Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1258

(09/2016)

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

Безопасность киберпространства –
Управление определением идентичности

Улучшенная аутентификация объектов на основании объединенных атрибутов

Рекомендация МСЭ-Т X.1258

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
Рекомендации, связанные с PKI	X.1340–X.1349
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

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

Рекомендация МСЭ-Т X.1258

Улучшенная аутентификация объектов на основании объединенных атрибутов

Резюме

Объединение атрибутов, получаемых от нескольких органов по присвоению атрибутов, может потребоваться для того, чтобы позволить полагающейся стороне повысить свое доверие к идентичности той или иной стороны. Объединение можно рассматривать как деятельность по сбору глобально определенных уникальных идентификаторов, которая характерна для всех органов по присвоению атрибутов. На практике объекты не имеют глобальных идентификаторов, а имеют различные идентификаторы и атрибуты объектов, присвоенные их различными поставщиками услуг определения идентичности (IdSP).

При таком сценарии для решения проблемы объединения атрибутов используется концепция федерации идентичностей. Например, если какой-либо электронный книжный магазин планирует предоставлять скидки пожилым людям, то этому магазину должен быть представлен объединенный набор атрибутов (кредитная карта и возрастная граница) от двух IdSP, но при этом данные IdSP не знают об участии друг друга. В случае стандартного управления определением федеративной идентичности тот или иной объект может представить атрибуты только одной идентичности, однако для данной транзакции требуются атрибуты двух идентичностей. Существует несколько методов создания федерации идентичностей: язык разметки утверждений безопасности (SAML), система Shibboleth, открытая идентичность (OpenID), открытая аутентификация (OAuth) и др.

В Рекомендации МСЭ-Т X.1258 представлена концепция объединения атрибутов, позволяющая тому или иному объекту объединять атрибуты, полученные от нескольких IdSP. Объединение атрибутов – это механизм сбора атрибутов какого-либо объекта, полученных от нескольких IdSP. Объединение атрибутов необходимо для динамического объединения атрибутов по запросу. IdSP может выполнить запрос на объединение, в случае если тот или иной объект хочет получить какую-либо услугу. Наряду с этим при аутентификации также может быть применен объектно-ориентированный механизм объединения атрибутов, чтобы ограничить утечку конфиденциальных данных.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	ITU-T X.1258	07.09.2016 г.	17-я	11.1002/1000/12850

Ключевые слова

Объединение атрибутов, управление определением федеративной идентичности.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1258

Улучшенная аутентификация объектов на основании объединенных атрибутов

1 Сфера применения

В настоящей Рекомендации приводится метод улучшенной аутентификации на основании объединения атрибутов объектов из разных доменов. В настоящей Рекомендации рассматриваются следующие темы:

– методы объединения нескольких атрибутов поставщиков услуг определения идентичности (IdSP); и

– улучшенная аутентификация на основании объединенных атрибутов.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 атрибут (attribute) [b-ITU-T X.1252]: Информация, связанная с объектом, которая означает какую-либо его характеристику.

3.2.1 аутентификация (объекта) ((entity) authentication) [b-ITU-T X.1252]: Процесс, используемый для достижения достаточной меры доверия в отношении связи между объектом и представленной информацией идентичности.

ПРИМЕЧАНИЕ. – Использование термина "аутентификация" в контексте управления определением идентичности (IdM) означает аутентификацию объекта.

3.1.3 круг доверия (circle of trust) [b-ITU-T X.1251]: Набор критериев, установленных для объединения организаций в федерацию в целях доверенного доступа к ресурсам друг друга. Следует отметить, что круг доверия представляет собой также конечный результат объединения организаций в федерацию.

3.1.4 федерация (federation) [b-ITU-T X.1252]: Ассоциация пользователей, поставщиков услуг и поставщиков услуг данных идентичности.

3.1.5 идентичность (identity) [b-ITU-T X.1252]: Представление того или иного объекта в виде одного или нескольких атрибутов, которые позволяют однозначно и в достаточной мере распознать объекты в том или ином контексте. В целях управления определением идентичности (IdM) термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), то есть разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует с другими объектами.

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 количество всех возможных атрибутов бесконечно.

3.1.6 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.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 объединение атрибутов (attribute aggregation): Механизм сбора атрибутов, полученных от нескольких поставщиков услуг определения идентичности (IdSP).

ПРИМЕЧАНИЕ. – После того как атрибуты собраны, они должны быть объединены и утверждены для целей аутентификации и авторизации.

3.2.2 домен (domain): Область охвата управлением, относящаяся к одному поставщику услуг определения идентичности (IdSP).

3.2.3 поставщик услуг (service provider (SP)): Объект, который предоставляет услуги клиентам или другим поставщикам услуг.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

CoT	Circle of Trust		Круг доверия
DB	Database	БД	База данных
ID	Identity		Идентичность
IdM	Identity Management		Управление определением идентичности
IdSP	Identity Service Provider		Поставщик услуг определения идентичности
LS	Linking Service		Услуга связывания
OAuth	Open Authentication		Открытая аутентификация
OpenID	Open Identity		Открытая идентичность
PKI	Public Key Infrastructure		Инфраструктура открытых ключей
SAML	Security Assertion Markup Language		Язык разметки утверждений безопасности
SP	Service Provider		Поставщик услуг
SSO	Single Sign-On		Однократная регистрация входа
VC	Virtual Collaboration		Виртуальное сотрудничество

5 Условные обозначения

Нет.

6 Общие положения

Как правило, электронное управление определением идентичности (IdM) охватывает управление цифровыми идентичностями любого вида. Одной из отправных точек IdM может являться разработка справочников, например поддерживаемых в [b-ITU-T X.500]. В [b-ITU-T X.509] определяются сертификаты, содержащие атрибуты идентичности. Сертификаты, определенные в [b-ITU-T X.509], и системы, применяющие инфраструктуру открытых ключей (PKI), используются для проверки онлайновой идентичности того или иного субъекта. Таким образом управление определением идентичности может рассматриваться как управление информацией.

Идентичность того или иного объекта может состоять из атрибутов, которые характеризуют данный объект в различных контекстах. В зависимости от контекста и ситуации могут требоваться разные идентичности. Система управления определением идентичности обеспечивает средства для управления этими идентичностями в цифровом мире. Управление определением идентичности – это набор функций и возможностей, таких как создание/удаление идентичности, обнаружение

информации и обмен ею. В реальном мире человек выбирает, какая информация может быть раскрыта другим людям с учетом контекста и критичности информации. В свою очередь в цифровом мире данная задача выполняется системой управления определением идентичности.

