OCF "Ipanema" – Distributed Key Management for Secure Multicast – Security WG CR 1967

Legal Disclaimer

IETF group core backgrounds:

https://tools.ietf.org/html/rfc8613

Group IDs:
Straw-man proposal of Group ID format:
https://tools.ietf.org/html/draft-ietf-core-oscore-groupcomm-09#appendix-C

senderid/recipientid vs groupid in the Request flow:
How the Group ID must be set as the "ID Context":
https://tools.ietf.org/html/draft-ietf-core-oscore-groupcomm-09#section-2.1.1
(Whereas in OSCORE contexts for unicast, we use the recommended default for "ID Context" from RFC 8613, i.e. an empty string)

How Clients use "senderid" and "groupid" in Requests:
https://tools.ietf.org/html/draft-ietf-core-oscore-groupcomm-09#section-4.2
https://tools.ietf.org/html/draft-ietf-core-oscore-groupcomm-09#section-8.2

Other recommendations in the group OSCORE draft:
AAD modifications for group OSCORE over OSCORE:
https://tools.ietf.org/html/draft-ietf-core-oscore-groupcomm-09#section-4.3
(If we're not using signatures in phase 1, may be we can skip doing this until phase 2)

Group flag bit:
https://tools.ietf.org/html/draft-ietf-core-oscore-groupcomm-09#section-11.1
(Perhaps we don't need this for phase 1)

Changes to Core Security SPEC

Terms & Definitions

1.1
Simple Secure Multicast

delivery of UPDATE request messages from a Client to a group of Servers using network-layer multicast, where the messages are protected with a simple security mechanism

1.2

Simple Secure Multicast Client Context

OSCORE Security Context parameters provisioned to the Client of a *Simple Secure Multicast Group* to enable *End-to-End Security* of *Simple Secure Multicast* requests sent to Servers of that *Simple Secure Multicast Group*

1.3

Simple Secure Multicast Group

group of Servers and one (1) associated Client provisioned with credentials to enable *Simple Secure Multicast* from the Client to the set of Servers

1.4

Simple Secure Multicast Request

OSCORE-protected UPDATE request message delivered from a Client to a group of Servers using *Simple Secure Multicast*

1.5

Simple Secure Multicast Server Context

OSCORE Security Context parameters provisioned to Servers of a *Simple Secure Multicast Group* to enable *End-to-End Security* of *Simple Secure Multicast* requests sent by the Client of that *Simple Secure Multicast Group*

Symbols and Abbreviations

SSM	Simple Secure Multicast

Changes to Clause 5.1, Core Sec Spec

5.1 Security Model of Operation

Editor's note: insert immediately after new text introduced in CR1657

As shown in Figure 1W, Simple Secure Multicast (SSM) enables a Client to securely communicate an UPDATE request to a group of Servers with a single non-confirmable UPDATE request delivered via networking-layer multicast.

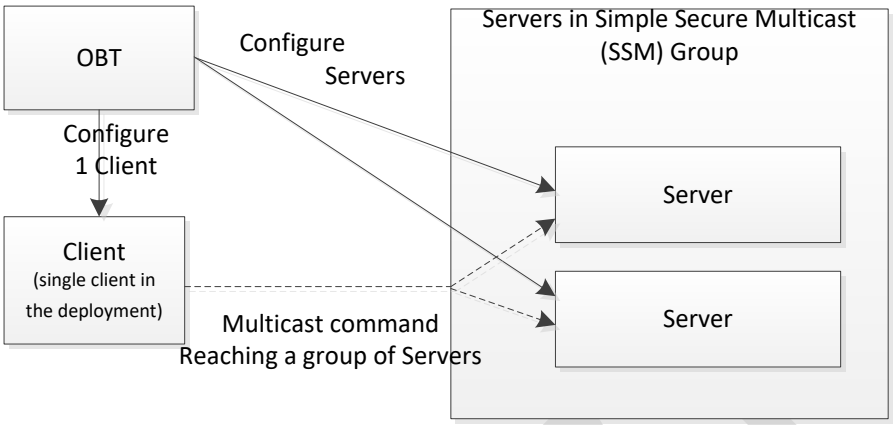

Figure 1W – Single request reaches a group of Servers

The Security model for SSM is described in Figure 3X and the accompanying steps.

