

# МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ  
ЭЛЕКТРОСВЯЗИ МСЭ

# Y.4805

(08/2017)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ  
ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА  
ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ,  
ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

Интернет вещей и "умные" города и сообщества –  
Идентификация и безопасность

---

**Требования к услуге идентификатора для  
обеспечения функциональной  
совместимости различных приложений  
"умного" города**

Рекомендация МСЭ-Т Y.4805

## РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

## ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ, ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и межплатформенное программное обеспечение	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
Совершенствование СПП	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.3099
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999
ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА И СООБЩЕСТВА	
Общие положения	Y.4000–Y.4049
Определения и терминология	Y.4050–Y.4099
Требования и сценарии использования	Y.4100–Y.4249
Инфраструктура, возможность установления соединений и сети	Y.4250–Y.4399
Структуры, архитектуры и протоколы	Y.4400–Y.4549
Услуги, приложения, вычисления и обработка данных	Y.4550–Y.4699
Управление, контроль и рабочие характеристики	Y.4700–Y.4799
<b>Идентификация и безопасность</b>	<b>Y.4800–Y.4899</b>
Анализ и оценка	Y.4900–Y.4999

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

## Рекомендация МСЭ-Т Y.4805

### Требования к услуге идентификатора для обеспечения функциональной совместимости различных приложений "умного" города

#### Резюме

В Рекомендации МСЭ-Т Y.4805 определен набор требований для услуг идентификатора в приложениях "умного" города, предназначенных для обеспечения функциональной совместимости и безопасности таких систем. Этот набор требований может дополнительно служить руководством по разработке новых услуг идентификатора для "умных" городов. В набор входят функции безопасности для обеспечения целостности услуг и конфиденциальности данных. В Рекомендации определен полный список требований к услуге идентификатора, включая требования безопасности, для услуги идентификатора.

#### Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.4805	22.08.2017 г.	20-я	<a href="http://handle.itu.int/11.1002/1000/13267">11.1002/1000/13267</a>

#### Ключевые слова

Конфиденциальность данных, идентификатор, целостность услуги, "умный" город.

---

\* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL <http://handle.itu.int/>, после которого укажите 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/>.

© ITU 2017

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 документы .....	1
3 Определения .....	1
3.1 Термины, определенные в других документах .....	1
3.2 Термины, определенные в настоящей Рекомендации .....	1
4 Сокращения и акронимы .....	2
5 Соглашения по терминологии .....	2
6 Услуги идентификатора для приложений "умного" города.....	2
6.1 Модель услуги.....	3
6.2 Модель данных .....	3
6.3 Модель функционирования .....	3
7 Требования к услугам идентификатора в приложениях "умного" города.....	3
7.1 Общие требования к услугам идентификатора.....	3
7.2 Общие требования безопасности .....	4
7.3 Требования, относящиеся к модели услуги .....	5
7.4 Требования к модели данных .....	6
7.5 Требования к модели функционирования .....	7
Библиография .....	9



### Требования к услуге идентификатора для обеспечения функциональной совместимости различных приложений "умного" города

#### 1 Сфера применения

В настоящей Рекомендации определен набор требований для услуг идентификатора в приложениях "умного" города, предназначенных для обеспечения функциональной совместимости и безопасности таких систем. Этот набор требований может дополнительно служить руководством по разработке новых услуг идентификатора для "умных" городов. В набор входят функции безопасности для обеспечения целостности услуг и конфиденциальности данных. В Рекомендации определен полный список требований к услуге идентификатора, включая требования безопасности, для услуги идентификатора.

#### 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 приложение (application)** [b-ITU-T Y.2261]: Структурированный набор возможностей, которые обеспечивают дополнительную функциональность, поддерживаемую одной или несколькими услугами, которые могут предоставляться через интерфейс API.

