# Вступление

Этот документ и все другие части, связанные с ним, были разработаны в ответ на мировой спрос на устройства Интернета вещей (IoT), ориентированные на умный дом, такие как бытовая техника, дверные замки, камеры безопасности, датчики и исполнительные механизмы; они должны быть смоделированы и надежно управляться локально и удаленно через IP-сеть.

Хотя существовала некоторая связь между устройствами, универсального языка для Интернета вещей не было разработано. Вместо этого производителям устройств приходилось выбирать между разрозненными фреймворками, ограничивающими свою долю рынка, или разработкой в ​​нескольких экосистемах, увеличивая свои затраты. Затем на конечных пользователей ложится бремя: определить, совместимы ли продукты, которые они хотят, с экосистемой, в которую они купили, или найти способы интегрировать свои устройства в свою сеть и попытаться самостоятельно решить проблемы совместимости.

Помимо умного дома развертыванию Интернета вещей в коммерческих средах препятствует недостаточная безопасность. Этой проблемы можно избежать, используя безопасную структуру связи IoT, которую решает этот стандарт.

Целью этих документов является подключение следующих 25 миллиардов устройств для Интернета вещей, обеспечивая безопасное и надежное обнаружение устройств и возможность подключения между несколькими ОС и платформами. Существует множество предложений и форумов, в которых используются разные подходы, но ни одно решение не удовлетворяет большинство ключевых требований. Этот документ и связанные с ним части позволяют объединить отрасль вокруг единого, безопасного и совместимого подхода.

# Сфера

This document defines security objectives, philosophy, Resources and mechanisms that impacts OCF base layers of [ISO/IEC 30118-1. ISO/IEC 30118-1](#_bookmark3) contains informative security content. The OCF Security Document contains security normative content and may contain informative content related to the OCF base or other OCF documents.

# Нормативные ссылки

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 30118-1 *Information technology* – *Open Connectivity Foundation (OCF) Document* – *Part*

*1: Core specification*

<https://www.iso.org/standard/53238.html>

Latest version available at:

<https://openconnectivity.org/specs/OCF_Core_Specification.pdf>

ISO/IEC 30118-2, Information technology – Open Connectivity Foundation (OCF) Document –

*Part 2: Security specification*

<https://www.iso.org/standard/74239.html>

Latest version available at:<https://openconnectivity.org/specs/OCF_Security_Specification.pdf>

ISO/IEC 30118-8, *Information technology – Open Connectivity Foundation (OCF) Document –*

*Part 8: Device to Cloud Services*,

<https://www.iso.org/standard/79360.html>

Latest version available at:

[https://openconnectivity.org/specs/OCF\_OCF\_Device\_To\_Cloud\_Services\_Specification.pdf](https://openconnectivity.org/specs/OCF_Cloud_Specification.pdf)

IETF RFC 6749, *The OAuth 2.0 Authorization Framework*, October 2012,

<https://tools.ietf.org/html/rfc6749>

IETF RFC 6750*, The OAuth 2.0 Authorization Framework: Bearer Token Usage*, October 2012,

<https://tools.ietf.org/html/rfc6750>

IETF RFC 8323, CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets,

February 2018, <https://tools.ietf.org/html/rfc8323>

oneM2M Release 3 Documents, <http://www.onem2m.org/technical/published-drafts>

OpenAPI document, aka *Swagger RESTful API Documentation Specification*, Version 2.0

<https://github.com/OAI/OpenAPI-Specification/blob/master/versions/2.0.md>

# 3. Термины, определения и сокращенные термины

## 3.1 Термины и определения

For the purposes of this document, the terms and definitions given in [ISO/IEC 30118-1,](#_bookmark3) [ISO/IEC](#_bookmark4)

[30118-2,](#_bookmark4) [ISO/IEC 30118-8](#_bookmark5) and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following

addresses:

– ISO Online browsing platform: available at <https://www.iso.org/obp>

– IEC Electropedia: available at <http://www.electropedia.org/>

### 3.1.1 Access Token

учетные данные, используемые для авторизации соединения с OCF Cloud и доступа к защищенным ресурсам

Примечание 1 к записи: токен доступа - это строка, в то время как устройство OCF не имеет внутренней логики, основанной на его содержимом, и только пересылает токен как есть

### 3.1.2 Authorization Provider

сервер, выдающий токены доступа (3.1.1) через посредника клиенту после успешной аутентификации пользователя OCF Cloud (3.1.4) и получения авторизации

Примечание 1 к записи: Также известен как сервер авторизации в IETF RFC 6749.

### 3.1.3 Регистрация устройства

процесс, посредством которого Устройство регистрируется / регистрируется в инфраструктуре OCF Cloud (с использованием сертификата устройства и уникальных учетных данных) и становится готовым к дальнейшей удаленной работе через облачный интерфейс (например, подключение к удаленным ресурсам или публикация собственных ресурсов для доступа)

### 3.1.4 Пользователь облака OCF

человек или организация, разрешающие набору Устройств взаимодействовать друг с другом через облако OCF

Примечание 1 к записи: Для каждого Устройства пользователь облака OCF является либо тем же, либо представителем лица или организации, которые подключили это Устройство. Пользователь облака OCF делегирует органу управления облаком OCF полномочия по маршрутизации между устройствами, зарегистрированными пользователем облака OCF. OCF Cloud делегирует пользователю OCF Cloud право выбирать набор устройств, которые могут регистрироваться и использовать сервисы OCF Cloud.

