Mutual TLS (mTLS) Support and Validation on AMF

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Products or Functional Area	AMF
Applicable Platforms	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

AMF supports mutual TLS secure channel for SBI interfaces. With the mTLS Support for SBI interfaces, AMF handles mutual TLS requests from the server and the client, and supports HTTP2 over TLS secure channel for all NF interfaces.

This feature also supports in generating alarms when the certificates expire within a configured threshold period.

Relationships

The mTLS Support for SBI interfaces feature has the relationship with TLS Transport Support feature. For related information, see the *TLS Transport Support* chapter in this document.

Prerequisites

The mTLS Support for SBI interfaces feature has the following prerequisite:

- User should procure and configure Certificate Authority (CA) certificates and other certificates/keys necessary for the server and the client.

For client and server certificate configuration, ca-certificate configuration, and uri-scheme https in profile nf-client configuration, see the *TLS Transport Support* chapter in this document.

How it Works

This section describes how this feature works.

TLS protocol is used for transport layer protection.

AMF supports TLS versions 1.2 and 1.3 for all inbound and outbound HTTPS, and outbound TCP transport.

AMF supports enabling mutual TLS for the SBI endpoint.

Limitations

This feature has the following limitations in this release:

- Mutual TLS secure channel support feature for AMF provides transport layer encryption between the nodes for security compliance purposes only.
- AMF does not support NF security requirements as per 3GPP specifications of 5G.
- As AMF supports L1-X1 over UDP in Cisco format only, AMF does not support mTLS on the L1-X1 interface.
- AMF does not support dynamic mTLS CLI change configuration.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   instance instance-id instance_id
      endpoint sbi
         uri-scheme {http | https}
         mtls-enable {false | true}
         certificate-name certificate_name
         end
```

NOTES:

- **instance instance-id** *instance_id* —Specify the instance ID.
- **endpoint** *sbi*—Specify the endpoint as sbi.
- **uri-scheme {http | https}**—Specify the uri-scheme as https. The default value is http.
- **mtls-enable {false | true}**—Specify the mTLS configuration as either true or false.
- **certificate-name** *certificate_name*—Specify the certificate name for the server which is used by AMF for HTTPS messages. The list of certificate names is obtained from the **nf-tls** command.

Configuration Example

The following is an example configuration.

```
config
   instance instance-id 1
      endpoint sbi
         uri-scheme https
         mtls-enable true
         certificate-name serv-cert
         end
```

Configuration Verification

To verify the configuration:

```
endpoint sbi
uri-scheme https
certificate-name serv-cert
mtls-enable true
vip-ip 209.165.201.1
exit
```