LOCAL CERTIFICATION AUTHORITY CREATOR

Model: LCA-DL30

USERS MANUAL

M-SYSTEM CO., LTD.

5-2-55, Minamitsumori, Nishinari-ku, Osaka 557-0063 JAPAN
Tel: +81-6-6659-8201 Fax: +81-6-6659-8510

http://www.m-system.co.jp/

E-mail: info@m-system.co.jp

Table of Contents

1. INTRODUCTION 3

2. WEB SERVER CERTIFICATE 4

3. LOCAL CERTIFICATION AUTHORITY. 5

4. HOW TO USE LCA-DL30 6

4.1 System requirements 6
4.2 Installation 6
4.3 Creating a Local Certification Authority 7
4.4 Creating and Transferring Web Server Certificate 8
4.5 Installing Local Certification Authority Certificate 10
4.5.1 Local Certification Authority Certificate 10
4.5.2 Installing via LCA-DL30 10
Windows (Chrome, Edge) 10
Windows (Firefox) 12
4.5.3 Using Certification Authority Certificate 17
Windows (Chrome, Edge) 17
Windows (Firefox) 17
4.5.4 Installing from DL30-G 18
Windows (Chrome, Edge, Firefox) 18
iOS (Safari) 18
Android (Chrome) 21
4.6 Importing Certificate 23
4.7 Rebuilding Local Certification Authority 24
4.8 Switching Display Language 24

5. LICENSE 25

1. INTRODUCTION

DL30-G version 2.0 or later supports HTTPS for enhancing secure communication.
This users manual describes how to create certificates which are indispensable when using HTTPS.

2. WEB SERVER CERTIFICATE

This section describes the purpose of web server certificates and how they are used.

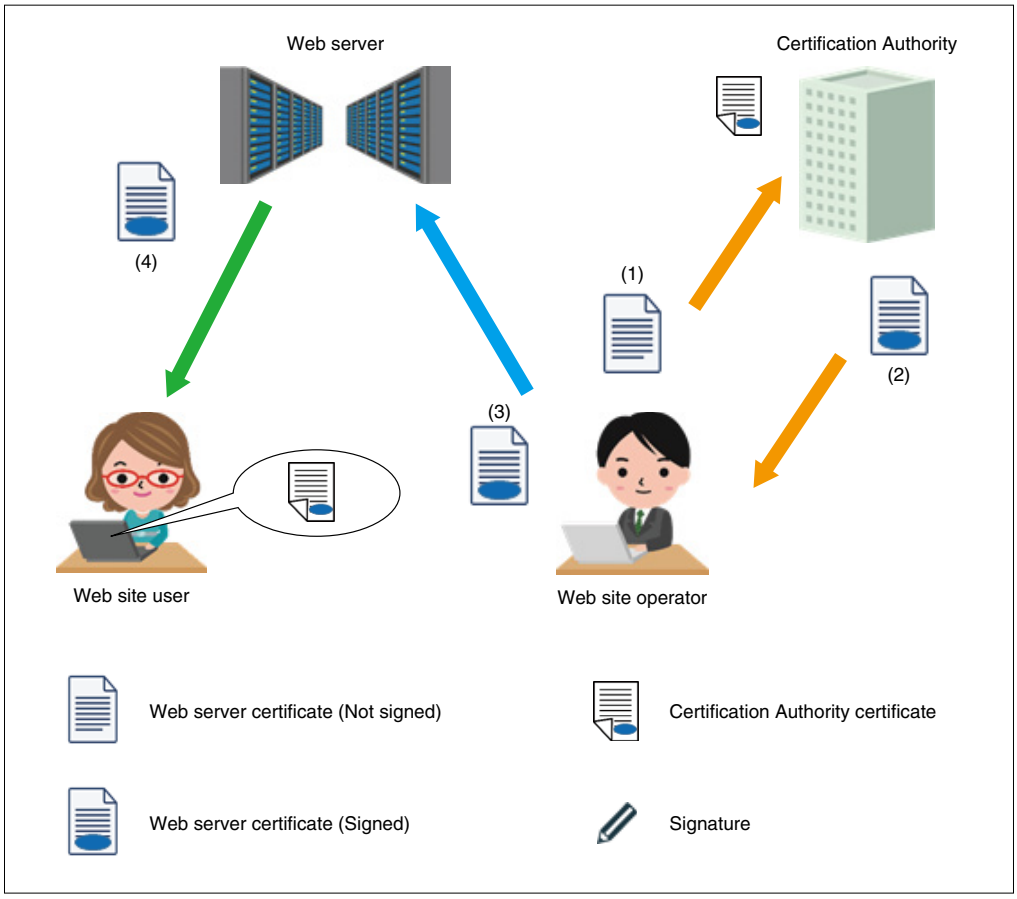
For further understanding, refer to relevant web sites or tutorial documents for terminologies such as 'route CA', 'intermediate CA', 'electronic signature', 'SSL/TLS', etc.

Below is the usual procedure followed when opening a web site using HTTPS.

(1) The web site operator creates a web server certificate and sends the certificate to a Certification Authority to be signed.

(2) The Certification Authority verifies the identity of the web site operator and the web server, signs the web server certificate and returns the certificate to the web site operator.

(3) The web site operator installs the certificate on the web server.



As a web site user accesses the web server via a browser using HTTPS, the web server certificate signed by the Certification Authority is downloaded ((4) in the above figure).

In order to verify the signature, a certificate for the Certification Authority who has singed the web server certificate needs to be confirmed.
For prompt verification, major Certification Authority certificates are pre-installed in browsers.
If verified, the site user can assure that the web site the user is accessing is not a spoofed web site.

The web server certificate also allows encrypted communication between the web server and the user, preventing stealing and alteration of communication data.

As described above, communication security is ensured by HTTPS.