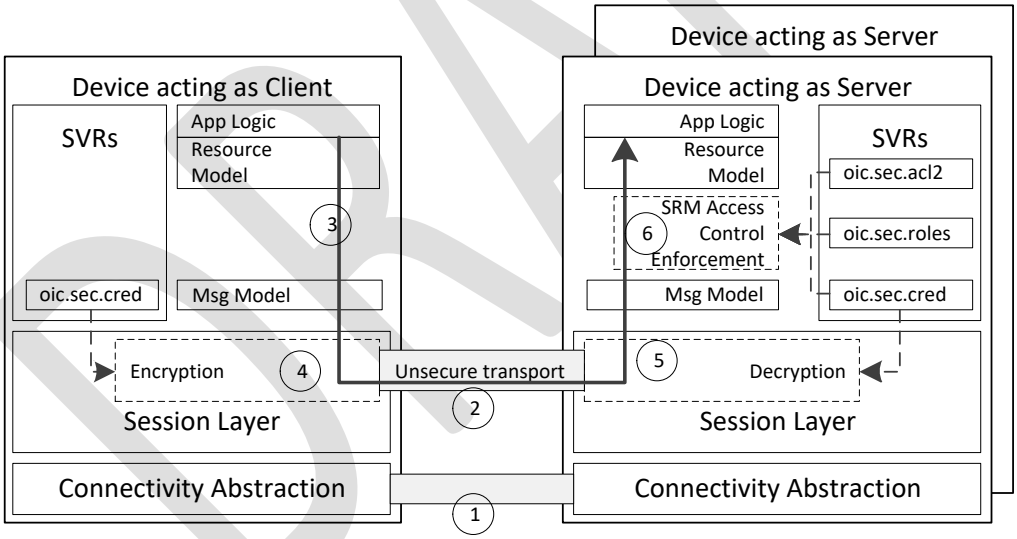

Figure 2X – OCF Layers for Simple Secure Multicast

1) The Client and Servers in the SSM Group are configured with encryption/decryption. The Client knows the preconfigured multicast address to use and how to create the actual payload of the command to send.
2) Messages are exchanged over an unsecure transport connection.
3) The Client generates an UPDATE request message to the Servers.

4) The Client encapsulates the UPDATE request message into an End-to-End Secured request message of the unsecured channel. The multicast address is left unencrypted in the Secured request message.

   The Client sends the Secured UPDATE request message to the multicast URL of the Servers, using the URL of the multicast enabled resource.

5) The Servers decrypt the message. The UPDATE request message is treated as being received over an authenticated encrypted ("auth-crypt") connection and associated with a "deviceUUID" (which can be the Device UUID of the Client).

6) The Server determines whether access to the Resource is permitted as described in step 4c of the Security model for direct Device-to-Device interaction shown in Figure 2.

New sub clause of Clause 5, Core Security

5.y Overview of Simple Secure Multicast

The Security model for SSM is described in Figure XXX of clause 5.1 and the accompanying steps.OCF uses the OSCORE protocol IETF RFC 8613 for the Security of SSM Messages. The Client transforms a CoAP-encoded UPDATE request message into an OSCORE request message which can be forwarded towards the Servers of the SSM Group using network-layer multicast; the Server then processes the OSCORE request message to extract the UPDATE request message.

Note: OSCORE is also used, albeit slightly differently, for End-to-End Security of Unicast Messages.

The intended use of the SSM feature is only for updating Resources with one non-confirmable multicast request. Other CRUDN operations (e.g. RETRIEVE, confirmable UPDATE, etc) are not supported because the SSM protocol is not designed to send individual responses back on the request. Hence when sending such operation by means of SSM, the individual Servers will silently ignore the request message and not send a response.

The OSCORE specification supports transporting OSCORE messages using the CoAP protocol already used in OCF specifications. The payload of the OSCORE message is a CBOR Object Signing and Encryption (COSE) object (see IETF RFC 8152) in which all elements of the CoAP-encoded UPDATE request message, other than those parts which are needed for delivering the message to the receiving Device, are encrypted and integrity protected. OSCORE also includes replay protection.

The setup of the OSCORE security context for an SSM Group is a 1-N relationship:

– the SSM Client Context of the SSM Group is only provisioned once in the Client of the SSM Group, and
– copies of the SSM Server Context of the SSM Group are provisioned to one or more Servers in the SSM Group.

Figure X1 depicts the relationship of the SSM Client Context and SSM Server Context.