**3.1.2 идентификатор (identifier)** [b-ITU-T Y.2091]: Идентификатор – это последовательность цифр, букв и символов или данных в любой иной форме, которая используется для идентификации абонента(ов), пользователя(ей), сетевого элемента(ов), функции(й), сетевого(ых) объекта(ов), обеспечивающих услуги/приложения, или других объектов (например, физических или логических объектов). Идентификаторы могут использоваться для регистрации или авторизации. Они могут быть либо открытыми для всех сетей и используемыми совместно ограниченным количеством сетей, либо частными для конкретной сети (частные ID, как правило, не раскрываются третьим сторонам).

**3.1.3 преобразование идентификатора (identifier resolution)** [b-ITU-T Y.4108]: Функция, которая преобразует идентификатор в связанную с ним информацию и наоборот.

**3.1.4 интернет вещей (Internet of things (IoT))** [b-ITU-T Y.4000]: Глобальная инфраструктура для информационного общества, которая поддерживает передовые услуги путем взаимного соединения (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.

ПРИМЕЧАНИЕ 1. – Благодаря использованию возможностей идентификации, а также сбора, обработки и передачи данных, IoT обеспечивает полное использование вещей для предоставления услуг для всех типов приложений, обеспечивая при этом выполнение требований безопасности и неприкосновенности частной жизни.

ПРИМЕЧАНИЕ 2. – В широком смысле IoT можно воспринимать как концепцию, имеющую технологические и социальные последствия.

**3.1.5 функциональная совместимость (interoperability)** [b-ITU-T Y.101]: Способность двух и более систем или приложений обмениваться информацией и на взаимной основе пользоваться полученной в результате обмена информацией.

##### 3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

**3.2.1 администрирование идентификатора (identifier administration):** Способность выполнять функции, поддерживающие управление идентификаторами и атрибутами идентификаторов на протяжении их жизненного цикла. К числу этих функций относятся регистрация новых идентификаторов, удаление существующих идентификаторов, изменение или обновление любой информации, связанной с идентификатором, а также другие соответствующие административные функции, определенные в схеме конкретного идентификатора согласно определению 3.1.2, выше.

**3.2.2 услуга идентификатора (identifier service):** Сетевая информационная услуга, которая выполняется через интернет и осуществляет преобразование идентификатора согласно определению 3.1.3 и администрирование идентификатора согласно определению 3.2.1, выше.

**3.2.3 корневая услуга для услуги идентификатора (root service of identifier service):** Корневая услуга – это ключевой элемент на вершине иерархической услуги идентификатора или именованная. Например, DNS определяет свою корневую услугу как набор корневых серверов имен и данных на вершине системы именованного интернета.

## 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ID	Identifier	Идентификатор
IoT	Internet of Things	Интернет вещей
TTL	Time-To-Live	Предписанное время жизни
UTF-8	8-bit Unicode Transformation Format	8-битовый формат преобразования Юникода

## 5 Соглашения по терминологии

Ключевое слово **"требуется"** означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящему документу.

Ключевое слово **"рекомендуется"** означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом для заявления о соответствии настоящему документу данное требование не является обязательным.

Ключевые слова **"может факультативно"** означают необязательное требование, которое допустимо, но не имеет какого бы то ни было 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 предоставлять эту функцию факультативно и при этом заявлять о соответствии спецификации.

В тексте настоящей Рекомендации и приложениях к ней иногда встречаются слова "должен", "не должен", "следует" и "может", и в этом случае их следует понимать, соответственно, как "требуется", "запрещается", "рекомендуется" и "может факультативно". Использование таких фраз или ключевых слов в дополнениях или материалах, в явной форме обозначенных как информативные, должно пониматься как не несущее нормативного смысла.

