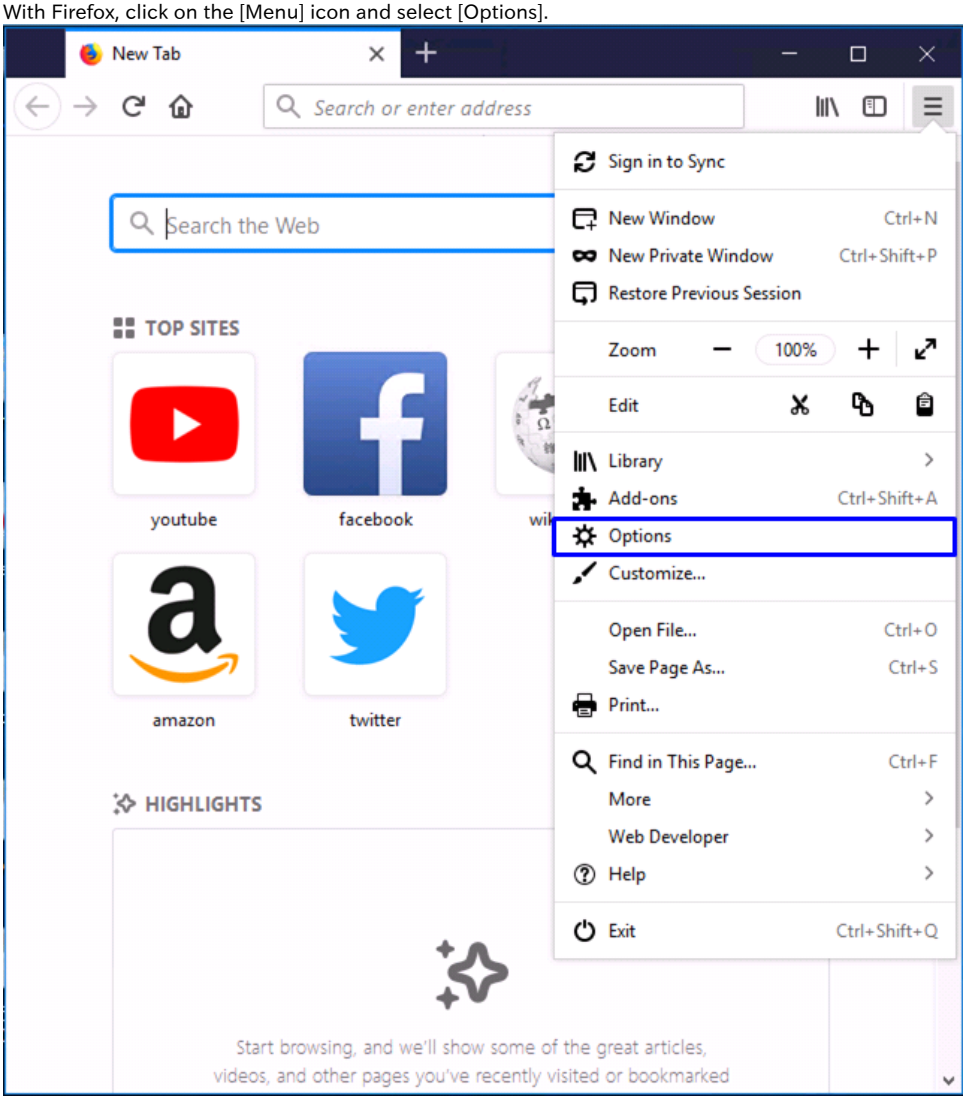
Checking Existence of the Certificate Using Firefox

Revision History			
Rev.	Date (YYYY/MM/DD)	Description	Editor
V.1.0	2018/2/26	First revision	NII