С учетом технологий и стандартов в отношении управления определением идентичности системные методы IdM подразделяются на традиционные, централизованные и федеративные. Традиционный метод характеризуется тем, что поставщик услуг (SP) обрабатывает идентичности и совмещен с поставщиком услуг определения идентичности (IdSP). Объект создает свою цифровую идентичность (ID) для каждого поставщика услуг, от которого он хочет получить услуги. Обычно различные поставщики услуг не обмениваются информацией об идентичности объекта, и данный подход, как правило, является более затратным как для объекта, так и для поставщиков услуг. Для формирования цифровой идентичности объекта каждому поставщику услуг может многократно требоваться его собственный набор атрибутов.

Централизованный метод изначально разрабатывается для решения проблемы отсутствия гибкости в традиционном методе. В нем поставщики услуг обмениваются информацией об идентичности, и он основан на принципе однократной аутентификации, то есть однократной регистрации входа (SSO). В данном методе сделана попытка избежать неудобств и избыточности, характерных для традиционного метода, и объектам дается возможность взаимодействия с различными поставщиками услуг без необходимости осуществлять лишнюю аутентификацию.

Каждый поставщик услуг, который имеет доверительные отношения с IdSP, будет полностью полагаться на результаты аутентификации объекта, обеспеченной данным IdSP. Поставщик услуг определения идентичности отвечает за аутентификацию объекта и представление поставщикам услуг информации об атрибутах объекта в рамках домена, который может представлять собой компанию, университет и т. д. и состоять из объектов, нескольких поставщиков услуг и одного поставщика услуг определения идентичности. Однократная аутентификация (SSO) обеспечивает объектам большое удобство, поскольку они должны осуществлять процесс аутентификации только один раз. В дальнейшем объекты могут использовать полученные регистрационные данные у всех поставщиков услуг, к которым они хотят получить доступ. Вместе с тем слабым местом централизованного метода является то, что IdSP обладает полным контролем над информацией об этих объектах и может использовать ее любым образом по своем усмотрению. Это обстоятельство является главной причиной того, почему централизованный метод не получил широкого признания.

Для решения проблем, присущих централизованному методу, был представлен метод федеративной идентичности, основанный на распределении задачи аутентификации по нескольким поставщикам услуг определения идентичности, которые принадлежат к различным доменам. Концепция федеративной идентичности опирается на доверительные отношения, которые устанавливаются между несколькими поставщиками услуг определения идентичности и соответствующими доменами. Для передачи распределенной информации об идентичности между поставщиком услуг определения идентичности (IdSP) и поставщиком услуг (SP) требуется наличие доверительных отношений между этими двумя сторонами. Эти доверительные отношения называются кругом доверия (CoT), который может включать одного или нескольких IdSP и SP. Применительно к какому-либо кругу доверия, в случае если пользователь прошел аутентификацию у IdSP, то ему разрешен доступ к поставщикам услуг, входящим в этот круг доверия, без дополнительной аутентификации. Таким образом в каком-либо одном круге доверия пользователю необходимо пройти аутентификацию только один раз [b-ITU-T X.1251].

Управление определением федеративной идентичности является одним из способов устранения риска, связанного с наличием лишь одного поставщика услуг определения идентичности, и уменьшения интенсивности обмена информацией с IdSP в процессе аутентификации. Идентичности, выданные в одном домене, благодаря этим соглашениям между поставщиками услуг определения идентичности будут признаны поставщиками услуг в других доменах, и принцип однократной регистрации входа соблюдается даже при наличии различных доменов.

Для поставщиков услуг преимущество федеративных идентичностей заключается в том, что они могут обрабатывать информацию о меньшем количестве объектов. Метод управления определением федеративной идентичности используется в рамках инициативы Kantara [b-Kantara], проекта Shibboleth [b-Shibboleth] и проекта Higgins [b-Higgins]. В методах, основанных на федеративной идентичности, идентичности распределяются между различными IdSP, а информация об объектах может быть доступна любым иным третьим сторонам (IdSP) федерации.

7 Архитектуры и последовательности выполнения методов объединения атрибутов

При первоначальных исследованиях в области объединения атрибутов, получаемых от нескольких органов по присвоению атрибутов, предполагалось, что объект имеет глобально определенный уникальный идентификатор, который является общим для всех органов по присвоению атрибутов. В действительности у объектов нет глобально определенных идентификаторов, а есть различные идентификаторы объекта, присвоенные им различными IdSP.

Проект Liberty Alliance [b-Liberty], предшествовавший инициативе Kantara [b-Kantara], стал первой группой, которая изучала проблему объединения атрибутов и выдвинула принцип федерации идентичностей [b-Chadwick]. Однако оставалась нерешенной проблема отсутствия стандартного способа объединения атрибутов объекта, утвержденных несколькими органами, с тем чтобы они использовались поставщиком услуг в процессе принятии решений, связанных с управлением доступом.

Целесообразно рассмотреть несколько сценариев использования, чтобы понять необходимость объединения атрибутов.

– В случае если какой-либо электронный книжный магазин планирует предоставлять скидки пожилым людям, то этому магазину должен быть представлен объединенный набор атрибутов (реквизиты кредитной карты и документальное подтверждение возраста), полученных от нескольких IdSP. В этом примере требуется, чтобы объект представил атрибуты двух идентичностей.

– Предположим, что какой-либо исследователь захочет приобрести компьютер, используя федеративный банковский счет, в онлайновом магазине, который предлагает скидки для работников сферы образования. В этом случае исследователь должен представить доказательство того, что он является членом образовательной организации и что у него есть специальный счет в его банке. Необходимо собрать атрибуты, хранящиеся в нескольких различных идентичностях, а результат объединения этих атрибутов должен быть передан поставщику услуг. Этот процесс называется объединением атрибутов [b-Klingenstein].

Совместное и скоординированное использование ресурсов, имеющихся в динамичных и мультиструктурных сообществах, лежит в основе все более широкого круга компьютерных приложений – от совместных научных исследований до здравоохранения. Совершенно необходимо, чтобы такое совместное использование тщательно контролировалось. Поставщики ресурсов и потребители должны четко и тщательно определить, что подлежит совместному использованию, кому оно разрешено и на каких условиях оно осуществляется. Группа отдельных лиц и/или учреждений, определенных этими правилами совместного использования, образует так называемое виртуальное сотрудничество (VC). Одной из проблем является обеспечение самоуправления, с тем чтобы в рамках виртуального сотрудничества можно было без труда создавать и вести базу членов и их функции в собственных группах, а также средства управления доступом к своим ресурсам, особенно если эти совместно используемые ресурсы размещены в нескольких учреждениях. В сценарии виртуального сотрудничества поставщик услуг определения федеративной идентичности (IdSP), как правило, не может представить все атрибуты, которые необходимы участвующим в нем поставщикам услуг (SP). Эти связанные с виртуальным сотрудничеством атрибуты, например его название, статус членства, список рассылки членам и т. д., необходимо собирать из других источников. В управлении атрибутами пользователей должны участвовать несколько отдельных органов по присвоению атрибутов [b-Hulsebosch].