## 3.2 Сокращенные термины

Для целей этого документа применяются символы и сокращенные термины, приведенные в ISO / IEC 30118-1, ISO / IEC 30118-2 и ISO / IEC 30118-8.

# 4. Условные обозначения и организация документа

### 4.1 Conventions

In this document a number of terms, conditions, mechanisms, sequences, parameters, events, states, or similar terms are printed with the first letter of each word in uppercase and the rest lowercase (e.g., Network Architecture). Any lowercase uses of these words have the normal technical English meaning.

In this document, to be consistent with the IETF usages for RESTful operations, the RESTful operation words CRUDN, CREATE, RETRIVE, UPDATE, DELETE, and NOTIFY will have all letters capitalized. Any lowercase uses of these words have the normal technical English meaning.

### 4.2 Notation

In this document, features are described as required, recommended, allowed or DEPRECATED as follows:

Required (or shall or mandatory)(M).

– These basic features shall be implemented to comply with Core Architecture. The phrases "shall not", and "PROHIBITED" indicate behaviour that is prohibited, i.e. that if performed means the implementation is not in compliance.

Recommended (or should)(S).

– These features add functionality supported by Core Architecture and should be implemented. Recommended features take advantage of the capabilities Core Architecture, usually without imposing major increase of complexity. Notice that for compliance testing, if a recommended feature is implemented, it shall meet the specified requirements to be in compliance with these guidelines. Some recommended features could become requirements in the future. The phrase "should not" indicates behaviour that is permitted but not recommended. Allowed (may or allowed)(O).

– These features are neither required nor recommended by Core Architecture, but if the feature is implemented, it shall meet the specified requirements to be in compliance with these guidelines.

DEPRECATED.

– Although these features are still described in this document, they should not be implemented except for backward compatibility. The occurrence of a deprecated feature during operation of an implementation compliant with the current document has no effect on the implementation’s operation and does not produce any error conditions. Backward compatibility may require that a feature is implemented and functions as specified but it shall never be used by implementations compliant with this document.

Conditionally allowed (CA).

– The definition or behaviour depends on a condition. If the specified condition is met, then the definition or behaviour is allowed, otherwise it is not allowed.

Conditionally required (CR).

– The definition or behaviour depends on a condition. If the specified condition is met, then the definition or behaviour is required. Otherwise the definition or behaviour is allowed as default unless specifically defined as not allowed.

Strings that are to be taken literally are enclosed in "double quotes".

Words that are emphasized are printed in italic.

In all of the Property and Resource definition tables that are included throughout this document the "Mandatory" column indicates that the item detailed is mandatory to implement; the mandating of inclusion of the item in a Resource Payload associated with a CRUDN action is dependent on the applicable schema for that action.

### 4.3 Data types

Resources are defined using data types derived from JSON values as defined in clause 4.3 in [ISO/IEC 30118-1](#_bookmark3)

# 5. Обзор безопасности

## 5.1 Преамбула

Устройство авторизовано для связи с облаком OCF, если доверенный посредник предоставил Устройство.

- Устройство и посредник подключаются через DTLS с использованием "/ oic / sec / cred"

- Устройство предоставлено Посредником со следующей информацией:

- URL-адрес OCF Cloud

- Имя провайдера авторизации для определения происхождения токена доступа

- Токен доступа / код авторизации, который проверяется / обменивается облаком OCF

- UUID облака OCF

Определения OpenAPI 2.0 (приложение A), используемые в этом документе, являются нормативными. Это включает в себя то, что все определенные полезные данные должны соответствовать указанным определениям OpenAPI 2.0. Приложение A содержит все определения OpenAPI 2.0 для типов ресурсов, определенных в этом документе.

## 5.2 Подготовка устройств к облаку OCF и обзор регистрации устройств

Как упоминалось в начале пункта 0, связь между устройством и облаком OCF регулируется другими критериями по сравнению с устройствами, которые находятся в одной локальной сети. Устройство настроено для подключения к облаку OCF с помощью посредника, как указано в разделах ресурсов CoAPCloudConf в ISO / IEC 30118-8. Подготовка включает удаленное подключение и локальные данные, такие как URL-адрес, по которому можно найти среду хостинга OCF Cloud, проверяемый токен доступа OCF Cloud и, при необходимости, имя поставщика авторизации, выпустившего токен доступа.

ПРИМЕЧАНИЕ. Устройство, которое подключается к OCF Cloud, по-прежнему сохраняет право собственности, установленное при подключении к DOTS.

## 5.3 Обзор учетных данных

Устройства могут использовать учетные данные для подтверждения личности и роли (ролей) сторон в двунаправленной связи.

Токены доступа предоставляются облаку OCF после установления сеанса аутентификации с облаком OCF для проверки идентификатора пользователя, с которым должно быть связано Устройство.

# 6. Подготовка устройства для OCF Cloud

## 6.1 Общие положения об облачном обеспечении

Устройство, которое подключается к облаку OCF, должно поддерживать ресурс «oic.r.coapcloudconf» на устройстве и следующие SVR в облаке OCF: «/ oic / sec / account», «/ oic / sec / session», «/ oic. / сек / tokenrefresh ".

Ожидается, что в облаке OCF будет использоваться безопасный механизм для связывания посредника с пользователем облака OCF. Выбор механизма остается за OCF Cloud. Рекомендуемое решение основано на потоке типа разрешения авторизации OAuth2.0, указанном в IETF RFC 6749, где посредник действует как пользовательский агент и представляет пользователю пользовательский интерфейс авторизации - см. Рисунок 1. Ожидается, что OCF Cloud обеспечит подходящую аутентификацию. используется для аутентификации пользователя облака OCF.