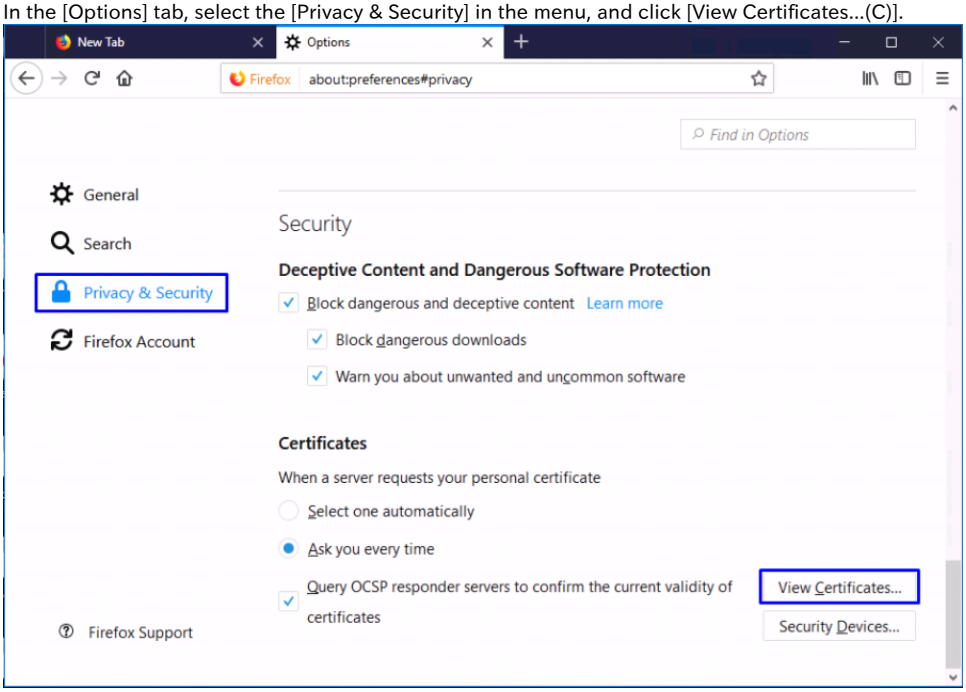
Checking Existence of the Certificate

Note 1: The [Issued To], [Issued By] and [Expiration] in the screenshots are just examples and will be different from those for the actual certificate.
Note 2: All screenshots are from Windows10 (Firefox 58.0).

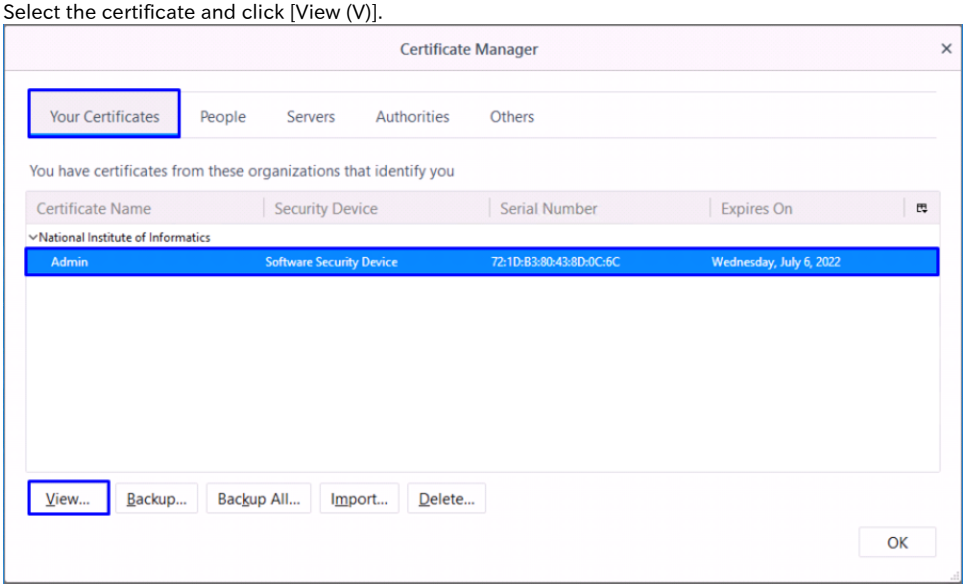
1. With Firefox, click on the [Menu] icon and select [Options].



