OCF “Ipanema” – End-to-End Security (OBT Spec changes) – Security WG CR 3258

Legal Disclaimer

Changes to clauses 2 & 3

1 Scope

This document defines mechanisms supported by an OCF Onboarding Tool (OBT). This document contains security normative content for the OBT and may contain informative content related to the OCF base or OCF Security Specification other OCF documents.

2 Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IETF RFC 8613, *Object Security for Constrained RESTful Environments (OSCORE)*, July 2019 https://www.rfc-editor.org/info/rfc8613

ISO/IEC 30118-1:2018 Information technology -- Open Connectivity Foundation (OCF) Specification -- 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 30118-2:2018 Information technology – Open Connectivity Foundation (OCF) Specification – 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 30118-3:2018 Information technology -- Open Connectivity Foundation (OCF) Specification -- Part 3: Bridging specification
https://www.iso.org/standard/74240.html
Latest version available at:https://openconnectivity.org/specs/OCF_Bridging_Specification.pdf

ISO/IEC 30118-7:2018, Information technology – Open Connectivity Foundation (OCF) Specification – Part 7: Wi-Fi Easy Setup specification
Latest version available at:
https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification.pdf

NIST Special Publication 800-90A Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

Open Connectivity Foundation (OCF) Specification – Cloud Security Specification
Latest version available at:
https://openconnectivity.org/specs/OCF_Cloud_Security_Specification.pdf

3 Terms, definitions, and abbreviated terms

3.1

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO/IEC 30118-2 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/

End of changes to clauses 2 & 3

NEW sub clause of Clause 6

6.X Provisioning an OSCORE Security Context for End-to-End Security of Unicast Messages

ISO/IEC 30118-2:2018 describes how Object Security for Constrained RESTful Environments (OSCORE) protocol IETF RFC 8613 for End-to-End Security of Unicast Messages.

OSCORE communication between two Devices is enabled by provisioning an OSCORE Security Context in a credential entry of the "/oic/sec/cred" Resource in each of the two Devices. The present clause provides the requirements on the CMS for this provisioning. For the purposes of this description, let Device A and Device B denote the two Devices.

Prior to provisioning, the CMS generates three values: idA; idB; and an OSCORE Master Secret.

– The CMS selects a value for idA (identifying the OSCORE Security Context for messages sent from Device A to Device B) conforming to the following criteria:
  – The total length of idA in bits shall be a multiple of 8 between 16 and 56 inclusive, which corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14 characters inclusive.
  – The first byte of idA shall be 0x01.

NOTE 1: The value 0x01 is the OSCORE Identifier Namespace Prefix value assigned for "Directly Provisioned OSCORE Security Context" in ISO/IEC 30118-2.

  – The value of idA should be distinct from all values of "recipientid" in credential entries on Device B at the time of provisioning.

– The CMS selects a value for idB (identifying the OSCORE Security Context for messages sent from Device B to Device A) conforming to the following criteria:
  – The total length of idB in bits shall be a multiple of 8 between 16 and 56 inclusive, which corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14 characters inclusive.
  – The first byte of idB shall be 0x01. See Note 1.
  – The value of idB should be distinct from all values of "recipientid" in credential entries on Device A at the time of provisioning.

– The CMS shall generate a 256-bit secret value (the OSCORE Master Secret). The CMS should use a NIST SP-800-90A-compliant RNG to guarantee sufficient entropy.

The CMS then independently provisions credential entries to Device A and Device B.

The CMS provisions the following credential entry to Device A:

– The "subjectuuid" shall be the Device UUID of Device B (that is, the value of "/oic/sec/doxm:deviceuuid" on Device B).

– The "credtype" shall have the value 64.

NOTE 2: The value 64 is the "credtype" value specified for a directly provisioned OSCORE Security Context in ISO/IEC 30118-2.

– The "privatedata" Property of the credential entry shall be the OSCORE Master Secret generated by the CMS.

– The "oscore" Property shall be present, and shall include the following Properties:

  – The "senderid" Property shall be set to the lowercase hexadecimal representation of idA with the "0x" encoding prefix omitted.

  – The "recipientid" Property shall be set to the lowercase hexadecimal representation of idB with the "0x" encoding prefix omitted.

The CMS separately provisions the following credential entry to Device B:

– The "subjectuuid" shall be the Device UUID of Device A (that is, the value of "/oic/sec/doxm:deviceuuid" on Device A).

– The "credtype" shall have the value 64. See Note 2.

– The "privatedata" Property of the credential entry shall be the OSCORE Master Secret generated by the CMS.

– The "oscore" Property shall be present, and shall include the following Properties:

  – The "senderid" Property shall be set to the lowercase hexadecimal representation of idB with the "0x" encoding prefix omitted.

  – The "recipientid" Property shall be set to the lowercase hexadecimal representation of idA with the "0x" encoding prefix omitted.