3. LOCAL CERTIFICATION AUTHORITY.

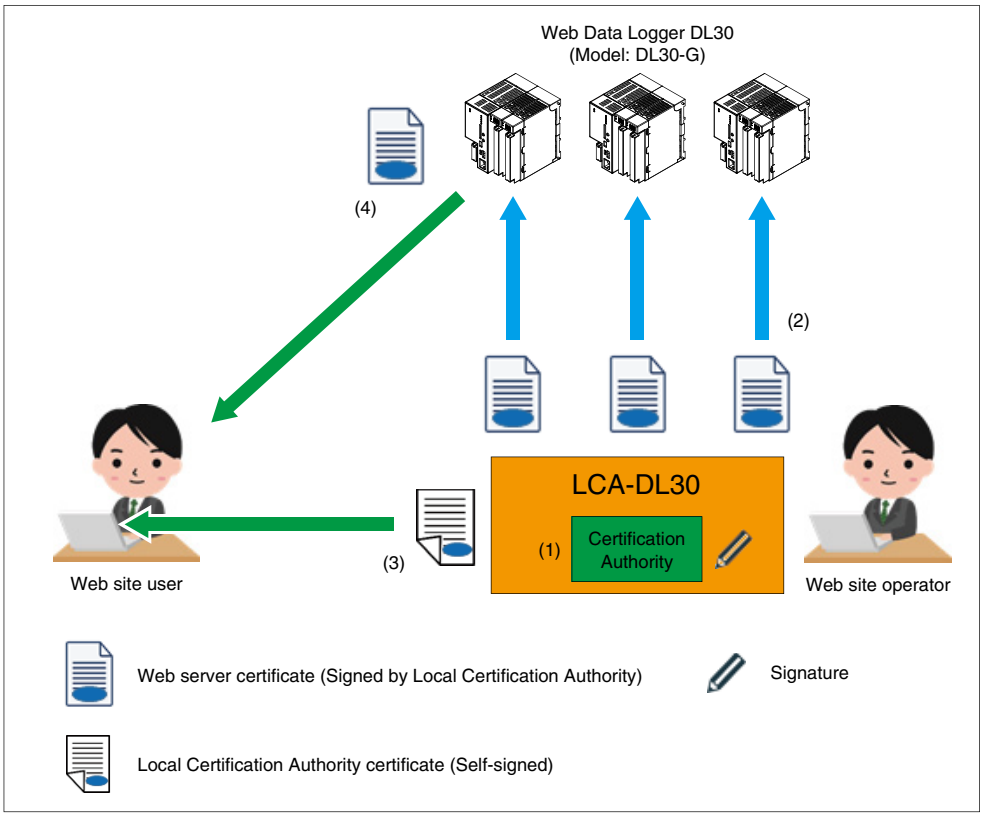
When accessing a general web site where a large number of unspecified users are expected, it is inevitable to verify the identity of the web server by a third party Certification Authority. However, as far as simple web servers built in industrial equipment are concerned, one is the web server operator and its user at the same time in many cases. That is, the operator of the web server accesses its own web site as a user.
In such a case, it will not be a problem if verification of identity by a third party Certification Authority is omitted.

M-System's Local Certification Authority Creator (model: LCA-DL30) facilitates simplification of such verification.

The software program can be downloaded from the M-System web site: ➔ http://www.m-system.co.jp/

Below is the procedure followed using Local Certification Authority Creator when the user and Certification Authority are identical.

(1) A Certification Authority is created in your PC at an initial startup of LCA-DL30 after it has been installed.
(2) A web server certificate is created for each device, signed automatically, and transferred to the device.
(3) The Local Certification Authority certificate is manually installed in the browser/OS of the terminal of the user.



What is different from normal HTTPS connection is that the certificate for the Local Certification Authority of LCA-DL30 is not pre-installed in browsers and needs to be manually installed ((3) in the above figure).

With LCA-DL30, verification of identity of the web server required when using HTTPS can be simplified. LCA-DL30 can also be used in an LAN environment, allowing HTTPS in a local network.

NOTES

- Files generated by LCA-DL30 contain data which is important in terms of security. Handle such data with utmost care.
- The HTTPS server of DL30-G and LCA-DL30 CANNOT guarantee complete data security. Handling of data is at your own risk and responsibilities.

4. HOW TO USE LCA-DL30

4.1 System requirements

■ **SYSTEM REQUIREMENTS**

HARDWARE	REQUIREMENT
PC	IBM PC/AT or compatible
Operating System	Windows 10 Home, Professional, Enterprise editions (32-bit / 64-bit)
Other than OS	DOT.NET Framework 4 or later
CPU	2 GB or more
Hard disk area	60 MB or more (Separately secure hard disk space for user data)
Display resolution	XGA (1024 x 768) or more
Language	English / Japanese

4.2 Installation

The software program can be downloaded from the M-System web site.
➔ http://www.m-system.co.jp/

Download the compressed file on your PC, and decompress the file that contains 'Setup.exe'.
Execute 'Setup.exe' and install the program by following the instructions on the installer.

A security warning message may appear during the installation.
Confirm that the compressed files are ones downloaded from the M-System's HTTPS server before continuing the installation.

4.3 Creating a Local Certification Authority

The Local Certification Authority is automatically created at an initial startup of LCA-DL30 after installation.

(1) The [Organization Name] dialog as shown in Figure 4.1 will appear at an initial startup of LCA-DL30. *1
Enter the name of your company, organization, etc., to represent the Local Certification Authority and click [OK].

(2) The confirmation dialog as shown in Figure 4.2 will appear.
Click [OK].

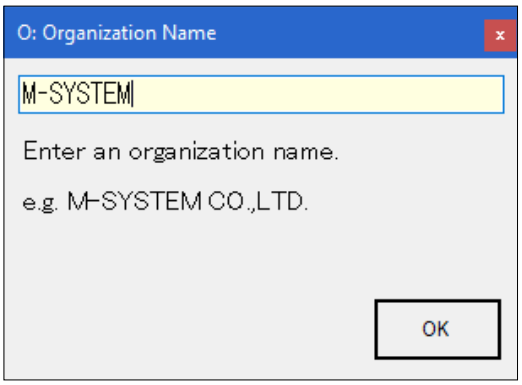


Figure 4.1 Organization Name entry screen

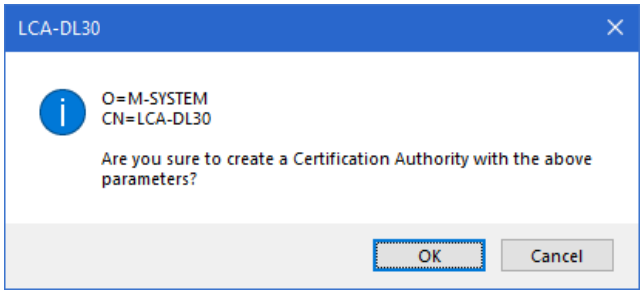


Figure 4.2 Confirmation dialog

*1 The [Organization Name] dialog only appears at the initial startup of LCA-DL30.

