователя, функции поставщика услуг, функции терминала пользователя, функции комбинированной аутентификации.

9.1 Логические компоненты

9.1.1 Функции аутентификации пользователя

Функции аутентификации пользователя включают три функции: функцию аутентификации пользователя, функцию IdSP и функцию управления политикой IdSP.

Функция аутентификации пользователя − это функция, необходимая для выполнения операции верификации и для аутентификации пользователя.

Функция IdSP − это функция, необходимая для получения запроса на аутентификацию от (функции запросчика аутентификации в составе) функций комбинированной аутентификации и выполнения операции идентификации. Кроме того, функция IdSP необходима для получения запроса на выход и выполнения операции выхода из системы.

Функция управления политикой IdSP − это функция, необходимая для управления политикой аутентификации IdSP, которая содержит тип метода аутентификации и уровень гарантии аутентификации, обеспечиваемый функцией аутентификации пользователя.

9.1.2 Функции поставщика услуг

Функции поставщика услуг включают две функции: функцию запросчика аутентификации и функцию управления политикой поставщика услуг.

Функция запросчика аутентификации − это функция, необходимая для отправки запроса на аутентификацию для (функции IdSP в составе) функций комбинированной аутентификации.

Функция управления политикой поставщика услуг − это функция, необходимая для управления политикой аутентификации поставщика услуг, которая содержит уровень гарантии аутентификации, требуемый для предоставления обслуживания.

9.1.3 Функции терминала пользователя

Функции терминала пользователя включают две функции: функцию запросчика обслуживания и функцию клиента аутентификации.

Функция запросчика обслуживания − это функция, необходимая для отправки запроса на обслуживание для (функции запросчика аутентификации в составе) функций поставщика услуг.

Функция клиента аутентификации − это функция, необходимая для связи с (функцией аутентификации пользователя в составе) функцией однофакторной аутентификации для выполнения аутентификации пользователя.

9.1.4 Функции комбинированной аутентификации

Функции комбинированной аутентификации включают восемь функций: функцию IdSP, функцию запросчика аутентификации, функцию управления требуемым уровнем гарантии, функцию управления обеспечиваемым уровнем гарантии, функцию управления существующим уровнем гарантии, функцию управления определением идентичности пользователя, функцию оценки уровня гарантии и функцию выбора IdSP.

Функция IdSP − это функция, необходимая для получения запроса на аутентификацию от (функции запросчика аутентификации в составе) функций поставщика услуг и выполнения операции идентификации. Кроме того, функция IdSP принимает запрос на завершение обслуживания и выполняет операцию выхода из системы.

Функция запросчика аутентификации − это функция, необходимая для отправки запроса на аутентификацию или запроса на выход для (функции IdSP в составе) функций однофакторной аутентификации.

Функция управления требуемым уровнем гарантии − это функция, необходимая для управления уровнем гарантии аутентификации, требуемым каждой функцией поставщика услуг через операции установления/обновления/завершения.

Функция управления обеспечиваемым уровнем гарантии − это функция, необходимая для управления типом метода аутентификации и уровнем гарантии аутентификации, обеспечиваемым каждой функцией однофакторной аутентификации через операции установления/обновления/завершения.

Функция управления существующим уровнем гарантии − это функция, необходимая для управления существующим уровнем гарантии аутентификации каждого пользователя.

Функция управления определением идентичности пользователя − это функция, необходимая для управления информацией, подтверждающей идентичность, каждого пользователя через функцию создания/обновления/аннулирования.

Функция оценки уровня гарантии − это функция, необходимая для верификации результата аутентификации пользователя, представленного функцией IdSP в составе функций однофакторной аутентификации, для оценки существующего уровня гарантии пользователя и для проверки, соответствует ли существующий уровень гарантии пользователя требуемому уровню гарантии поставщика услуг.

Функция выбора IdSP − это функция, необходимая для выбора одной или нескольких функций однофакторной аутентификации для пользователя с целью соответствия требуемому уровню гарантии поставщика услуг.

Следует заметить, что в ряде существующих структур управления определением идентичности (IdM) вместо функции IdSP и функции запросчика аутентификации может использоваться другая функция − функция поставщика сопряжения услуг определения идентичности.

9.2 Шаблоны

9.2.1 Запрос на обслуживание

На рисунке 11 показан базовый шаблон выполнения запроса на обслуживание в общей структуре комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности.