Существует несколько методов создания федерации идентичностей, например язык разметки утверждений безопасности (SAML), система Shibboleth [b-Shibboleth], федерация веб-услуг [b-WS-Federation], инициатива Kantara [b-Kantara], открытая идентичность [b-OpenID], открытая аутентификация [b-OAuth], CardSpace [b-CardSpace], Проект Higgins [b-Higgins] и др. В зависимости от того, кто выступает в роли медиатора процесса в целом, методы объединения атрибутов можно разделить на три категории: методы IdSP-медиатора, методы поставщика услуг – медиатора и методы объекта-медиатора.

7.1 Методы поставщика услуг определения идентичности – медиатора

7.1.1 Связывание идентичности

Метод, представленный структурой Liberty Alliance, является одним из первых методов решения проблемы объединения атрибутов с помощью ее принципа федерации идентичностей, см. рисунок 1, [b-Liberty]. На этом рисунке IdSP разрешают объекту создать двустороннюю связь (CoT3) между двумя IdSP. При перемещении объекта между услугами первый IdSP (IdSP 1 на рисунке 1) спрашивает данный объект, хочет ли он объединить данного IdSP (IdSP 1) в федерацию с другим IdSP (IdSP 2). На данном этапе оба IdSP взаимодействуют друг с другом в целях создания индикатора связи. При получении доступа к услугам от SP один IdSP представит данный индикатор SP вместе с атрибутами, содержащими утверждения. SP может использовать этот индикатор для получения других атрибутов, содержащих утверждения, от другого IdSP. Объединив атрибуты, полученные от обоих IdSP, SP может принять решение о возможности доступа объекта к услуге.

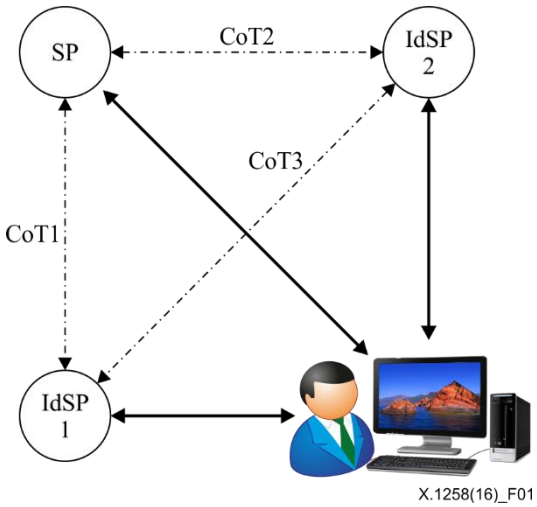

Рисунок 1 – Архитектура метода связывания идентичности

На рисунке 2 показана схематическая последовательность управляющих команд по объединению атрибутов с помощью метода связывания идентичности.

1) Объект направляет запрос на предоставление услуги поставщику услуг.
2) Если поставщику услуг необходимо разрешение объекта на пользование услугой, он направляет запрос аутентификации и утверждения аутентификации.
3) Объект перенаправляется к первому поставщику услуг определения идентичности (IdSP 1) для аутентификации.
4) IdSP 1 аутентифицирует объект и запрашивает дополнительные атрибуты.
5) IdSP 1 возвращает утверждение аутентификации.
6) Объект представляет утверждение аутентификации поставщику услуг.
7) Поставщик услуг просит второго поставщика услуг определения идентичности (IdSP 2) представить дополнительные атрибуты, относящиеся к объекту.
8) IdSP 2 представляет дополнительный атрибут.
9) Поставщик услуг проверяет утверждения и дает объекту разрешение на доступ к услуге.

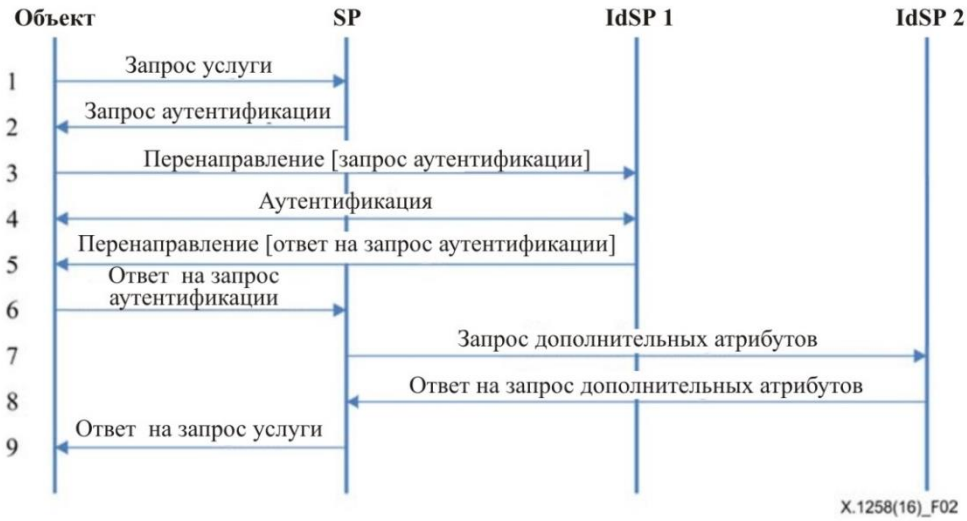

Рисунок 2 – Последовательность объединения атрибутов с использованием метода связывания идентичности

7.1.2 Опосредование идентичности

Существует IdSP-посредник, и у SP есть полностью доверенное соединение с этим IdSP; другие IdSP неизвестны SP, и они имеют доверительные отношения только с IdSP-посредником (IdSP 1) – см. рисунок 3 [b-Klingenstein]. Если объект хочет объединить атрибуты, полученные от нескольких IdSP, то вначале он будет перенаправлен к IdSP-посреднику (IdSP 1 на рисунке 3), а затем IdSP-посредник перенаправляет этот объект к нескольким другим IdSP. После того как этот объект аутентифицирован индивидуально каждым IdSP, он возвращает утверждение IdSP-посреднику. После этого IdSP-посредник проверяет каждое утверждение, получает атрибуты от этих IdSP и объединяет все полученные атрибуты. IdSP-посредник может заполнить объединенный набор собственными атрибутами объекта и повторно заверяет утверждения. Далее IdSP-посредник направляет SP все повторно заверенные утверждения атрибутов. Затем SP принимает решение, может ли объект получить доступ к услуге на основании объединенных атрибутов. Поскольку SP не знает о других IdSP, а имеет отношения только с IdSP-посредником, он считает, что все атрибуты были выпущены этим IdSP-посредником.

