

Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2723

(11/2013)

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

Сети последующих поколений – Безопасность

Поддержка OAuth в сетях последующих поколений

Рекомендация МСЭ-Т Y.2723

ITU-T

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
IP TV 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-Т Y.2723

Поддержка OAuth в сетях последующих поколений

Резюме

В Рекомендации Y.2723 описаны механизмы и процедуры использования определенной Целевой группой по инженерным проблемам интернета "Системы авторизации OAuth 2.0 (OAuth)" для сценариев, в которых роль сервера авторизации выполняет поставщик сетей последующих поколений (СПП).

В парном документе – Рекомендации Y.2724 "Система поддержки OAuth и OpenID в сетях последующих поколений" – приводится контекст, архитектурные аспекты и структура высокого уровня для использования OAuth в СПП.

В настоящей Рекомендации определены требования, относящиеся к ограничению выбора вариантов OAuth, а также дополнительные требования, которые обеспечивают соответствие использования OAuth требованиям к безопасности и управлению определением идентичности в СПП.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.2723	15.11.2013 г.	13-я

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/>.

© ITU 2014

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Сфера применения	1
2 Справочные материалы	1
3 Определения	1
3.1 Термины, определенные в других документах	1
3.2 Термины, определенные в настоящей Рекомендации	2
4 Сокращения и акронимы	2
5 Соглашения по терминологии	2
6 Поддержка OAuth в СПП	2
6.1 Выбор типов клиента OAuth на основании требований к безопасности СПП ..	2
6.2 Выбор типов разрешений на авторизацию	3
6.3 Рекомендации относительно вариантов OAuth для поддерживаемых СПП клиентов	3
6.4 Аутентификация владельца ресурсов	4
6.5 Аспекты безопасности	5
Библиография	6

Введение

Рекомендация МСЭ-Т Y.2723 обеспечивает основу для поддержки и использования OAuth и OpenID в сетях последующих поколений (СПП). Основу настоящей Рекомендации в отношении определения конкретных методов поддержки OAuth образует Рекомендация МСЭ-Т Y.2724.

ПРИМЕЧАНИЕ. – В настоящей Рекомендации не вводится каких-либо изменений или уточнений в протокол OAuth. Она предназначена только для обеспечения поддержки и использования OAuth сетями СПП.

Рекомендация МСЭ-Т Y.2723

Поддержка OAuth в сетях последующих поколений

1 Сфера применения

В настоящей Рекомендации описываются механизмы и процедуры поддержки протокола авторизации OAuth 2.0 (OAuth) в сетях последующих поколений (СПП). Механизмы и процедуры, описываемые в настоящей Рекомендации, могут использоваться для поддержки прикладных услуг в среде, характеризующейся наличием нескольких услуг и нескольких поставщиков. В настоящей Рекомендации предполагается, что услуга авторизации OAuth предоставляется СПП.

2 Справочные материалы

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.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта.*
- [ITU-T Y.2701] Рекомендация МСЭ-Т Y.2701 (2007 г.), *Требования к безопасности для сетей последующих поколений версии 1.*
- [ITU-T Y.2702] Рекомендация МСЭ-Т Y.2702 (2008 г.), *Требования к аутентификации и авторизации для СПП варианта 1.*
- [ITU-T Y.2720] Рекомендация МСЭ-Т Y.2720 (2009 г.), *Структура управления определением идентичности в СПП.*
- [ITU-T Y.2721] Рекомендация МСЭ-Т Y.2721 (2010 г.), *Требования к управлению определением идентичности СПП и случаи применения.*
- [ITU-T Y.2724] Рекомендация МСЭ-Т Y.2724 (2013 г.), *Основа поддержки OAuth и OpenID в СПП.*
- [IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework.*
<<http://datatracker.ietf.org/doc/rfc6749/>>

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 маркер доступа (access token) [IETF RFC 6749]: Маркеры доступа – это регистрационные данные, используемые для доступа к защищенным ресурсам. Маркер доступа – это строка, представляющая авторизацию, выданную клиенту. Эта строка обычно непрозрачна для клиента. Маркеры представляют конкретные области и значения продолжительности доступа, предоставляемые владельцем ресурсов и обеспечиваемые сервером ресурсов и сервером авторизации.

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

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

3.1.4 разрешение на авторизацию (authorization grant) [IETF RFC 6749]: Разрешение на авторизацию – это регистрационные данные, представляющие авторизацию владельца ресурсов (для доступа к его защищенным ресурсам), используемую клиентом для получения маркера доступа.

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

3.1.6 клиент (client) [IETF RFC 6749]: Приложение, делающее запросы на использование защищенных ресурсов от имени владельца ресурсов и с его авторизацией. Термин "клиент" не подразумевает каких-либо конкретных характеристик реализации (например, выполняется ли приложение на сервере, настольном компьютере или на других устройствах).

