Iotivity
OCF Guide

Iotivity User Guide (DRAFT)

The content of this UG is drawn from the Iotivity Documentation and Wiki pages.

summary

Contents

Iotivity User Guide Abstract

The content of this UG is drawn from the Iotivity Documentation and Wiki pages.

summary

Notice

Notice

Topics:

- Trademarks

Here's a shortdesc...

This product is meant for educational purposes only. Some of the trademarks mentioned in this product appear for identification purposes only. Not responsible for direct, indirect, incidental or consequential damages resulting from any defect, error or failure to perform. Any resemblance to real persons, living or dead is purely coincidental. Void where prohibited. Some assembly required. Batteries not included. Use only as directed. Do not use while operating a motor vehicle or heavy equipment. Do not fold, spindle or mutilate. Do not stamp. No user-serviceable parts inside. Subject to change without notice. Drop in any mailbox. No postage necessary if mailed in the United States. Postage will be paid by addressee. Post office will not deliver without postage. Some equipment shown is optional. Objects in mirror may be closer than they appear. Not recommended for children. Your mileage may vary.

No other warranty expressed or implied. This supersedes all previous notices.

Trademarks

Preface

Preface

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed finibus rutrum pharetra. Etiam porttitor purus non felis semper, vel lobortis sem ullamcorper. Donec ut interdum turpis, non placerat lacus. Quisque placerat lacus id magna rhoncus, nec lacinia massa blandit. Pellentesque faucibus, dolor vitae accumsan pretium, arcu mauris eleifend felis, a iaculis justo nisl vel quam. Fusce laoreet turpis et finibus molestie. Suspendisse maximus scelerisque dui, vel vestibulum libero porttitor id. In et libero erat. Integer et dolor eget tellus dictum fermentum. Nunc velit elit, eleifend et placerat non, convallis eget mauris. Fusce congue ipsum ac commodo tincidunt. Mauris varius vulputate ante sit amet consequat. Cras et finibus est, fringilla vestibulum turpis. Quisque consectetur felis at nibh vulputate, id bibendum sapien venenatis. Mauris dapibus accumsan ornare.

About this Document

The content of this UG is drawn from the Iotivity Documentation and Wiki pages.

Revision: 0.1

Acknowledgements

acks here...

Part I

Overview

This is the overview of Part I ...

Fusce porta leo sem, non luctus lectus fermentum et. Nunc lacus mi, ultricies et ex sit amet, porttitor convallis ligula. Praesent convallis nibh id lectus pellentesque, et rutrum nibh molestie. Nunc ac convallis lectus. Aliquam eu sem eget est mollis iaculis quis eu mauris. Vestibulum iaculis turpis a urna sagittis, vitae pellentesque augue venenatis. Fusce ut efficitur arcu. Mauris volutpat velit quis purus consequat, sit amet molestie mauris aliquam. Curabitur dolor eros, congue eget erat sed, suscipit auctor erat. Cras convallis ex in sem placerat ornare non at felis.

Part II

Data Model

OCF formally defines a sophisticated resource-based data model.

Part III

Security

Topics:

OCF defines a sophisticated security model...

Chapter

1

Security Overview

OCF security is built on two orthogonal pillars: data integrity and confidentiality, and access control.

The integrity and confidentiality of in-flight data is handled by transport-level encryption (DTLS/TLS). The integrity of data at rest is the responsibility of the implementation; OCF provides some recommendations but no mandatory features.

Access control is composed of authentication and authorization. Authentication is based on cryptographic credentials; authorization is based on Access Control Lists.

Encryption and access control are orthogonal. All access to resources is governed by access control, whether communications are encrypted or not. It follows that every resource must have an ACL.

Provisioning of security-related resources (identity, credentials, ACLs) is an important aspect of OCF security.

- Security Services
- Security Management Service
- Security Resources
- Security Protocols
- etc...

Chapter

2

Security Configuration and Provisioning

Topics:

Security provisioning and configuration...

Concepts:

- Device Identity
- Device Credential
- Device Ownership
- Device Onboarding
- Ownership Transfer
- Security Provisioning
- Security Configuration

Security states:

- *RESET*
- *Ready For Ownership Transfer Method (RFOTM)*
- *Ready For Provisioning (RFPRO)*
- *Ready For Normal Operation (RFNOP)*
- *Soft Reset*

Dynamic Security Configuration and Provisioning

Dynamic security provisioning and configuration...

