Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2725
(07/2014)

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

Сети последующих поколений – Безопасность

Поддержка OpenID в сетях последующих поколений

Рекомендация МСЭ-Т Y.2725

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.2725

Поддержка OpenID в сетях последующих поколений

Резюме

В Рекомендации МСЭ-T Y.2725 определяются механизмы и процедуры поддержки и использования протокола OpenID в сценариях, в которых роль поставщика OpenID выполняет поставщик услуг СПП.

В Рекомендации МСЭ-T Y.2724 приводятся принципы поддержки и использования протоколов OAuth и OpenID СПП. В Рекомендации МСЭ-T Y.2725, которая основывается на Рекомендации МСЭ-T Y.2722 и Рекомендации МСЭ-T Y.2724, определяются конкретные механизмы поддержки OpenID.

ПРИМЕЧАНИЕ. – В Рекомендации МСЭ-T Y.2725 не производятся какие-либо изменения или уточнения протокола OpenID. В ней речь идет только о поддержке и использовании OpenID СПП.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-T Y.2725	18.07.2014 г.	13-я	11.1002/1000/12079

* 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.2725

Поддержка OpenID в сетях последующих поколений

1 Сфера применения

В настоящей Рекомендации описываются механизмы и процедуры поддержки протокола OpenID в СПП. Механизмы и процедуры, описываемые в настоящей Рекомендации, могут использоваться для поддержки прикладных услуг в среде с наличием нескольких поставщиков услуг. В настоящей Рекомендации предполагается, что поставщик СПП является поставщиком протокола OpenID.

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.2701] Рекомендация МСЭ-Т Y.2701 (2007 г.), *Требования к безопасности для СПП 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.), *Принципы поддержки протоколов OAuth и OpenID в сетях последующих поколений*.

[OASIS XRI SYNTAX] *Extensible Resource Identifier (XRI) Syntax V2.0*.

3 Определения

3.1 Термины, определенные в других документах

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

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

3.1.2 авторизация (authorization) [b-ITU-T X.800]: Предоставление прав и, на основе этих прав, предоставление доступа.

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

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

3.1.5 клиент (client) [b-IETF RFC 6749]: Приложение, делающее запросы на защищенные ресурсы от имени владельца ресурсов и при его авторизации. Термин "клиент" не подразумевает каких-либо конкретных характеристик реализации (например, выполняется ли приложение на сервере, настольном компьютере или на других устройствах).

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

FE	Functional Entity	Функциональный объект
FRA	Functional Requirements and Architecture	Функциональные требования и архитектура
IdM	Identity Management	Управление определением идентичности
IdP	Identity Provider	Поставщик данных идентичности
IETF	Internet Engineering Task Force	Целевая группа по инженерным проблемам интернета
IP	Internet Protocol	Протокол Интернет
OAuth	OAuth 2.0 Authorization Protocol	Протокол авторизации OAuth 2.0
OP	OpenID Provider	Поставщик OpenID
SAML	Security Assertion Markup Language	Язык разметки утверждений безопасности
URI	Uniform Resource Identifier	Унифицированный идентификатор ресурса
WS	Web Server	Веб-сервер

5 Соглашения по терминологии

Ключевые слова "**требуется**" 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.

6 Поддержка OpenID в СПП

В настоящем пункте описываются основные аспекты поддержки OpenID в СПП.

6.1 Эталонная модель

В соответствии со спецификацией OpenID [b-OpenID v.2] сервер IdP OpenID участвует во всей последовательности операций при аутентификации. В том что касается общего обзора структуры OAuth и OpenID см. [ITU-T Y.2724].

