Mutual TLS (mTLS) Support and Validation

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	For related information, see the *TLS Transport Support* chapter in this document.

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

The AMF supports the mutual TLS secure channel for SBI interfaces. With the mTLS Support for SBI interfaces, the AMF performs the following:

- Handles mutual TLS requests from the server and the client
- Supports HTTP2 over the 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. The following are the roles associated with the AMF:

- Server Configuration in AMF, on page 3
- Client Configuration in AMF, on page 4

For related information, see the *TLS Transport Support* chapter in this document.

Prerequisites

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

- The user must procure and configure the following:
  - Certificate Authority (CA) certificates
  - Other certificates or keys necessary for the server and the client
- For more information on the following topics, see the *TLS Transport Support* chapter in this document.
  - For the client, and the server certificate configuration
  - For the ca-certificate configuration
  - For uri-scheme https, in the profile nf-client configuration

How it Works

This section describes how this feature works. It has the following synopsis:

- The TLS protocol is used for transport layer protection.
- The AMF supports TLS versions 1.2 and 1.3 for all inbound and outbound HTTPS, and outbound TCP transport.
- The AMF supports enabling mutual TLS for the SBI endpoint.

Limitations

This feature has the following limitations:

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

Server Configuration in AMF

The AMF acts as the server for all peer NFs over the SBI interface.

The SBI interface servers characteristics are determined by **instance instance <id> endpoint sbi** configurations.

The server certificates get configured at the SBI endpoint.

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
  exit
 exit
exit
```

Configuration Verification

To verify the configuration, use the following command:

```
amf# show running-config instance instance-id 1 endpoint sbi
```

Client Configuration in AMF

The AMF acts as client-to-peer NFs while sending notifications or updates. The characteristics of the client configurations are determined by using the **endpoint-profile** configuration. The server name gets configured, when the URI scheme is in a secured (HTTPS) environment for locally configured NF profiles and NRF-related configurations.

Feature Configuration

To configure this feature, use the following configuration. The following commands help in enabling the mTLS option along with the server name at the NF and NRF-related configurations:

```
config
   profile nf-client
      nf-type ausf
         ausf-profile AUP1
         locality LOC1
         service type nausf-auth
         endpoint-profile ep_profile_name
            type EP1
            locality LOC1
            uri-scheme https
            server-name server_name
   group nrf
      mgmt MGMT_name
         service type nrf nnrf-nfm
         endpoint-profile ep_profile_name
            name mgmt-prof
            uri-scheme https
            server-name server_name
   group nrf
      discovery udmdiscovery
         service type nrf nnrf-disc
         endpoint-profile ep_profile_name
            name EP1
            uri-scheme https
            server-name server_name
            end
```

NOTES:

- **profile nf-client nf-type ausf ausf-profile** *AUP1*—Specify the required NF client profiles and provide the local configuration.
- **service type nausf-auth** | **service type nrf nnrf-nfm** | **service type nrf nnrf-disc**—Specify the service names as per the 3GPP standards.
- **group nrf mgmt** *MGMT_name*—Specify the NRF self-management group configurations.
- **instance instance-id** *instance_id*—Specify the instance ID.
- **endpoint-profile** *ep_profile_name*—Specify the endpoint-profile name.
- **uri-scheme {http | https}**—Specify the uri-scheme as https. The default value is http.
- **server-name** *server_name*—Specify the **DNS name** (FQDN) of the peer NF and the **server-name** must match the DNS attribute of the **subjectAltName** field in the peer NF certificates.

Configuration Example

The following is an example configuration.

```
config
 group nrf mgmt MGMT
  service type nrf nnrf-nfm
   endpoint-profile
    name mgmt-prof
    uri-scheme https
    server-name server_name
    endpoint-name mgmt-1
     primary ip-address ipv4 209.165.201.1
     primary ip-address port 9051
    exit
   exit
  exit
 exit
 profile nf-client nf-type ausf
  ausf-profile AUP1
   locality LOC1
    priority 30
    service name type nausf-auth
     endpoint-profile EP1
      capacity 30
      uri-scheme https
      server-name server_name
      endpoint-name EP1
       priority 56
       primary ip-address ipv4 209.165.201.1
       primary ip-address port 9047
      exit
     exit
    exit
   exit
  exit
 exit
```

Configuration Verification

To verify the configuration, use the following command:

```
amf(config)# show full-configuration profile
```