PARAMETER ITEM	DESCRIPTION
Organization Name	Enter the company/organization name as the name of the Local Certification Authority of LCA-DL30. Available characters First character : A-Z, a-z, " _ (underline)" Second and after: A-Z, a-z, 0-9, " _ (underline)", " , (comma)", " . (period)", " - (hyphen)", " (blank)"

(3) When the Local Certification Authority has been created, the LCA-DL30 main screen as shown below appears.
Confirm that the entered name is displayed for "O" in the [Certification Authority] frame.

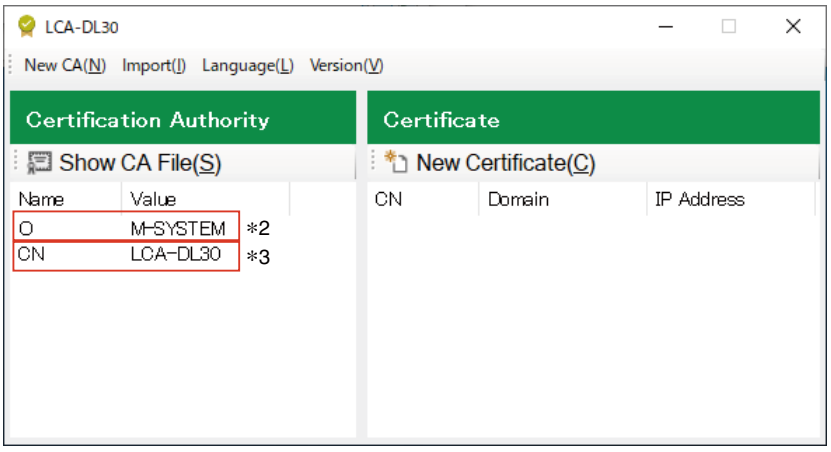


Figure 4.3 Main Screen

*2. The organization name cannot be changed once the Local Certification Authority has been created.
To change the organization name, rebuild the Certification Authority with referring to "4.7 Rebuilding Local Certification Authority" on page 24.

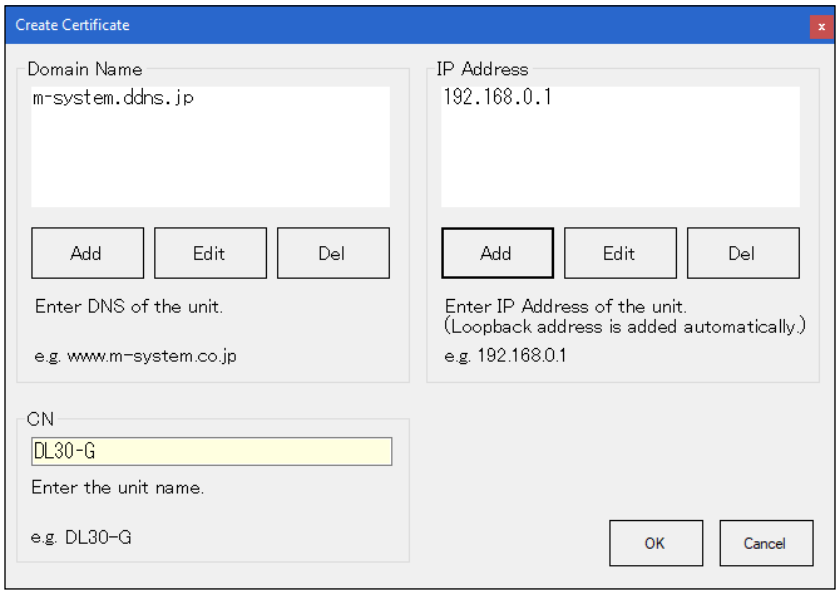
*3. "LCA-DL30" is for display only and cannot be edited or deleted.

4.4 Creating and Transferring Web Server Certificate

In order to create a Web server certificate for DL30-G and transfer the certificate to the device, follow the procedure below.

(1) Click [New Certificate(C)] on the main screen to display the [Create Certificate] window.

(2) Click [Add] and enter the domain name or IP address of the DL30-G
When two or more DL30-G units exist, add the domain name or IP address for each unit or simply register one unit per certificate by repeating from step (1) for another unit, according to need.
Click [OK].



4.4 [Create Certificate] window

PARAMETER ITEM	DESCRIPTION
Domain Name	Enter the domain name of DL30-G for accessing the device via the internet using alphanumeric characters (Japanese domain name not allowed). Up to 8 domain names can be registered.
IP Address	Enter the IP address of DL30-G for accessing the device via the internet or LAN using alphanumeric characters (Not compatible with IPv6). Up to 8 IP addresses can be registered.
CN	Available characters First character : A-Z, a-z, " _ (underline)" Second and after: A-Z, a-z, 0-9, " _ (underline)", " , (comma)", " . (period)", " - (hyphen)", " (blank)"

(3) As the confirmation dialog appears, click [Yes] to display the [Transfer] window.

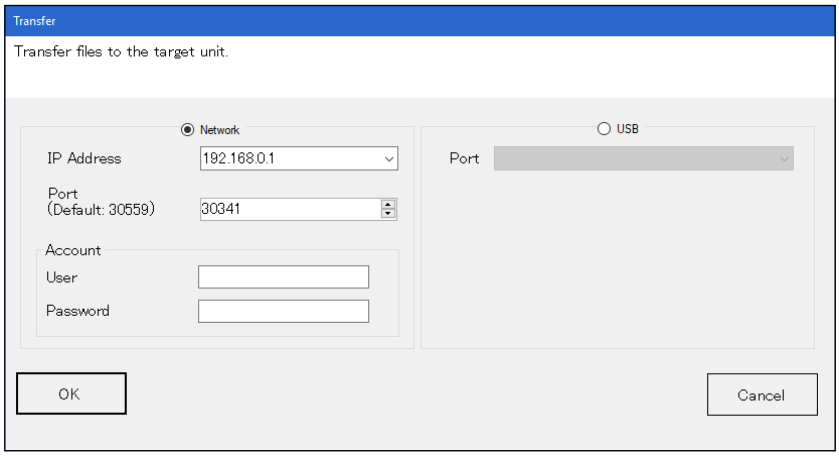


Figure 4.5 [Transfer] window

(4) In the same manner as the connection setting on DL30GCFG, select the connection method between [Network] and [USB].
Enter the IP Address or Domain Name, and the user name and password of the DL30-G to connect.
Click [OK] to start the transfer of the Certificate to the device.