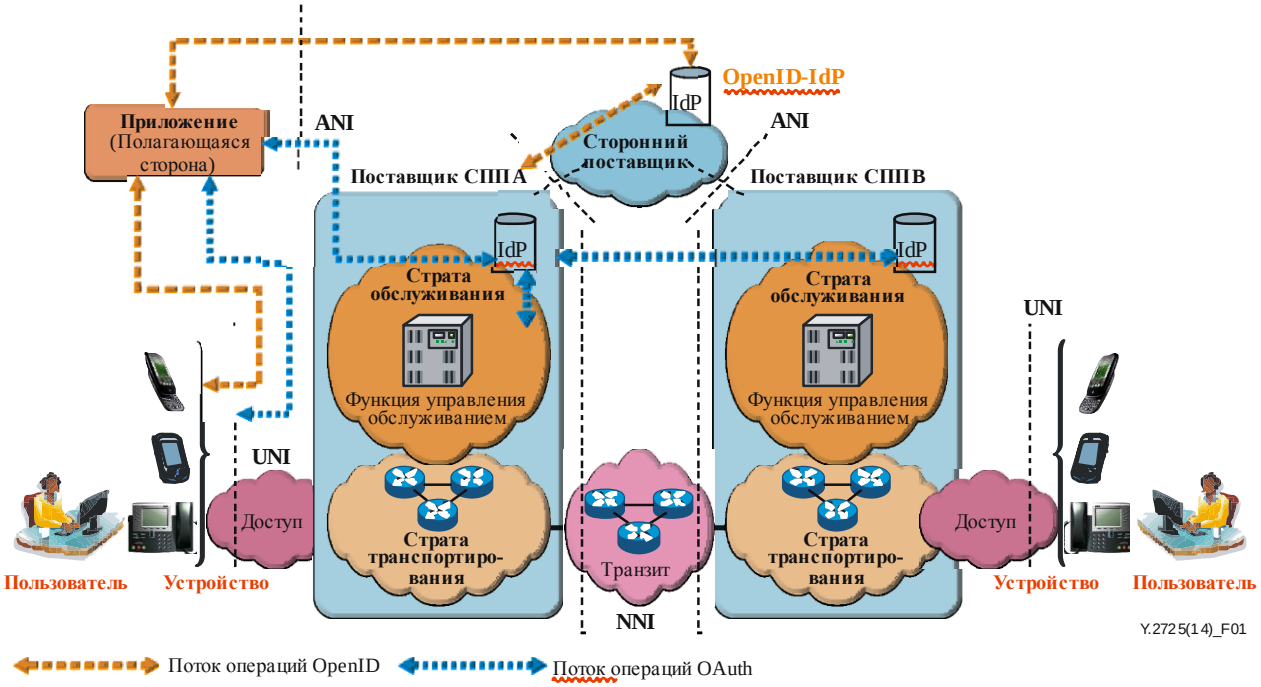

Рисунок 1 – Потоки протоколов OpenID и OAuth в СПП

6.2 Форматы сообщений протокола в условиях СПП

В [b-OpenID v.2] определяется два типа форматов сообщений протокола:

- кодирование пары ключ/значение формой;
- кодирование HTTP.

В разделе 4.1.1 [b-OpenID v.2] разъясняется, что "кодирование пары ключ/значение формой используется для вычисления подписи и для прямых ответов полагающимся сторонам".

В отношении кодирования HTTP в разделе 4.1.2 [b-OpenID v.2] разъясняется, что "данная модель применяется к сообщениям, направляемым от агента пользователя полагающейся стороне и поставщику OpenID (OP), а также к сообщениям, направляемым OP полагающейся стороной".

Требуется, чтобы поддерживаемые СПП объекты выполняли требования при направлении сообщения протокола.

6.3 Типы передач

В [b-OpenID v.2] определяется два типа передач:

- прямая передача;
- непрямая передача.

В разделе 5.1 [b-OpenID v.2] разъясняется, что прямая передача инициируется полагающейся стороной в направлении URL конечной точки OP. Она используется для установления связей и проверки утверждений аутентификации.

В разделе 5.2 [b-OpenID v.2] разъясняется, что при непрямой передаче сообщения проходят через агента пользователя. Она может быть инициирована либо полагающейся стороной, либо OP. Непрямая передача используется для запросов и ответов аутентификации.

Требуется, чтобы поддерживаемые СПП объекты выполняли эти требования в условиях инициирования передачи.

6.4 Создание подписей

Аутентификацией OpenID поддерживается два алгоритма создания подписей:

- HMAC-SHA1 – длина ключа 160 бит;
- HMAC-SHA256 – длина ключа 256 бит.