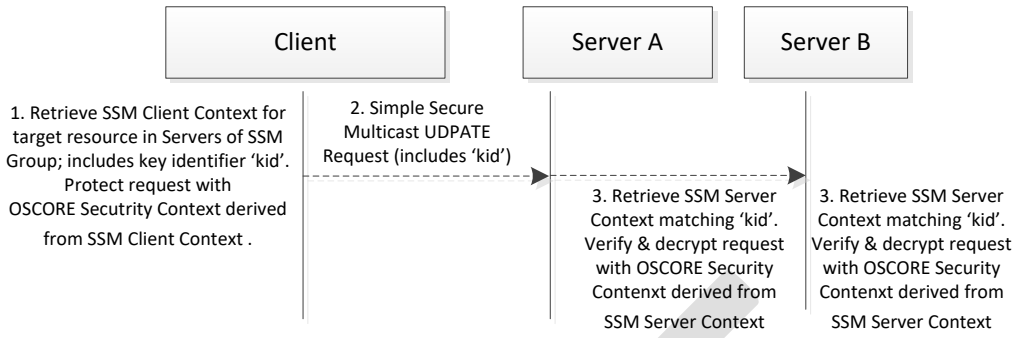

Figure 3 Relationship diagram for Simple Secure Multicast messages

Figure X2 depicts the full setup and usage.

