WHITE PAPER

Smart Commercial Buildings Work Group

OPEN CONNECTIVITY FOUNDATION®

# Simple Secure Multicast

## EXPLAINING SSM

October 22, 2020

# Introduction

The Open Connectivity Foundation (OCF) Core Framework will have a new feature called Simple Secure Multicast (SSM). The SSM feature is intended to fill a gap in the interaction models of OCF. The OCF Core Framework is designed to be rest full and the interaction model is to use unicast CRUDN actions. Where CRUDN stands for CREATE, RETRIEVE UPDATE, DELETE and NOTIFY operations. However, there are use cases, especially in the lighting domain, that require a single action that will action on multiple devices. For example, a hallway that is illuminated by more than one light. When using electrical wiring, these lamps are connected in such way that all lamps are turned on/off simultaneously. When using IP, the logical choice is to send a multicast message to a group and each of the members of that group will act upon the message at the same time. This will create the same end user experience: all devices of the group will turn on/off at the same time. This approach sounds simple, however the multicast message needs to be sent in such way that it is secure, e.g. only the members that are allowed to send a command are able to do so and all members receiving the command should be able to decode the message. Securing the link with DTLS is not possible, so the multicast messaging should be secured using OSCORE. With OSCORE the payload of the message is encrypted, and the encrypted payload can be sent to a multicast address. The message can then be received and decrypted by more than one server.

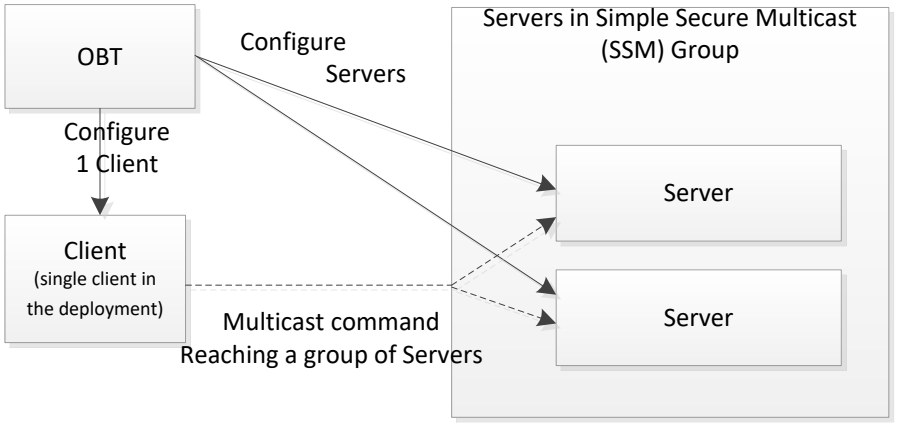


**Figure 1 Schematic overview of SSM group communication**

# Simple Secure Multicast

The OCF Core Framework has been designed to securely transport data between clients and servers. In this document, a description is given of how to use Simple Secure Message in OCF to send a single command to multiple devices. Since the client server concept is already prevalent within OCF, the same structure is applied when designing SSM. The Client is able to send a multicast message to one or more servers that will receive the command. The onboarding tool (OBT) is responsible for configuring the security context.

In OSCORE, two-way communication is expected. Hence, a client will have credentials to encrypt data and the server will have to have the credentials to decrypt the data. When a result is sent back from a server to a client, the roles are reversed. This is why OSCORE has two sets of credentials to implement an UPDATE operation.

To simplify securing multicast messaging the next restrictions are placed on the design:

- The multicast messages are "send" only, e.g. no communication is expected back.
- There is a single group of devices that can receive the multicast messages.
- All the devices will listen to the same address and port, the previously used address and port for OCF device discovery.

It may seem as if these restrictions are making the solution less useful, but the OCF Core Framework will help to overcome these restrictions.