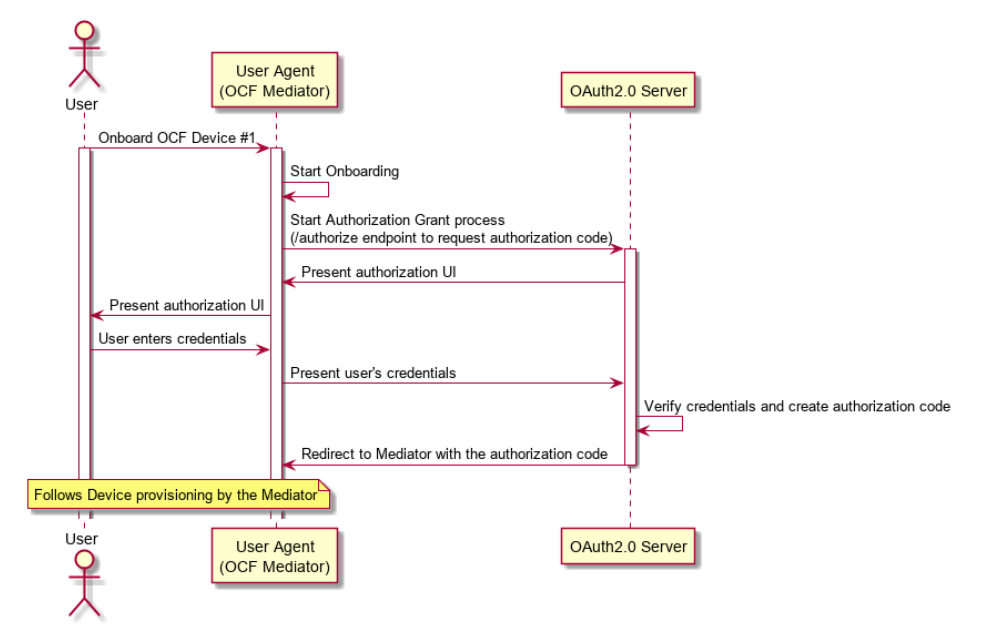


Рисунок 1 - Авторизация и подготовка пользователей с использованием потока предоставления кода авторизации

## 6.2 Подготовка устройства посредником

Посредник и Устройство должны использовать безопасный сеанс, чтобы настроить Устройство для подключения к облаку OCF.

Посредник получает код авторизации или непосредственно токен доступа от сервера авторизации, как описано в ISO / IEC 30118-8. Это значение затем используется устройством для регистрации в облаке OCF, как описано в пункте 0. Во время регистрации устройства OCF Cloud обменивает код авторизации для маркера доступа, возвращает его обратно на устройство OCF и связывает сеанс TLS с соответствующий UUID устройства. Облако OCF поддерживает карту, где хранятся токен доступа и посредник, предоставленный UUID устройства.

Посредник подготавливает Устройство, как описано в ISO / IEC 30118-8. Посредник предоставляет URI облака OCF свойству «cis» ресурса «oic.r.coapcloudconf», UUID облака OCF - свойству «sid» ресурса «oic.r.coapcloudconf» и токену доступа для каждого устройства или коду авторизации для свойство "at" ресурса "oic.r.coapcloudconf" на устройстве. Обмениваемый и возвращенный подготовленный токен доступа должен обрабатываться устройством как токен доступа с типом токена-носителя, как определено в IETF RFC 6750. Предоставленное значение "at" соответствует собственному формату данных и может включать несколько значений, упорядоченных / сцепленных вместе. в одну строку (например, "{\" токен \ ": \" abc \ ", \" client\_id \ ": \" 1234 \ ", \" idp \ ": \" identityProvider1 \ "}" является действительным "в " Стоимость имущества).

См. Рисунок 2 для подробного обзора рекомендованного потока, который включает необязательное предоставление кода авторизации OAuth 2.0.

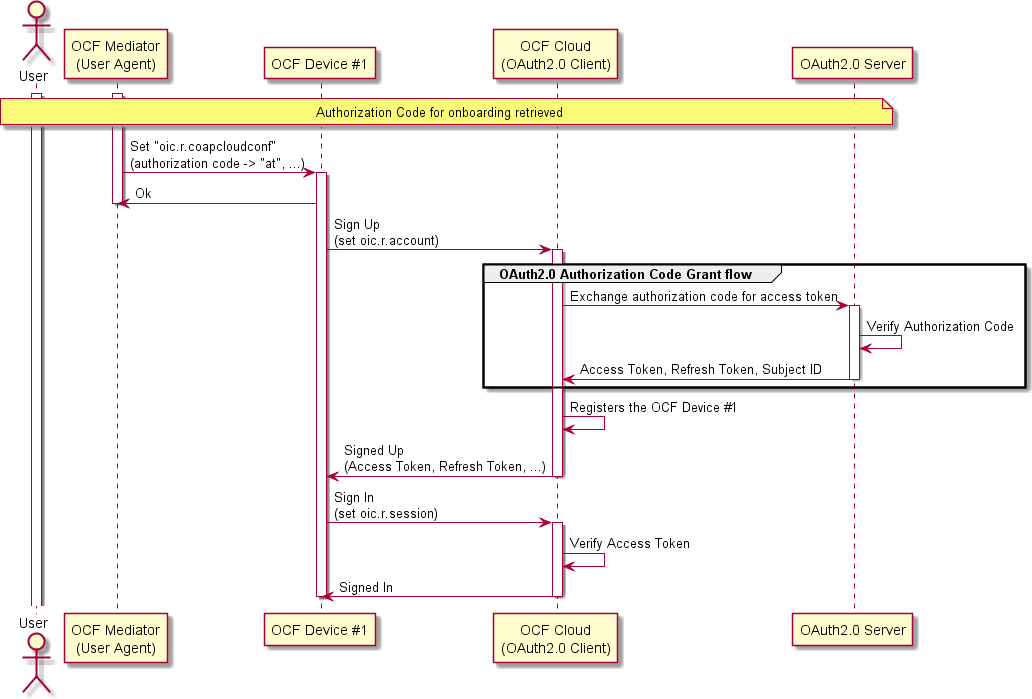


Рисунок 2 - Подготовка устройства с использованием потока предоставления кода авторизации