В настоящем пункте содержатся рекомендации по использованию алгоритма HMAC-SHA256. Процедура создания подписи сообщения, определенная в разделе 6.1 [b-OpenID v.2], удовлетворяет требованиям СПП к безопасности.

6.5 Процедуры аутентификации OpenID в СПП

6.5.1 Запросы аутентификации

Согласно рекомендациям раздела 13 [b-OpenID v.2], рекомендуется, чтобы полагающиеся стороны использовали протокол Yadis для публикации своих достоверных URL параметра "return_to". Полагающаяся сторона может факультативно опубликовать эту информацию в любом URL, и рекомендуется, чтобы она опубликовала ее в параметре "realm", с тем чтобы поставщик мог проверить указатели URL параметра "return_to".

Согласно требованиям настоящей Рекомендации, рекомендуется, чтобы полагающиеся стороны использовали протокол Yadis для публикации своих достоверных URL параметра "return_to" в СПП.

Запросы аутентификации определяются в разделе 9 [b-OpenID v.2].

Указанные ниже требования применяются к взаимодействию полагающейся стороны и конечного пользователя. Требуется, чтобы полагающаяся сторона обеспечила:

- инициирование аутентификации OpenID;
- нормализацию идентификатора, предоставляемого пользователем;
- обнаружение необходимой информации для инициирования запросов.

6.5.1.1 Инициирование аутентификации OpenID

В разделе 7.1 [b-OpenID v.2] содержится следующая рекомендация: "для инициирования аутентификации OpenID рекомендуется, чтобы полагающаяся сторона представила конечному пользователю форму, в которой имеется поле для ввода идентификатора, предоставляемого пользователем".

Рекомендуется, чтобы атрибут "name" поля формы имел значение "openid_identifier", с тем чтобы агент пользователя мог автоматически определить, что это форма OpenID. Расширения браузера или другое программное обеспечение, которое поддерживает аутентификацию OpenID, может и не обнаружить поддержку полагающейся стороны, если этот атрибут не задан надлежащим образом.

В настоящей Рекомендации требуется включение поля "openid_identifier" в форму, которую объект полагающейся стороны представляет в СПП.

6.5.1.2 Нормализация идентификатора, предоставляемого пользователем

В [b-OpenID v.2] определяется три типа идентификаторов: URI "http" или "https", (часто упоминаемые в настоящем документе как "URL"), или XRI [OASIS XRI SYNTAX 2.0].

Требуется, чтобы вводимые конечным пользователем данные были нормализованы в идентификаторе; описанная в разделе 7.2 [b-OpenID v.2] процедура удовлетворяет требованиям СПП к нормализации.

6.5.1.3 Обнаружение необходимой информации для инициирования запросов

В [b-OpenID v.2] объясняется, что "обнаружение – это процесс, при котором полагающаяся сторона использует идентификатор, чтобы искать (обнаруживать) необходимую информацию для инициирования запросов".

В аутентификации OpenID имеется три пути, по которым осуществляется обнаружение, как это описано в разделе 7.3 [b-OpenID v.2].

В [b-OpenID v.2] определяется два метода обнаружения:

- обнаружение на основе XRDS;
- обнаружение на основе HTML.

Результатом использованного обнаружения XRI [b-OASIS XRI SYNTAX 2.0] является документ XRDS. Это – документ XML с записями для услуг, которые связаны с идентификатором, как это определено в разделе 7.3.2.1 [b-OpenID v.2].

Требуется, чтобы обнаружение на основе HTML поддерживалось полагающимися сторонами. Оно используется только для обнаружения заявленных идентификаторов. Требуется, чтобы идентификаторами OP являлись идентификаторы XRI [b-OASIS XRI SYNTAX 2.0] или URL, которые поддерживают обнаружение XRDS. Для использования обнаружения на основе HTML требуется, чтобы документ HTML был доступен в URL заявленного идентификатора, как это определено в разделе 7.3.3 [b-OpenID v.2].

