OCF 2.3 – RBSTG: Bridging Security Editorial Cleanup – Sec WG CR 2685

Legal Disclaimer

**** Section 2 Normative References ****

Z-Wave Plus Device Type Specification

https://www.silabs.com/documents/login/miscellaneous/SDS11847-Z-Wave-Plus-Device-Type-Specification.pdf

Z-Wave Plus Role Type Specification

https://www.silabs.com/documents/login/miscellaneous/SDS14224-Z-Wave-Plus-v2-Device-Type-Specification.pdf

Zigbee 053474, *Zigbee Specification*, August 2015
http://www.zigbee.org/zigbee-for-developers/zigbee-3-0/

****** End of Change ******

****** Section 3.1 Terms and Definitions ******

3.1.y

Bridge

Note 1 to entry: The details are defined in OCF Bridging Specification.

3.1.X

Bridging Platform

Note 1 to entry: The details are defined in OCF Bridging Specification

****** End of Change ******

****** Section 3.2 Acronyms and Abbreviations ******

Symbol	Description
AC	Access Control
ACE	Access Control Entry
ACL	Access Control List
AES	Advanced Encryption Standard. See NIST FIPS 197, "Advanced Encryption Standard (AES)"
AMS	Access Management Service
CMS	Credential Management Service
CRUDN	CREATE, RETREIVE, UPDATE, DELETE, NOTIFY
CSR	Certificate Signing Request
CVC	Code Verification Certificate
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EKU	Extended Key Usage
EPC	Embedded Platform Credential
EPK	Embedded Public Key
DOTS	Device Ownership Transfer Service
DPKP	Dynamic Public Key Pair
ID	Identity/Identifier
JSON	JavaScript Object Notation. See OCF Core Specification.
JWE	JSON Web Encryption. See IETF RFC 7516, "JSON Web Encryption (JWE)"
JWS	JSON Web Signature. See IETF RFC 7515, "JSON Web Signature (JWS)"
KDF	Key Derivation Function
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NVRAM	Non-Volatile Random-Access Memory
OC	Owner Credential
OCSP	Online Certificate Status Protocol
OBT	Onboarding Tool
OCF	Open Connectivity Foundation. See OCF Core Specification.
OID	Object Identifier
OOB	Out Of Band
OTM	Owner Transfer Method
OWASP	Open Web Application Security Project. See https://www.owasp.org/
PE	Policy Engine
PIN	Personal Identification Number
PPSK	PIN-authenticated pre-shared key
PRF	Pseudo Random Function
PSI	Persistent Storage Interface
PSK	Pre Shared Key
RAML	RESTful API Modeling Language. See OCF Core Specification.
RBAC	Role Based Access Control
RM	Resource Manager
RNG	Random Number Generator
SACL	Signed Access Control List
SBAC	Subject Based Access Control
SEE	Secure Execution Environment
SRM	Secure Resource Manager
SVR	Security Virtual Resource
SW	Software

UAID	Unique Authenticable Identifier
URI	Uniform Resource Identifier. See OCF Core Specification.
VOD	Virtual OCF Device. See OCF Bridging Specification

Table 1 – Acronyms and abbreviations

****** End of Change ******

****** Section Z (introduced in CR 2595) ******

Z.1 Bridging Security

Z.1.1 Universal Requirements for Bridging to another Ecosystem

The Bridge shall go through OCF ownership transfer as any other onboardee would.

The software of an Bridge shall be field updatable. (This requirement need not be tested but can be certified via a vendor declaration.)

Each VOD shall be onboarded by an OCF OBT. Each Virtual Bridged Device should be provisioned as appropriate in the Bridged Protocol. In other words, VODs and Virtual Bridged Devices are treated the same way as physical Devices. They are entities that have to be provisioned in their network.

Each VOD shall implement the behaviour required by the OCF Core Specification and the OCF Security Specification. Each VOD shall perform authentication, access control, and encryption according to the security settings it received from the OCF OBT. Each Virtual Bridged Device shall implement the security requirements of the Bridged Protocol.