(5) On the main screen, the certificate which has been just created is displayed on the [Certificate] frame.

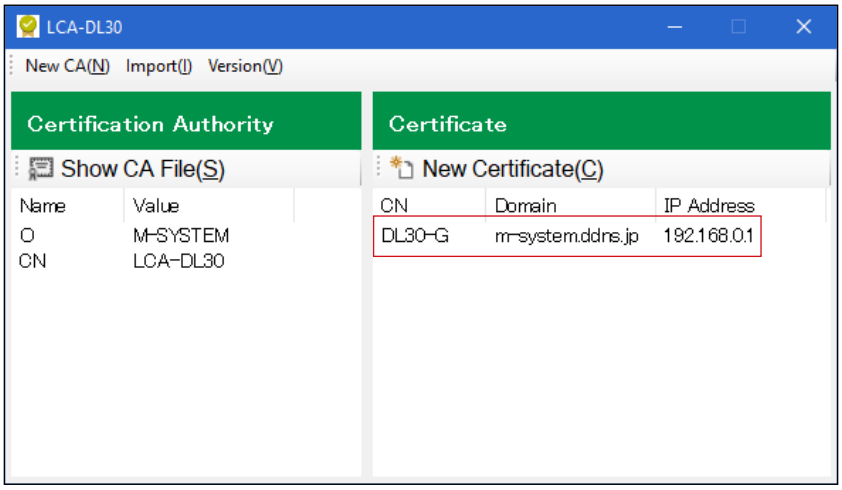


Figure 4.6 List of Certificates

(6) When two or more DL30-G units exist, right-click on the relevant certificate on the main screen to display the submenu, and select [Create / Transfer] to display the [Transfer] window.
Follow the step (4).

Even if the LCA-DL30 is restarted, the registered Certification Authority and Certificates will remain on the list unless they are deleted.
To delete a Certificate, right-click on the Certificate to display the submenu and select [Delete].

NOTES

- DO NOT access the DL30-G web server when transferring the certificate to the device.
- A security warning will appear when accessing over HTTPS if the Domain Name or IP Address is wrong. Please pay close attention when entering the Domain Name or IP Address.
- The Web server certificate expires in 730 days (approx. 2 years) after it has been transferred. Be sure to retransfer the certificate regularly before expiration date as the browser cannot connect to the DL30-G device via HTTPS protocol once it has expired.

4.5 Installing Local Certification Authority Certificate

4.5.1 Local Certification Authority Certificate

The certificate for the Local Certification Authority created on "4.3 Creating a Local Certification Authority" on page 7 needs to be installed on the terminal which connects to the DL30-G web server.

This procedure must be performed on every terminal to connect to the device which has certificate signed by this Local Certification Authority.

If not, a security warning will appear on the browser when the DL30-G is accessed over HTTPS without the certificate.

The installation method varies depending on the software environment of the terminal.

4.5.2 Installing via LCA-DL30

Windows (Chrome, Edge)

(1) Click [Show CA File(S)] on the main screen to display the [Certificate] window.
Click [Install Certificate..] to start the [Certificate Import Wizard].

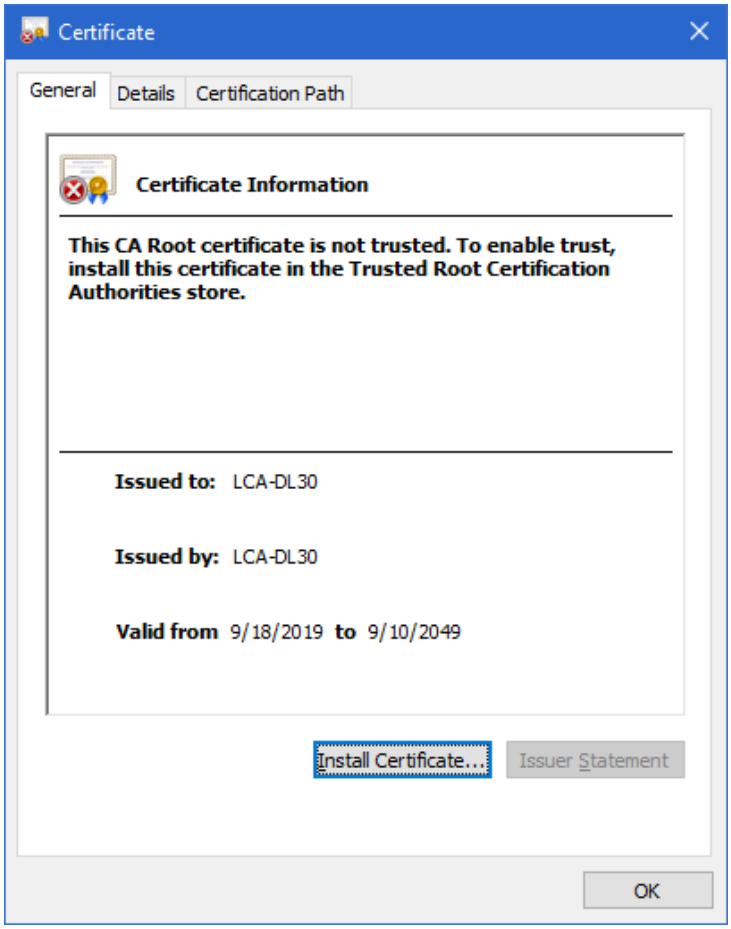


Figure 4.7 [Certificate] window when [General] tab is selected

(2) As the [Welcome to the Certificate Import Wizard] screen of the Wizard appears, select [Current User] as the store location, and click [Next].