The message that will be sent will be part of the overall OCF architecture. So, a client can already detect during the discovery phase which resources are enabled for SSM communication. This is conveyed as an extra end point in the list of OCF resources. If the endpoint starts with the OCF multicast address, then the resource can receive SSM message on the IP address and its URI. The URI has to be the same for all implementations. Hence this is achieved by using the example URI of the resource type of the SSM enabled resource.

For example, to create a simple lamp that can turn on/off, only the binary switch resource must be used. This resource type has "/BinarySwitchResURI" as URL. Sending the follow command will turn off all light devices that have implemented the resource and enabled SSM:

```
UPDATE [All OCF Nodes multicast group]/BinarySwitchResURI

{
```

```
      "value": false
}
```

The Client will know by design that no response is expected when sending the multicast command. This is not an issue since the resource is also available via unicast operations. If a client wants to know, it can check if the wanted value is set by doing a unicast retrieve operation after sending the multicast command or applying the NOTIFY operation before sending the multicast command. This has to be applied for all devices that the clients want to know if the state change happened. This is similar as the OSCORE group communication feature which is in draft state.
The introspection feature of OCF indicates what a client can send to a specific resource. The usage of this feature does not change with SMM.

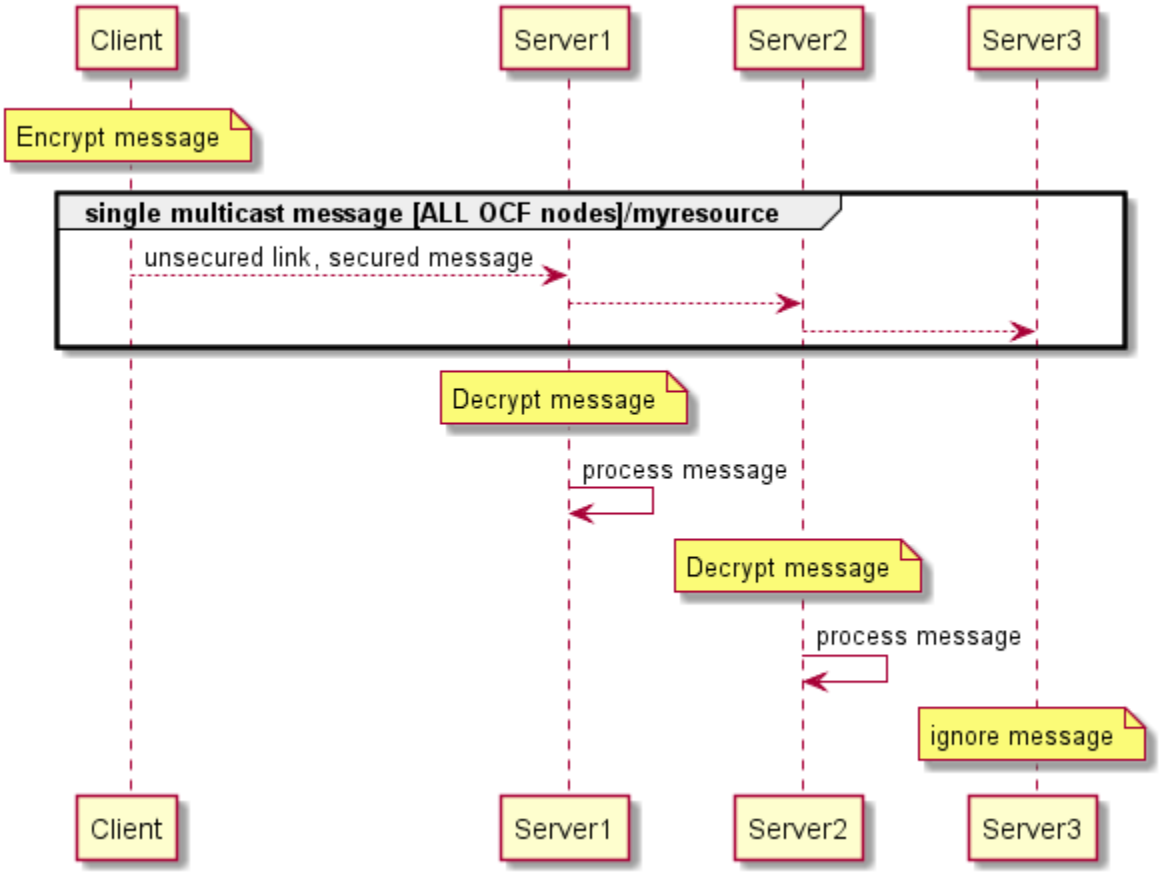