In addition, in order to be considered secure from an OCF perspective, the Bridge Platform shall use appropriate ecosystem-specific security options for communication between the Virtual Bridged Devices instantiated by the Bridge and Bridged Devices. This security shall include mutual authentication, and encryption and integrity protection of messages in the bridged ecosystem.

A VOD may authenticate itself to the DOTS using the Manufacturer Certificate Based OTM (see section 7.3.6) with the Manufacturer Certificate and corresponding private key of the Bridge which instantiated that VOD.

A VOD may authenticate itself to the OCF Cloud (see Section 10.4.1) using the Manufacturer Certificate and corresponding private key of the Bridge which instantiated that VOD.

Z.1.2 Additional Security Requirements specific to Bridged Protocols

Z.1.2.1 Additional Security Requirements specific to the AllJoyn Protocol

For AllJoyn translator, an OCF OBT shall be able to block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge, by using the Bridge Device's "oic.r.securemode" Resource specified in the OCF Bridging Specification.

Z.1.2.2 Additional Security Requirements specific to the Bluetooth LE Protocol

An Bridge shall block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge.

Z.1.2.3 Additional Security Requirements specific to the oneM2M Protocols

The Bridge shall implement oneM2M application access control as specified in the oneM2M Security Specification.

An Bridge shall block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge.

Z.1.2.4 Additional Security Requirements specific to the U+ Protocol

An Bridge shall block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge.

Z.1.2.5 Additional Security Requirements specific to the Z-Wave Protocol

An Bridge shall block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge.

Z.1.2.6 Additional Security Requirements specific to the Zigbee Protocol

An Bridge shall block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge.

****** End of Change ******

****** Change to Annex AAA.2 (BLE) ******

Figure 1 shows how communications in both ecosystems of OCF-BLE Bridge Platform are secured by their own security.

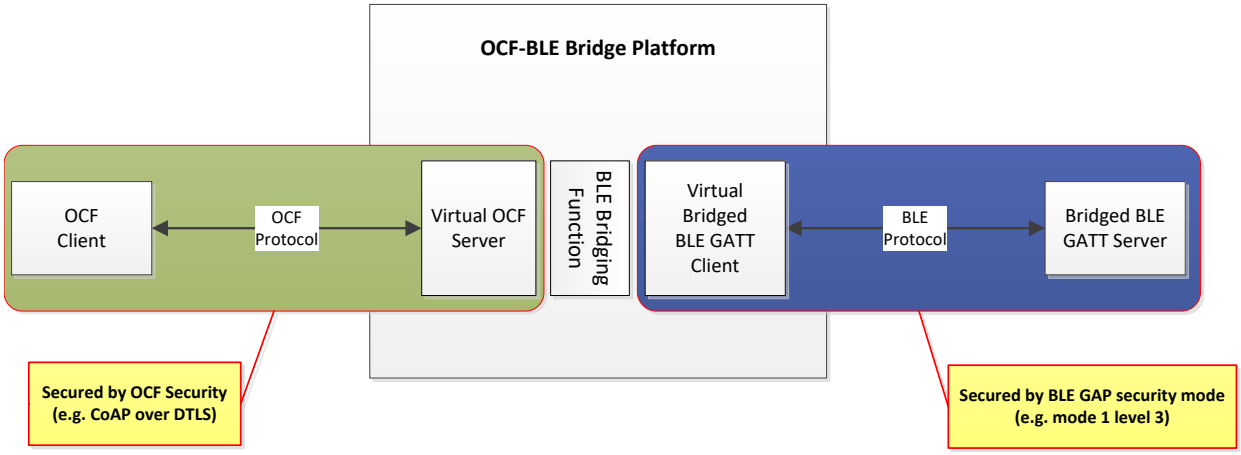

Figure 1 Security in OCF-BLE Bridge

****** End of Change ******

****** Change to Annex AAA.5 (Z-Wave) ******

Figure 3 presents how OCF Client and Bridged Z-Wave Server communicate based upon their own security.