1) Функция запросчика обслуживания направляет запрос на обслуживание функции запросчика аутентификации в составе функций поставщика услуг.
2) Когда функция запросчика аутентификации в составе функций поставщика услуг принимает запрос на обслуживание, она направляет запрос на аутентификацию функции IdSP в составе функций комбинированной аутентификации, если функция запросчика аутентификации заключает, что для предоставления прикладной услуги требуется аутентифицировать функцию терминала пользователя.
3) Когда функция IdSP принимает запрос на обслуживание, она направляет запрос на аутентификацию функции оценки уровня гарантии.
4) Функция оценки уровня гарантии получает от функции управления существующим уровнем гарантии информацию о существующем уровне гарантии терминала пользователя и направляет функции выбора IdSP запрос на выбор IdSP вместе с информацией о существующем уровне гарантии терминала пользователя.
5) Функция выбора IdSP получает информацию о требуемом уровне гарантии поставщика услуг и предоставляет уровень гарантии каждого IdSP от функций управления требуемым уровнем гарантии и управления обеспечиваемым уровнем гарантии, соответственно. Затем функция выбирает IdSP из списка доступных IdSP и направляет его название функции оценки уровня гарантии.
6) Функция оценки уровня гарантии получает от функции управления определением идентичности пользователя идентификатор терминала пользователя в выбранном IdSP, если таковой необходим, и направляет запрос на аутентификацию функции запросчика аутентификации. Далее функция запросчика аутентификации направляет запрос на аутентификацию функции IdSP в составе функций выбранного IdSP.
7) Функция IdSP направляет запрос на аутентификацию функции аутентификации. Кроме того, функция аутентификации выполняет аутентификацию пользователя с клиентом аутентификации в составе функций терминала пользователя.
8) Функция аутентификации возвращает функции оценки уровня гарантии результат аутентификации через функцию IdSP в составе функций IdSP и через функцию запросчика аутентификации в составе функций комбинированной аутентификации.
9) Функция оценки уровня гарантии оценивает и обновляет существующий уровень гарантии терминала пользователя.
10) Если существующий уровень гарантии терминала пользователя недостаточен для предоставления обслуживания (то есть ниже требуемого уровня гарантии), функция оценки уровня гарантии повторно просит функцию выбора IdSP осуществить выбор IdSP. Далее повторяются шаги 5−9.
11) Если существующий уровень гарантии терминала пользователя достаточен для предоставления обслуживания на шаге 10, функция оценки уровня гарантии направляет функции IdSP результат аутентификации.
12) Функция IdSP создает утверждение и отправляет его запросчику аутентификации в составе функций поставщика услуг.