## 6 Услуги идентификатора для приложений "умного" города

Для рассмотрения услуг идентификатора (ID) для приложений "умного" города используются их модели услуги, данных и функционирования. В модели услуги исследуется структура услуги для услуги идентификатора в целях обеспечения наиболее эффективной поддержки приложений "умного" города, включая компоненты услуги и взаимосвязь этих компонентов. В модели данных определяется необходимая структура данных, которая потребуется для поддержки атрибутов идентификатора в приложениях "умного" города, а также для операций обеспечения безопасности и управления, осуществляемых по идентификаторам и атрибутам идентификаторов. В модели функционирования предусматриваются основные операции, которые должна обеспечивать услуга идентификатора, а также важнейшие функции, позволяющие выполнять связанные, прозрачные и надежные операции между различными компонентами услуги идентификатора, в соответствующих случаях.



## **6.1 Модель услуги**

Услуга идентификатора для приложений "умного" города должна поддерживать приложения, используемые из разных городов и управляемые разными организациями и/или поставщиками услуг. Обеспечить возможность такой услуги идентификатора может модель распределенной услуги.

Модель услуги для услуги идентификатора относится к структуре услуги для услуги идентификатора, в том что касается ее компонентов услуги, в распределенной сетевой среде.

Услуга идентификатора для приложений "умного" города может состоять из большого числа компонентов услуги, при этом каждый компонент управляется разными организациями и/или поставщиками услуг. Каждый компонент услуги идентификатора может отвечать за локальный домен идентификаторов, используемых в приложениях "умного" города. Эти компоненты услуги должны работать совместно, для того чтобы обеспечивать идентификацию любого объекта "умного" города по глобальному уникальному идентификатору, а также преобразование и обновление в реальном времени информации, связанной с идентификатором.

С другой стороны, тот или иной компонент услуги в услуге идентификатора может использоваться и управляться отдельными организациями независимо от других. Любое нарушение одного компонента не должно нарушать услугу, обеспечиваемую другими компонентами. Администрирование идентификатора и информации идентификатора может выполняться каким-либо отдельным компонентом услуги идентификатора независимо от других.

## **6.2 Модель данных**

Модель данных услуги идентификатора обозначает структуру данных, которые необходимы для поддержки преобразования и администрирования идентификаторов. Структура данных должна быть достаточно гибкой для поддержки существующих приложений "умного" города и обеспечения возможности обратной совместимости.

Идентификатор в услуге идентификатора для "умного" города не только обеспечивает идентификацию объекта "умного" города, но также служит ссылкой на информацию, связанную с идентифицированным субъектом. Модель данных услуги идентификатора должна определять структуру данных, которая позволяет связать все типы данных с идентификатором. Она также должна определять общие механизмы, позволяющие устанавливать доверие и/или выдавать удостоверение на основании информации, связанной с идентификатором, с тем чтобы пользователи могли в случае необходимости проверять информацию.

## **6.3 Модель функционирования**

Модель функционирования услуги идентификатора обозначает основные операции, которые должны обеспечиваться услугой идентификатора для поддержки приложений "умного" города, а также определяет, как эти операции должны выполняться услугой идентификатора. Модель функционирования также должна определять важные функции, которые позволяют выполнять связанные операции различными компонентами услуги идентификатора.

Гораздо более важно то, что услуга идентификатора для приложений "умного" города должна обеспечивать четко определенные встроенные услуги безопасности в каждой из операций в рамках своей услуги. Услуги безопасности должны включать опции для защиты целостности услуги и конфиденциальности данных, а также безотказности услуги всегда, когда это необходимо.

# **7 Требования к услугам идентификатора в приложениях "умного" города**

## **7.1 Общие требования к услугам идентификатора**

### **7.1.1 Совместимость с существующими принципами "умного" города**

Услуга идентификатора для "умных" городов должна учитывать существующие принципы в приложениях "умного" города. Это требуется для того, чтобы существующие приложения "умного" города продолжали функционировать, а также для обеспечения механизмов установления интерфейсов с другими приложениями "умного" города. Услуга идентификатора должна быть достаточно гибкой для поддержки любого соглашения об именовании в существующих приложениях "умного" города.