В целях управления доступом Устройство должно идентифицировать Облако OCF, используя UUID Облака OCF в поле Общее имя сертификата Конечного объекта, используемого для аутентификации Облака OCF.

AMS должна настроить записи ACE2 на устройстве так, чтобы посредник (-ы) был единственным устройством (-ами) с разрешением UPDATE для ресурса «oic.r.coapcloudconf».

AMS должен настроить записи ACE2 на устройстве, чтобы разрешить запросы из облака OCF. По запросу посредника AMS удаляет старые записи ACL2 с предыдущим UUID облака OCF. Этот запрос происходит до того, как посредник настроит "oic.r.coapcloudconf" для нового облака OCF. Посредник также просит AMS установить UUID облака OCF в качестве свойства «субъекта» для новых записей ACL2. AMS может использовать свойство sid ресурса oic.r.coapcloudconf в качестве текущего UUID облака OCF. AMS может либо предоставить запись с подстановочными знаками для облака OCF, либо предоставить запись, в которой перечислены все ресурсы, опубликованные на устройстве.

Если OCF Cloud предоставляет значение «redirecturi» в качестве ответа во время регистрации устройства, предполагается, что перенаправляемое в OCF Cloud имеет тот же UUID OCF Cloud и использует тот же якорь доверия. В противном случае представленный UUID облака OCF не будет соответствовать подготовленным записям ACL2.

Посредник должен предоставить ресурс «oic.r.coapcloudconf» со свойствами, указанными в таблице 1. Эти данные после предоставления используются устройством для выполнения регистрации устройства в облаке OCF. Не ожидается, что устройство OCF будет иметь какую-либо внутреннюю логику, основанную на значениях свойств «at» и «apn». Значения этих свойств передаются в облако OCF как есть. После первоначальной регистрации Устройство должно использовать обновленные значения, полученные из облака OCF. Если пользователь облака OCF хочет, чтобы устройство перерегистрировалось в облаке OCF, он может использовать посредника для повторной подготовки ресурса «oic.r.coapcloudconf» с новыми значениями.

Таблица 1 - Сопоставление свойств ресурсов «oic.r.account» и «oic.r.coapcloudconf»

|  |  |  |  |
| --- | --- | --- | --- |
| Property Title | oic.r.coapcloudconf | oic.r.account | Description |
| Authorization Provider Name | apn | authprovider | The name of Authorization Provider through which Access Token was  obtained. |
| OCF Cloud URL | cis | - | This is the URL connection is established between  Device and OCF Cloud. |
| Access Token | at | accesstoken | Access Token used to authorize the TLS  connection for  communication with the OCF Cloud, or the  Authorization Code which is then verified and  exchanged for the Access Token during Device  Registration. |
| OCF Cloud UUID | sid | - | This is the identity of the OCF Cloud that the Device is configured to use. |

# 7. Аутентификация устройства с помощью OCF Cloud

## 7.1 Аутентификация устройства с помощью OCF Cloud Общие

Механизмы аутентификации устройства в пунктах 10.2, 10.3 и 10.4 ISO / IEC 30118-2 подразумевают, что Устройство авторизовано для связи с любым другим Устройством, отвечающим критериям, указанным в «/ oic / sec / cred»; Ресурс «/ oic / sec / acl2» (или ресурс «/ oic / sec / acl1» серверов OIC1.1) дополнительно используется для ограничения доступа к определенным ресурсам. В данном пункте описывается аутентификация устройства для OCF Cloud, в которой используются несколько иные критерии, как описано в ISO / IEC 30118-2. Устройство, получающее доступ к облаку OCF, должно установить сеанс TLS. Сеанс TLS с взаимной аутентификацией устанавливается с использованием сертификата сервера и сертификата клиента.

Каждое Устройство идентифицируется токеном доступа, полученным в ответе о регистрации устройства. Облако OCF содержит таблицу ассоциаций облака OCF, которая сопоставляет токен доступа, идентификатор пользователя и UUID устройства. Регистрация Устройства должна происходить, пока Устройство находится в состоянии RFNOP. После регистрации устройства обновленный токен доступа, UUID устройства и идентификатор пользователя используются устройством для последующего подключения к облаку OCF.

## 7.2 Подключение устройства к OCF Cloud

Устройство должно установить TLS-соединение, используя учетные данные на основе сертификата. Соединение должно быть установлено после того, как Устройство будет инициализировано посредником.

Сеанс TLS устанавливается между Устройством и Облаком OCF, как указано в IETF RFC 8323. Ожидается, что Облако OCF предоставит сертификат, подписанный якорем доверия, который присутствует в кредитных записях Устройства. Ожидается, что эти записи кредита будут настроены Посредником.

Устройство должно проверять идентичность OCF Cloud на основе учетных данных, содержащихся в записях ресурсов «/ oic / sec / cred» Устройства.