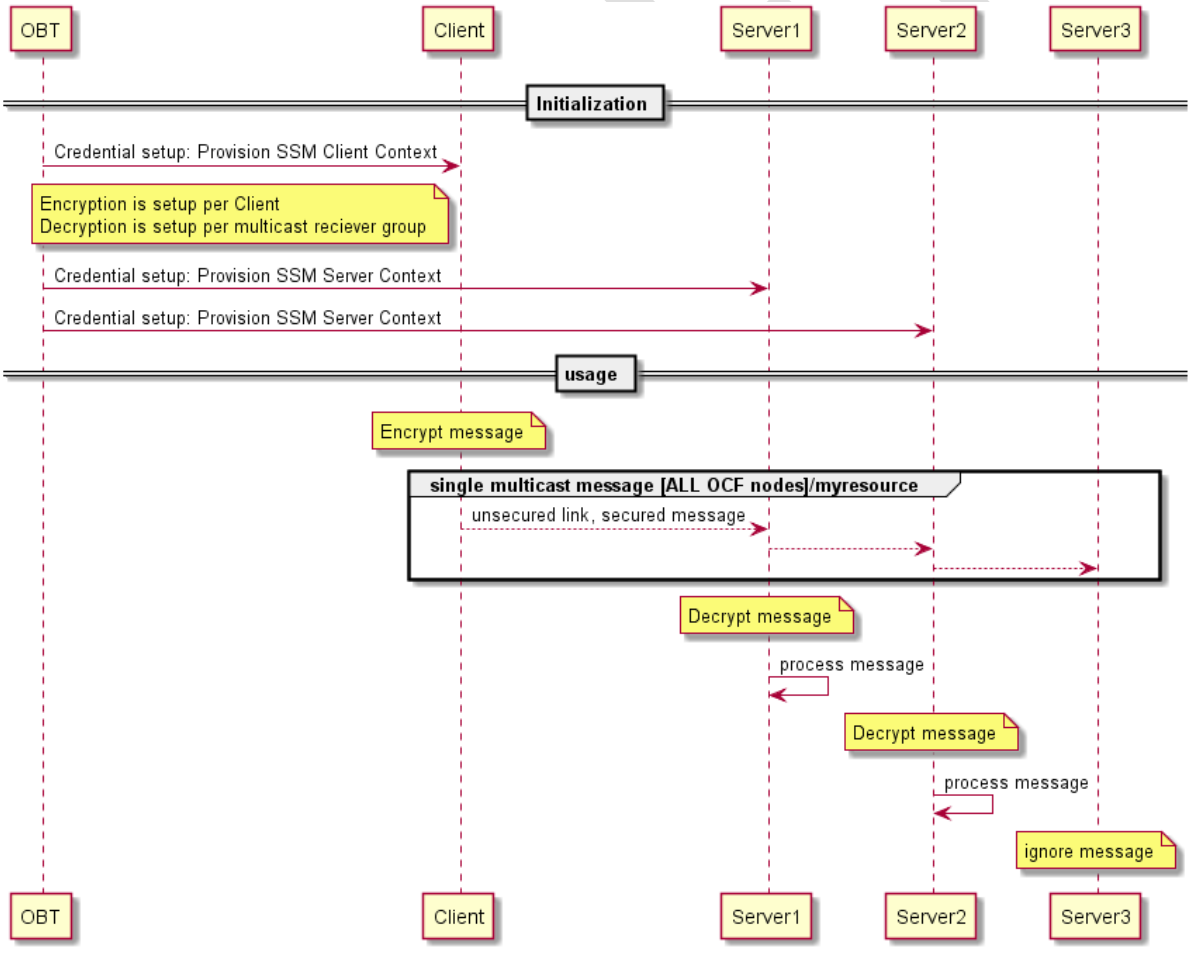

Figure 4 Setup and usage of Secure Simple Multicast

The first message after onboarding is implicitly trusted by the Server as being a valid message. This is due to the replay window not yet being set up by the Server. The Server stores the received information so that the replay protection is enabled after receiving the first message.

NEW sub clauses of Clause 9.3

9.3.x Credentials for Simple Secure Multicast

There are two distinct credential types used for provisioning OSCORE Security Context parameters used in Simple Secure Multicast (SSM): one for the SSM Client Context identified using "credtype" :"128"; and one for the SSM Server Context identified using "credtype" : "256". In a Client of an SSM Group, the Client's OSCORE Security Context (Sender context) is derived from a provisioned SSM Client Context. In the Servers of an SSM Group, the Server's OSCORE Security Context (Recipient Context) is derived from a provisioned SSM Server Context.

For both of these credential types, the "privatedata" Property of the credential entry in the "/oic/sec/cred" Resource contains the value of the OSCORE Master Secret of the SSM Group, which is generated by the OBT.

A SSM Client Context credential entry shall expose the OSCORE Configuration ("oscore") Property, which for this credential type shall include:

- The "senderid" Property containing the OSCORE Sender ID parameter.
    - This value is selected and provisioned by the OBT.
- The “desc” Property containing a description of the usage of the security context
    - This Property contains a human-readable description intended for identifying the corresponding SSM Group when a Security Domain contains multiple SSM Groups.
    - This value is selected and provisioned by the OBT
- The "ssn" Property contains a read-only value used to store the OSCORE Sender Sequence Number.

NOTE: The value of "senderid" is expected to be lowercase hexadecimal encoded with "0x" encoding prefix omitted.

An SSM Server Context credential entry shall include the OSCORE Configuration ("oscore") Property, which shall include:

- The "recipientid" Property containing the OSCORE Group Recipient ID parameter.
    - This value is equal for all Servers in the SSM Group, and is the same as the value of the "senderid" of the Client Context for the SSM Group
    - This value is selected and provisioned by the OBT
- The “desc” Property containing a description of the usage of the security context

- This Property contains a human-readable description intended for identifying the corresponding SSM Group when a Security Domain contains multiple SSM Groups.
- This value is selected and provisioned by the OBT

NOTE: The value of "recipientid" is expected to be lowercase hexadecimal encoded with "0x" encoding prefix omitted.

See clause Q.3.3 for description of the OSCORE parameters used in SSM.

Changes to Table 21, Clause 13.3.1

Table 1 – Properties of the "oic.sec.creds" Property

Property Title	Property Name	Value Type	Value Rule	Mandatory	Access Mode	Device State	Description
Credential ID	credid	UINT16	0 – 64K-1	Yes	RW		Short credential ID for local references from other Resource
Subject UUID	subjectuuid	String	uuid	Yes	RW		A uuid that identifies the subject to which this credential applies or "*" if any identity is acceptable
Role ID	roleid	oic.sec.roletype	-	No	RW		Identifies the role(s) the subject is authorized to assert.
Credential Type	credtype	oic.sec.credtype	bitmask	Yes	RW		Represents this credential's type. 0 – Used for testing 1 – Symmetric pair-wise key 2 – Symmetric group key 4 – Asymmetric signing key 8 – Asymmetric signing key with certificate 16 – PIN or password 32 – Asymmetric encryption key 128 - Simple Secure Multicast Client Context 256 - Simple Secure Multicast Server Context
Credential Usage	credusage	oic.sec.credusagetype	String	No	RW		Used to resolve undecidability of the credential. Provides indication for how/where the cred is used "oic.sec.cred.trustca": certificate trust anchor "oic.sec.cred.cert": identity certificate "oic.sec.cred.rolecert": role certificate "oic.sec.cred.mfgtrustca": manufacturer certificate trust anchor "oic.sec.cred.mfgcert": manufacturer certificate
Public Data	publicdata	oic.sec.pubdatatype	-	No	RW		Public credential information 1:2: ticket, public SKDC values 4, 32: Public key value 8: A chain of one or more certificate
Private Data	privatedata	oic.sec.privdatatype	-	No	-	RESET	Server shall set to manufacturer default
					RW	RFOTM	Set by DOTS after successful OTM
					W	RFPRO	Set by authenticated DOTS or CMS
					-	RFNOP	Not writable during normal operation.
					W	SRESET	DOTS may modify to enable transition to RFPRO.
Optional Data	optionaldata	oic.sec.optdatatype	-	No	RW		Credential revocation status information 1, 2, 4, 32: revocation status information 8: Revocation information
Period	period	String	-	No	RW		Period as defined by IETF RFC 5545. The credential should not be used if the current time is outside the Period window.