## **7.1.2 Расширяемость**

В разных приложениях "умного" города могут требоваться различные данные, связанные со своими идентификаторами. Требуется, чтобы услуга идентификатора для "умных" городов поддерживала структуру определенных в приложении данных и метаданных и обеспечивала возможность регистрации приложениями своей структуры данных и метаданных. Система преобразования и администрирования идентификатора должна иметь возможность обрабатывать все типы данных, связанных с идентификаторами.

## **7.1.3 Эффективность при преобразовании**

Требуется, чтобы услуга идентификатора для "умных" городов была эффективной по показателю времени, в особенности при преобразовании идентификатора. Если услуга идентификатора поддерживает также администрирование идентификатора, рекомендуется разрешать определять для администрирования отдельный интерфейс услуг.

Услуга преобразования может факультативно использовать различные методы повышения эффективности. Это может быть, например, измерение скорости реагирования на другие услуги идентификатора, кеширование, уменьшение или оптимизация числа запросов и обработки дефектных или не отвечающих серверов идентификаторов.

Для достижения более высокой производительности услуга идентификатора может также определять механизмы кеширования в целях снижения объема сетевого трафика, обусловленного запросами на преобразование.

## **7.1.4 Масштабируемость**

Требуется, чтобы услуга идентификатора для "умных" городов была масштабируемой в части поддержки постоянно растущего числа идентификаторов для "умных" городов, а также постоянно растущего числа приложений. Для поддержки такой масштабируемости требуется модель распределенной услуги. В модели распределенной услуги управление услугой осуществляется таким образом, чтобы отдельные организации могли самостоятельно управлять своей собственной услугой идентификатора и использовать ее. Необязательно, чтобы каждая операция услуги идентификатора могла выполнять множественную репликацию услуги (зеркальное отражение) для обеспечения резервирования услуги и балансировки нагрузки. Также необязательно определять механизмы поддержки концепции кластеров услуг, запросов идентификаторов услуг и/или услуг.

## **7.1.5 Международная поддержка**

Требуется, чтобы услуга идентификатора для "умных" городов поддерживала Юникод, который включает большинство символов, используемых в настоящее время во всем мире. Существует несколько способов кодирования символов Юникода при передаче по сети. Для обеспечения максимальной эффективности и совместимости рекомендуемым методом кодирования для услуг идентификатора для "умного" города является 8-битовый формат преобразования Юникода (UTF-8).

## **7.2 Общие требования безопасности**

### **7.2.1 Безопасное преобразование**

Требуется, чтобы услуга идентификатора для "умных" городов имела надлежащий уровень безопасности в части преобразования идентификатора. Она должна обеспечивать целостность услуги, с тем чтобы клиенты могли проверять любые данные, полученные от услуги идентификатора. Она должна также обеспечивать вариант с надлежащим уровнем конфиденциальности данных в процессе преобразования во время передачи по сети.

### **7.2.2 Избирательный контроль доступа**

Многие приложения "умного" города требуют избирательного контроля доступа к своей идентификационной информации. Требуется, чтобы услуга идентификатора для "умного" города разрешала определять контроль доступа для информации, связанной с ее идентификатором. В целях достижения максимальной гибкости такой контроль доступа должен определяться независимо от администратора сервера. Для осуществления этого требуется, чтобы услуга идентификатора могла реализовать интерфейс для аутентификации и авторизации клиентов.

### 7.2.3 Интерфейс распределенного управления и администрирования

Приложения "умного" города, которые участвуют в процессе контроля и управления в реальном времени устройствами IoT, могут также требовать изменения или обновления данных статуса, связанных со своим идентификатором. Требуется, чтобы услуга идентификатора для "умного" города обеспечивала безопасный административный интерфейс, для того чтобы приложения могли управлять атрибутами идентификатора и обновлять эти атрибуты своевременно.