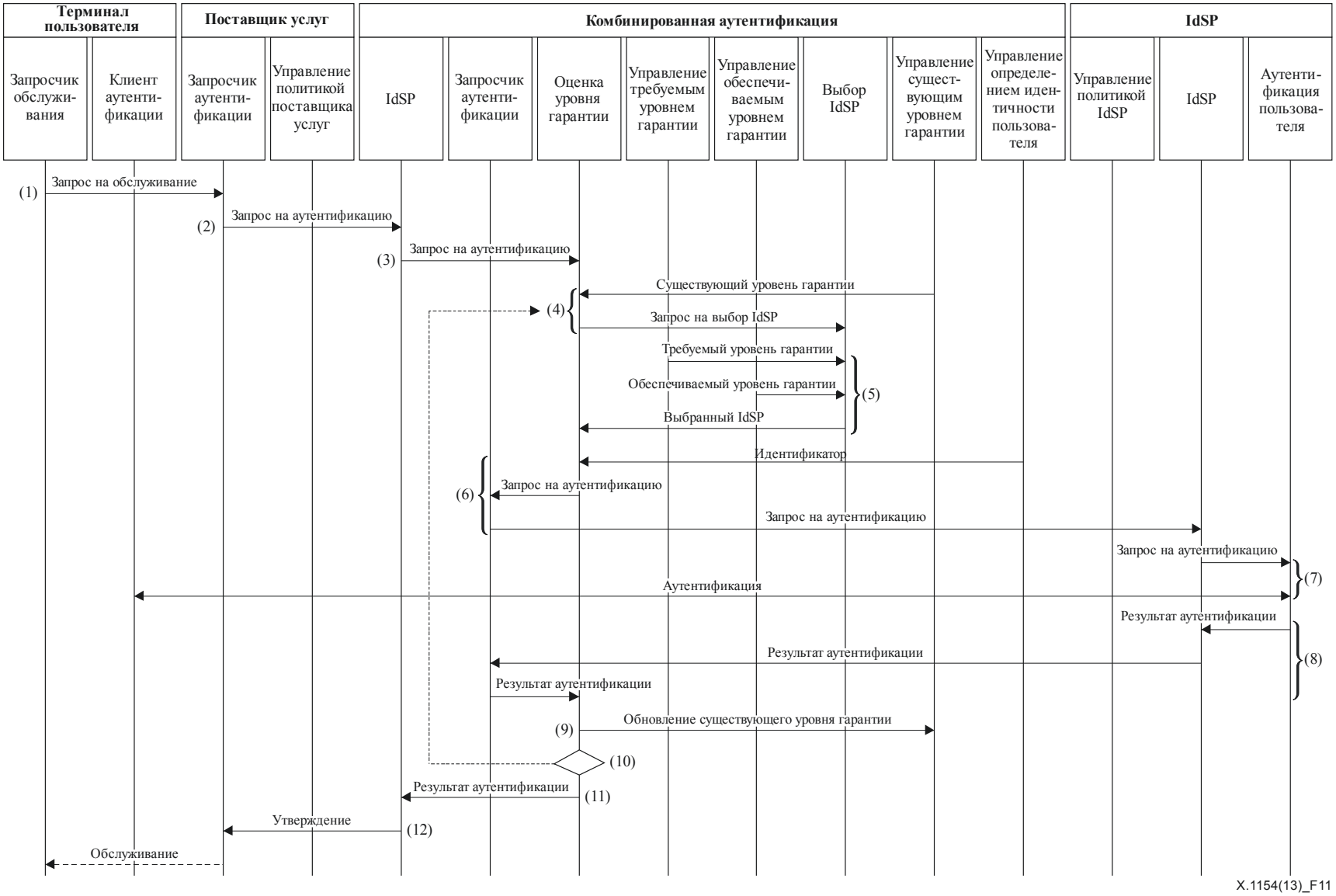

Рисунок 11 − Базовый шаблон выполнения запроса на обслуживание в общей структуре комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности

9.2.2 Завершение обслуживания

На рисунке 12 показан базовый шаблон выполнения завершения обслуживания в общей структуре комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности.

1) Функция запросчика обслуживания направляет функции запросчика аутентификации в составе функций поставщика услуг запрос на завершение обслуживания.
2) Когда функция запросчика аутентификации в составе функций поставщика услуг принимает запрос на завершение обслуживания, она направляет функции IdSP в составе функций комбинированной аутентификации запрос на выход.
3) Когда функция IdSP принимает запрос на выход, она направляет функции оценки уровня гарантии запрос на завершение.
4) Функция оценки уровня гарантии получает список IdSP, к которым зарегистрирован вход терминала пользователя, и направляет через функцию запросчика аутентификации всем входящим в список функциям IdSP запрос на выход.
5) Функция IdSP возвращает результат выхода.
6) Когда функция оценки уровня гарантии принимает результат выхода, существующий уровень гарантии обновляется.
7) Если функция оценки уровня гарантии принимает все результаты выхода, она возвращает функции IdSP результат завершения.
8) Функция IdSP возвращает функции запросчика аутентификации результат выхода.
9) Функция запросчика аутентификации возвращает запросчику обслуживания результат завершения обслуживания.

