Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2724

(11/2013)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – Безопасность

Принципы поддержки протоколов OAuth и OpenID в сетях последующих поколений

Рекомендация МСЭ-Т Y.2724

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по СПП	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Пакетные сети	Y.2600–Y.2699
Безопасность	**Y.2700–Y.2799**
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
БУДУЩИЕ СЕТИ	Y.3000–Y.3499
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999

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

Рекомендация МСЭ-T Y.2724

Принципы поддержки протоколов OAuth и OpenID в сетях последующих поколений

Резюме

В Рекомендации МСЭ-T Y.2724 описываются принципы поддержки и использования разработанных IETF открытого протокола авторизации (OAuth) и протокола OpenID в среде сетей последующих поколений (СПП). Оба протокола определены для общего использования во Всемирной паутине.

Повышенные требования к безопасности и управлению определением идентичности СПП требуют точного ограничения вышеупомянутых протоколов. В настоящей Рекомендации даются пояснения относительно возможности применения этих протоколов в СПП и приводятся руководящие принципы высокого уровня в отношении их использования.

В сопутствующей Рекомендации МСЭ-T Y.2723 "Поддержка протокола OAuth в сетях последующих поколений" содержится подробный набор профилей СПП.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-T Y.2724	15.11.2013 г.	13-я	11.1002/1000/11914

* 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 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

Рекомендация МСЭ-Т Y.2724

Принципы поддержки протоколов OAuth и OpenID в сетях последующих поколений

1 Сфера применения

В настоящей Рекомендации описываются принципы поддержки и использования сетями последующих поколений (СПП) протоколов OAuth и OpenID. Сфера применения настоящей Рекомендации включает:

- функциональные принципы поддержки СПП протоколов OAuth и OpenID;
- требования к поддержке СПП протоколов OAuth и OpenID;
- сценарии использования протоколов OAuth и OpenID (приведены в Дополнении I).

ПРИМЕЧАНИЕ. – Пользователи Рекомендации и операторы, использующие описанную технологию, должны соблюдать все применимые национальные и региональные законы, нормативные акты и политические принципы.

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 Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2720] Рекомендация МСЭ-Т Y.2720 (2009 г.), *Структура управления определением идентичности в СПП.*

[ITU-T Y.2722] Рекомендация МСЭ-Т Y.2722 (2011 г.), *Механизмы управления определением идентичности в СПП.*

[IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework.* <http://tools.ietf.org/html/rfc6749>

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 жетон доступа (access token) [IETF RFC 6749]: Жетоны доступа – это полномочия, используемые для доступа к защищенным ресурсам. Жетон доступа является строкой, которая представляет выданную клиенту авторизацию. Эта строка обычно невидима клиенту. Жетоны описывают конкретные рамки и длительность доступа, предоставляемого владельцу ресурса, соблюдение которых обеспечивается сервером ресурса и сервером авторизации.

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

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

3.1.3 авторизация (authorization) [b-ITU-T X.800]: Предоставление прав, которое включает предоставление доступа на основании прав доступа.

3.1.4 сервер авторизации (authorization server) [IETF RFC 6749]: Сервер, выдающий клиенту жетоны доступа после успешной аутентификации владельца ресурса и получения авторизации.

3.1.5 клиент (client) [IETF RFC 6749]: Приложение, делающее запросы в отношении защищенного ресурса от имени владельца этого ресурса; при этом осуществляется его авторизация. Термин "клиент" не подразумевает каких-либо конкретных характеристик реализации (например, в отношении того, выполняется ли это приложение на сервере, настольном компьютере или иных устройствах).

3.1.6 объект (entity) [b-ITU-T X.1252]: Что-либо, что существует отдельно и обособленно и может быть определено в контексте.

ПРИМЕЧАНИЕ. – Объектом может быть физическое лицо, животное, юридическое лицо, организация, активный или пассивный предмет, устройство, применение программного обеспечения, услуга и т. п., или группа таких объектов. В контексте электросвязи примерами объектов являются точки доступа, абоненты, пользователи, сетевые элементы, сети, применения программного обеспечения, услуги и устройства, интерфейсы и т. п.