## 7.3 Требования, относящиеся к модели услуги

### 7.3.1 Функциональная совместимость: модель распределенной услуги

Требуется, чтобы услуга идентификатора для приложений "умного" города поддерживала модель распределенной услуги. Услуга идентификатора должна состоять из компонентов распределенной услуги, которые будут поддерживать и одноранговый и иерархический уровни администрирования услуги.

Модель распределенной услуги однорангового уровня требуется для распределенного управления услугой идентификатора в рамках разных приложений "умного" города, как внутри, так и за пределами любых городских границ. Благодаря такому управлению каждое приложение "умного" города может обеспечивать собственную услугу идентификатора независимо, работая при этом совместно с приложениями своего ранга (см. рисунок 1).

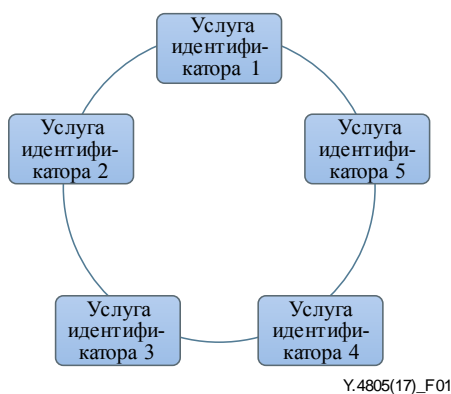


Рисунок 1 – Модель распределенной услуги однорангового уровня

Модель распределенной услуги иерархического уровня подходит для приложений "умного" города, отражающих иерархическую структуру управления организацией. Это позволяет любой организации обеспечивать общедоступную услугу идентификатора в нескольких доменах дочерних компаний, но при этом оставляя каждому дочернему предприятию возможность использовать свою услугу идентификатора всегда, когда это необходимо (см. рисунок 2).

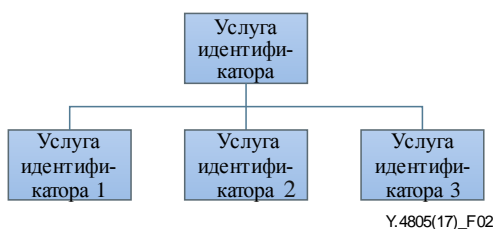


Рисунок 2 – Модель распределенной услуги иерархического уровня

### 7.3.2 Функциональная совместимость: распределенная корневая услуга

Для всех иерархических услуг требуется корневая услуга в качестве основы иерархии услуги. Примером такой услуги служит корневая услуга DNS. Требуется, чтобы услуга идентификатора для приложений "умного" города обеспечивала корневую услугу, которая используется в качестве стартовой точки для регистрации любых компонентов услуги в иерархии услуги. Она также должна использоваться для обеспечения надежных ссылок услуги на любые компоненты услуги всегда, когда

это необходимо. Такая корневая услуга требуется также для любой иерархической услуги идентификатора для приложения "умного" города. Корневая услуга должна быть распределена так, чтобы на нее не воздействовала какая-либо единичная точка отказа. Должно быть также разрешено управление однорангового уровня со стороны многих участников, с тем чтобы этот корень не был под контролем какого-либо одного объекта. В условиях, когда разные государства и организации используют свои собственные экземпляры корневого сервера для услуги идентификатора, они должны принимать надлежащие меры для предотвращения появления единичных точек отказа.

### **7.3.3 Безопасность: корень доверия**

Корневая услуга необходима в качестве основы доверия в иерархической услуге идентификатора. В среде иерархической услуги идентификатора услуга идентификатора должна выдавать удостоверения своим производным услугам идентификатора. Рекомендуется, чтобы удостоверением любой услуги идентификатора был открытый ключ, подписанный услугой идентификатора более высокого уровня, и чтобы эти удостоверения использовались для обеспечения средства подтверждения целостности услуги по запросу клиента. Требуется, чтобы любой клиент, использующий услугу идентификатора, имел возможность отслеживать ее удостоверение вплоть до корневой услуги, для того чтобы проверить подлинность услуги идентификатора.