Static Configuration and Provisioning

For development and testing purposes, static provisioning configuration may be more convenient that dynamic configuration.

```
{
   "acl": {
       "aclist2": [
           {
               "aceid": 1,
               "subject": { "conntype": "anon-clear" },
               "resources": [
                   { "href": "/oic/res" },
                   { "href": "/oic/d" },
                   { "href": "/oic/p" },
                   { "href": "/oic/sec/doxm" }
               ],
               "permission": 2
           },
           {
               "aceid": 2,
               "subject": { "conntype": "auth-crypt" },
               "resources": [
                   { "href": "/oic/res" },
                   { "href": "/oic/d" },
                   { "href": "/oic/p" },
                   { "href": "/oic/sec/doxm" }
               ],
               "permission": 2
           },
           {
               "aceid": 3,
               "subject": { "uuid":
"32323232-3232-3232-3232-323232323232" },
               "resources": [{ "wc": "*" }],
               "permission": 7
           },
           {
               "aceid": 4,
               "subject": { "uuid":
"31393139-3139-3139-3139-313931393139" },
               "resources": [{ "href": "/a/led" }],
               "permission": 7
           },
           {
               "aceid": 5,
               "subject": { "uuid":
"37373737-3737-3737-3737-373737373737" },
               "resources": [{ "href": "/a/led" }],
               "permission": 6
           }
       ],
       "rowneruuid" : "31313131-3131-3131-3131-313131313131"
   },
   "pstat": {
```

```
        "dos": {"s": 3, "p": false},
        "isop": true,
        "rowneruuid": "31313131-3131-3131-3131-313131313131",
        "cm": 0,
        "tm": 0,
        "om": 4,
        "sm": 4
        },
    "doxm": {
        "oxms": [0],
        "oxmsel": 0,
        "sct": 9,
        "owned": true,
        "deviceuuid": "31313131-3131-3131-3131-313131313131",
        "devowneruuid": "32323232-3232-3232-3232-323232323232",
        "rowneruuid": "31313131-3131-3131-3131-313131313131"
    },
    "cred": {
        "creds": [
            {
                "credid": 1,
                "subjectuuid": "32323232-3232-3232-3232-323232323232",
                "credtype": 1,
                "period": "20150630T060000/20990920T220000",
                "privatedata": {
                    "data": "AAAAAAAAAAAAAAAA",
                    "encoding": "oic.sec.encoding.raw"
                }
            },
            {
                "credid": 2,
                "subjectuuid": "31393139-3139-3139-3139-313931393139",
                "credtype": 1,
                "period": "20150630T060000/20990920T220000",
                "privatedata": {
                    "data": "BBBBBBBBBBBBBBBB",
                    "encoding": "oic.sec.encoding.raw"
                }
            }
        ],
        "rowneruuid": "32323232-3232-3232-3232-323232323232"
    }
}
```

A	intercooler
B	expansion tank

Figure 1: Configuration file for server

An SVR configuration file for a client that owns the server:

```
      {
    "acl": {
        "aclist2": [
            {
                "aceid": 1,
                "subject": { "conntype": "anon-clear" },
                "resources": [
                    { "href": "/oic/res" },
                    { "href": "/oic/d" },
```

```
                    { "href": "/oic/p" },
                    { "href": "/oic/sec/doxm" }
                ],
                "permission": 2
            },
            {
                "aceid": 2,
                "subject": { "conntype": "auth-crypt" },
                "resources": [
                    { "href": "/oic/res" },
                    { "href": "/oic/d" },
                    { "href": "/oic/p" },
                    { "href": "/oic/sec/doxm" }
                ],
                "permission": 2
            }
        ],
        "rowneruuid" : "32323232-3232-3232-3232-323232323232"
    },
    "pstat": {
        "dos": {"s": 3, "p": false},
        "isop": true,
        "rowneruuid": "32323232-3232-3232-3232-323232323232",
        "cm": 0,
        "tm": 0,
        "om": 4,
        "sm": 4
        },
    "doxm": {
        "oxms": [0],
        "oxmsel": 0,
        "sct": 9,
        "owned": true,
        "deviceuuid": "32323232-3232-3232-3232-323232323232",
        "devowneruuid": "32323232-3232-3232-3232-323232323232",
        "rowneruuid": "32323232-3232-3232-3232-323232323232"
    },
    "cred": {
        "creds": [
            {
                "credid": 1,
                "subjectuuid": "31313131-3131-3131-3131-313131313131",
                "credtype": 1,
                "privatedata": {
                    "data": "AAAAAAAAAAAAAAAA",
                    "encoding": "oic.sec.encoding.raw"
                }
            }
        ],
        "rowneruuid": "32323232-3232-3232-3232-323232323232"
    }
}
```