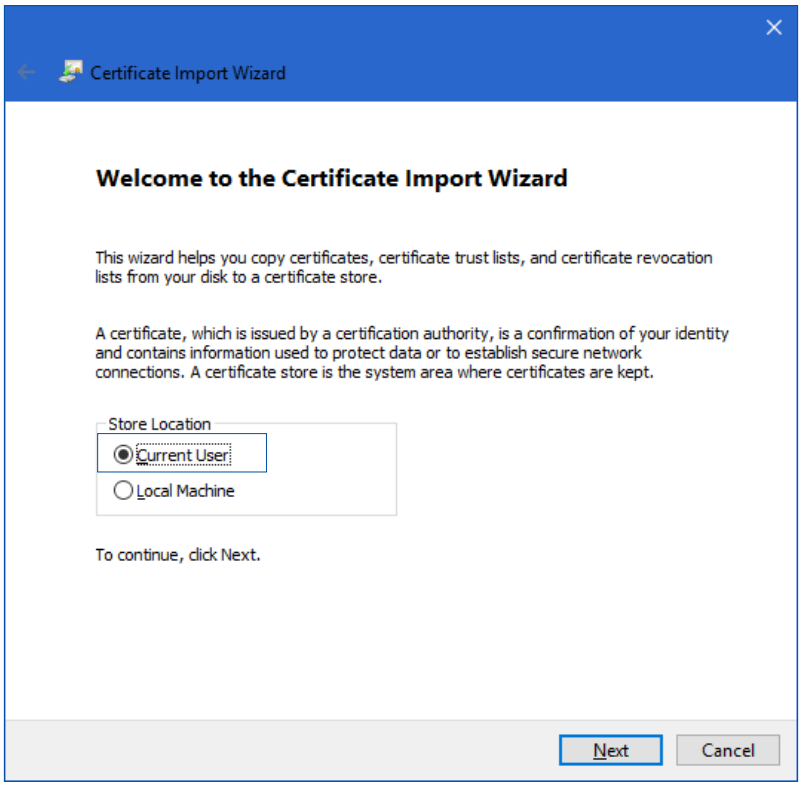


Figure 4.8 Initial View of [Certificate Import Wizard]

(3) As the [Certificate Store] screen of the Wizard appears, select [Place all certificates in the following store], and click [Browse].

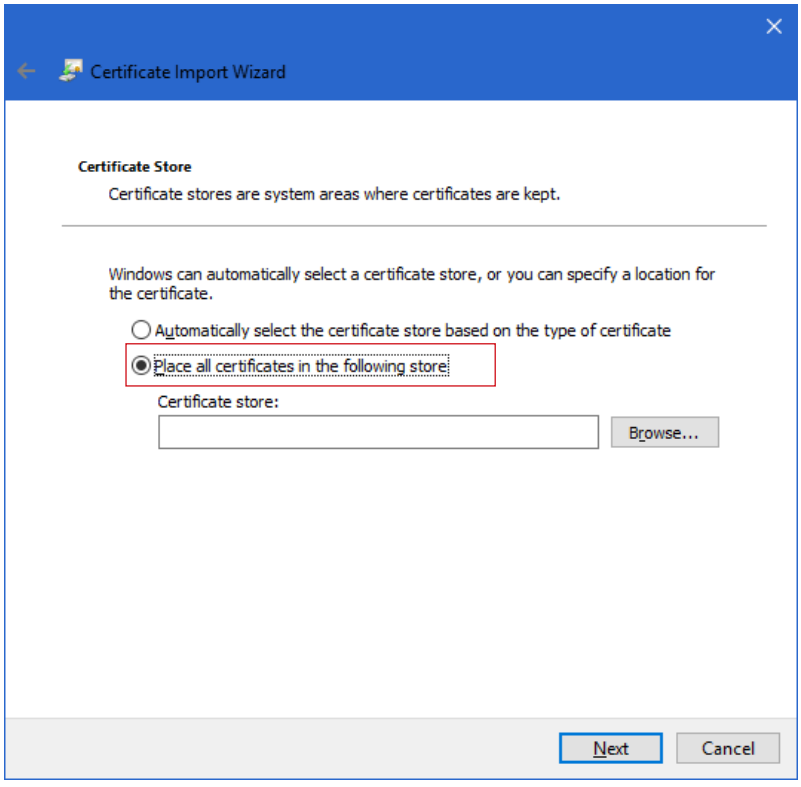


Figure 4.9 [Certificate Store] screen

(4) As the [Select Certificate Store] dialog appears, select the [Trusted Root Certification Authorities] folder, and click [OK].

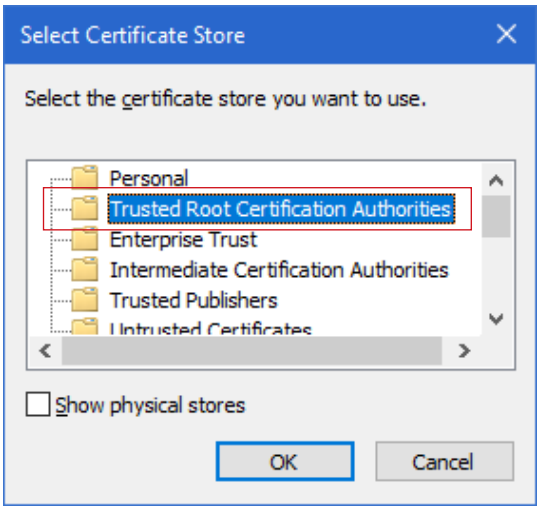


Figure 4.10 [Select Certificate Store] dialog

(5) A Windows security warning may appear while the wizard is running.
Read the warning message and determine whether there are any problems as the User (yourself) is the Route Certification Authority on the LCA-DL30, and click [OK].

Windows (Firefox)

(1) Click [Show CA File(S)] on the main screen to display the [Certificate] window.
Click the [Details] tab, then click [Copy to File...].