Credential Refresh Method	crms	oic.sec.crmtype	array	No	RW		Credentials with a Period Property are refreshed using the credential refresh method (crm) according to the type definitions for "oic.sec.crm".

Changes to "Alternative in-transit protection mechanisms" Introduced in CR 1657

Q Alternative in-transit protection mechanisms

Q.1 Introduction to in-transit protection mechanisms

In addition to the DTLS protection mechanisms for device-to-device communication specified in clause 10 and clause 11.2, and TLS protection specified in OCF Cloud Security document, OCF supports the following in-transit protection mechanisms:

- Security of Unicast Messages using OSCORE, specified in clause Q.2.
- Simple Secure Multicast, specified in Clause Q.3

Q.2 Security of Unicast Messages using OSCORE

Q.2.2 OSCORE ID Namespace Prefix

….

Table Y –OSCORE Identifier Namespace Prefix

Value	Interpretation	Applicable clauses
0x00	Reserved for future use	
0x01	Directly provisioned OSCORE Security Context	Q.2.4
0x02	Simple Secure Multicast	Q.3
0x03-0x0F	Reserved for future use	

New Clause Q.3 for Simple Secure Multicast

Q.3 Simple Secure Multicast

Q.3.1 Introduction to Simple Secure Multicast

The communication model is that one (1) Client communicates to a group of Servers with a single UPDATE request, as shown in Figure 1X. Each Server receives the UPDATE request at approximately the same time and can execute the UPDATE request at approximately the same time. As example of this kind of communication is sending an “on” command to a group of lights, all lights that are member of that group turn on at approximately the same time. Sending UPDATE requests to a group of devices can be achieved on IP by means of sending messages to a predefined URL on a multicast address.

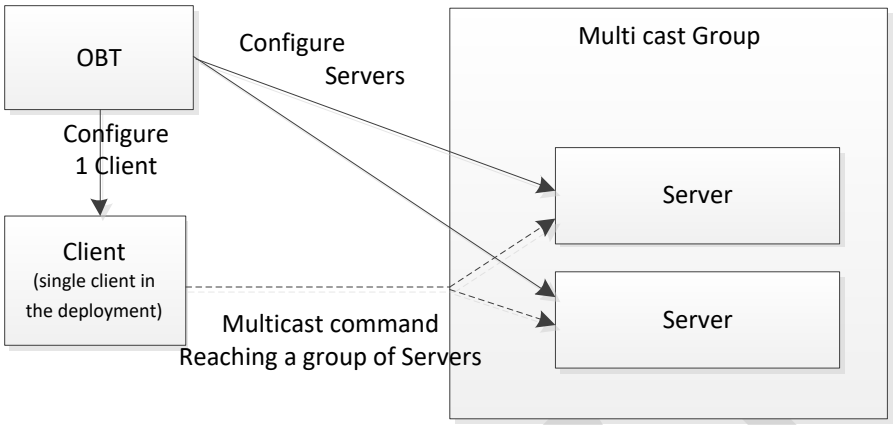

Figure 5X – Simple Multicast requests

Security of SSM is accomplished by applying an application layer of in-transit protection and below the resource-access authorization layer, using OSCORE IETF RFC 8613.

Relative to an exchange of an UPDATE non-confirmable message:

– The Device acting as a Client (that is, sending an UPDATE request message) acts as an OSCORE client. Within the scope of clause Q.3, the single Client is assumed to support OSCORE and perform OSCORE client processing.

– The Device acting as a Server (that is, receiving an UPDATE request message) acts as an OSCORE server. Within the scope of clause Q.3, all Servers are assumed to support OSCORE and perform OSCORE server processing.