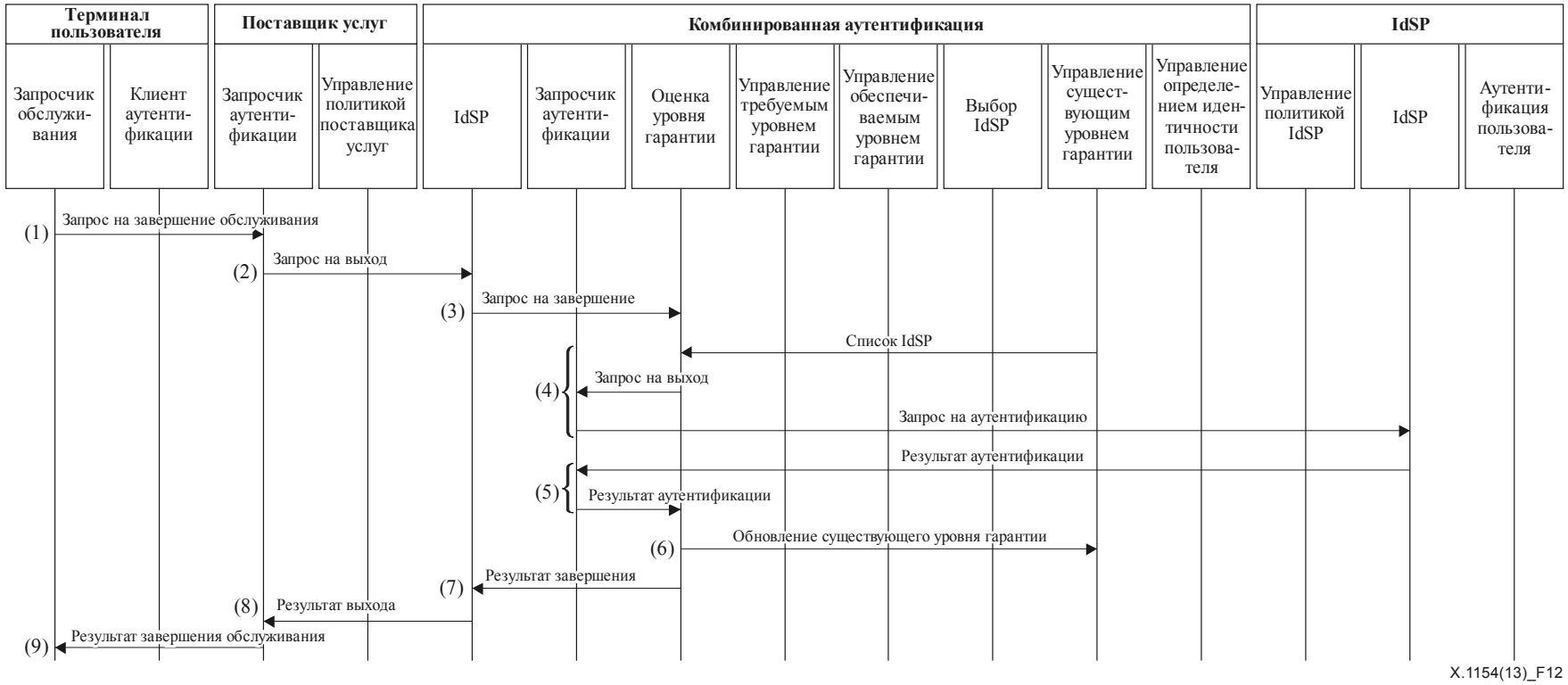

Рисунок 12 − Базовый шаблон выполнения запроса на завершение обслуживания в общей структуре комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности

9.2.3 Управление требуемым уровнем гарантии функций поставщика услуг

Для целей управления требуемым уровнем гарантии функций поставщика услуг в составе функций комбинированной аутентификации, требуемый уровень гарантии направляется от функции управления политикой поставщика услуг к функции управления требуемым уровнем гарантии через операции установления/обновления/завершения.

9.2.4 Управление обеспечиваемым уровнем гарантии функций IdSP

Для целей управления обеспечиваемым уровнем гарантии функций IdSP в составе функций комбинированной аутентификации, требуемый уровень гарантии направляется от функции управления политикой IdSP к функции управления обеспечиваемым уровнем гарантии через операции установления/обновления/завершения.

Приложение A

Аспекты комбинированной аутентификации

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

A.1 Достижение оцениваемого уровня гарантии аутентификации

Вследствие того что комбинированная аутентификация является аутентификацией, в которой используется несколько регистрационных данных, для достижения оцениваемого уровня гарантии требуется использование разных регистрационных данных. Иными словами, при использовании одних и тех же регистрационных данных простая комбинация нескольких методов аутентификации или IdSP приведет к полной неудаче обеспечения уровня гарантии.

Для достижения оцениваемого уровня гарантии требуется процесс проверки того, являются ли используемые в комбинированной аутентификации регистрационные данные разными. Рекомендуется выполнять этот процесс проверки до обновления существующего уровня гарантии аутентификации.

В модели, где функция комбинированной аутентификации и функции аутентификации пользователя реализованы в одном объекте (например, комбинированную аутентификацию обеспечивает один IdSP), процесс проверки может легко выполняться в этом IdSP. Кроме того, процесс проверки может выполняться при выполнении операции создания/обновления.