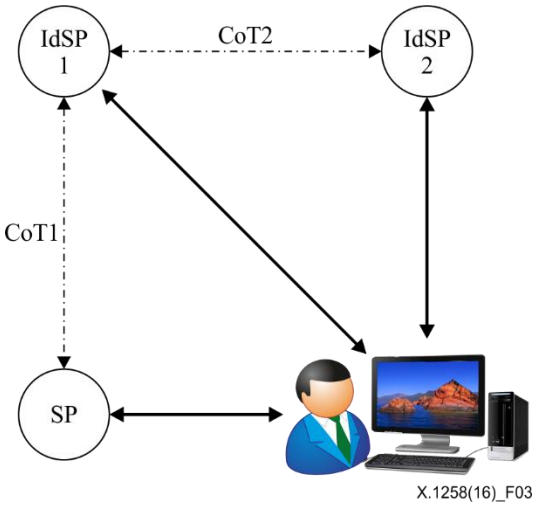

Рисунок 3 – Архитектура метода опосредования идентичности

На рисунке 4 показана схематическая последовательность управляющих команд по объединению атрибутов с помощью метода опосредования идентичности.

1) Объект направляет запрос на предоставление услуги поставщику услуг.
2) Если поставщику услуг необходимо разрешение объекта на пользование услугой, он направляет запрос аутентификации и утверждения аутентификации.
3) Объект перенаправляется к первому поставщику услуг определения идентичности (IdSP 1) для аутентификации.
4) IdSP 1 перенаправляет объект ко второму поставщику услуг определения идентичности (IdSP 2).
5) IdSP 2 получает запрос на аутентификацию и получение атрибутов.
6) IdSP 2 аутентифицирует объект.
7) IdSP 2 возвращает результат аутентификации и утверждения атрибутов.
8) Объект передает результат аутентификации и утверждения атрибутов первому поставщику услуг определения идентичности.
9) IdSP 1 добавляет дополнительные атрибуты, подписывает утверждения и возвращает их объекту.
10) Объект представляет утверждения поставщику услуг.
11) Поставщик услуг проверяет утверждения и дает объекту разрешение на доступ к услуге.

Рисунок 4 – Последовательность объединения атрибутов с использованием метода опосредования идентичности

7.1.3 Ретрансляция идентичности

Метод ретрансляции идентичности аналогичен методу опосредования идентичности, но не требует прочных доверительных отношений между SP и IdSP-посредником. Хотя в методе посредника требуется, чтобы SP полностью доверял доверенному IdSP, в действительности может оказаться невозможным обеспечить абсолютное доверие между IdSP-посредником и SP. В методе ретрансляции идентичности промежуточный IdSP (или IdSP-ретранслятор – IdSP 1 на рисунке 5) может действовать как IdSP-посредник. Тогда эта последовательность аналогична последовательности метода посредника. Вначале объект перенаправляется к IdSP-ретранслятору,

а затем IdSP-ретранслятор перенаправляет этот объект к нескольким другим IdSP. После того как этот объект аутентифицирован индивидуально каждым IdSP, он возвращает утверждения IdSP-ретранслятору. После этого IdSP-ретранслятор объединяет все утверждения в одно утверждение и передает его SP. Отличие между моделями опосредования и ретрансляции заключается в подписании утверждений атрибутов. IdSP-ретранслятор не подписывает утверждения атрибутов, а просто ретранслирует утверждения, подписанные исходным IdSP. Далее SP получает зашифрованные утверждения атрибутов от различных IdSP и IdSP-ретранслятора и принимает решение, может ли объект получить доступ к услуге на основании объединенных атрибутов. В данном методе необходимы доверительные отношения между поставщиками услуг определения идентичности и поставщиком услуг.

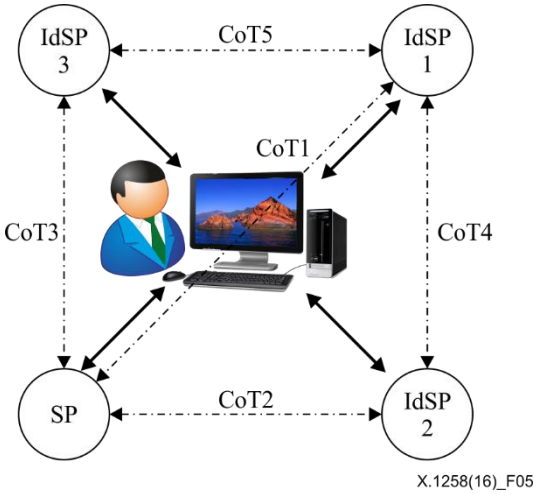

Рисунок 5 – Архитектура метода ретрансляции идентичности

На рисунке 6 показана схематическая последовательность управляющих команд по объединению атрибутов с помощью метода ретрансляции идентичности.

1) Объект направляет запрос на предоставление услуги поставщику услуг.
2) Если поставщику услуг необходимо разрешение объекта на пользование услугой, он направляет запрос аутентификации и утверждения аутентификации.
3) Объект перенаправляется к первому поставщику услуг определения идентичности (IdSP 1) для аутентификации.
4) IdSP 1 перенаправляет объект ко второму поставщику услуг определения идентичности (IdSP 2).
5) IdSP 2 получает запрос на аутентификацию и получение атрибутов.
6) IdSP 2 аутентифицирует объект.
7) IdSP 2 возвращает результат аутентификации и утверждения атрибутов.
8) Объект передает результат аутентификации и утверждения атрибутов первому поставщику услуг определения идентичности.
9) IdSP 1 добавляет дополнительные атрибуты, подписывает утверждения и возвращает их объекту.
10) Объект представляет утверждения поставщику услуг.
11) Поставщик услуг проверяет утверждения и дает объекту разрешение на доступ к услуге.