### **7.3.4 Безопасность: репликация и зеркальное отражение**

Любая услуга идентификатора в распределенной услуге идентификатора может факультативно устанавливать несколько услуг репликации для предотвращения возникновения какой-либо единичной точки отказа. Для обеспечения одновременного администрирования идентификатора требуется, чтобы на сайтах репликации было несколько услуг идентификатора однорангового уровня. В этом случае требуется, чтобы были установлены механизмы для предотвращения возникновения условий состязания, когда несколько сайтов репликации одновременно пытаются обновить одну и ту же запись идентификатора.

### **7.3.5 Функциональная совместимость: услуга кеширования**

Требуется, чтобы услуга идентификатора поддерживала кеширование, которое поможет сократить необязательный сетевой трафик. Рекомендуется, чтобы результат преобразования идентификатора содержал стандартное поле "Предписанное время жизни" (TTL), указывающее срок действительности данных. Специализированная услуга кеширования может быть факультативно развернута для поддержки определенного сообщества пользователей.

### **7.3.6 Функциональная совместимость: поддержка услуги итерационного и рекурсивного преобразования**

Рекомендуется, чтобы услуга идентификатора итерационно или рекурсивно отправляла запросы другому экземпляру услуги идентификатора от имени конечного клиента. Осуществляющая такие запросы услуга идентификатора может кешировать возвращаемые ответы.

## **7.4 Требования к модели данных**

### **7.4.1 Безопасность: общая схема для контроля доступа к атрибутам идентификатора**

Многие приложения "умного" города требуют контроля доступа к атрибутам идентификатора. Для любого конкретного идентификатора возможно, что только какое-либо подмножество его атрибутов является общедоступным, тогда как все остальные атрибуты доступны только для конкретных авторизованных сторон после преобразования идентификатора.

Требуется, чтобы модель данных услуги идентификатора для приложений "умного" города включала общую схему контроля доступа к атрибутам идентификатора. В частности, в любом подмножестве атрибутов идентификатора должно быть разрешено определять контроль доступа на основе роли или на основе принадлежности к группе.

### **7.4.2 Безопасность: поддержка проверки удостоверения**

В среде распределенных вычислений целостность услуги обеспечивает только средство подтверждения того, что данные поступают от авторизованной услуги. Она необязательно выдает какое-либо удостоверение надежности и безопасности данных. Требуется, чтобы услуга идентификатора для

приложений "умного" города обеспечивала целостность услуги, как это рассматривалось ранее в настоящей Рекомендации, а также обеспечивала варианты проверки удостоверения. Рекомендуется определять проверку удостоверения как варианты цифровой подписи третьей стороны, связанной с атрибутами идентификатора, либо как ссылки на услугу проверки третьей стороны, которая может использоваться для проверки подлинности или надежности атрибутов идентификатора.

#### **7.4.3 Безопасность: поддержка дискреционного администрирования и владения идентификатором**

Требуется, чтобы модель данных услуги идентификатора обеспечивала варианты для отдельного администратора идентификатора, независимо от услуги хостинга, и разрешала дискреционное администрирование идентификатора и его атрибутов. Реализации услуги идентификатора должны обеспечивать средства защиты идентификатора и его атрибутов, с тем чтобы в идентификатор и его атрибуты возможно было внести только разрешенные изменения.

Разрешение дискреционного администрирования важно в приложениях "умного" города, где каждый идентифицированный субъект может взаимодействовать напрямую с услугой идентификатора для выполнения обновления его атрибутов в реальном времени, не обращаясь к какому-либо централизованному администратору сервера. Оно также минимизирует потенциальные риски нарушения безопасности в результате неразрешенных изменений идентификаторов, размещенных в услуге идентификатора.