С другой стороны, в модели, где функция комбинированной аутентификации и функции аутентификации пользователя реализованы в одном объекте (например, поставщик услуг использует нескольких IdSP, обеспечивающих однофакторную аутентификацию), для процесса проверки требуется дополнительный обмен данными между функцией комбинированной аутентификации и функцией аутентификации пользователя. Как правило, в функции аутентификации пользователя требуется функция, выполняющая отправку данных для идентификации регистрационных данных. Кроме того, в функции комбинированной аутентификации требуется функция, выполняющая подтверждение использования разных регистрационных данных путем сравнения всех данных, принимаемых от функций аутентификации пользователя.

В случае применения метода аутентификация с использованием инфраструктуры открытых ключей (PKI), эта функция в функции аутентификации пользователя может направлять открытый ключ в качестве данных, обозначающих регистрационные данные, а функция в функции комбинированной аутентификации может сравнивать эти данные напрямую.

Однако в случае применения метода аутентификации с совместно используемым секретным ключом (например, с паролем), этой функции в функции аутентификации пользователя запрещено направлять сам совместно используемый секретный ключ в качестве данных, обозначающих регистрационные данные.

A.2 Выбор одного или более IdSP

Требуется, чтобы функция выбора IdSP обнаруживала и выбирала подходящего(их) IdSP, когда поставщик услуг принимает от терминала запрос на обслуживание.

Для выбора подходящего IdSP требуется надежная реализация функции управления требуемым уровнем гарантии и функции управления обеспечиваемым уровнем гарантии.

Кроме того, в IdSP (модель, в которой один IdSP обеспечивает функцию комбинированной аутентификации) или в поставщике услуг (модель, в которой этот поставщик услуг обеспечивает функцию комбинированной аутентификации) требуется надежная реализация функции управления существующим уровнем гарантии.

Далее, требуется, чтобы функция оценки уровня гарантии надежным образом получала информацию о существующем уровне гарантии аутентификации, требуемом уровне гарантии и обеспечиваемом уровне гарантии аутентификации.

A.3 Эффективный уровень гарантии аутентификации

В некоторых случаях эффективный уровень гарантии аутентификации может быть ниже оцениваемого уровня гарантии вследствие изменения уровня гарантии аутентификации в результате воздействия различных факторов окружающей среды.

В этом случае в IdSP требуется функция, направляющая поставщику услуг информацию об эффективном уровне гарантии аутентификации. Наряду с этим в поставщике услуг требуется функция, обновляющая и оценивающая существующий уровень гарантии аутентификации пользователя на основе информации об эффективном уровне гарантии аутентификации.

A.4 Аспекты безопасности многофакторной аутентификации

Существуют два типа многофакторной аутентификации: первый тип − с использованием в многофакторной аутентификации одних регистрационных данных для верификации и второй тип − с использованием для верификации нескольких регистрационных данных.

Первый тип аутентификации базируется на сертификате открытого ключа, который хранится в смарт-карте или на одноразовом пароле, используемом аппаратным устройством.

Второй тип аутентификации базируется на комбинировании одноразового пароля и биометрических факторов.

В случае первого типа многофакторной аутентификации для хранения регистрационных данных требуется использование устойчивых к взлому аппаратных устройств.

A.5 Аспекты безопасности аутентификации по нескольким методам

В случае аутентификации по нескольким методам требуется, чтобы никакие регистрационные данные не выводились (или не угадывались) другими регистрационными данными.

A.6 Аспекты безопасности множественной аутентификации

В случае множественной аутентификации требуется, чтобы никакие регистрационные данные не выводились (или не угадывались) другими регистрационными данными.

Дополнение I

Взаимосвязь с соответствующими стандартами

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Взаимосвязь с [ITU-T X.1141]

На рисунке I.1 показана взаимосвязь модели, описанной в настоящей Рекомендации, и модели, описанной в разделе 10, и языком разметки утверждений безопасности (SAML 2.0) Рекомендации [ITU-T X.1141]. Серые прямоугольники − функции, определенные в SAML.