Clause Q.3.2 details the assumptions and prerequisites for correct functioning of SSM. Clause Q.3.3 describes the process for encapsulating an UPDATE request message into an SSM Request at the Client of an SSM Group, and subsequent extraction of an UPDATE request message from an SSM Request at the Server of an SSM Group. Clause Q.3.4 specifies how a Client generates an OSCORE Common Context and OSCORE Sender Context from an SSM Client Context and specifies how a Server generates an OSCORE Common Context and OSCORE Recipient Context from an SSM Server Context.

Q.3.2 Assumptions and Prerequisites for Simple Secure Multicast

As shown in the following example, any Server of the SSM Group can generate an SSM Request which other Servers in the SSM Group will interpret as being securely sent by the Client of the SSM Group, for the purposes of privilege escalation. The security of SSM relies on the assumption that no Server in the SSM Group attempts to generate an SSM Request using the credentials for the SSM Group. SSM should only be used in scenarios where the Security Domain Owner is confident that this is a valid assumption.

SSM Requests are delivered to SSM-capable Servers via the All OCF Nodes multicast address defined in [CORE]. As specified in [CORE], all Servers subscribe to this multicast address to facilitate discovery of "oic/res", and consequently all Servers can receive SSM Requests delivered in this manner. A Server that supports the reception of SSM Requests for

one or more Resources that it hosts shall populate the All OCF nodes multicast address in the "eps" Parameter of the Resource Links of those Resources in the "oic/res" discovery response.

The configured Client is aware of Multicast enabled Servers by means of detecting the multicast enabled resources in the Device discovery "oic/res" responses. The Client also knows how to create the multicast request to that resource, by means of the Introspection Device Data hosted on the Device. Therefore, the Client is able to send an UPDATE request to the multicast enabled Resources.

The Client of an SSM Group cannot form SSM Requests for the SSM Group until the Client is provisioned with the SSM Client Context for the SSM Group. Likewise, each Server in an SSM Group cannot process SSM Requests for the SSM Group until the Server is provisioned with the SSM Server Context for the SSM Group. The SSM Client Context and SSM Server Context are provisioned by an OBT as specified in [OBT_SPEC]. Clause Q.3.4 specifies how the OSCORE Sender Context at a Client is derived from an SSM Client Context, and how the OSCORE Recipient Context at a Server is derived from an SSM Server Context.

The UPDATE request encapsulated in an SSM Request includes a local URI path for a target Resource. A Server in the SSM Group for whom the request is intended, will process the request using the Resource at this local URI path, if such a Resource exists and the Resource matches the Resource Type and OCF Interface in the request. The SSM feature is designed with the assumption that the local URI path, Resource Type and supported OCF Interfaces on the intended Servers are consistent; but the SSM feature does not specify how such consistency is achieved.

The UPDATE request message itself is expected to contain information in such way that the Server can determine if the received UPDATE request message is intended for the Server, but the specification of this information is not part of the SSM feature.

Q.3.3 OSCORE protection and verification of Simple Secure Multicast Requests

All OSCORE message processing requirements in clauses 8.1 and 8.2 in IETF RFC 8613 apply.

If a Client has an established SSM Client Context associated with an SSM Group, then the following call flow applies whenever the Client sends a multicast non-confirmable UPDATE request targeting multicast enabled Resources hosted on one or more Servers of the SSM Group.

1) The Client shall apply the OSCORE request protection processing to the UPDATE request as specified in Clause 8.1 in IETF RFC 8613, using the OSCORE Security Context derived from the SSM Client Context as specified in clause Q.3.4. See ISO/IEC 30118-1:2018 for details on setting the Proxy-URI option.

   The Client shall send the resulting OSCORE request message to the predefined All OCF Nodes multicast address. Dependent on the deployment scenario the different scopes as [REF to scope section] can be used.

2) All Servers subscribed to the predefined multicast address receive a copy of the OSCORE request message. Each Server supporting SSM which receives the OSCORE request message shall apply the OSCORE request verification and decryption processing in clause 8.2 of IETF RFC 8613 with the following clarifications:

   a) At Step 2 in clause 8.2 of IETF RFC 8613

i) If either the decompression or the COSE message fails to decode, the Server shall ignore the message and shall not respond.

ii) The Server attempts to retrieve the SSM Server Contexts with "recipientID" matching the 'kid' parameter. If the Server fails to retrieve an SSM Server Context with "recipientID" matching the 'kid' parameter received, then the Server shall ignore the message and shall not respond.

b) At step 6 in clause 8.2 of IETF RFC 8613, if the decryption failed then the Server shall ignore the message and shall not respond.