Chapter

3

Encryption Services

Topics:

Data integrity and confidentiality are ensured via transport layer encryption. OCF requires support for DTLS for UDP and TLS for TCP communications.

Establishment of a secure communication channel using (D)TLS requires two things: and agreed-upon cipher suite, and cryptographic credentials. The latter are used for mutual authentication: servers authenticate clients, and vice-versa.

It follows that OCF devices must be configured with the credentials and the cipher suites necessary for secured communication. Static configuration provisions the necessary information at build time or during runtime initialization (e.g. by reading a fixed configuration file). Devices may also be configured dynamically, over the network. OCF defines a detailed model of dynamic provisioning (described in Provisioning Services on page 30).

Related information

The TLS Handshaking Protocols (IETF RFC 5246)
Intro to DTLS
An overview of the SSL or TLS handshake

(D)TLS Configuration

OCF devices must be properly configure to use (D)TLS security.

(D)TLS requires that communicating parties negotiate a *Cipher Suite* and exchange the information necessary for mutual authentication.

If Symmetric Key credentials are being used, each party must be provisioned with the ID and credential of the other. See

(D)TLS Cipher Suites

Establishing a (D)TLS session requires negotiation of a *Cipher Suite*.

OCF supports the following cipher suites:

- TLS_ECDH_ANON_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ANON_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA256
- TLS_PSK_WITH_AES_128_CCM_8 (* 8 OCTET Authentication tag *)
- TLS_PSK_WITH_AES_256_CCM_8
- TLS_PSK_WITH_AES_128_CCM (* 16 OCTET Authentication tag *)
- TLS_PSK_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- ...etc...

See section 11.2 of the OCF Security Specification, version 1.3.0

Related information

RFC 4279: Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)

RFC 4492: Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)

RFC 5489: ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)

RFC 6655: AES-CCM Cipher Suites for Transport Layer Security (TLS)

RFC 7251: AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS

(D)TLS Authentication

(D)TLS requires mutual authentication using cryptographic credentials

(D)TLS requires mutual authentication

Chapter 4

Access Control Services

Topics:

OCF access control is provided through authentication and authorization services.

blah

Authentication Services

Authentication is the process of verifying the identity of a participant in a transaction, such as the sender of a request message. OCF authentication is based on cryptographic credentials.

There are two basic types of cryptography used for credential authentication, symmetric and asymmetric.

Symmetric cryptography uses the same (secret) cryptographic key for both encryption and decryption. The key is often called a "Pre-Shared Key" (PSK), since both parties to the transaction must be provisioned with it.

Asymmetric cryptography uses a pair of keys, one a private (secret) key and the other a public key. The private key is never shared. Senders use their private key to "sign" their messages, and receivers use the public key of the sender to verify the signature. Asymmetric cryptography is often referred to as "Public-Key Cryptography".

Closely related to asymmetric cryptography is the use of "certificate authorities" to certify ownership of key pairs. Using a public key to verify the signature of a message ensures that the sender is in possession of the private key that signed the message; it does not, however, authenticate the *identity* of the sender. A certificate authority (CA) is an entity that issues digital certificates that certify ownership of a public key by the entity named in the certificate.

OCF authentication services support the following credential types:

- Symmetric Pairwise Key (Pre-Shared Key or PSK)
- Symmetric Group Key
- Asymmetric Signing Key
- Asymmetric Signing Key with Certificates
- PIN or Password
- Assymetric Encryption Key

OCF engines maintain a Credentials Database that stores credentials and associated device IDs. The database is accessible as a resource (/oic/sec/cred). Provisioning of the database is described in Provisioning Services on page 30.