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

ПРИМЕЧАНИЕ. – В среде СПП, определенной в [b-ITU-T Y.2091], идентификатор представляет собой серию цифр, букв и символов или данных в любой другой форме, используемую для определения абонента(ов), пользователя(ей), элемента(ов) сети, функции(й), объекта(ов) сети, предоставляющего(их) услуги/приложения, или других объектов (например, физических или логических объектов).

3.1.8 поставщик данных идентичности (identity provider, IdP) [b-ITU-T X.1252]: См. поставщик услуг определения идентичности (IdSP).

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

3.1.10 жетон обновления (refresh token) [IETF RFC 6749]: Жетоны обновления выдаются клиенту сервером авторизации и используются для получения нового жетона доступа, если текущий жетон доступа становится недействительным или истекает срок его действия, либо для получения дополнительных жетонов доступа с такими же или более узкими рамками (жетоны доступа могут иметь более короткий срок действия и меньше прав, чем это санкционировано владельцем ресурса). Выдача жетонов обновления является факультативной и осуществляется по усмотрению сервера авторизации. Если сервер авторизации выдает жетон обновления, то это указывается при выдаче жетона доступа.

3.1.11 владелец ресурса (resource owner) [IETF RFC 6749]: Объект, имеющий возможность предоставлять доступ к защищенному ресурсу. В тех случаях, когда владельцем ресурса является физическое лицо, он называется конечным пользователем.

3.1.12 сервер ресурса (resource server) [IETF RFC 6749]: Сервер, на котором размещаются защищенные ресурсы, имеющий возможность принимать запросы в отношении защищенных ресурсов и отвечать на эти запросы с использованием жетонов доступа.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

AKA	Authentication and Key Agreement	Соглашение об аутентификации и ключе
ANI	Application-to-Network Interface	Интерфейс приложение-сеть
FE	Functional Entity	Функциональный объект
GBA	Generic Bootstrapping Architecture	Общая архитектура начальной загрузки
IdM	Identity Management	Управление определением идентичности

IdP	Identity Provider		Поставщик данных идентичности
IdSP	Identity Service Provider		Поставщик услуг определения идентичности
IMPI	IP Multimedia Private Identity		Закрытый идентификатор системы передачи мультимедийных данных на базе IP
IMSI	International Mobile Subscriber Identity		Международный идентификатор абонента подвижной связи
NGN	Next Generation Networks	СПП	Сети последующих поколений
SAML	Security Assertion Markup Language		Язык разметки утверждений безопасности
SNI	Service Network Interface		Интерфейс услуга-сеть
UNI	User Network Interface		Интерфейс пользователь-сеть

5 Соглашения по терминологии

В настоящей Рекомендации:

Ключевые слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу.

Ключевые слова "рекомендуется" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии этому документу это требование не является обязательным.

Ключевые слова "запрещается" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу.

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

В тексте настоящей Рекомендации и ее дополнениях иногда встречаются слова "должен", "не должен", "следует" и "может". В этом случае их следует понимать как "требуется, чтобы", "запрещается", "рекомендуется" и "может факультативно", соответственно. Появление таких фраз или ключевых слов в дополнении или материалах, однозначно помеченных, как информативных, должно пониматься, как не несущее нормативного смысла.

6 Принципы поддержки протоколов OAuth и OpenID в СПП

Как описано в [ITU-T Y.2720] сеть СПП состоит из многих функциональных элементов, которые используют идентификаторы объектов для выполнения своих функций в целях поддержки и содействия в оказании услуги открытой аутентификации другим поставщикам. Такие механизмы могут поддерживаться с использованием протоколов OpenID и OAuth, как показано на рисунке 1. На этом рисунке изображено использование протоколов OpenID и OAuth в СПП.