Согласно требованиям настоящей Рекомендации, требуется, чтобы полагающаяся сторона выполняла требования при осуществлении обнаружения, и рекомендуется, чтобы идентификатор соответствовал формату XRI или URL.

6.5.2 Ответы на запрос аутентификации

Согласно рекомендациям раздела 10 [b-OpenID v.2], при поступлении запросов аутентификации от агента пользователя посредством непрямой передачи рекомендуется, чтобы OP определил, что авторизованный конечный пользователь желает завершить аутентификацию. Если авторизованный конечный пользователь желает завершить аутентификацию, рекомендуется, чтобы OP направил положительное утверждение полагающейся стороне.

В настоящей Рекомендации требуется включение параметра "return_to" в запросы авторизации.

ПРИМЕЧАНИЕ. – Методы определения авторизованных конечных пользователей и получения одобрения на возврат утверждения аутентификации OpenID не относятся к сфере применения данной спецификации.

6.5.2.1 Положительные утверждения

Положительные утверждения – это непрямые ответы на запросы; в отношении информации о параметрах ответов см. раздел 10.1 [b-OpenID v.2].

В соответствии с [b-OpenID v.2] требуется, чтобы при непрямой передаче полагающейся стороне через агента пользователя OP:

- проверил, что URL параметра "return_to" соответствует одной из конечных точек полагающейся стороны;
- определил, что авторизованный конечный пользователь желает завершить аутентификацию;
- создал ответ с параметром "nonce";
- подписал положительный ответ;
- направил положительное утверждение полагающейся стороне через агента пользователя.

6.5.2.2 Отрицательные утверждения

Если OP не может определить конечного пользователя или конечный пользователь не подтверждает или не может подтвердить запрос аутентификации, рекомендуется, чтобы OP направил отрицательное утверждение полагающейся стороне в качестве непрямого ответа. См. также раздел 10.2 [b-OpenIDv.2]

При получении отрицательного утверждения в ответ на запрос режима "checkid_immediate" рекомендуется, чтобы полагающаяся сторона построила новый запрос аутентификации, используя режим "checkid_setup".

6.5.2.2.1 Отрицательные утверждения в ответ на срочные запросы

Если запрос является срочным, у конечного пользователя нет возможности взаимодействия со страницами на OP для предоставления идентификационных регистрационных данных или подтверждения запроса. Отрицательное утверждение для срочного запроса принимает форму, определенную в разделе 10.2.1 [b-OpenID v.2].

6.5.2.2.2 Отрицательные утверждения в ответ на несрочные запросы

В связи с тем, что OP может отобразить страницы конечному пользователю и запросить регистрационные данные от конечного пользователя, отрицательный ответ на несрочный запрос является окончательным. Он принимает форму, определенную в разделе 10.2.2 [b-OpenID v.2].

Если полагающаяся сторона получает ответ "cancel", то есть аутентификация была неуспешной, то требуется, чтобы полагающаяся сторона рассматривала конечного пользователя как неаутентифицированного.

6.5.3 Проверка утверждений

В соответствии с [b-OpenID v.2] требуется, чтобы при получении положительного утверждения полагающаяся сторона:

- проверила обратный URL;
- проверила обнаруженную информацию;
- проверила параметр "nonce";
- проверила подписи.

Если утверждение проверено и оно содержит заявленный идентификатор, то теперь пользователь является аутентифицированным с помощью данного идентификатора.

6.6 Аспекты безопасности

В разделе 15 (Аспекты безопасности) спецификации OpenID 2.0 [b-OpenID v.2] приведены руководящие указания по безопасности для предотвращения атак, агенты пользователя, интерфейс пользователя, идентификаторы URL HTTP и HTTPS и варианты протокола. В настоящей Рекомендации рекомендуется поддержка всех аспектов безопасности в СПП.

Решения также должны отвечать требованиям безопасности СПП и IdM, указанным в [ITU-T Y.2701], [ITU-T Y.2720] и [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-OpenIDv.2] OpenID Authentication 2.0.
http://openid.net/specs/openid-authentication-2_0.html

[b-Yadis] Yadis Protocol.
http://infogrid.org/trac/wiki/Yadis

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

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, 2015 г.