**Figure 1 Sending Secure Simple Multicast messages**

The OBT is made responsible for setting up the key distribution to use the SSM feature. Each OCF secure domain can have one or more SSM keys. To keep Secure multicast message simple, all Client & Servers will be part of the same group. The Client and Servers are recognized during onboarding on the secure domain that supports SSM credentials. The OBT will create the SSM credentials on the first onboarding occurrence of an SSM enabled device. Setting up and distributing SSM credential materials are done in the same way as all other keying materials.

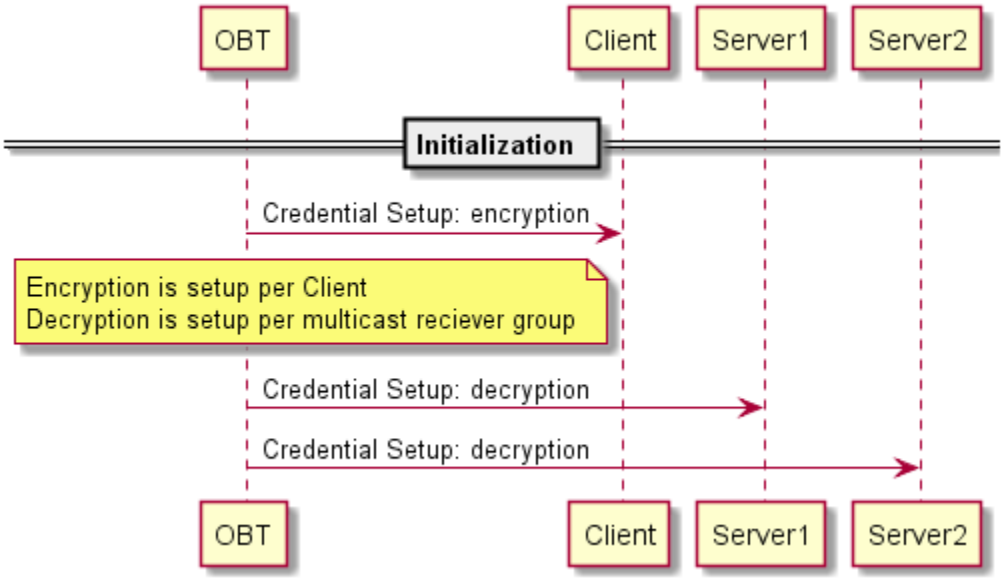


**Figure 2 Configuring Secure Simple Multicast**

The binary switch resource is taken as example, this resource does not have any properties to indicate grouping itself, which has to be taken care of when deploying devices. There is further development on resource modelling that will take grouping into account. To enable these new resources SSM had to be developed first as enabler.

# References


Open Connectivity Foundation (OCF) ISO/IEC 30118

Concise Binary Object Representation (CBOR) https://tools.ietf.org/html/rfc7049

The Constrained Application Protocol (CoAP) https://tools.ietf.org/html/rfc7252

Datagram Transport Layer Security https://tools.ietf.org/html/rfc6347

Object Security for Constrained RESTful Environments https://tools.ietf.org/html/rfc8613

Group OSCORE - Secure Group Communication for CoAP https://datatracker.ietf.org/doc/draft-ietf-core-oscore-groupcomm/

Standardized rt values: https://www.iana.org/assignments/core-parameters/core-parameters.xhtml#rt-link-target-att-value