OCF "Gaborone" – Remove unused abbreviations EPC, EPK, DPKP, UAID – Security WG CR 2030

Legal Disclaimer

THIS IS A DRAFT SPECIFICATION DOCUMENT ONLY AND HAS NOT BEEN ADOPTED BY THE OPEN CONNECTIVITY FOUNDATION. THIS DRAFT DOCUMENT MAY NOT BE RELIED UPON FOR ANY PURPOSE OTHER THAN REVIEW OF THE CURRENT STATE OF THE DEVELOPMENT OF THIS DRAFT DOCUMENT. THE OPEN CONNECTIVITY FOUNDATION AND ITS MEMBERS RESERVE THE RIGHT WITHOUT NOTICE TO YOU TO CHANGE ANY OR ALL PORTIONS HEREOF, DELETE PORTIONS HEREOF, MAKE ADDITIONS HERETO, DISCARD THIS DRAFT DOCUMENT IN ITS ENTIRETY OR OTHERWISE MODIFY THIS DRAFT DOCUMENT AT ANY TIME. YOU SHOULD NOT AND MAY NOT RELY UPON THIS DRAFT DOCUMENT IN ANY WAY, INCLUDING BUT NOT LIMITED TO THE DEVELOPMENT OF ANY PRODUCTS OR SERVICES. IMPLEMENTATION OF THIS DRAFT DOCUMENT IS DONE AT YOUR OWN RISK AMEND AND IT IS NOT SUBJECT TO ANY LICENSING GRANTS OR COMMITMENTS UNDER THE OPEN CONNECTIVITY FOUNDATION INTELLECTUAL PROPERTY RIGHTS POLICY OR OTHERWISE. IN CONSIDERATION OF THE OPEN CONNECTIVITY FOUNDATION GRANTING YOU ACCESS TO THIS DRAFT DOCUMENT, YOU DO HEREBY WAIVE ANY AND ALL CLAIMS ASSOCIATED HEREWITH INCLUDING BUT NOT LIMITED TO THOSE CLAIMS DISCUSSED BELOW, AS WELL AS CLAIMS OF DETRIMENTAL RELIANCE.

The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other countries. *Other names and brands may be claimed as the property of others.

Copyright © 2019 Open Connectivity Foundation, Inc. All rights reserved.

Copying or other form of reproduction and/or distribution of these works are strictly prohibited.

******* Start of changes in clause 3.1.30*******

******* End of changes *******

******* Start of changes in clause 3.2*******

******* End of changes *******

1.1 Abbreviated terms

1.1.1
AC
Access Control

1.1.2
ACE
Access Control Entry

1.1.3
ACL
Access Control List

1.1.4
AES
Advanced Encryption Standard

Note 1 to entry: See NIST FIPS 197, "Advanced Encryption Standard (AES)"

1.1.5
AMS
Access Management Service

1.1.6
CMS
Credential Management Service

1.1.7
CRUDN
CREATE, RETREIVE, UPDATE, DELETE, NOTIFY

1.1.8
CSR
Certificate Signing Request

1.1.9
CVC
Code Verification Certificate

1.1.10
ECC
Elliptic Curve Cryptography

DRAFT

1.1.11
ECDSA
Elliptic Curve Digital Signature Algorithm

1.1.12
EKU
Extended Key Usage

1.1.13
DOTS
Device Ownership Transfer Service

1.1.14
ID
Identity/Identifier

1.1.15
JSON
JavaScript Object Notation.

Note 1 to entry: See ISO/IEC 30118-1:2018.

1.1.16
JWS
JSON Web Signature.

Note 1 to entry: See IETF RFC 7515, "JSON Web Signature (JWS)"

1.1.17
KDF
Key Derivation Function

1.1.18
MAC
Message Authentication Code

1.1.19
MITM
Man-in-the-Middle

1.1.20
NVRAM
Non-Volatile Random-Access Memory

1.1.21
OC
Owner Credential

1.1.22
OCSP
Online Certificate Status Protocol

1.1.23
OBT
Onboarding Tool

DRAFT

1.1.24
OID
Object Identifier

1.1.25
OTM
Owner Transfer Method

1.1.26
OWASP
Open Web Application Security Project.

Note 1 to entry: See https://www.owasp.org/

1.1.27
PE
Policy Engine

1.1.28
PIN
Personal Identification Number

1.1.29
PPSK
PIN-authenticated pre-shared key

1.1.30
PRF
Pseudo Random Function

1.1.31
PSI
Persistent Storage Interface

1.1.32
PSK
Pre Shared Key

1.1.33
RBAC
Role Based Access Control

1.1.34
RM
Resource Manager

1.1.35
RNG
Random Number Generator

1.1.36
SBAC
Subject Based Access Control

1.1.37
SEE
Secure Execution Environment

DRAFT

1.1.38
SRM
Secure Resource Manager

1.1.39
SVR
Security Virtual Resource

1.1.40
SW
Software

1.1.41
URI
Uniform Resource Identifier

Note 1 to entry: See ISO/IEC 30118-1:2018.

1.1.42
VOD
Virtual OCF Device

Note 1 to entry: See ISO/IEC 30118-3:2018

******* Start of changes to 7.3.8 *******

1.1.1 Establishing Owner Credentials

Once the OBT and the new Device have authenticated and established an encrypted connection using one of the defined OTM methods.

Owner credentials may consist of certificates signed by the OBT or other authority, OCF Security Domain access information, provisioning functions, shared keys, or Kerberos tickets.

The OBT might then provision the new Device with additional credentials for Device management and Device-to-Device communications. These credentials may consist of certificates with signatures, PSK, etc.

DRAFT