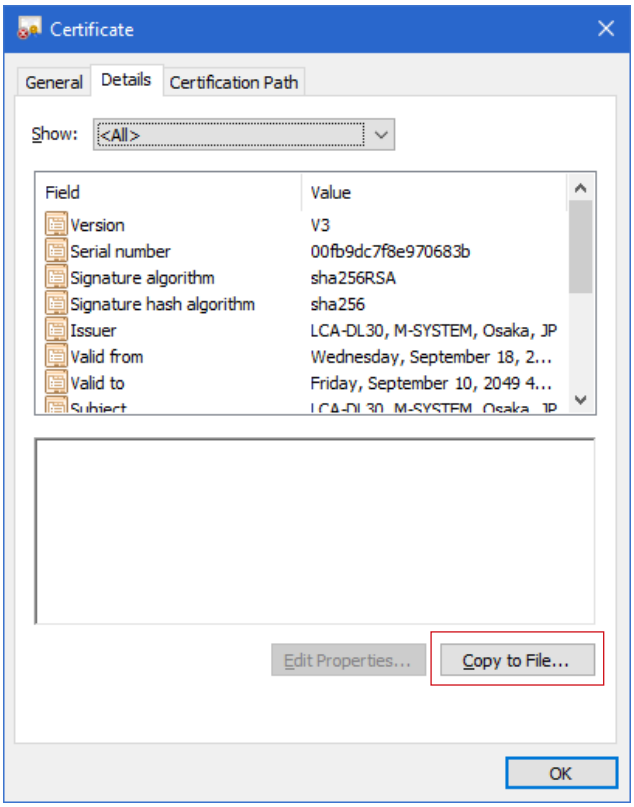


Figure 4.11 [Certificate] window when [Details] tab is selected

(2) As the [Export File Format] screen of the Wizard appears, select [Base-64 encoded X.509 (.CER)] as the format, and click [Next].

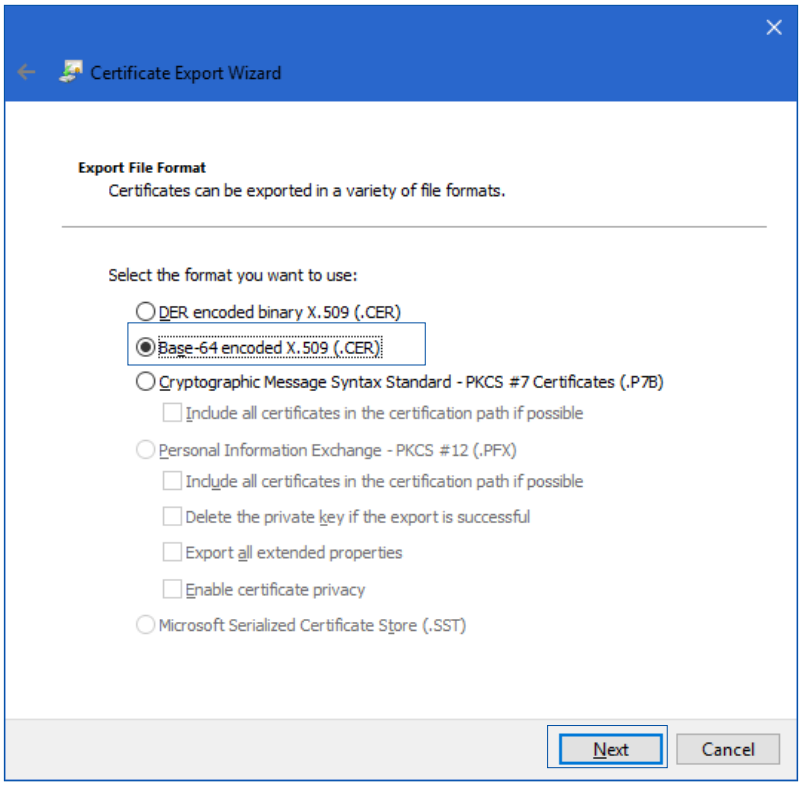


Figure 4.12 [Export File Format] screen of [Certificate Export Wizard]

(3) Enter the File name, click [Browse] to specify the save location (ex. desktop), and save. Close the [Certificate Export Wizard].

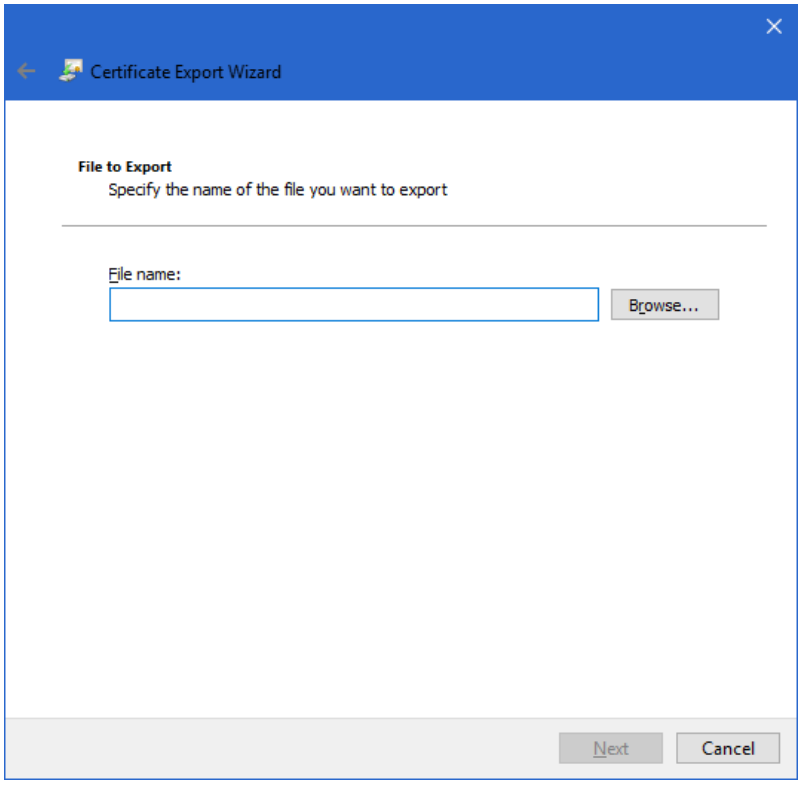


Figure 4.13 [File to Export] screen of [Certificate Export Wizard]

(4) Start the Firefox browser.
Right-click on the menu at the right top and select [Options] to open the [Options] tab.