3.1.7 конфиденциальные клиенты (confidential clients) [IETF RFC 6749]: Клиенты, способные сохранять конфиденциальность своих регистрационных данных (например, клиент, реализуемый на защищенном сервере с ограниченным доступом к регистрационным данным клиента) или способные обеспечить безопасность аутентификации клиента с применением других средств.

3.1.8 публичные клиенты (public clients) [IETF RFC 6749]: Клиенты, неспособные сохранять конфиденциальность своих регистрационных данных (например, клиенты, функционирующие на устройстве, используемом владельцем ресурсов, например, установленное собственное приложение или приложение на базе веб-обозревателя) и неспособные обеспечить безопасность аутентификации клиента с применением каких-либо других средств.

3.1.9 владелец ресурсов (resource owner) [IETF RFC 6749]: Объект, способный предоставить доступ к защищенному ресурсу. Если владельцем ресурсов является физическое лицо, оно именуется конечным пользователем.

3.1.10 сервер ресурсов (resource server) [IETF RFC 6749]: Сервер, на котором размещаются защищенные ресурсы, способный принимать запросы на защищенные ресурсы с использованием маркеры доступа и отвечать на них.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

IdM	Identity Management	Управление определением идентичности
NGN	Next Generation Network	СПП Сети последующих поколений
OAuth	OAuth 2.0 Authorization Protocol	Протокол авторизации OAuth 2.0
SAML	Security Assertion Markup Language	Язык разметки утверждений безопасности
URI	Uniform Resource Identifier	Унифицированный идентификатор ресурса

5 Соглашения по терминологии

Отсутствуют.

6 Поддержка OAuth в СПП

В настоящем разделе описываются основные аспекты поддержки OAuth в СПП.

6.1 Выбор типов клиента OAuth на основании требований к безопасности СПП

В [IETF RFC 6749] определяются два типа клиентов OAuth: конфиденциальные и публичные клиенты.

Публичные клиенты не отвечают требованиям к аутентификации для третьих сторон – поставщиков приложений СПП [ITU-T Y.2702], поскольку публичные клиенты не могут быть аутентифицированы поставщиком СПП [ITU-T Y.2724]. В настоящей Рекомендации рекомендуется, чтобы СПП поддерживали только конфиденциальных клиентов. Клиенты должны отвечать следующим требованиям:

- 1) Клиент OAuth СПП должен обладать возможностью прохождения аутентификации с конкретными уровнями гарантии [ITU-T Y.2702], [ITU-T X.1254].
- 2) Клиент OAuth СПП должен быть зарегистрированным на сервере авторизации, как указано в разделе 2 [IETF RFC 6749].

OAuth 2.0 [IETF RFC 6749] определяет следующие профили клиента: веб-приложение, приложение на базе пользователя-агента и собственное приложение. Веб-приложение – это профиль частного клиента, тогда как два последних приложения – профили публичных клиентов. В настоящей Рекомендации описывается поддержка СПП только для клиента профиля веб-приложения.

6.2 Выбор типов разрешений на авторизацию

В [IETF RFC 6749] определяются следующие типы разрешений на авторизацию: код авторизации, неявное, регистрационные данные, определяемые паролем владельца ресурсов, и регистрационные данные клиента. Наряду с этим IETF в настоящее время ведет работу по определению расширения, которое указывает тип разрешения на авторизацию SAML версии 2.0 для OAuth 2.0.

В [IETF RFC 6749] поясняется, что "при выдаче маркера доступа в потоке неявного разрешения сервер авторизации не проводит аутентификации клиента. В некоторых случаях идентичность клиента может быть проверена с помощью идентификатора URI перенаправления, используемого для доставки клиенту маркера доступа. Маркер доступа может быть открыт владельцу ресурсов или другим приложениям, имеющим доступ к пользователю-агенту владельца ресурсов".

Таким образом, потоки OAuth, в которых используется тип неявных разрешений, не приводят к аутентификации, которая отвечала бы требованиям к аутентификации поставщика приложений СПП – третьей стороны [ITU-T Y.2702].

Настоящая Рекомендация посвящена поддержке со стороны СПП конфиденциального клиента профиля веб-приложения при использовании следующих разрешений на авторизацию:

- код авторизации;
- регистрационные данные, определяемые паролем владельца ресурсов;
- регистрационные данные клиента;
- утверждение SAML 2.0.

6.3 Рекомендации относительно вариантов OAuth для поддерживаемых СПП клиентов

Потоки [IETF RFC 6749] оптимизированы для нескольких клиентских профилей двух типов клиентов. В RFC указываются варианты выбора типов разрешений на авторизацию, параметров и требований безопасности.

В настоящем пункте даются рекомендации по поддержке конфиденциальных клиентов профиля веб-приложения. В этом пункте рассматриваются также те требования и дополнительные параметры, выбор которых существенно необходим для поддержки OAuth в СПП.

6.3.1 Регистрация клиента

В разделе 2.2 [IETF RFC 6749] рекомендуется регистрировать идентификаторы URI перенаправления клиентов на сервере авторизации, поскольку клиенты с зарегистрированными URI позволяют обеспечить более высокую степень безопасности.