3) If any of the following criteria are met, then the CRUDN request message shall be silently discarded, and a response shall not be sent:

– The operation of the CRUDN request is not the non-confirmable UDPATE operation on a multicast address.

– The UPDATE request message is not intended for the Server - see clause Q.3.3 for further details.

– There is no Resource hosted on the Server at the local URI path in the UPDATE request message.

4) The Server shall process the UPDATE request message (encapsulated in the OSCORE request message). The Server shall treat the value of "subjectuuid" in the credential entry which contains the OSCORE Security Context used to verify and decrypt the OSCORE request message in Step 2 as Client's Device UUID for access control processing. The Server shall treat the connection type as "auth-crypt" for access control processing. The Server shall not send a response.

The mechanism outlined is for sending a message in a send and forget mode, i.e. sending a message to a group of Servers, where each Server does not acknowledge the receipt. Since multicast requests are typically unreliable (e.g. non-confirmable messages) the best practice is to send the same UPDATE request more than once in a short time frame. This is sufficient since the multicast communication has in most cases a unicast variant for the same UPDATE request.

Notification (see clause 11.3) may be used to verify if the actual UPDATE request has been executed. If a subset of the group of Servers did not receive the UPDATE request, unicast (confirmable) messages can be used to complete the desired overall state of the system.

Q.3.4 Creating OSCORE Security Context for Simple Secure Multicast

The present clause specifies how

– a Client of an SSM Group creates a OSCORE Security Context from a SSM Client Context provisioned to a credential entry of the Client.

– a Server of an SSM Group creates a OSCORE Security Context from a SSM Server Context provisioned to a credential entry of the Server.

All configurable parameters of the OSCORE Security Context are either:

– fixed to the OSCORE-specified default value, or

– directly provisioned by an OBT to a credential entry of the "/oic/sec/cred" Resource.

The following parameters of the OSCORE Security Context used for encryption by the Client of an SSM Group shall be set to the default values defined in clause 3.2 of IETF RFC 8613 (this information is not configured by the OBT):

– AEAD Algorithm,
– HKDF,
– Master Salt,
– ID Context.

The following parameters of the OSCORE Security Context parameters used for encryption by the Client of an SSM Group are derived from the SSM Client Context provisioned to a credential entry of "/oic/sec/cred" of the Client:

– The "subjectuuid" may be any schema compliant value. This Property serves no purpose when used in an SSM Client Context.
– The credential entry is identified as an SSM Client Context when the "credtype" matches the value specified for a SSM Client Context in Table 21, clause 13.1.1.
– The "privatedata" Property contains a 256-bit value which shall be used as the OSCORE Master Secret.
– The OSCORE Configuration parameters ("oscore") Property is present, and includes the following Properties:
  – The "senderid" Property shall be used as the OSCORE Sender ID of the OSCORE Security Context. The "recipientid" Property value shall be interpreted as the hexadecimal representation of a 56-bit value. The first byte of this value is expected to have the value assigned in Table Y for Simple Secure Multicast.
  – The "desc" Property is not used in security processing. This Property is described in clause 9.3.x.

On the Device shutting down, for each such credential entry, the Device shall write the value of corresponding OSCORE Sender Sequence Number as "ssn" Property to non-volatile memory. In event of a crash, devices should apply Appendix B.1.1 of IETF RFC 8613.

The following parameters of the OSCORE Security Context used by a Server of an SSM Group for verification and decryption shall be set to the default values defined in clause 3.2 of IETF RFC 8613 (this information is not configured by the OBT):

– AEAD Algorithm,
– HKDF,
– Replay Window,
– Master Salt,
– ID Context.

The following parameters of the OSCORE Security Context parameters used by a Server of an SSM Group for verification and decryption are derived from the SSM Server Context provisioned to a credential entry of "/oic/sec/cred" of the Server:

– The "subjectuuid" is used for access control processing as described in Step 4 of clause Q.3.3.
– The credential entry is identified as an SSM Server Context when the "credtype" matches to the value specified for an SSM Server Context in Table 21, clause 13.1.1.
– The "privatedata" Property of the credential entry contains a 256-bit value which shall be used as the OSCORE Master Secret.