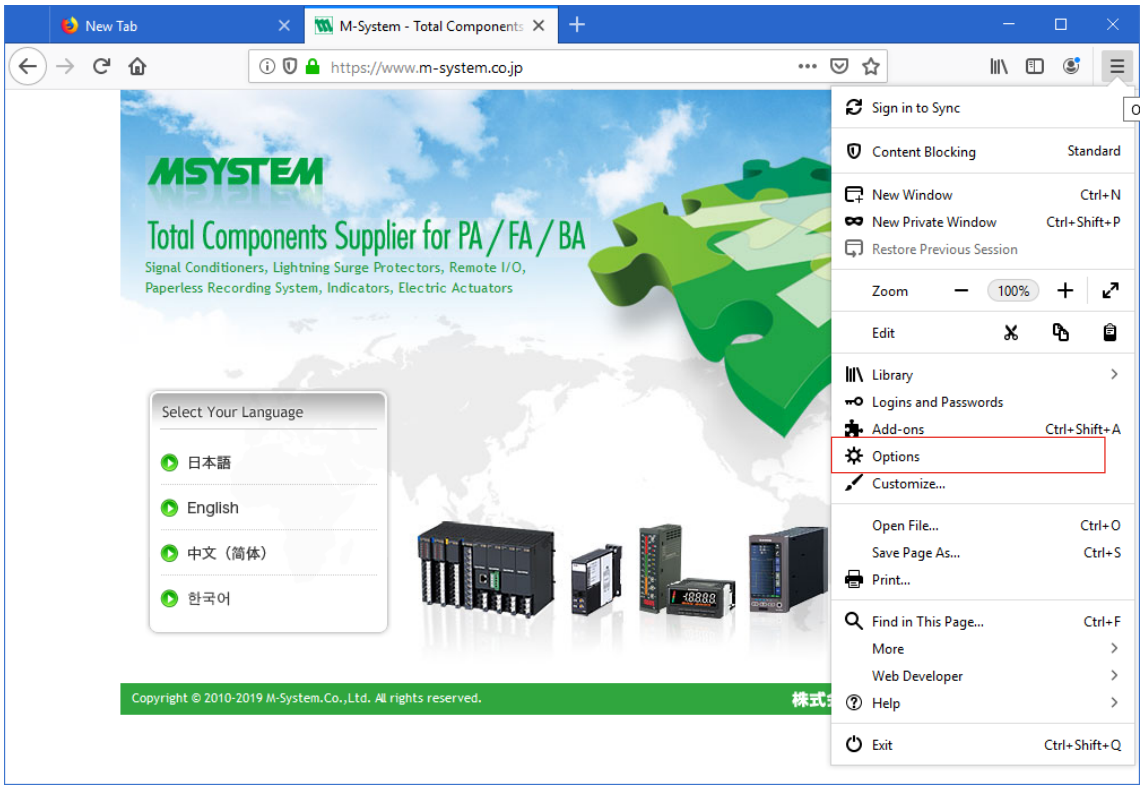


Figure 4.14 Firefox browser

(5) Click [Privacy & Security] to display 'Security' options.

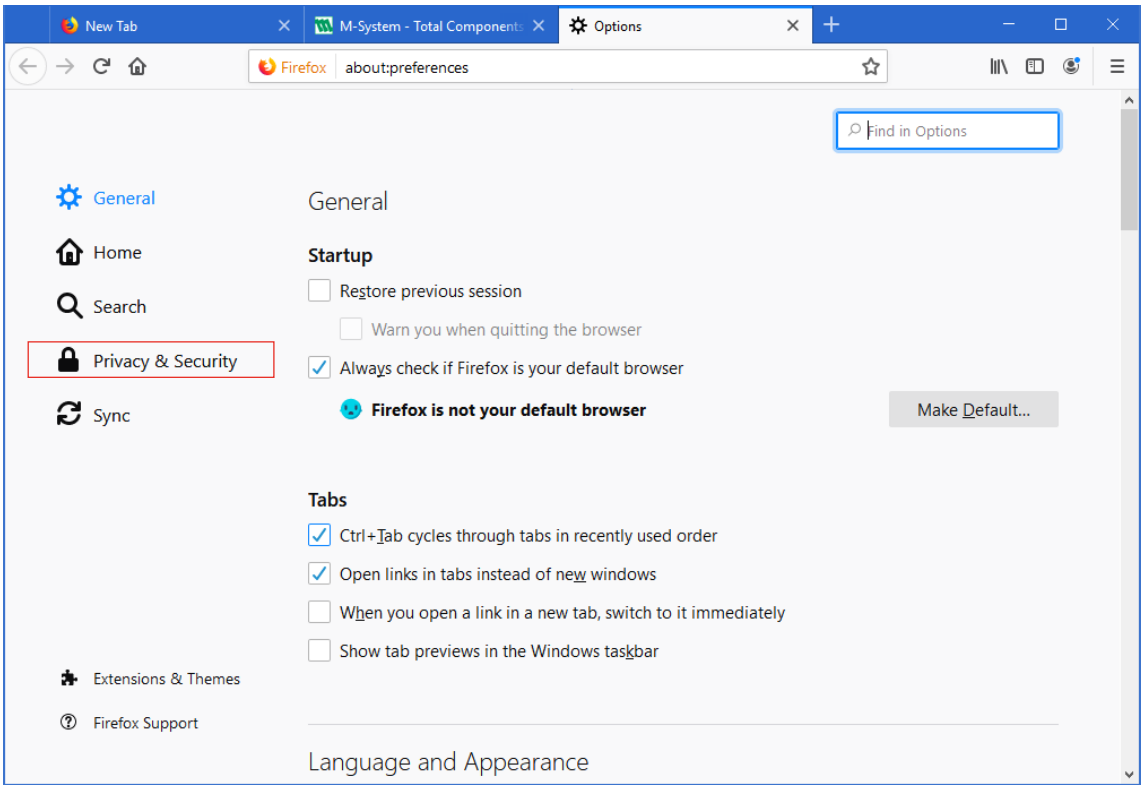


Figure 4.15 Firefox [Options] screen

(6) Click [View Certificates...] to display the [Certificate Manager] window.