Ожидается, что OCF Cloud проверит сертификат производителя, предоставленный Устройством.

Предполагается, что пользователь облака OCF доверяет облаку OCF, к которому подключается Устройство. Подключение к OCF Cloud не должно происходить без согласия пользователя OCF Cloud. Предполагается, что пользователь облака OCF имеет либо соглашение о предоставлении услуг с поставщиком облака OCF, либо использует облако OCF Cloud, предоставленное производителем.

Если аутентификация не удалась, свойство «clec» ресурса «oic.r.coapcloudconf» на Устройстве должно быть обновлено о состоянии сбоя, если оно поддерживается Устройством. Если аутентификация прошла успешно, Устройство и OCF Cloud должны установить зашифрованный канал в соответствии с согласованным набором шифров.

На рисунке 3 показана последовательность подключения устройства к OCF Cloud и шаги, описанные в таблице 2.

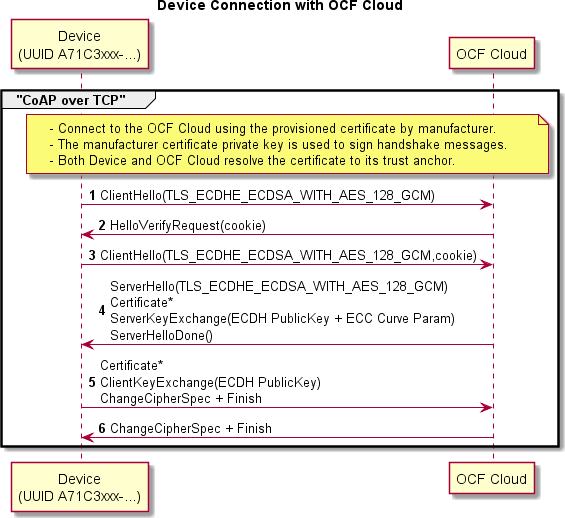


Figure 3 – Device connection with OCF Cloud

Table 2 – Device connection with the OCF Cloud flow

|  |  |
| --- | --- |
| **Steps** | **Description** |
| 1 - 6 | TLS connection between the OCF Cloud and Device.  The Device’s manufacturer certificate may contain data attesting to the Device hardening and security properties |

## 7.3 Соображения безопасности

Когда сервер OCF получает запрос, отправленный через облако OCF, тогда сервер OCF разрешает этот запрос, используя идентификатор облака OCF, а не идентификатор клиента OCF. Если нет механизма, с помощью которого облако OCF разрешает только те взаимодействия, которые пользователь намеревается между клиентами OCF и сервером OCF через облако OCF, и запрещает все другие взаимодействия, тогда клиенты OCF могут получить повышенные привилегии, отправив запрос через облако OCF. . Это крайне нежелательно с точки зрения безопасности. Следовательно, ожидается, что реализации OCF Cloud предоставят некоторый механизм, с помощью которого OCF Cloud предотвращает получение клиентами OCF повышенных привилегий при отправке запроса через OCF Cloud. В настоящем выпуске документа детали механизма оставлены на усмотрение реализации.

Соображения безопасности в отношении сертификата производителя, как описано в пункте 7.3.6.5 ИСО / МЭК 30118-2, также применимы при аутентификации устройства с помощью облака OCF.

Устройство должно проверить сертификат TLS облака OCF, как это определено IETF RFC 6125 и в соответствии с его требованиями к аутентификации идентичности сервера.

«Uid» и «di» значение свойства ресурса «/ oic / d» могут рассматриваться как личная информация в некоторых регулирующих регионах, и ожидается, что OCF Cloud обеспечит защиту, соответствующую его регулирующим регулирующим органам.

# 8. Целостность и конфиденциальность сообщений

## 8.1 Семантика облачных сессий

Обмен сообщениями между Облаком OCF и Устройством осуществляется только в том случае, если Устройство и Облако OCF аутентифицируют друг друга, как описано в п. 0. Наборы асимметричных шифров, как описано в п. 8.2, должны использоваться для установления защищенного сеанса и для шифрования / дешифрования между OCF. Облако и устройство. Конечная точка OCF, отправляющая сообщение, должна зашифровать и аутентифицировать сообщение с использованием набора шифров, как описано в п. 8.2, а конечная точка OCF должна проверить и расшифровать сообщение перед его обработкой.

## 8.2 Наборы шифров для учетных данных OCF Cloud

Все Устройства, поддерживающие учетные данные облачного сертификата OCF, должны реализовывать:

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

Все устройства, поддерживающие учетные данные облачного сертификата OCF, должны реализовывать:

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

# 9. Ресурсы по безопасности

## 9.1 Ресурс учетной записи

Ресурс учетной записи определяет свойства на основе создания учетной записи на основе токена доступа IETF RFC 6749. Механизм получения учетных данных описан в пункте 0. Ресурс учетной записи используется для регистрации устройства. Ресурс учетной записи создается в облаке OCF как SVR «oic/sec/account» и используется Устройствами с поддержкой облака для регистрации в облаке OCF. Он должен быть доступен только по защищенному каналу; незащищенный канал не должен иметь доступ к этому Ресурсу.

Во время процесса регистрации устройства облако OCF может предоставить отдельный URI другого облака OCF («перенаправлено» в облако OCF). Ожидается, что как исходные, так и перенаправленные облака OCF принадлежат одному и тому же поставщику; предполагается, что они имеют один и тот же UUID, и предполагается, что для них установлен внеполосный канал связи. Устройству не нужно выполнять регистрацию устройства в перенаправляемом облаке OCF, и облако OCF может игнорировать такие попытки. Ожидается, что перенаправленное в облако OCF будет принимать токен доступа, предоставленный Устройству исходным облаком OCF.