#### **7.4.4 Функциональная совместимость: расширяемая модель данных**

Идентификаторы для приложений "умного" города используются в целях связывания разных видов информации с идентифицированным субъектом. Требуется, чтобы модель данных для услуги идентификатора была достаточно гибкой, чтобы поддерживать новые типы данных, которые должны быть определены для атрибутов идентификатора в приложениях "умного" города. Приложение "умного" города должно иметь возможность определять собственный тип данных и регистрировать его в услуге идентификатора.

#### **7.4.5 Функциональная совместимость: адаптивная схема именования**

Существует большое число приложений "умного" города, имеющих собственные схемы идентификации. Изменить схемы именования этих приложений на практике сложно. Требуется, чтобы услуга идентификатора для приложений "умного" города определяла гибкую схему именования для поддержки адаптации имен, используемых существующими приложениями "умного" города.

### **7.5 Требования к модели функционирования**

#### **7.5.1 Безопасность: безопасные операции**

Требуется, чтобы услуга идентификатора для "умных" городов поддерживала полный набор защищенных операций с идентификатором, включая следующие:

- 1) создание и регистрация нового идентификатора и привязка к идентификатору набора атрибутов;
- 2) разрешение или запрос атрибутов, связанных с любым зарегистрированным идентификатором;
- 3) безопасное обновление или изменение атрибутов идентификатора, связанных с существующим идентификатором;
- 4) удаление идентификатора или аннулирование любых атрибутов, связанных с идентификатором.

Услуга идентификатора должна обеспечивать стандартные протокольные интерфейсы для поддержки любой из этих операций. Услуга идентификатора должна также обеспечивать надлежащие механизмы аутентификации и авторизации для содействия безопасности этих операций.

#### **7.5.2 Функциональная совместимость: связанное функционирование услуги идентификатора в распределенной среде**

Требуется, чтобы каждая услуга идентификатора в иерархии услуги работала связанным образом в распределенной среде. Получив запрос на услугу, услуга идентификатора, получившая запрос, должна выполнять его рекурсивно и итерационно. В рекурсивном режиме услуга идентификатора должна перенаправить запрос на услугу ответственной услуге идентификатора, получить ответ ответственной

услуги идентификатора и вернуть результат обратно клиенту. В итерационном режиме услуга идентификатора должна вернуть клиенту ссылку на ответственную услугу идентификатора и дать команду клиенту повторно отправить свой запрос ответственной услуге идентификатора.

### **7.5.3 Безопасность: доверие в иерархии услуги идентификатора**

Требуется, чтобы каждая услуга идентификатора в распределенной иерархии получала удостоверение услуги от услуги идентификатора более высокого уровня в иерархии. Рекомендуется, чтобы удостоверения выдавались в форме подписанного открытого ключа или какого-либо сертификата открытого ключа. Такое удостоверение необходимо при обеспечении целостности услуги в распределенной среде. Удостоверение следует использовать также как средство безотказности услуги в определенных условиях. Клиент, взаимодействующий с любой услугой идентификатора, должен иметь опцию отслеживания удостоверения своей услуги по всей цепи вплоть до корневой услуги идентификатора, с тем чтобы проверить ее подлинность. Рекомендуется кэширование этой проверки во избежание излишних повторных операций при условии, что срок кэшированной проверки истечет или произойдет иное превышение времени.

## Библиография

- [b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions.*
- [b-ITU-T Y.2091] Рекомендация МСЭ-Т Y.2091 (2011 г.), *Термины и определения для сетей последующих поколений.*
- [b-ITU-T Y.2261] Рекомендация МСЭ-Т Y.2261 (2006 г.), *Эволюция сетей КТСОП/ЦСИС по направлению к СПП.*
- [b-ITU-T Y.4000] Рекомендация МСЭ-Т Y.4000/Y.2060 (2012 г.), *Обзор интернета вещей.*
- [b-ITU-T Y.4108] Recommendation ITU-T Y.4108/Y.2213 (2008), *NGN service requirements and capabilities for network aspects of applications and services using tag-based identification.*







## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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
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
<b>Серия Y</b>	<b>Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города</b>
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи