WSO2-2025-4494 - Use case 3

You have clients that use mTLS to connect to the WSO2 products,
and use certificate-based authentication for System REST API or SOAP service access.

Part A: Validate and mitigate issues for System REST APIs

For IS 5.9.0 and IS KM 5.9.0 you first need to update the product and then perform the configurations detailed in the **"WSO2-2025-4494 - Mitigation steps for System REST APIs"** document.

For other products and versions, if you have the configuration below, the System REST APIs are not vulnerable; no further action is needed.

- For IS 5.10.0 and above; IS KM 5.10.0 and above; APIM 3.0.0 and above; OB IAM 2.0.0; OB AM 2.0.0:
  `<PRODUCT_HOME>/repository/conf/deployment.toml`

  ```
  [intermediate_cert_validation]
  enable = true
  cert_cns = ["CN1", "CN2"]
  ```

- For IS 5.8.0 and below; IS KM 5.7.0 and below; APIM 2.6.0 and below; OB KM 1.5.0 and below; OB AM 1.5.0 and below:
  `<PRODUCT_HOME>/repository/conf/identity/identity.xml`

  ```
  <IntermediateCertValidation enable="true">
      <IntermediateCerts>
          <CertCN>CN1</CertCN>
          <CertCN>CN2</CertCN>
      </IntermediateCerts>
      <ExemptContext>
      </ExemptContext>
  </IntermediateCertValidation>
  ```

If the above configuration is not present, you first need to update the product and then perform the configurations detailed in the "WSO2-2025-4494 - Mitigation steps for System REST APIs" document.

Part B: Validate and mitigate issues for SOAP services

WSO2 API Manager and WSO2 Open Banking AM products are not affected with this use case, since certificate-based authentication for SOAP services capability is not available in those products.

For the other products, if you have the following configuration, the SOAP services are vulnerable.

- For IS 5.9.0 and above; IS KM 5.9.0 and above; OB IAM 2.0.0:
  `<PRODUCT_HOME>/repository/conf/deployment.toml`

  ```
  [admin_console.authenticator.mutual_ssl_authenticator]
  enable = true
  ```

- For IS 5.8.0 and below; IS KM 5.7.0 and below; OB KM 1.5.0 and below:
  `<PRODUCT_HOME>/repository/conf/security/authenticators.xml` under
  `<Authenticators>`

  ```
  <Authenticator name="MutualSSLAuthenticator">
      <Priority>5</Priority>
      <Config>
          …
      </Config>
  </Authenticator>
  ```

You first need to update the product and then perform the configurations as mentioned in the "WSO2-2025-4494 - Mitigation steps for SOAP Services" document.