Операция RETRIEVE для ресурса «/oic/sec/account» Облака OCF не разрешена, и ожидается, что Облако OCF отклонит все попытки выполнить такую операцию.

Операция UPDATE в ресурсе OCF Cloud "/oic/sec/account" ведет себя следующим образом:

- Устройство, намеревающееся зарегистрироваться в облаке OCF, должно отправить ОБНОВЛЕНИЕ со следующими Свойствами «di» («di» Значение свойства ресурса «/oic/d») и «accesstoken», как настроено Посредником («в« Значение свойства » ресурса "oic.r.coapcloudconf"). Облако OCF проверяет, что это тот же "accesstoken", который был назначен посреднику для соответствующего значения свойства "di". «Accesstoken» - это разрешение Устройству на доступ к OCF Cloud. Если «apn» был включен, когда Посредник ОБНОВЛЯЛ ресурс «oic.r.coapcloudconf», Устройство также должно включать свойство «authprovider» при регистрации в облаке OCF. Если "apn" не указан, то свойство "authprovider" не должно быть включено в запрос UPDATE.

- Облако OCF возвращает «accesstoken», «uid», «refreshtoken» и «expiresin». Оно также может возвращать «redirecturi». Полученный «accesstoken» должен обрабатываться Устройством как маркер доступа с типом «Bearer», как определено в IETF RFC 6750. Этот «accesstoken» должен использоваться для следующего запуска сеанса учетной записи с использованием SVR «oic / sec / session». Полученный «маркер обновления» должен обрабатываться устройством как маркер обновления, как определено в IETF RFC 6749. Устройство хранит значения ответа облака OCF. Если получено «redirecturi», Устройство должно использовать полученное значение в качестве нового URI облака OCF вместо значения свойства «cis» ресурса «oic.r.coapcloudconf» для дальнейших подключений.

Операция DELETE на ресурсе OCF Cloud "/oic/sec/account" должна вести себя следующим образом:

- Для отмены регистрации в облаке OCF должна быть отправлена операция DELETE с "accesstoken" и либо "uid", либо "di" Свойствами, которые необходимо отменить регистрацию в облаке OCF. В случае, если свойство «di» опущено в операции DELETE, ожидается, что OCF Cloud отменит регистрацию устройства с соответствующим значением свойства «accesstoken». При УДАЛЕНИИ с помощью OCF Cloud Устройство также должно удалить значения, хранящиеся внутри. После отмены регистрации в облаке OCF Устройство может подключиться к любому другому облаку OCF. Для отмены регистрации устройства необходимо снова выполнить шаги 0, чтобы зарегистрироваться в облаке OCF. Ресурс «oic.r.account» определен в таблице 3.

Table 3 – Definition of the "oic.r.account" Resource

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fixed URI** | **Resource Type Title** | **Resource Type ID ("rt" value)** | **OCF**  **Interfaces** | **Description** | **Related Functional Interaction** |
| /oic/sec/account | Account | oic.r.account | oic.if.basel ine | Resource used for a Device to add itself under  a given credential | N/A |

1. [Table 4](#_bookmark41) defines the Properties of the "oic.r.account " Resource Type.

Table 4 – Properties of the "oic.r.account" Resource

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Property Title** | **Property Name** | **Value Type** | **Value Rule** | **Access Mode** | **Mandat ory** | **Description** |
| Device UUID | di | string | uuid | W | Yes | Unique Device identifier. Format pattern according to IETF RFC 4122. |
| Authorization Provider Name | authprovider | string | N/A | W | No | The name of Authorization Provider through which Access Token was obtained. |
| Access Token | accesstoken | string | Non- empty string | W | Yes | Access Token used to authorize and associate the TLS connection for  communication with the OCF Cloud with the  Device UUID, or the Authorization Code which is then verified and exchanged for the Access Token during Device Registration. |
| Access Token | accesstoken | string | Non- empty string | R | Yes | Access Token used to authorize and associate the TLS connection for  communication with the OCF Cloud with the Device UUID. |
| Refresh Token | refreshtoken | string | Non- empty string | R | Yes | Refresh token can be used to refresh the Access Token before getting expired. |
| Token Expiration | expiresin | integer | - | R | Yes | Access Token life time in seconds (-1 if permanent). |
| User ID | uid | string | uuid | R | Yes | Unique OCF Cloud User identifier. Format pattern according to IETF RFC 4122. |
| Redirect URI | redirecturi | string | - | R | No | Using this URI, the Client needs to reconnect to a redirected OCF Cloud. If provided, this value shall be used by the Device instead of Mediator-provided URI during the Device  Registration. |

## 9.2 Ресурс сеанса учетной записи

Ресурс «/ oic / sec / session», размещенный в облаке OCF, используется для создания соединений с облаком OCF после регистрации устройства через ресурс «/ oic / sec / account». Ресурсу «/ oic / sec / session» требуются UUID устройства, идентификатор пользователя и токен доступа, которые надежно хранятся на устройстве.

Ресурс «/ oic / sec / session» предоставляется облаком OCF. Он должен быть доступен только по защищенному каналу; незащищенный канал не может получить доступ к этому Ресурсу.

Операция RETRIEVE на ресурсе OCF Cloud "/ oic / sec / session" не разрешена, и ожидается, что OCF Cloud отклонит все попытки выполнить такую операцию.