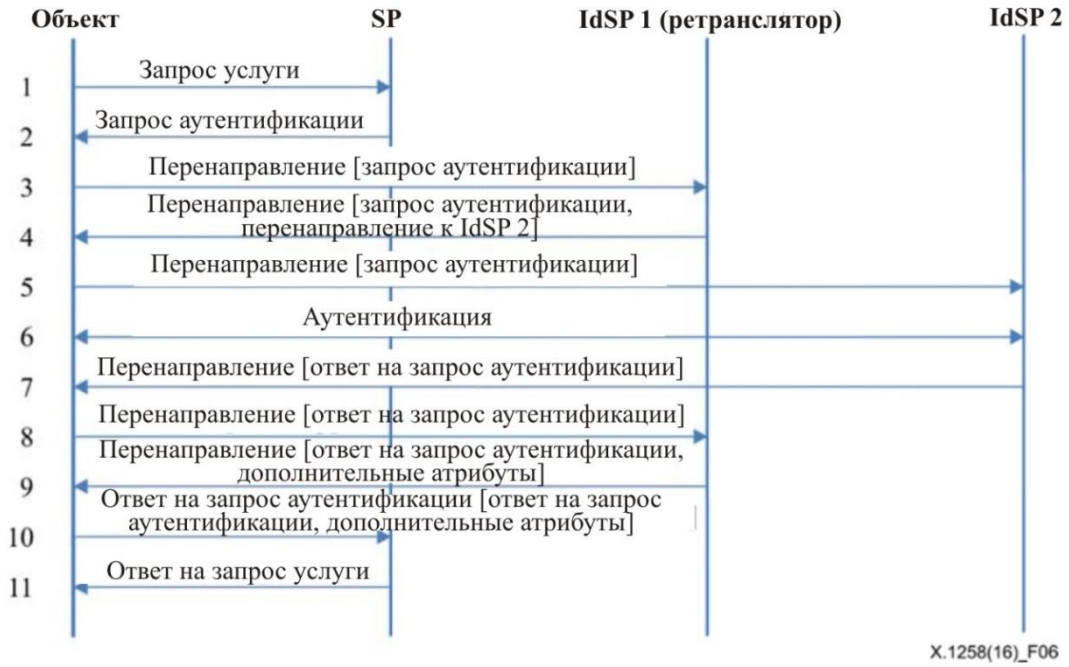

Рисунок 6 – Последовательность объединения атрибутов с использованием метода ретрансляции идентичности

7.2 Методы поставщика услуг – медиатора

7.2.1 База данных приложений

Метод базы данных приложений является простейшим из методов объединения атрибутов, см. рисунок 7 [b-Hulsebosch]. Помимо атрибутов, обеспечиваемых IdSP, SP должен сохранять дополнительные атрибуты объекта, например псевдоним, предпочтительные для данной конкретной услуги объекты, групповое членство и др. SP осуществляет управление добавленными атрибутами для приложений. Кроме того, эти атрибуты, хранящиеся в его базе данных, могут извлекаться и в дальнейшем, с тем чтобы SP мог принимать решение о возможности доступа объекта к определенной услуге.

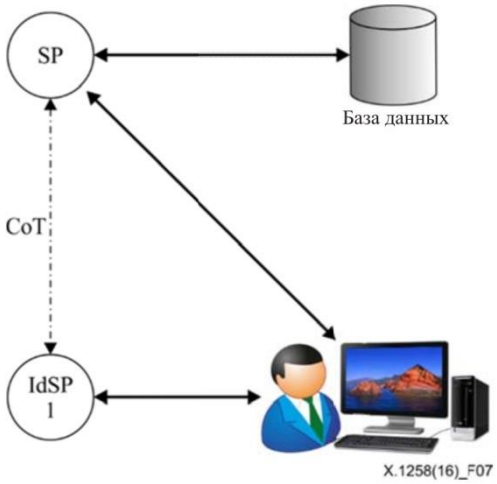

Рисунок 7 – Архитектура метода базы данных приложений

На рисунке 8 показана схематическая последовательность управляющих команд по объединению атрибутов с помощью базы данных приложений.

1) Объект направляет запрос на предоставление услуги поставщику услуг.
2) Если поставщику услуг необходимо разрешение объекта на пользование услугой, он направляет запрос аутентификации и утверждения аутентификации.
3) Объект перенаправляется к первому поставщику услуг определения идентичности (IdSP 1) для аутентификации.
4) IdSP 1 аутентифицирует объект.
5) После успешной аутентификации IdSP 1 возвращает результат аутентификации и утверждение.
6) Объект представляет утверждение аутентификации поставщику услуг.
7) При необходимости поставщик услуг извлекает дополнительные атрибуты объекта из своей базы данных.
8) Поставщик услуг проверяет утверждения и дает объекту разрешение на доступ к услуге.

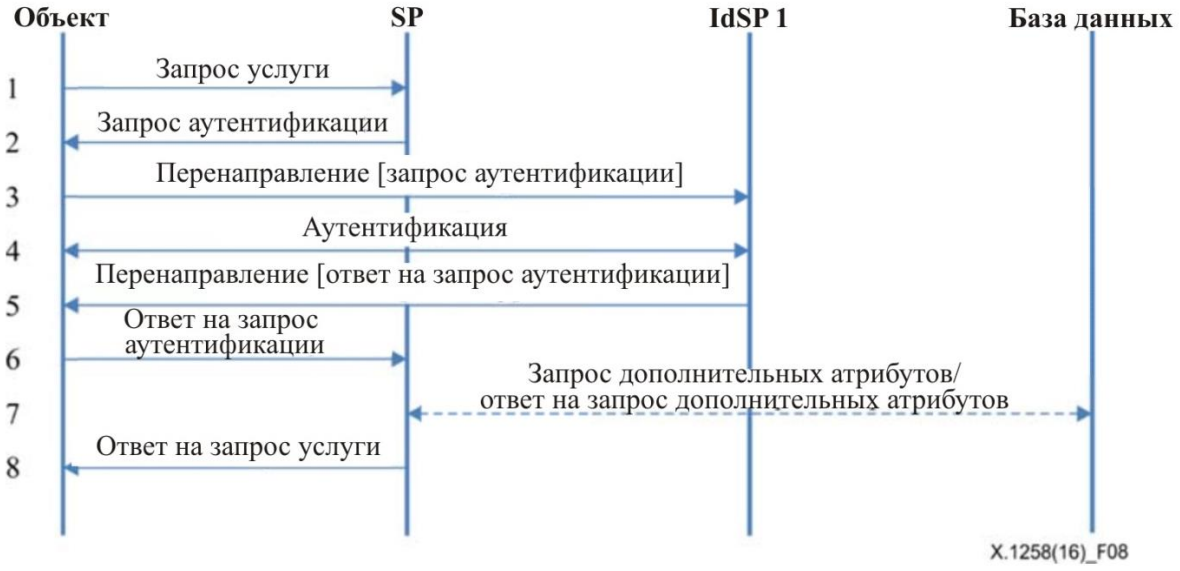

Рисунок 8 – Последовательность объединения атрибутов с использованием метода базы данных приложений

7.2.2 Поставщик услуг

Метод поставщика услуг (SP) позволяет объекту объединять полученные от нескольких IdSP атрибуты за один сеанс, см. рисунок 9 [b-Hulsebosch]. Объект поочередно перенаправляется к различным IdSP, которые его аутентифицируют по отдельности и возвращают утверждения атрибутов поставщику услуг. Тот в свою очередь объединяет утверждения атрибутов, полученные от IdSP, и принимает решение о возможности доступа объекта к определенной услуге.