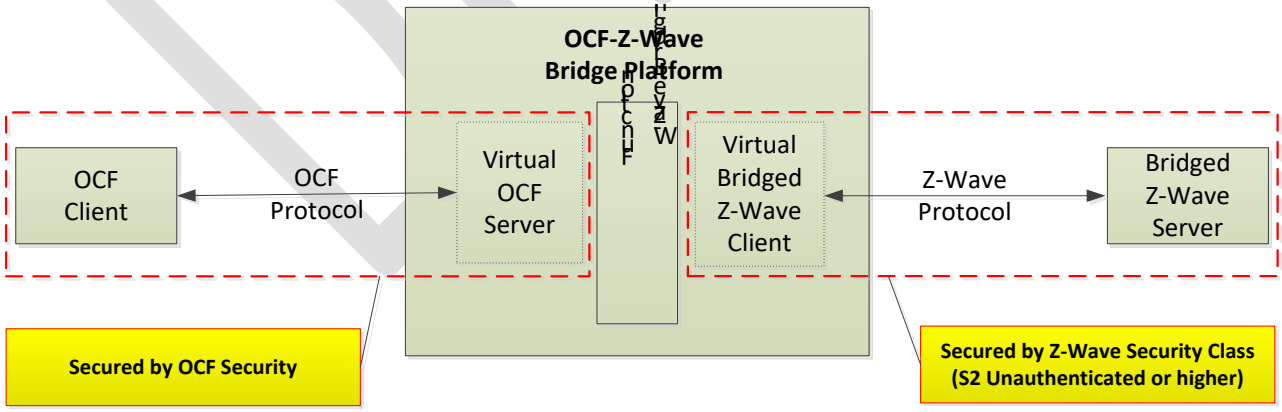

Figure 2 Security between OCF Client and Bridged Z-Wave Server

****** End of Change ******

****** Change to Annex AAA.6 (Zigbee) ******

Figure 3 shows how communications in both ecosystems of OCF-Zigbee Bridge Platform are secured by their own security.

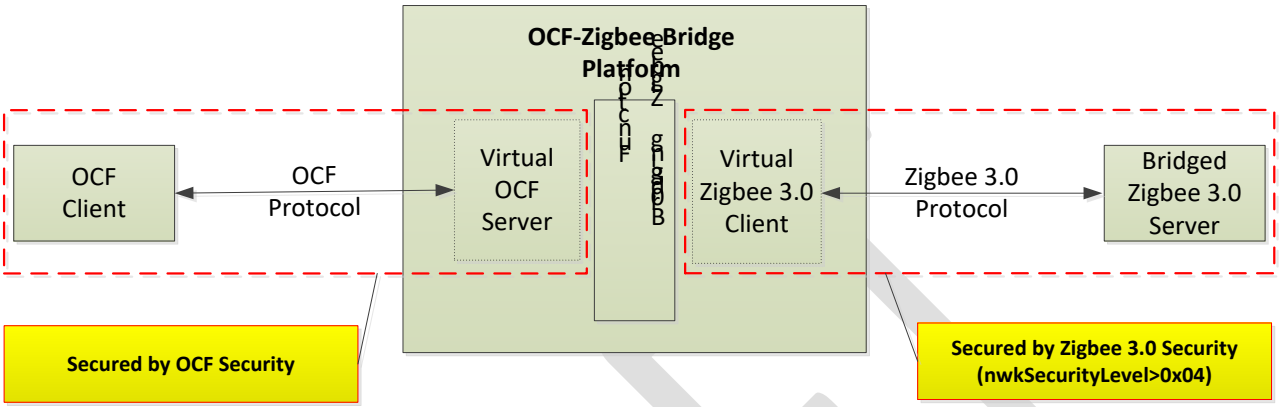

Figure 3 Security for OCF and Zigbee 3.0

****** End of Change ******