Операция UPDATE для ресурса OCF Cloud "/ oic / sec / session" определяется следующим образом:

- Устройство, подключающееся к облаку OCF, должно отправить сообщение с запросом UPDATE на ресурс «/ oic / sec / session» облака OCF. Сообщение должно включать значение свойства di ресурса / oic / d и uid, значение входа в систему («true» для установления соединения; «false» для отключения) и «accesstoken», возвращенные OCF Cloud. во время регистрации устройства. OCF Cloud проверяет, что это тот же токен доступа, который был возвращен устройству во время процесса регистрации устройства или во время обновления токена. Если Устройство пыталось установить соединение и предоставленные значения были подтверждены облаком OCF как правильные, OCF Cloud отправляет ответ с указанием оставшегося времени жизни связанного токена доступа (значение свойства "expiresin").

Ресурс "oic.r.session" определен в таблице 5.

Table 5 – Definition of the "oic.r.session" Resource

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fixed URI** | **Resource Type Title** | **Resource Type ID ("rt" value)** | **OCF**  **Interfaces** | **Description** | **Related Functional Interaction** |
| /oic/sec/session | Account Session | oic.r.session | oic.if.basel ine | Resource that enables a Device to manage its session using login or  logout | N/A |

1. [Table 6](#_bookmark44) defines the Properties of the "oic.r.session" Resource.

Table 6 – Properties of the "oic.r.session" Resource

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Property Title** | **Property Name** | **Value Type** | **Value Rule** | **Acces s**  **Mode** | **Mandat ory** | **Description** |
| User ID | uid | string | uuid | W | Yes | User ID provided by Device Registration  process. Format pattern according to IETF RFC 4122. |
| Device UUID | di | string | uuid | W | Yes | Unique Device UUID registered for a Device. Format pattern according to IETF RFC 4122. |
| Access Token | accesstoken | string | A string of at least one character | W | Yes | Access Token used to authorize and associate the TLS connection for  communication with the OCF Cloud with the Device UUID |
| Login Status | login | boolean | N/A | W | Yes | Action for the request: true = login, false = logout |
| Token Expiration | expiresin | integer | N/A | R | Yes | Remaining Access Token life time in seconds (-1 if permanent)  This Property is only provided to Device  during connection establishment (when "login"  Property Value equals "true"), it’s not available otherwise |

## 9.3 Ресурс обновления токена учетной записи

Ресурс «/ oic / sec / tokenrefresh» используется устройством для обновления токена доступа.

Ресурс «/ oic / sec / tokenrefresh» размещен в облаке OCF. Он должен быть доступен только по защищенному каналу; незащищенный канал не может получить доступ к этому Ресурсу.

Устройство должно использовать «/oic/sec/tokenrefresh» для обновления токена доступа с помощью облака OCF, когда время, указанное в «expiresin», приближается.

Операция RETRIEVE для ресурса "/ oic / sec / tokenrefresh" Облака OCF не разрешена, и ожидается, что Облако OCF отклонит все попытки выполнить такую операцию.

Операция UPDATE для ресурса "/ oic / sec / tokenrefresh" определяется следующим образом.

- Устройство, пытающееся обновить токен доступа, должно отправить сообщение с запросом UPDATE на ресурс «/ oic / sec / tokenrefresh» облака OCF. Сообщение должно включать в себя значение свойства "di" ресурса "/ oic / d", "uid" и "refreshtoken", возвращенные OCF Cloud.

- Ожидается, что ответ OCF Cloud будет включать «refreshtoken», новый «accesstoken» и «expiresin». Полученный «accesstoken» должен обрабатываться устройством как маркер доступа с типом маркера «носитель», как определено в IETF RFC 6750. Этот маркер доступа является разрешением для устройства на доступ к облаку OCF. Полученный «маркер обновления» должен обрабатываться устройством как маркер обновления, как определено в IETF RFC 6749. Полученный «маркер обновления» может быть новым маркером обновления или тем же, который был предоставлен устройством в запросе UPDATE. В случае, когда OCF Cloud предоставляет новый отдельный «маркер обновления», Устройство должно отбросить старое значение.

Значения ответа OCF Cloud «refreshtoken», «accesstoken» и «expiresin» надежно хранятся на Устройстве.

Ресурс «oic.r.tokenrefresh» определен в таблице 7.

Table 7 – Definition of the "oic.r.tokenrefresh" Resource

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fixed URI** | **Resource Type Title** | **Resource Type ID ("rt" value)** | **OCF**  **Interfaces** | **Description** | **Related Functional Interaction** |
| /oic/sec/tokenrefresh | Token Refresh | oic.r.tokenrefresh | oic.if.basel ine | Resource to manage the access-token using refresh token | N/A |

1. [Table 8](#_bookmark47) defines the Properties of the "oic.r.tokenrefresh" Resource.
2. **Table 8 – Properties of the "oic.r.tokenrefresh" Resource**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Property Title** | **Property Name** | **Value Type** | **Value Rule** | **Acce ss Mode** | **Mandat ory** | **Description** |
| User ID | uid | string | uuid | W | Yes | User ID provided by Sign-up process. Format pattern according to IETF RFC 4122. |
| Device UUID | di | string | uuid | W | Yes | Unique Device UUID registered for an OCF Cloud User account. Format pattern according to IETF RFC 4122. |
| Refresh Token | refreshtoke n | string | A string of at least one character | RW | Yes | Refresh token can be used to refresh the Access Token before getting expired. |
| Access Token | accesstoke n | string | A string of at least one character | R | Yes | Access Token used to authorize and associate the TLS connection for  communication with the OCF Cloud with the Device UUID. |
| Token Expiration | expiresin | integer | - | R | Yes | Access Token life time in seconds (-1 if permanent). |

# 10. Рекомендации по усилению безопасности

## 10.1 Общие рекомендации по усилению безопасности

В дополнение к списку конфиденциальных данных, приведенному в таблице 75 ISO / IEC 30118-2, любое Устройство, реализующее возможности подключения к облаку OCF, также должно обеспечивать разумную защиту информации в таблице 9.