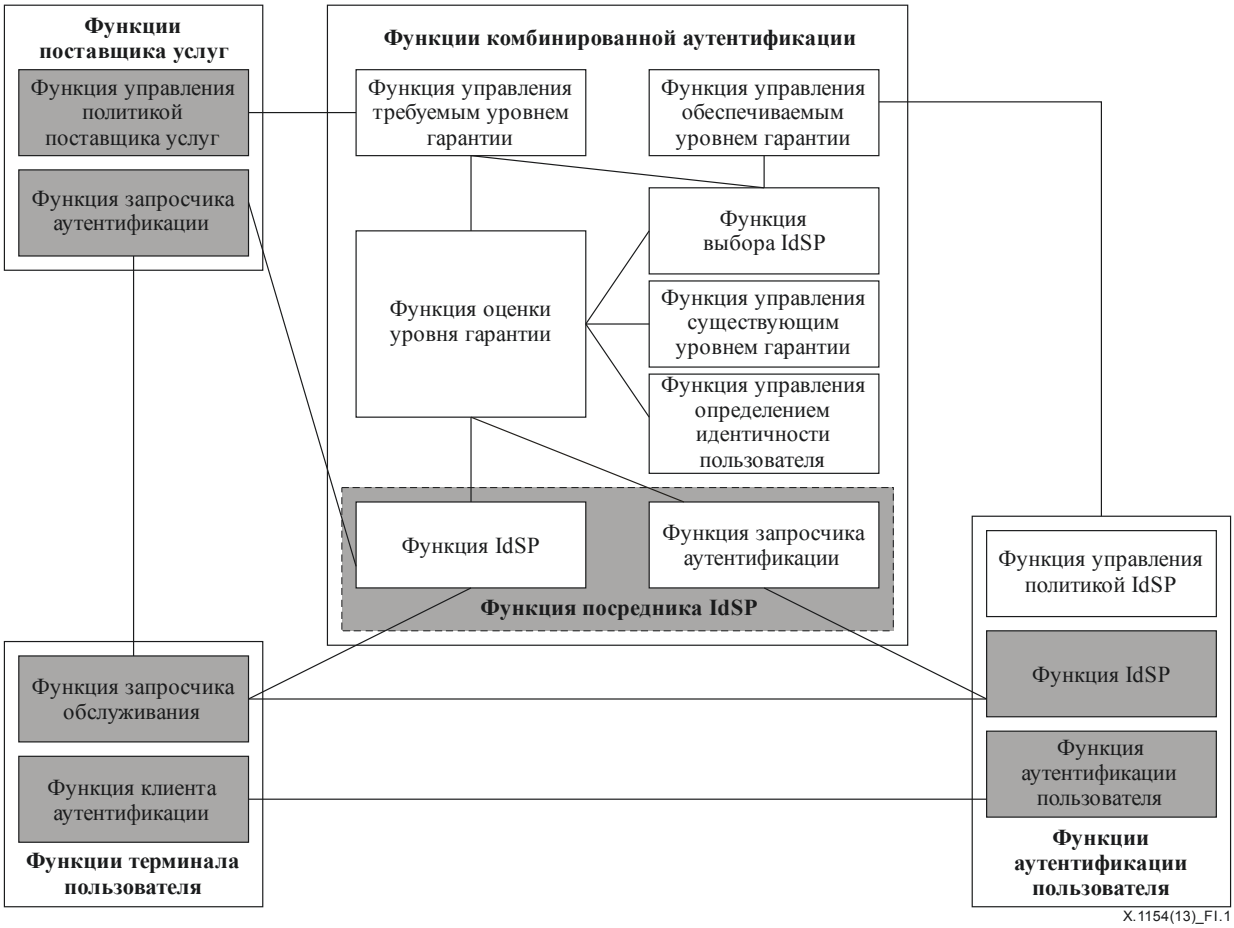

Рисунок I.1 − Взаимосвязь с [ITU-T X.1141]

I.2 Взаимосвязь с [ITU-T X.1254]

Структура в настоящей Рекомендации предназначена для обеспечения комбинированной аутентификации с использованием нескольких IdSP. Это значит, что представленная в настоящей Рекомендации структура, является примером реализации этапа аутентификации, описанного в [ITU-T X.1254], в среде с несколькими IdSP.

Библиография

[b-ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1084] Recommendation ITU-T X.1084 (2008), *Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems*.

[b-ITU-T X.1086] Recommendation ITU-T X.1086 (2008), *Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security*.

[b-ITU-T X.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure (TAI)*.

[b-ITU-T X.1151] Recommendation ITU-T X.1151 (2007), *Guideline on secure password-based authentication protocol with key exchange*.

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности*.

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, 2013 г.