– The OSCORE Configuration parameters ("oscore") Property is present, and includes the following Properties:
  – The "recipientid" Property shall be used as the OSCORE Recipient ID of the OSCORE Security Context. The "recipientid" Property value shall be interpreted as the hexadecimal representation of a 56-bit value. The first byte of this value is expected to have the value assigned in Table Y for Simple Secure Multicast.
  – The "desc" Property is not used in security processing. This Property is described in clause 9.3.x.

OBT SPEC

NEW sub clause of Clause 6

6.Y Provisioning Clients and Servers in a Simple Secure Multicast Group

ISO/IEC 30118-2:2018 specifies how Simple Secure Multicast (SSM) secures messages sent from a Client to multiple Servers in a SSM Group by applying an application layer of in-transit protection below the resource-access authorization layer, using Object Security for Constrained RESTful Environments (OSCORE) IETF RFC 8613. Within the scope of this clause, "Client" refers to the Client of the SSM Group and "Server(s)" refers to a Server(s) in the SSM Group.

SSM is enabled by provisioning an SSM Client Context in a credential entry of the "/oic/sec/cred" Resource of the Client, and provisioning (identical) copies of the SSM Server Context in a credential entry of the "/oic/sec/cred" Resource of the Servers. The present clause provides the requirements on the CMS for this provisioning.

The OBT recognizes during onboarding, by examining the "/oic/sec/doxm:sct" Property, that one or more Devices in the Security Domain support SSM Client Context credentials and/or SSM Server Context credentials. The OBT may prompt the End User to create one or more SSM Groups, or the OBT may create groups without any End User interaction.

On creation of an SSM Group, a corresponding SSM Client Context and SMS Server Context shall be generated by the CMS. The CMS generates three values: idGroup; an associated Device UUID, an OSCORE Master Secret, and SSM Group description.

– The CMS selects a value for idGroup (identifying the OSCORE Security Context for messages sent from the Client to the Servers) conforming to the following criteria:
  – The total length of idGroup 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 idGroup shall be 0x02.

NOTE 1: The value 0x02 is the OSCORE Identifier Namespace Prefix value assigned for "Simple Secure Multicast" in ISO/IEC 30118-2.

    - The value of idGroup should be distinct from all values of "recipientid" in credential entries of all Devices in the Security Domain.
- The CMS shall select an SSM-Group-subjectuuid which will be configured in the "subjectuuid" of the credential entry containing the SSM Server Context; the Servers use this "subjectuuid" for access control processing applied to verified SSM Requests as specified in ISO/IEC 30118-2:2018. The SSM-Group-subjectuuid would typically be the Device UUID (that is, the value in "/oic/sec/doxm:deviceuuid") of the Client; this will result in SSM requests from the Client have the same permissions as unicast requests from the Client (e.g. received via DTLS or OSCORE). However, a CMS can select a value for the SSM-Group-subjectuuid, which provides the flexibility for the AMS to configure the Servers with
    - One set of permissions, using ACEs with "subject" matching Client's Device UUID, for unicast requests received from the Client (e.g. received via DTLS or OSCORE), and
    - Another set of permissions, using ACEs with "subject" matching SSM-Group-subjectuuid (and different from the Client's Device UUID), for SSM requests received from the Client.
- 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 or End User should select a human-readable string for identifying the SSM Group. If a value is not selected, then this value defaults to the empty string.

The CMS then independently provisions credential entries to the Client and Servers of the SSM Group.

The CMS provisions the following credential entry, containing the SSM Client Context, to the Client of the SSM Group:

- The "subjectuuid" may be any schema compliant value. This Property serves no purpose when used in an SSM Client Context.
- The "credtype" shall have the value 128.

NOTE 2: The value 128 is the "credtype" value specified for a SSM Client 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 idGroup with the "0x" encoding prefix omitted.
    - The "desc" Property shall be set to the human-readable description for identifying the SSM Group.

The CMS separately provisions the following credential entry, containing the SSM Server Context, to Servers of the SSM Group:

- The "subjectuuid" shall be set to the SSM-Group-subjectuuid selected by the CMS.
- The "credtype" shall have the value 256.

NOTE 2: The value 256 is the "credtype" value specified for a SSM Server 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 "recipientid" Property shall be set to the lowercase hexadecimal representation of idGroup with the "0x" encoding prefix omitted.
- The "desc" Property shall be set to the human-readable description for identifying the SSM Group.

These provisioning steps may occur implicitly, that is, without End User interaction.