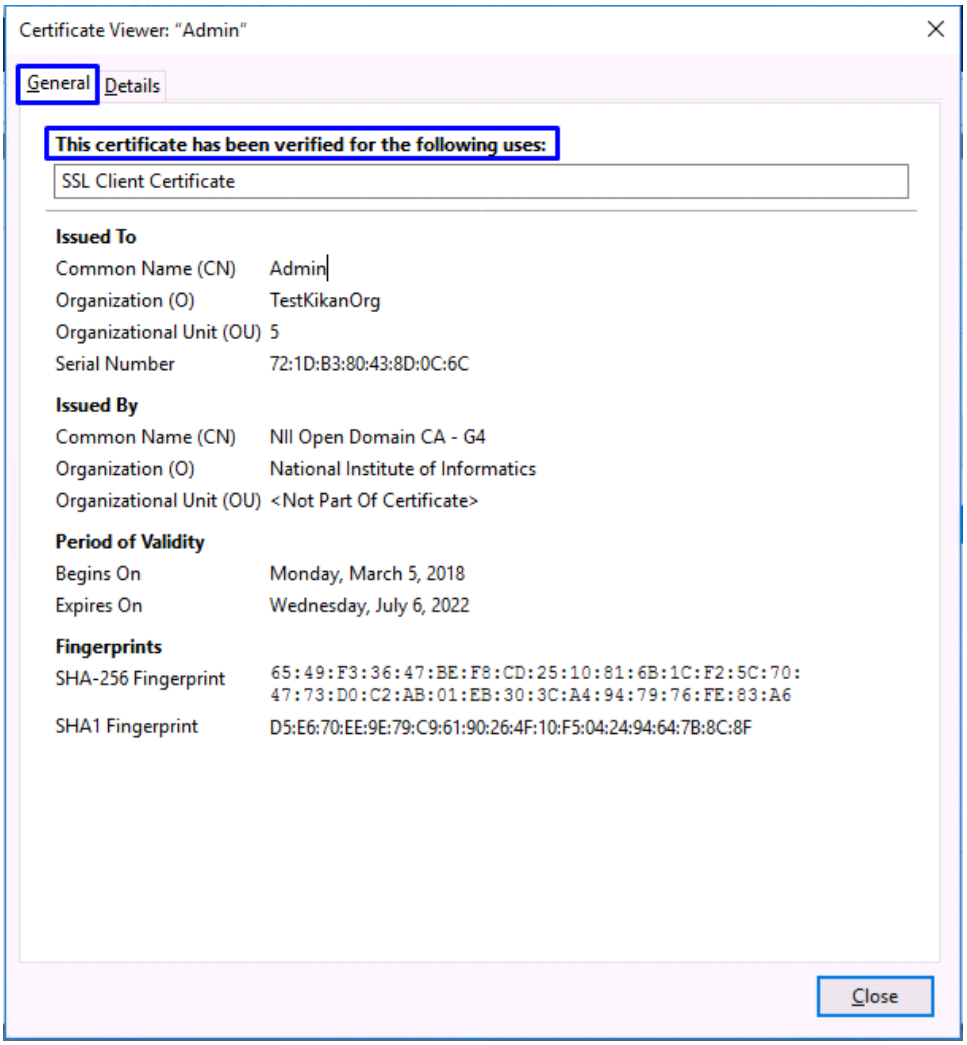
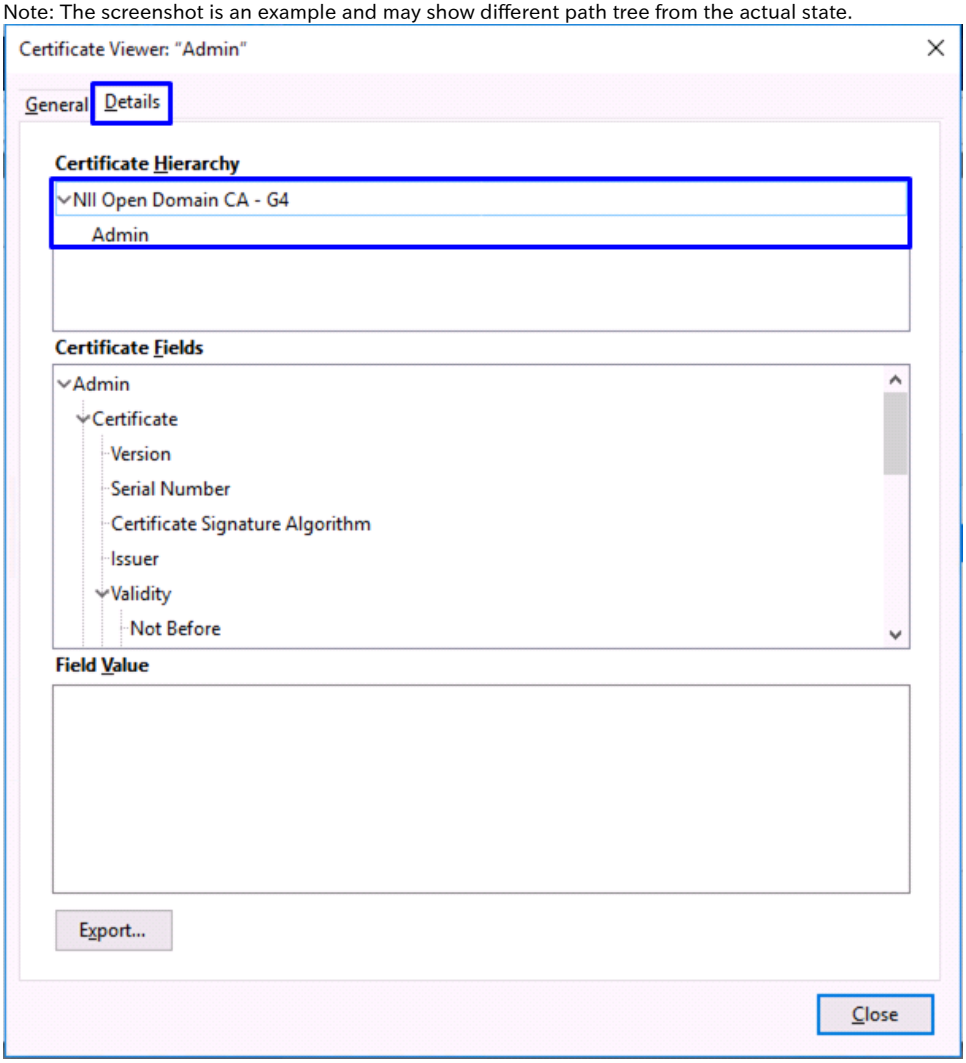
2. In the [Options] tab, select the [Privacy & Security] in the menu, and click [View Certificates...(C)].