When symmetric keys are used, OCF authentication services attach to outgoing messages the device id and credential (PSK) of the sending device, and, on the receiving end, extract the device ID and credential from the incoming message and look them up in the Credentials DB. If found, the messages is marked as authenticated and processing continues; otherwise, the message is rejected with an UNAUTHENTICATED response.

When asymmetric credentials are used, OCF authentication services use the sender's private key to sign outgoing messages, and on the receiving end use the sender's public key to verify the signature. ... etc. ...

Disposition: / Status:
TODO: flesh this out.

Related information

Authentication (Wikipedia)

Certificate Authority (Wikipedia)

Public-key Certificate (Wikipedia)

Symmetric-key Algorithm (Wikipedia)

Public-key Cryptography

Authorization Services

OCF authorization services grant or deny access requests.

blah

Chapter 5

Security Resources

Topics:

Security Virtual Resources

Security Virtual Resources (SVRs) ...

- /oic/sec/doxm - Device Ownership Transfer Management
- /oic/sec/pstat - Provisioning Status
- /oic/sec/cred - Credentials
- /oic/sec/acl2 - Access Control Lists
- /oic/sec/amacl - Access Management Service ACLs
- /oic/sec/sacl - Secure ACLs

Chapter

6

Security Management Services

Topics:

- Identity Provisioning and Management
- Ownership (Registration) Management
- Provisioning Services

Security management overview...

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce eget enim lobortis, laoreet turpis in, placerat urna. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Fusce congue pulvinar bibendum. Duis luctus, est a luctus sollicitudin, velit quam suscipit mauris, ut mollis tortor dui at mauris. Mauris sed pellentesque dui. Sed efficitur vulputate lectus, in varius erat molestie et. Nam consectetur nulla non nulla ultrices vestibulum nec quis tellus. Nulla sit amet congue libero, sed pulvinar tellus. Phasellus commodo, risus vitae hendrerit venenatis, eros lacus tempor turpis, at consequat tortor massa id neque. Mauris pellentesque et elit sed semper. Nam odio urna, ultrices non tristique maximus, pulvinar sit amet tortor.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin augue massa, ultrices nec maximus quis, ullamcorper commodo libero. Quisque finibus lectus enim, et maximus elit sagittis sit amet. Quisque vulputate feugiat metus tristique venenatis. Cras porta et urna ut consequat. Praesent sed imperdiet urna. Curabitur sit amet massa ex. Nunc gravida, tellus id bibendum pharetra, nisi risus posuere ligula, a blandit turpis libero sit amet tellus. Fusce a tincidunt erat, quis malesuada ante. Nullam placerat purus a condimentum euismod. Praesent lacinia eros vel magna bibendum, sed eleifend ligula convallis. Cras viverra ultricies leo, non interdum massa porta eu. Proin pharetra lobortis nunc, vitae cursus justo convallis eu.

Praesent volutpat, nisl vitae lacinia efficitur, odio magna elementum velit, ullamcorper gravida lectus est non mi. Quisque dignissim vitae turpis ut pulvinar. Duis et nunc ac neque vehicula faucibus a eu quam. Praesent vestibulum fermentum mauris, sed feugiat tellus. Morbi id felis mattis, hendrerit turpis sed, convallis nisl. Donec tempus tempor volutpat. Etiam venenatis est nec mauris egestas condimentum. Quisque sit amet maximus nisl. In vitae quam euismod, dignissim magna vel, bibendum orci.

Fusce porta leo sem, non luctus lectus fermentum et. Nunc lacus mi, ultricies et ex sit amet, porttitor convallis ligula. Praesent convallis nibh id lectus pellentesque, et rutrum nibh molestie. Nunc ac convallis lectus. Aliquam eu sem eget est mollis iaculis quis eu mauris. Vestibulum iaculis turpis a urna sagittis, vitae pellentesque augue venenatis. Fusce ut efficitur arcu. Mauris volutpat velit quis purus consequat, sit amet molestie mauris aliquam. Curabitur dolor eros, congue eget erat sed, suscipit auctor erat. Cras convallis ex in sem placerat ornare non at felis.

Identity Provisioning and Management

Every operational device on an OCF network must be provisioned with a unique *device identifier*.

blah

Ownership (Registration) Management

Every device on an OCF network must be registered to the network. OCF expresses this in terms of **device ownership**.