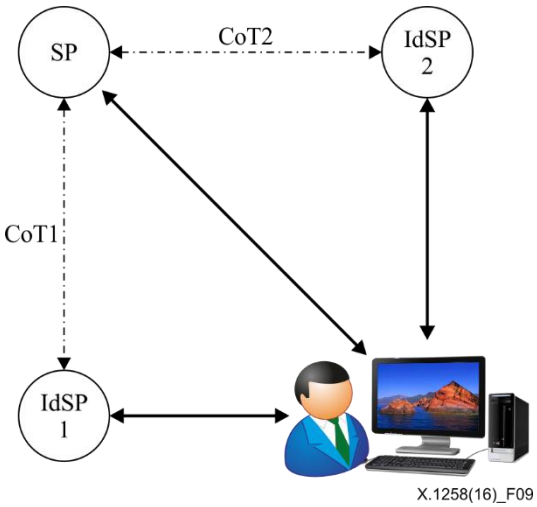

Рисунок 9 – Архитектура метода поставщика услуг

На рисунке 10 показана схематическая последовательность управляющих команд по объединению атрибутов с помощью метода SP.

1) Объект направляет запрос на предоставление услуги поставщику услуг.
2) Если поставщику услуг необходимо разрешение объекта на пользование услугой, он направляет запрос аутентификации и утверждения аутентификации.
3) Объект перенаправляется к первому поставщику услуг определения идентичности (IdSP 1) для аутентификации.
4) IdSP 1 аутентифицирует объект.
5) IdSP 1 возвращает результат аутентификации и утверждение.
6) Объект представляет утверждение аутентификации поставщику услуг.
7) Поставщик услуг просит объект представить относящиеся к нему дополнительные атрибуты.
8) Объект направляет запрос на предоставление услуги второму поставщику услуг определения идентичности (IdSP 2).
9) IdSP 2 аутентифицирует объект.
10) IdSP 2 представляет дополнительные атрибуты.
11) Объект представляет утверждения аутентификации поставщику услуг.
12) Поставщик услуг проверяет утверждения и дает объекту разрешение на доступ к услуге.

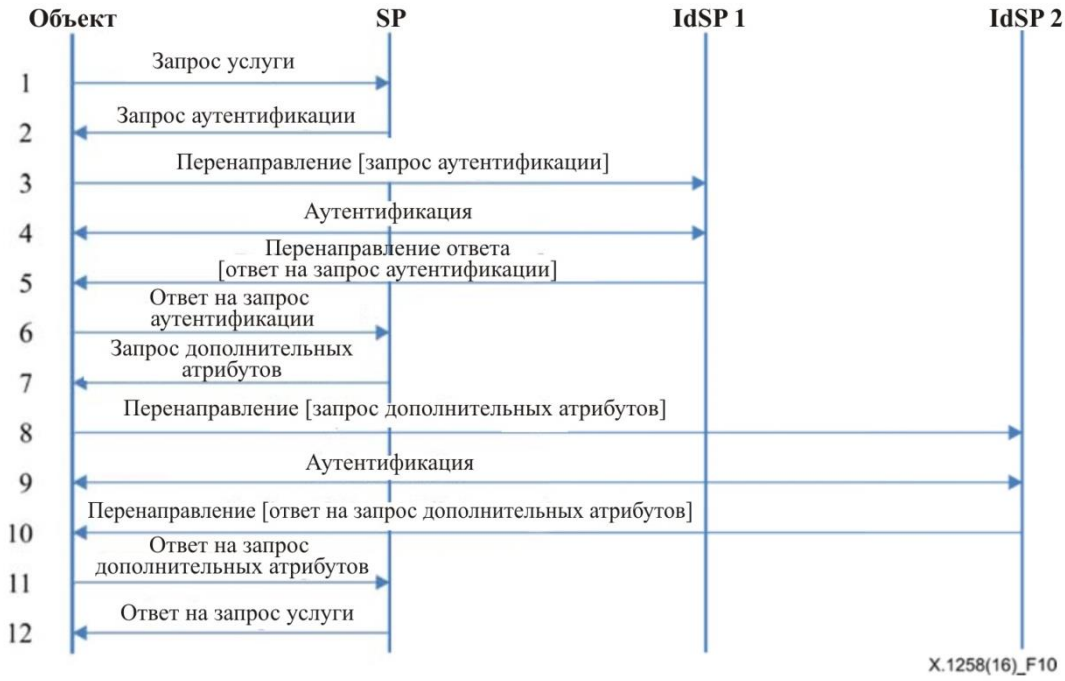

Рисунок 10 – Последовательность объединения атрибутов с использованием метода поставщика услуг

7.2.3 Услуга связывания

Метод услуги связывания (LS) является сочетанием метода связывания идентичности и метода ретрансляции идентичности. Поставщик услуги связывания – это особый тип SP (см. рисунок 11), который используется объектом посредством обеспечиваемого LS идентификатора [b-Chadwick], [b-Hulsebosch]. Этот идентификатор используется для связывания различных поставщиков услуг определения идентичности с помощью предоставляемых им постоянных идентификаторов, соответствующих LS, которые содержатся в так называемой таблице связывания. Если объект хочет получить доступ к услуге, то он обращается к SP и перенаправляется к первому IdSP (IdSP 1 на рисунке 11). IdSP 1 аутентифицирует этот объект, а затем через него возвращает SP утверждение, содержащее атрибуты объекта и идентификатор для LS. SP передает этот идентификатор LS для получения дополнительных атрибутов. На данном этапе возможны два варианта: LS может либо извлечь список связанных IdSP для данного постоянного идентификатора, используя таблицу связывания, и получить от каждого IdSP атрибуты, которые он затем объединяет и возвращает SP, либо направить список связанных IdSP обратно SP, и далее SP получает атрибуты от каждого IdSP. Затем SP принимает решение, может ли объект получить доступ к услуге на основании объединенных атрибутов.

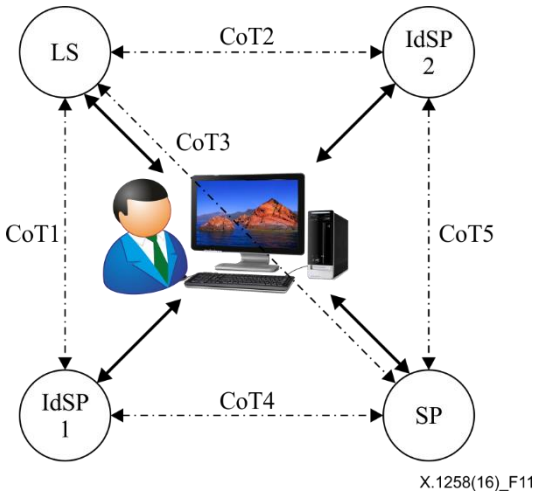

Рисунок 11 – Архитектура метода услуги связывания (LS)

На рисунке 12 показана схематическая последовательность управляющих команд по объединению атрибутов с помощью метода услуги связывания.