3. In the [Certificate Manager] screen, click [Your Certificates] and make sure that the certificate appears in the list.
Select the certificate and click [View (V)].



4. In the resulting [Certificate Viewer] dialog box, select the [General] tab and make sure that it says "This certificate has been verified for the following uses."


Certificate Viewer: "Admin"
General
Details
This certificate has been verified for the following uses:
SSL Client Certificate
Issued To
Common Name (CN) Admin
Organization (O) TestKikanOrg
Organizational Unit (OU) 5
Serial Number 72:1D:B3:80:43:8D:0C:6C
Issued By
Common Name (CN) NII Open Domain CA - G4
Organization (O) National Institute of Informatics
Organizational Unit (OU) <Not Part Of Certificate>
Period of Validity
Begins On Monday, March 5, 2018
Expires On Wednesday, July 6, 2022
Fingerprints
SHA-256 Fingerprint 65:49:F3:36:47:BE:F8:CD:25:10:81:6B:1C:F2:5C:70:47:73:D0:C2:AB:01:EB:30:3C:A4:94:79:76:FE:83:A6
SHA1 Fingerprint D5:E6:70:EE:9E:79:C9:61:90:26:4F:10:F5:04:24:94:64:7B:8C:8F
Close

5. Select the [Details] tab and make sure that all certificates from the Root CA through the client certificate are correctly chained.
   Note: The screenshot is an example and may show different path tree from the actual state.