An OCF *Device Ownership Transfer Service* provides device registration (ownership transfer) services.

Here is another use of the *DOXS* term.

Provisioning Services

Once a device has been provisioned with an identifier and registered with the network, it must be provisioned with security resources: credentials and access control lists (ACLs).

Lorem nulla, finibus vel risus at, feugiat porttitor dolor. Duis ut nulla sit amet nisi imperdiet laoreet. Curabitur tortor nibh, feugiat eget justo at, mattis commodo tortor. Cras nec risus vel magna suscipit pharetra et quis turpis. Pellentesque hendrerit tincidunt ante, quis aliquam enim laoreet ut. Donec tristique rutrum massa ut posuere. Duis non elit dapibus, pellentesque orci a, malesuada sem. Pellentesque pulvinar erat ut dui tincidunt cursus. Nulla iaculis tempus enim, sed finibus metus viverra eu. Proin ac rhoncus libero, sit amet convallis diam. Sed eu magna volutpat, suscipit elit eu, placerat justo. Fusce varius dolor orci, eget aliquet arcu luctus rhoncus. Quisque nec diam pulvinar, ultricies urna in, bibendum mi. Curabitur id odio in diam porta molestie. Aliquam eget dui augue. Vivamus a mollis leo.

Phasellus nisl felis, faucibus non arcu eget, ultricies lobortis ipsum. Nulla nulla purus, sagittis et cursus at, porttitor a felis. Nulla ut dolor enim. Vivamus imperdiet nunc sit amet lacus laoreet tincidunt. Mauris velit quam, faucibus eu consectetur vel, hendrerit et felis. Sed mattis dapibus auctor. Vivamus posuere eget magna in congue. Proin nisl massa, venenatis sit amet tempus eget, lobortis non nisi. Cras rhoncus posuere lectus vel tincidunt.

Etiam posuere mi purus, vel elementum nisl efficitur pretium. Maecenas vehicula pellentesque mauris a tincidunt. Nullam gravida neque vel ex porttitor eleifend. Integer semper neque quis arcu aliquet luctus. Fusce tortor ligula, ornare at facilisis id, dictum eu ante. Suspendisse pulvinar ex quis ullamcorper bibendum. Curabitur non ipsum dolor.

Related information

Key Management for Updating Crypto-keys over AIR (PDF)

Credential Provisioning and Management

OCF Credential Management Services ....

blah

ACL Provisioning and Management

OCF Access Control List management services ...

blah

Part IV

Add-ons

Topics:

- Cloud Programming

Iotivity implements some add-ons...

Chapter 7

Cloud Programming

Topics:

- Cloud Server
- Cloud Client

Iotivity Cloud overview (wiki)

There are three servers and a sample client in IoTivity Cloud project. This page will guide you how to install and run cloud servers. The sample client will let you to test server and how to make clients for cloud.

Related information

Iotivity Cloud - Programming Guide (Iotivity Wiki)

Cloud Server

Cloud Client

Appendix A

User Guide Appendix

This appendix describes things that you rarely need to know.

You can consult this section when you need detailed information about a specific component.

Glossary

AMS
: **A**CL **M**anagement **S**ervice(s)

Authentication
: Authentication verifies the identity of ...

Authorization
: Authorization refers to the process of granting or denying a request to access a resource.

Cipher Suite
: A cipher suite is ...

CMS
: **C**redential **M**anagement **S**ervice(s)

DOXS
: **D**evice **O**wnership **T**ransfer **S**ervice. An OCF DOXS provides device registration (ownership transfer) services.

RESET
: **RESET**. A security state indicating the device is in the (manufacturer-defined) default security state.

RFNOP
: **R**eady **F**or **N**ormal **O**peration. A security state indicating the device is properly provisioned and configured for normal operations.

RFOTM
: **R**eady **F**or **O**wnership **T**ranser **M**ethod. A security state indicating the device is properly provisioned and configured for ownership transfer.

RFPRO
: **R**eady **F**or **PRO**visioning. A security state indicating the device is properly provisioned and configured for security resource provisioning.

Soft Reset
: **S**oft **RESET**. A security state indicating the device is not operational but is owned (registered with the network).

TBS
: **T**o **B**e **S**igned. Refers to certificates and certificate lists.

Index