1) Объект направляет запрос на предоставление услуги поставщику услуг.
2) Если поставщику услуг необходимо разрешение объекта на пользование услугой, он направляет запрос аутентификации и утверждения аутентификации.
3) Объект перенаправляется к первому поставщику услуг определения идентичности (IdSP 1).
4) IdSP 1 аутентифицирует объект.
5) IdSP 1 возвращает утверждение аутентификации и идентификатор для LS.
6) Объект представляет утверждение и идентификатор для LS поставщику услуг.
7) Поставщик услуг направляет дополнительные запросы атрибутов объекту.
8) Объект перенаправляется к поставщику услуги связывания.
9) Поставщик услуги связывания просит второго поставщика услуг определения идентичности (IdSP 2) представить атрибуты.
10) IdSP 2 представляет эти атрибуты.
11) Атрибуты возвращаются объекту.
12) Объект представляет утверждения аутентификации поставщику услуг.
13) Поставщик услуг проверяет утверждения и дает объекту разрешение на доступ к услуге.

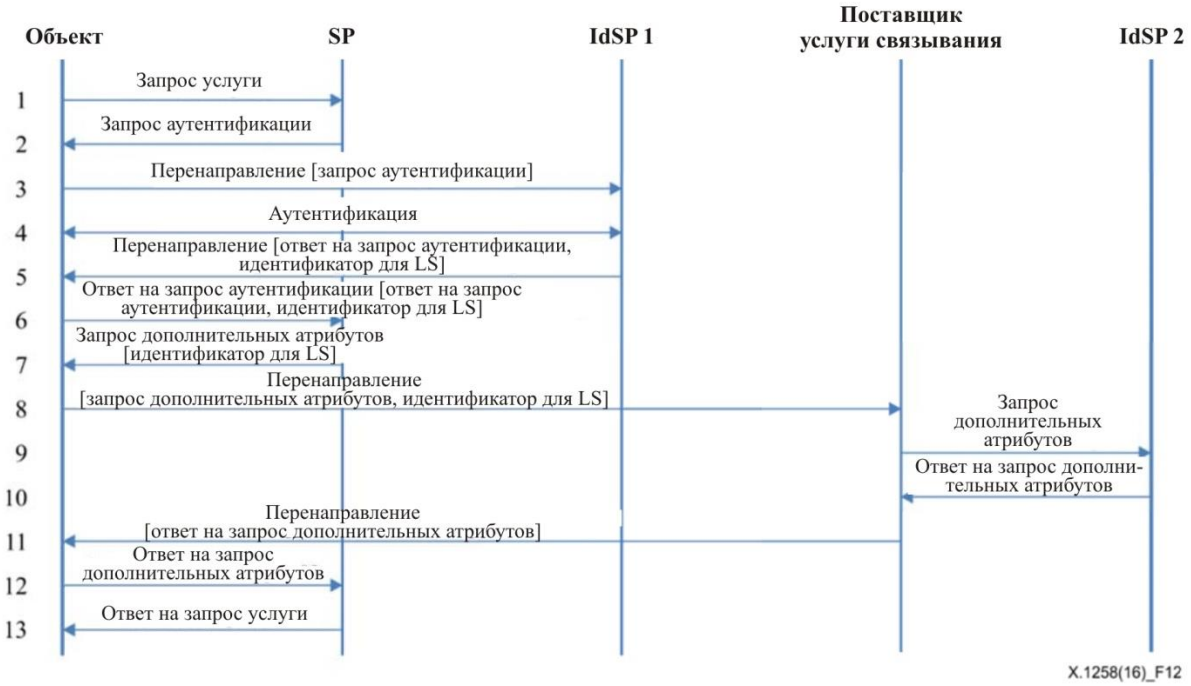

Рисунок 12 – Последовательность объединения атрибутов с использованием метода услуги связывания

7.3 Метод объекта-медиатора

В методе объекта-медиатора используется клиент (объект-агент или приложение), который имеет возможность объединять атрибуты, полученные от различных IdSP, см. рисунок 13 ([b-Klingenstein] и [b-Hulsebosch]). SP информирует клиента о списке доверенных IdSP. Клиент перенаправляет объект к каждому из этих IdSP. После соответствующей аутентификации у каждого IdSP клиент получает утверждения от всех IdSP и представляет объединенный набор утверждений поставщику услуг. Поставщик услуг проверяет каждое утверждение, извлекает все атрибуты и далее принимает решение, может ли объект получить доступ к услуге.

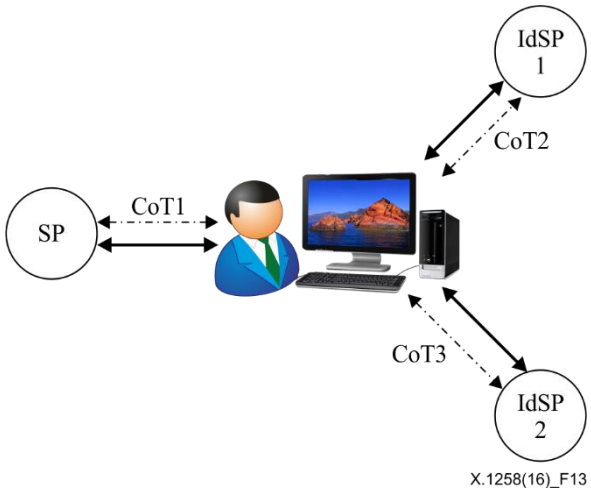

Рисунок 13 – Архитектура метода клиента

На рисунке 14 показана схематическая последовательность управляющих команд по объединению атрибутов с помощью метода клиента.

1) Объект направляет запрос на предоставление услуги поставщику услуг.
2) Если поставщику услуг необходимо разрешение объекта на пользование услугой, он направляет запрос аутентификации и утверждения аутентификации.
3) Первый поставщик услуг определения идентичности (IdSP 1) аутентифицирует объект.
4) IdSP 1 возвращает утверждение аутентификации.
5) Объект перенаправляется ко второму поставщику услуг определения идентичности (IdSP 2) для получения дополнительных утверждений атрибутов.
6) IdSP 2 аутентифицирует объект.
7) IdSP 2 возвращает утверждения аутентификации.
8) Объект представляет утверждения аутентификации поставщику услуг.
9) Поставщик услуг проверяет утверждения и дает объекту разрешение на доступ к услуге.

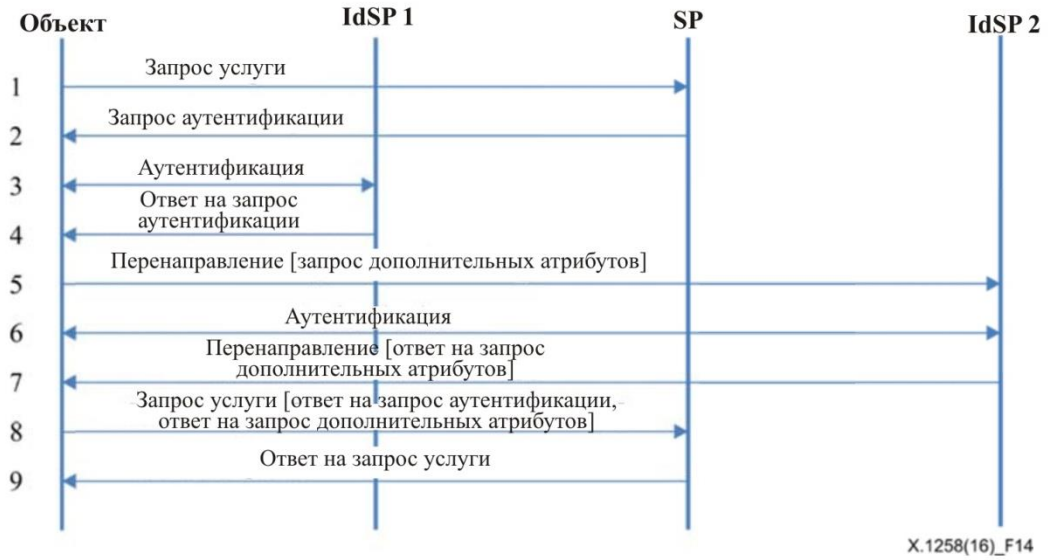

Рисунок 14 – Последовательность объединения атрибутов с использованием метода клиента

8 Сравнение методов объединенной аутентификации

Семь методов, изложенных в пункте 7, представляют собой новые подходы по сравнению с традиционной системой управления определением федеративной идентичности. В каждом из этих методов имеются дополнительные объекты или взаимодействия. С учетом данных изменений может проводиться анализ и сравнение этих семи методов по факторам, с тем чтобы выбрать приемлемый метод объединения. Проектировщик и разработчик должны учесть ряд вопросов – например, субъект опосредования, объединения или проверки атрибутов, трудности реализации и добавление новых элементов.

В пункте 7 представлен ряд методов объединения атрибутов на основе SAML. Эти методы могут взаимодействовать в зависимости от того, как они выражены в утверждении на языке SAML.

Проводится анализ методов объединения в отношении ролей его медиатора и исполнителя, а также дополнительного элемента. Результаты сравнения методов объединения показаны в таблице 1.

"Галочка" (✓) в ячейке таблицы 1 показывает, что метод объединения, указанный в строке, обеспечивает возможность, указанную в столбце, – точнее, соответствующая возможность должна поддерживаться в реализации данного метода.

Таблица 1 – Сравнение методов объединения

Метод объединения	Возможность						
	IdSP в роли медиатора	**SP в роли медиатора**	**Клиент в роли медиатора**	**Объединение IdSP**	**Объединение SP**	**Объединение клиентом**	**Дополнительный элемент**
Связывание идентичности	✓				✓		
Опосредование идентичности	✓			✓			
Ретрансляция идентичности	✓			✓			
База данных приложений		✓			✓		БД
Поставщик услуг		✓			✓		
Услуга связывания		✓			✓		LS
Клиент			✓			✓	Клиент

Что касается метода связывания идентичности, роль медиатора объединения играет IdSP, а роль исполнителя – SP. То есть протокол объединения атрибутов должен быть реализован в IdSP и SP. Однако в случае других методов роли медиатора и исполнителя может играть один и тот же поставщик. Возможно, поставщику будет проще выполнить объединение атрибутов, чем реализовать метод связывания идентичности. Что касается дополнительных элементов для объединения атрибутов, в методе базы данных приложений требуется своя собственная база данных; в методе услуги связывания требуется LS (поставщик услуги связывания) как особый тип поставщика услуг; в методе объекта-медиатора требуется клиент в качестве агента. С учетом этих критериев рекомендуется использовать метод опосредования идентичности и метод ретрансляции идентичности, относящиеся к методам IdSP-медиатора, и метод поставщика услуг, относящийся к методам поставщика услуг – медиатора.

Библиография

b-ITU-T X.500] Recommendation ITU-T X.500 (2016) | ISO/IEC 9594-1:2017, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

[b-ITU-T X.1251] Рекомендация МСЭ-Т X.1251 (2009), *Структура осуществляемого пользователем управления в отношении цифровой идентичности*

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

[b-CardSpace] *Introducing windows cardspace*. MSDN technical articles, Microsoft Corporation. Адрес (по состоянию на 19.12.2016 года): http://msdn.microsoft.com/en-us/library/aa480189.aspx

[b-Chadwick] Chadwick, D.W., Inman, G. (2009). Attribute aggregation in federated identity management. *IEEE Computer*, **42**(5), pp. 33–40. http://doi.ieeecomputersociety.org/10.1109/MC.2009.143

[b-Higgins] Higgins, *Project.* Адрес (по состоянию на 05.12.2016 года): http://www.eclipse.org/higgins/

[b-Hulsebosch] Hulsebosch, B., Wegdam, M., Zoetekouw, B., van Dijk, N., Poortinga-van Wijnen, R. (2012), Virtual collaboration attribute management. 41 pp. Адрес (по состоянию на 05.12.2016 года): https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/EDS+11-06+Attribute+Management+v1.0.pdf

[b-Kantara] Kantara, *Initiative.* Адрес (по состоянию на 19.12.2016 года): https://kantarainitiative.org/reports-recommendations/

[b-Klingenstein] Klingenstein, N. (2007). Attribute aggregation and federated identity. In: *Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, p. 26–29

[b-Liberty] Liberty Alliance, *ID-FF 1.2 Specifications*, Адрес (по состоянию на 05.12.2016 года): http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[b-OAuth] OAuth. Адрес (по состоянию на 19.12.2016 года): http://oauth.net/documentation/getting-started/

[b-OpenID] OpenID authentication 2.0. Адрес (по состоянию на 19.12.2016 года): http://openid.net/specs/openid-authentication-2_0.html

[b-Shibboleth] Shibboleth Consortium, *Open Source Project*. Адрес (по состоянию на 05.12.2016 года): https://shibboleth.net/

[b-WS-Federation] Web Services Federation Language (WS-Federation) Version 1.2. Адрес (по состоянию на 19.12.2016 года): http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
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	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии,
Женева, 2017 г.