В настоящей Рекомендации содержится требование, согласно которому поддерживаемые СПП клиенты должны регистрировать свои идентификаторы URI перенаправления на сервере авторизации.

6.3.2 Конфиденциальность сообщений в конечную точку перенаправления клиента

В разделе 3.1.2.1 [IETF RFC 6749] дается следующая рекомендация: "конечной точке перенаправления СЛЕДУЕТ требовать использование TLS согласно описанию в разделе 1.6, когда тип запрашиваемого ответа – "код" или "маркер" или когда запрос о перенаправлении приведет к передаче требующих защиты регистрационных данных по открытой сети". В настоящей Рекомендации содержится требование, согласно которому TLS следует использовать для передачи любой требующей защиты информации.

6.3.3 Аутентификация клиента

Клиенты, определяемые профилем веб-приложения, являются конфиденциальными клиентами. Ввиду этого требуется аутентификация клиента на сервере авторизации.

6.3.4 Процедуры авторизации

Настоящей Рекомендацией охватываются конфиденциальные клиенты профиля веб-приложения, которые используют процедуры авторизации следующих типов разрешений на авторизацию:

- код авторизации;
- регистрационные данные, определяемые паролем владельца ресурсов;
- регистрационные данные клиента;
- расширение SAML.

6.3.4.1 Код авторизации

Процедура авторизации конфиденциальных клиентов с использованием кода авторизации описывается в разделе 4.1 [IETF RFC 6749]. В настоящей Рекомендации содержится требование включения параметра *redirect_uri* в запросы на авторизацию.

К взаимодействию сервера авторизации с клиентами профиля веб-приложения при использовании кода авторизации применяются следующие требования. Сервер авторизации ДОЛЖЕН:

- аутентифицировать клиента, направившего запрос на авторизацию;
- обеспечить, чтобы значение параметра *redirect_uri* в запросе клиента на авторизацию соответствовало зарегистрированному значению для этого клиента;
- выдавать код авторизации только аутентифицированным и авторизованным клиентам;
- до выдачи маркера доступа убедиться, что код авторизации действителен.

6.3.4.2 Регистрационные данные, определяемые паролем владельца ресурсов

Процедура авторизации, в которой используется данный вид разрешения, оптимизирована для клиентов, пользующихся устойчивым доверием владельца ресурсов. Клиент использует регистрационные данные, определяемые паролем владельца ресурсов, для получения маркера доступа от сервера авторизации. Процедура, определенная в разделе 4.3 [IETF RFC 6749], отвечает требованиям к безопасности СПП.

ПРИМЕЧАНИЕ. – В [IETF RFC 6749] разрешено использование этой процедуры публичными клиентами. В настоящей Рекомендации рассматриваются только конфиденциальные клиенты, для которых требуется аутентификация на сервере авторизации.

В соответствии с [IETF RFC 6749] сервер авторизации при взаимодействии с клиентом, который использует такой тип разрешения, как регистрационные данные, определяемые паролем владельца ресурсов, ДОЛЖЕН:

- аутентифицировать клиента;
- проверить регистрационные данные, определяемые паролем владельца ресурсов, которые представил клиент;
- выдать маркер доступа, если клиент аутентифицирован сервером авторизации и представил действительные регистрационные данные, определяемые паролем владельца ресурсов.

6.4 Аутентификация владельца ресурсов

В спецификации OAuth [IETF RFC 6749] не говорится об аутентификации владельца ресурсов (например, конечного пользователя) сервером авторизации. В среде СПП механизм аутентификации владельца ресурсов должен отвечать требованиям [ITU-T Y.2702].

6.5 Аспекты безопасности

В разделе "Аспекты безопасности" спецификации OAuth 2.0 [IETF RFC 6749] представлены руководящие указания по безопасности для всех профилей клиентов OAuth 2.0 – веб-приложения, приложения на базе пользователя-агента и собственного приложения. В настоящей Рекомендации рекомендуется поддержка клиентов веб-приложений в СПП. Соответственно здесь применяются только аспекты безопасности [IETF RFC 6749], касающиеся клиентов веб-приложений. Наряду с этим в [b-IETF RFC 6819] приводится комплексная модель безопасности OAuth и справочная информация для разработки протокола. Содержащийся в [b-IETF RFC 6819] материал, имеющий отношение к клиентам веб-приложений, следует рассматривать для видов реализации, поддерживающих OAuth в СПП.

Решения также должны отвечать требованиям к безопасности СПП и IdM, указанным в [ITU-T Y.2701], [ITU-T Y.2720], [ITU-T Y.2721].

Библиография

- [b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ.*
- [b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности.*
- [b-IETF RFC 6819] IETF RFC 6819, *OAuth 2.0 Threat Model and Security Considerations.*
<http://datatracker.ietf.org/doc/rfc6819/>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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