Table 9 – Sensitive Data related to OCF Cloud

|  |  |  |
| --- | --- | --- |
| **Data** | **Integrity protection** | **Confidentiality protection** |
| OCF Cloud URL | Yes | Not required |
| OCF Cloud Identity | Yes | Not required |

# Приложение А (обязательное) Определения типов ресурсов

## A.1 Список определений типов ресурсов

Все пункты в Приложении A описывают типы ресурсов с языком определения RESTful API. Определения типов ресурсов, представленные в Приложении A, отформатированы для удобства чтения и поэтому могут иметь дополнительные разрывы строк.

Таблица A.1 содержит список определенных ресурсов безопасности в этом документе.

Table A.1 – Alphabetized list of security Resources

|  |  |  |
| --- | --- | --- |
| **Friendly Name (informative)** | **Resource Type (rt)** | **Clause** |
| Account | oic.r.account | [A.2](#_bookmark54) |
| Account Session | oic.r.session | [A.3](#_bookmark63) |
| Account Token Refresh | oic.r.tokenrefresh | [A.4](#_bookmark72) |

## A.2 Account Token

### A.2.1 Introduction

Sign-up using generic account provider.

### A.2.2 Well-known URI

/oic/sec/account

### A.2.3 Resource type

The Resource Type is defined as: "oic.r.account".

### A.3.5 Property definition

[Table A.4](#_bookmark69) defines the Properties that are part of the "oic.r.session" Resource Type.

### Table A.4 – The Property definitions of the Resource with type "rt" = "oic.r.session".

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Property name** | **Value type** | | **Mandatory** | **Access mode** | | **Description** |
| if | array: see schema | | No | Read Only | | The interface set supported by this Resource. |
| expiresin | integer | | Yes | Read Only | | Remaining  Access Token life time in seconds (-1 if permanent). This  Property is only provided to |
|  |  | |  |  | | Device during connection  establishment (when "login" Property Value equals "true"), it’s not available  otherwise. |
| rt | array:  schema | see | No | Read | Only | Resource Type of the Resource. |
| id | multiple types: see schema | | No | Read | Write |  |
| n | multiple types: see schema | | No | Read | Write |  |
| di | string | | Yes | Write | Only | Unique Device UUID registered for a Device. Format pattern  according to IETF RFC 4122. |
| accesstoken | string | | Yes | Write | Only | Access Token used to authorize and associate  the TLS  connection for communication with the OCF Cloud with the  Device UUID. |
| uid | string | | Yes | Write | Only | User ID provided by Device Registration  process. Format pattern  according to IETF RFC 4122. |
| login | boolean | | Yes | Write | Only | Action for the request: true =  login, false = logout. |

**A.3.6 CRUDN behaviour**

[Table A.5](#_bookmark71) defines the CRUDN operations that are supported on the "oic.r.session" Resource Type.

**Table A.5 – The CRUDN operations of the Resource with type "rt" = "oic.r.session".**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Create** | **Read** | **Update** | **Delete** | **Notify** |
|  |  | post |  |  |

## A.4 Token Refresh

### A.4.1 Introduction

Obtain fresh Access Token using the refresh token, client should refresh Access Token before it expires.

### A.4.2 Well-known URI

/oic/sec/tokenrefresh

### A.4.3 Resource type

The Resource Type is defined as: "oic.r.tokenrefresh".

### A.4.5 Property definition

994 [Table A.6](#_bookmark78) defines the Properties that are part of the "oic.r.tokenrefresh" Resource Type.

### Table A.6 – The Property definitions of the Resource with type "rt" = "oic.r.tokenrefresh".

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Property name** | **Value type** | | **Mandatory** | **Access mode** | | **Description** | |
| refreshtoken | string | | Yes | Write | Only | Refresh can be refresh Access  before expired. | token used to  the Token getting |
| uid | string | | Yes | Write | Only | User ID provided by Sign-up process. Format pattern  according to IETF RFC 4122. | |
| di | string | | Yes | Write | Only | Unique Device UUID registered for an OCF Cloud User account. Format pattern according to  IETF RFC 4122. | |
| if | array:  schema | see | No | Read | Only | The interface set supported by this  Resource. | |
| expiresin | integer | | Yes | Read | Only | Access Token life time in  seconds (-1 if permanent). | |
| accesstoken | string | | Yes | Read | Only | Access Token used to authorize and associate  the TLS  connection for communication with the OCF Cloud with the  Device UUID. | |
| refreshtoken | string | | Yes | Read | Only | Refresh can be refresh Access  before expired. | token used to  the Token getting |
| n | multiple types: see schema | | No | Read | Write |  | |
| rt | array: see schema | | No | Read Only | | Resource Type of the Resource. | |
| id | multiple types: see schema | | No | Read Write | |  | |

### A.4.6 CRUDN behaviour

[Table A.7](#_bookmark80) defines the CRUDN operations that are supported on the "oic.r.tokenrefresh" Resource Type.

### Table A.7 – The CRUDN operations of the Resource with type "rt" = "oic.r.tokenrefresh".

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Create** | **Read** | **Update** | **Delete** | **Notify** |
|  |  | post |  |  |