В соответствии со спецификацией OpenID [b-OpenID v.2] сервер IdP OpenID участвует во всей последовательности операций при аутентификации, а полагающаяся сторона имеет возможность направлять сообщение аутентификации непосредственно IdP СПП через протокол OAuth.

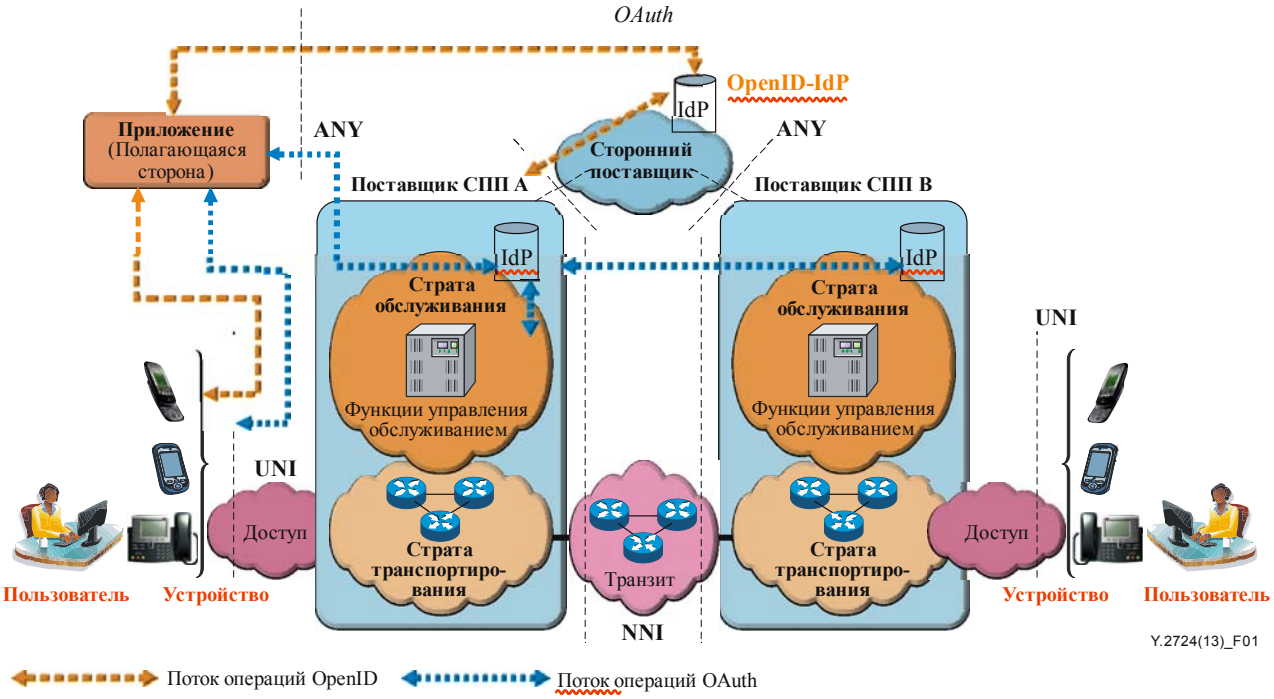

Рисунок 1 – Потоки протоколов OpenID и OAuth в СПП

6.1 Эталонная модель

На рисунке 1 представлен общий обзор структуры протоколов OAuth и OpenID.

На рисунке 2 изображена эталонная модель предоставления услуг авторизации OAuth и аутентификации OpenID в СПП. Поставщики СПП могут использовать протоколы OpenID и OAuth для оказания услуг IdSP и установления партнерских отношений с поставщиками контента и приложений и/или другими поставщиками услуг.

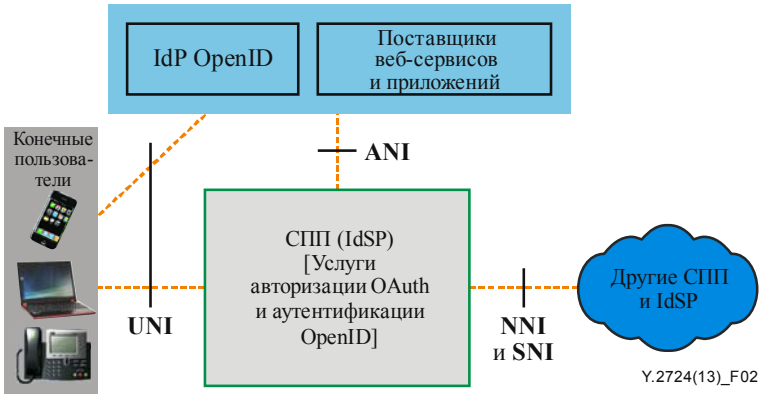

Рисунок 2 – Эталонная модель

6.2 Потоки протоколов OAuth и OpenID

В настоящем пункте представлено общее описание потоков сообщений протоколов OAuth и OpenID в СПП.

6.2.1 Объекты, участвующие в информационных потоках

В настоящем пункте определяются объекты (в том числе функциональные объекты, указанные в [ITU-T Y.2012]), которые участвуют в информационных потоках протоколов OAuth и OpenID.

6.2.2 Объекты, являющиеся общими для потоков OAuth и OpenID

Следующие объекты участвуют в потоках обоих протоколов – OAuth и OpenID:

- Функция конечного пользователя с возможностью веб-клиента (например, браузер).
- A-2: функциональный объект шлюза приложений (APL-GW-FE) [ITU-T Y.2012]. Данный функциональный объект должен иметь возможность поддержки протоколов OAuth и/или OpenID.

Как определено в [ITU-T Y.2012], "APL-GW-FE – это объект взаимодействия между различными функциями СПП и всеми внешними серверами приложений и средствами подключения услуг". Таким образом, выбор A-2 для обеспечения поддержки OpenID и OAuth весьма логичен. Кроме того, поскольку A-2 связан с S-5 – функциональным объектом профиля пользователя услуги (SUP-FE) [ITU-T Y.2012], он имеет возможность поддержки аутентификации устройств пользователя на основе AKA, включая общую архитектуру начальной загрузки (GBA). Метод аутентификации OpenID на основе GBA определен в [b-3GPP TS 33.220]. Еще один метод аутентификации OpenID на основе AKA, сходный в некоторых аспектах с GBA, описан в пункте 6.2.8 [ITU-T Y.2722]. Если и сервер авторизации OAuth, и IdP OpenID [ITU-T Y.2722] реализованы в объекте A-2, они могут использовать аутентификацию на основе AKA посредством взаимодействия с S-5.

6.2.3 Объекты, характерные для потока OAuth

Следующие объекты характеры для потока OAuth:

- Сервер веб-приложения, который оказывает услугу пользователю – клиенту OAuth. Клиент может, но не обязан выполняться на объекте СПП.
- Сервер авторизации, реализованный как часть объекта A-2.

  Сервер авторизации вначале выполняет аутентификацию пользователя, а затем выполняет авторизацию запроса клиента. Если обе процедуры завершаются успешно, OAuth обменивается результатами при выдаче жетонов доступа клиенту сервером авторизации. В целях поддержки аутентификации на основе AKA сервер авторизации должен иметь возможность взаимодействия с объектом S-5.
- Сервер ресурса.

  Сервер ресурса обслуживает запрос клиента в том случае, когда он сопровождается действительным жетоном доступа. Определены два типа процедур получения доступа к ресурсу с использованием жетонов доступа; в [b-IETF RFC 6750] определены жетоны носителя, а IETF в настоящее время работает над определением для жетонов MAC. Сервер ресурса может быть, а может и не быть расположен вместе с сервером авторизации в объекте A-2.

Высокий уровень информационных потоков OAuth для сценария использования веб-сервера (описанного в Дополнении I) изображен на рисунке 3, ниже, а его описание приводится под рисунком.

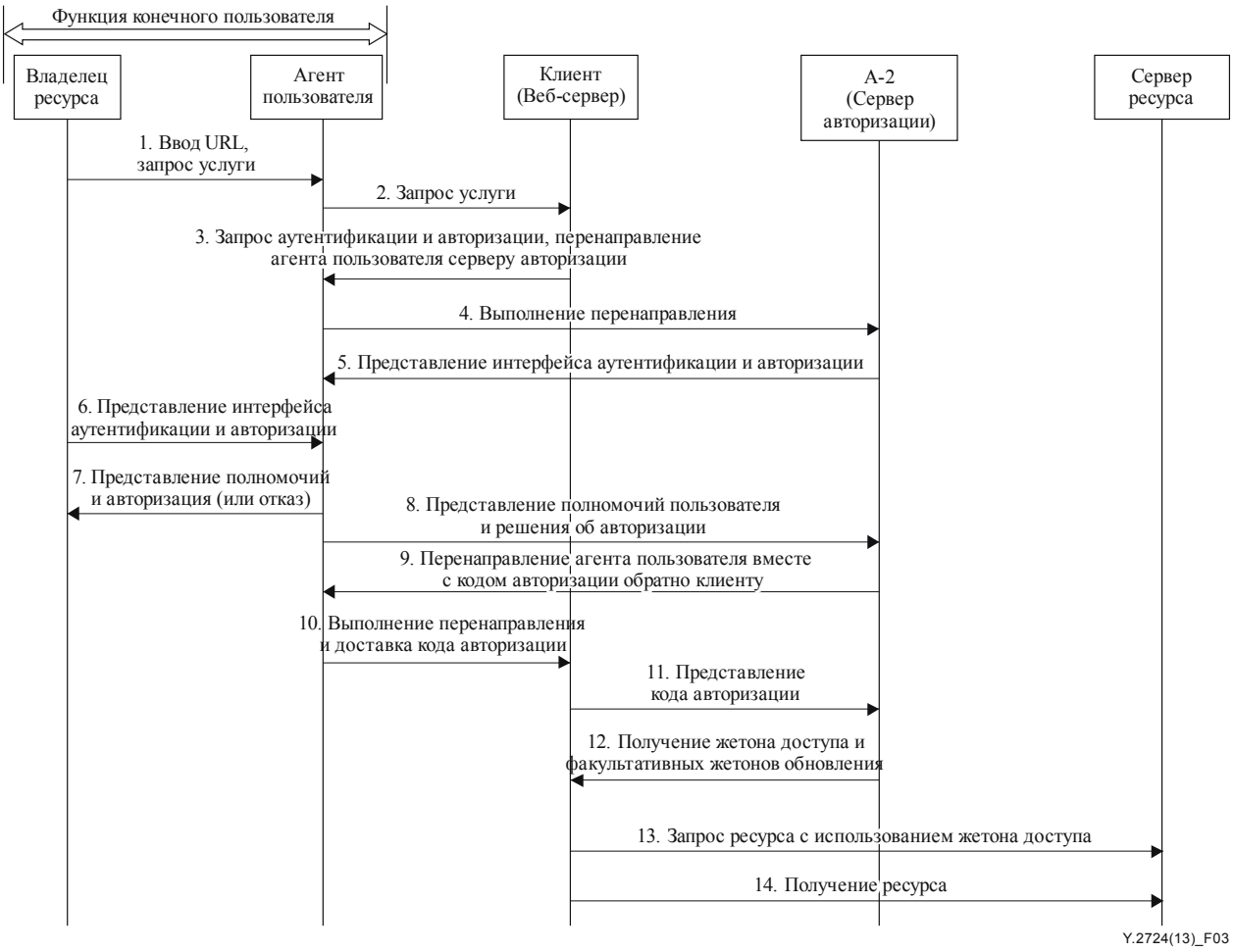

Рисунок 3 – Поток OAuth для сценария использования веб-сервера

1 Пользователь направляет агенту пользователя (например, браузеру) запрос услуги от клиента.

2 Агент пользователя представляет запрос клиенту.

3 Клиент составляет ответ и перенаправляет агента пользователя серверу авторизации для аутентификации пользователя и авторизации запроса клиента.

4 Агент пользователя выполняет перенаправление.

5 Сервер авторизации отвечает, предоставляя интерфейс аутентификации и авторизации агенту пользователя.

6 Агент пользователя отображает интерфейс аутентификации и авторизации пользователю (владельцу ресурса).

7 Пользователь предоставляет полномочия аутентификации и указывает решение авторизации, используя агент пользователя.

8 Агент пользователя направляет предоставленные пользователем данные серверу авторизации.

9 После аутентификации пользователя и обеспечения того, чтобы у пользователя имелся авторизованный запрос клиента, сервер авторизации перенаправляет агента пользователя обратно клиенту. В ответе содержится код авторизации.

10 Агент пользователя, выполняя перенаправление, доставляет код авторизации клиенту.

11 Клиент направляет код авторизации серверу авторизации.

12 Сервер авторизации отвечает, предоставляя жетон доступа и факультативные жетоны обновления.

13 Клиент направляет запрос серверу ресурса и представляет жетон доступа.

14 Сервер ресурса предоставляет запрашиваемый ресурс.

6.2.4 Объекты, характерные для потока OpenID

Следующие объекты характеры для потока OpenID:

- Сервер приложения, который использует аутентификацию, выполняемую IdP OpenID.
- IdP OpenID, реализованный как часть объекта A-2. В целях поддержки аутентификации на основе AKA этот объект должен иметь возможность взаимодействия с объектом S-5.
- Объект S-5, который участвует в аутентификации OpenID, если в СПП выполняется аутентификация функции конечного пользователя на основе AKA, как это описано в [ITU-T Y.2722].

Информационные потоки OpenID изображены на рисунке 4 и описаны ниже. В тексте и на рисунке описана процедура OpenID для случая, при котором IdP и сервером приложения создан разделенный секрет. Этот секрет используется для подписания IdP сообщения с результатом аутентификации и для его верификации сервером приложения.

Рисунок 4 – Поток OpenID

1 Браузер пользователя направляет запрос услуги серверу приложения; в запросе содержится идентификатор OpenID пользователя.

2 На основе идентификатора OpenID сервер приложения находит IdP OpenID пользователя. Сервер приложения перенаправляет браузер пользователя IdP OpenID для аутентификации.

3 Браузер выполняет запрос перенаправления.

4 IdP OpenID аутентифицирует пользователя посредством обмена информацией через браузер пользователя.

5 Если IdP OpenID выполняет аутентификацию на основе AKA (например, как это описано в [ITU-T Y.2722]), то ему необходимо взаимодействовать с объектом S-5. Такие виды взаимодействия обозначены пунктирной линией со стрелкой.

6 IdP OpenID перенаправляет браузер пользователя обратно серверу приложения с ответом, содержащим подписанное сообщение с результатом аутентификации.

7 Браузер выполняет запрос перенаправления и доставляет подписанное сообщение серверу приложения.

8 После валидации подписи и проверки результата аутентификации сервер приложения уведомляет пользователя о том, успешно ли пройдена аутентификация. Процедуры подписания и валидации определены в [b-OpenID v.2].

Дополнение I

Избранные сценарии использования

(Это дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Сценарий использования: веб-сервер

Описание

Элис осуществляет доступ к приложению, которое выполняется на веб-сервере по адресу: www.X-printphotos.example, и дает указание распечатать ее фотографии, хранящиеся на сервере www.X-storephotos.example. Элис является абонентом поставщика услуг СПП, который управляет сервером авторизации OAuth по адресу: www.X-carrier.example. Приложение по адресу: www.X-printphotos.example получает от Элис авторизацию для осуществления доступа к ее фотографиям, не узнавая ее полномочия аутентификации на серверах www.X-storephotos.example или www.X-carrier.example.

Предварительные условия

- Элис зарегистрирована на сервере www.X-carrier.example, чтобы иметь возможность аутентификации.
- Приложением по адресу: www.X-printphotos.example установлены полномочия аутентификации с помощью сервера авторизации OAuth по адресу: www.X-carrier.example.
- Приложение по адресу: www.X-storephotos.example имеет возможность валидации жетона доступа, выданного сервером авторизации по адресу: www.X-carrier.example.

Конечные условия

В результате успешной процедуры приложение www.X-printphotos.example получает код авторизации от сервера www.X-carrier.example. Этот код связан с приложением по адресу: www.X-printphotos.example и URL-адресом обратного вызова, предоставленным приложением. Приложение по адресу: www.X-printphotos.example использует код авторизации для получения жетона доступа от сервера www.X-carrier.example. Приложение по адресу: www.X-carrier.example выдает жетон доступа после аутентификации приложения по адресу: www.X-printphotos.example и валидации кода авторизации, который оно представило. Приложение по адресу: www.X-printphotos.example использует жетон доступа для получения доступа к фотографиям Элис по адресу: www.X-storephotos.example.

ПРИМЕЧАНИЕ. – При истечении срока действия жетона доступа услуге по адресу: www.X-printphotos.example необходимо повторить процедуру OAuth, чтобы получить от Элис авторизацию для доступа к ее фотографиям по адресу: www.X-storephotos.example. И наоборот, если Элис хочет предоставить приложению долгосрочный доступ к ее ресурсам по адресу: www.X-storephotos.example, сервер авторизации по адресу: www.X-carrier.example может выдать жетоны с длительным сроком действия. Эти жетоны могут быть обменены на жетоны доступа с коротким сроком действия, необходимые для доступа к серверу www.X-storephotos.example.

Требования

- Сервер www.X-printphotos.example, на котором размещается клиент OAuth, должен иметь возможность выдачи запросов перенаправления по протоколу HTTP агенту пользователя Элис – браузеру.
- Сервер авторизации по адресу: www.X-carrier.example должен иметь возможность аутентификации Элис. Метод аутентификации выходит за рамки протокола OAuth.
- Приложение по адресу: www.X-carrier.example должно получить от Элис авторизацию для доступа приложения www.X-printphotos.example к ее фотографиям.
- Приложение по адресу: www.X-carrier.example может определить для Элис рамки доступа, который запрашивает приложение www.X-printphotos.example, при обращении к ней за авторизацией.

- Сервер авторизации по адресу: www.X-carrier.example должен иметь возможность аутентификации приложения по адресу: www.X-printphotos.example и валидации кода авторизации, прежде чем выдать жетон доступа. Приложение по адресу www.X-printphotos.example должно предоставить URL-адрес обратного вызова серверу авторизации по адресу: www.X-carrier.example (ПРИМЕЧАНИЕ. – URL-адрес следует предварительно зарегистрировать на сервере www.X-carrier.example).
- Требуется, чтобы сервер авторизации по адресу: www.X-carrier.example вел запись, которая связывает код авторизации с приложением по адресу: www.X-printphotos.example и URL-адресом обратного вызова, предоставленным приложением.
- Жетоны доступа – это жетоны носителя (они не связаны с конкретным приложением, например, www.X-printphotos.example), и они должны иметь короткий срок действия.
- Сервер авторизации по адресу: www.X-carrier.example должен сделать код авторизации недействительным после его первого использования.
- Не должно требоваться ручное вмешательство Элис в процедуру авторизации OAuth (например, ввод URL-адреса или пароля). (Аутентификация Элис на сервере www.X-carrier.example выходит за рамки протокола OAuth).

I.2 Сценарий использования: полномочия клиента

Описание

Компания Good-X-Pay подготавливает расчетные ведомости по заработной плате сотрудников для компании Good-X-Work. Для этого приложение по адресу: www.Good-X-Pay.example получает аутентифицированный доступ к данным о присутствии сотрудников, хранящимся по адресу: www.Good-X-Work.example. Аутентификация выполняется сервером авторизации, который является частью СПП и имеет URL-адрес: www.X-carrier.example.

Предварительные условия

- Приложением по адресу: www.Good-X-Pay.example созданы посредством регистрации идентификатор и разделенный секрет совместно с сервером авторизации по адресу: www.X-carrier.example.
- Определены рамки доступа, осуществляемого приложением по адресу: www.Good-X-Pay.example к данным, хранящимся по адресу: www.Good-X-Work.example.

Конечные условия

В результате успешной процедуры приложение по адресу: www.Good-X-Pay.example получает жетон доступа после аутентификации на сервере авторизации по адресу: www.X-carrier.example. Далее, приложение по адресу: www.Good-X-Pay.example использует жетон доступа для получения доступа к данным о присутствии, хранящимся по адресу: www.Good-X-Work.example.

Требования

- Требуется аутентификация приложения по адресу: www.Good-X-Pay.example на сервере авторизации по адресу: www.X-carrier.example.
- Метод аутентификации должен быть основан на использовании идентификатора и разделенного секрета, которые представляются приложением, выполняемым по адресу: www.Good-X-Pay.example, серверу авторизации по адресу: www.X-carrier.example в первоначальном запросе по протоколу HTTP.
- В связи с тем, что эта процедура приводит к предоставлению доступа к конфиденциальным данным компании Good-X-Work, данная компания должна установить отношения доверия с компанией Good-X-Pay и сервером авторизации по адресу: www.X-carrier.example.

I.3 Сценарий использования: утверждение

Описание

Компания Good-X-Pay подготавливает расчетные ведомости по заработной плате сотрудников для компании Good-X-Work. Для этого приложение по адресу: www.Good-X-Pay.example получает аутентифицированный доступ к данным о присутствии сотрудников, хранящимся по адресу: www.Good-X-Work.example. Сервер www.Good-X-Work.example предоставляет доступ к приложению по адресу: www.Good-X-Pay.example после получения жетона доступа, выданного сервером авторизации www.X-carrier.example. Сервер авторизации www.X-carrier.example аутентифицирует приложение по адресу: www.Good-X-Pay.example посредством валидации утверждения, которое было представлено приложением www.Good-X-Pay.example.

В данном сценарии использования описывается решение, являющееся альтернативой решению, которое описано в сценарии использования полномочий клиента.

Предварительные условия

- Приложением по адресу: www.Good-X-Pay.example получено утверждение аутентификации от стороны, которая пользуется доверием сервера авторизации www.X-carrier.example.
- Определены рамки доступа, осуществляемого приложением по адресу: www.Good-X-Pay.example к данным, хранящимся по адресу: www.Good-X-Work.example.
- Сервером авторизации www.X-carrier.example установлены доверительные отношения с утверждающей стороной, и у него имеется возможность валидации ее утверждений.

Конечные условия

В результате успешной процедуры приложение по адресу: www.Good-X-Pay.example получает жетон доступа после аутентификации на сервере авторизации по адресу: www.X-carrier.example путем представления утверждения (например, утверждения SAML). Это приложение получает доступ к данным о присутствии сотрудников, используя жетон доступа.

Требования

- Требуется аутентификация приложения по адресу: www.Good-X-Pay.example на сервере авторизации www.X-carrier.example.
- Сервер авторизации www.X-carrier.example должен иметь возможность валидации утверждений, выданных утверждающей стороной и представленных приложением, которое выполняется по адресу: www.Good-X-Pay.example.
- Компания Good-X-Work должна установить доверительные отношения с компанией Good-X-Pay и сервером авторизации www.X-carrier.example.

Библиография

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

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

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks.*

[b-IETF RFC 6750] IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage*.

[b-OpenID v.2] OpenID Authentication 2.0
<http://openid.net/specs/openid-authentication-2_0.html>

[b-3GPP TS 33.220] 3GPP TS 33.220 (2013) *Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture, Release 12*.

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, 2014 г.