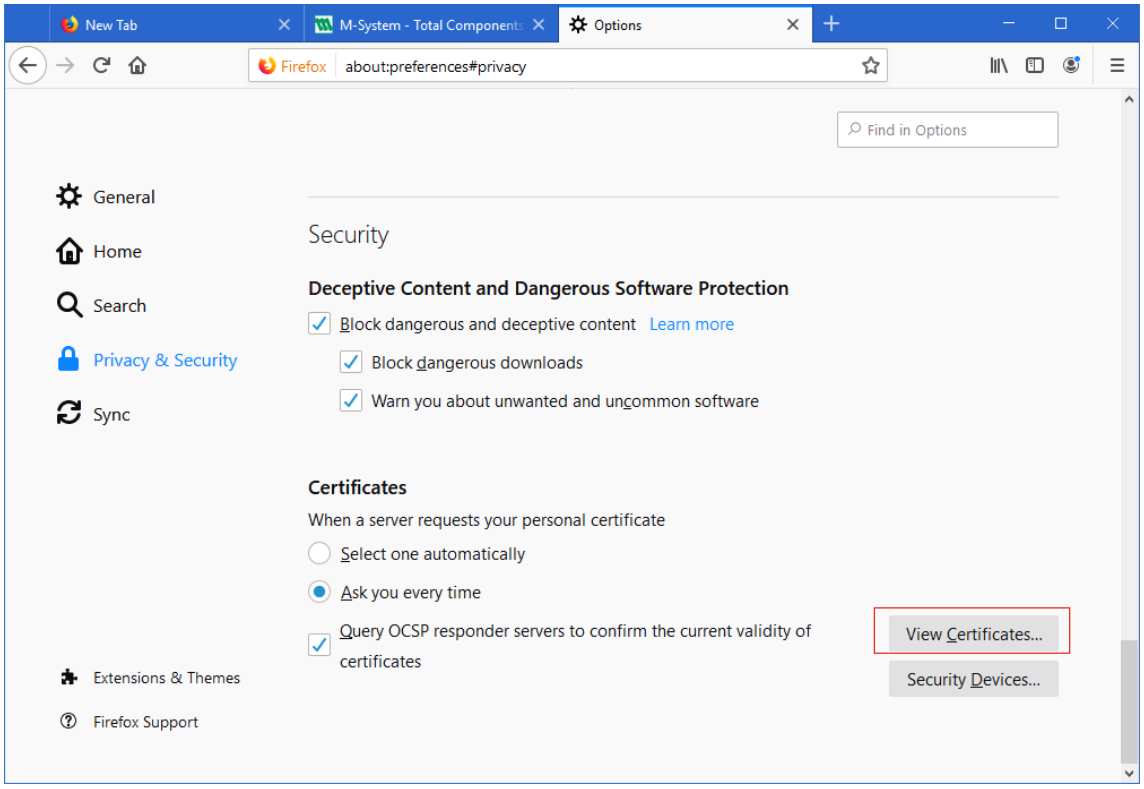


Figure 4.16 Firefox [Privacy & Security] screen

(7) Click [Import] to display the File Selector window.

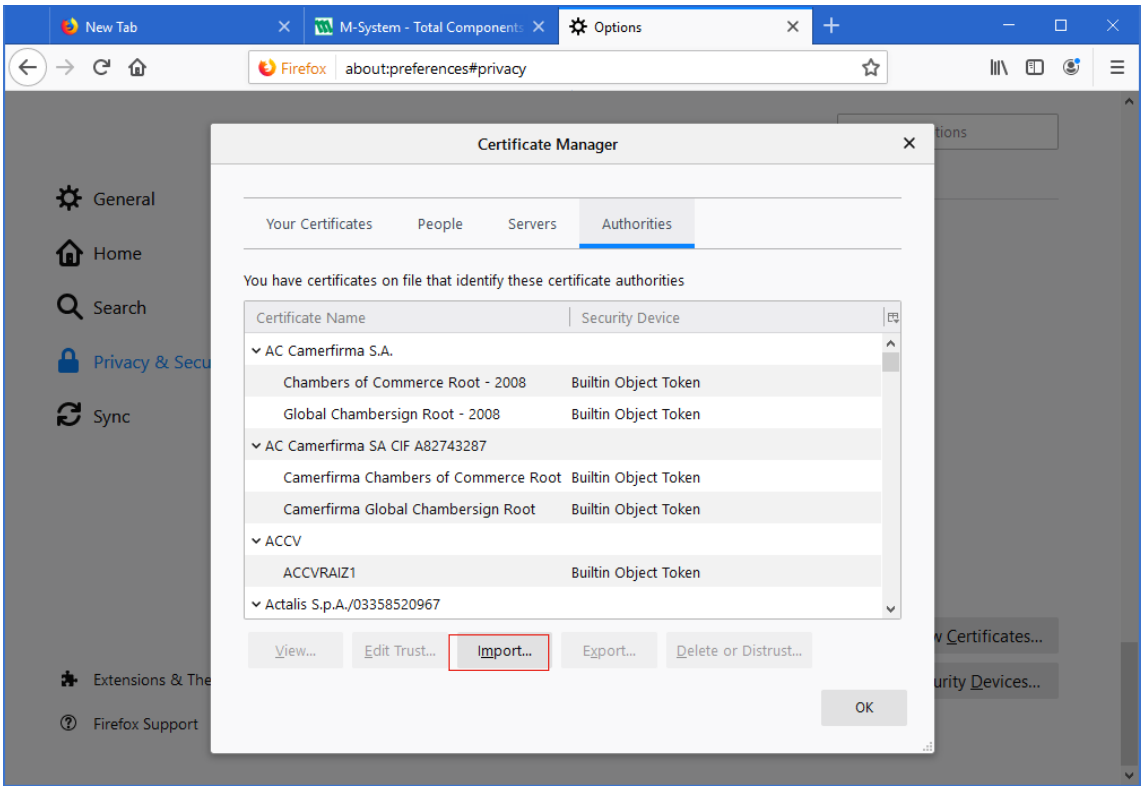


Figure 4.17 Firefox [Certificate Manager] window

(8) Locate the file (.CER) saved in (3), and click [Open] to display the [Downloading Certificate] dialog.

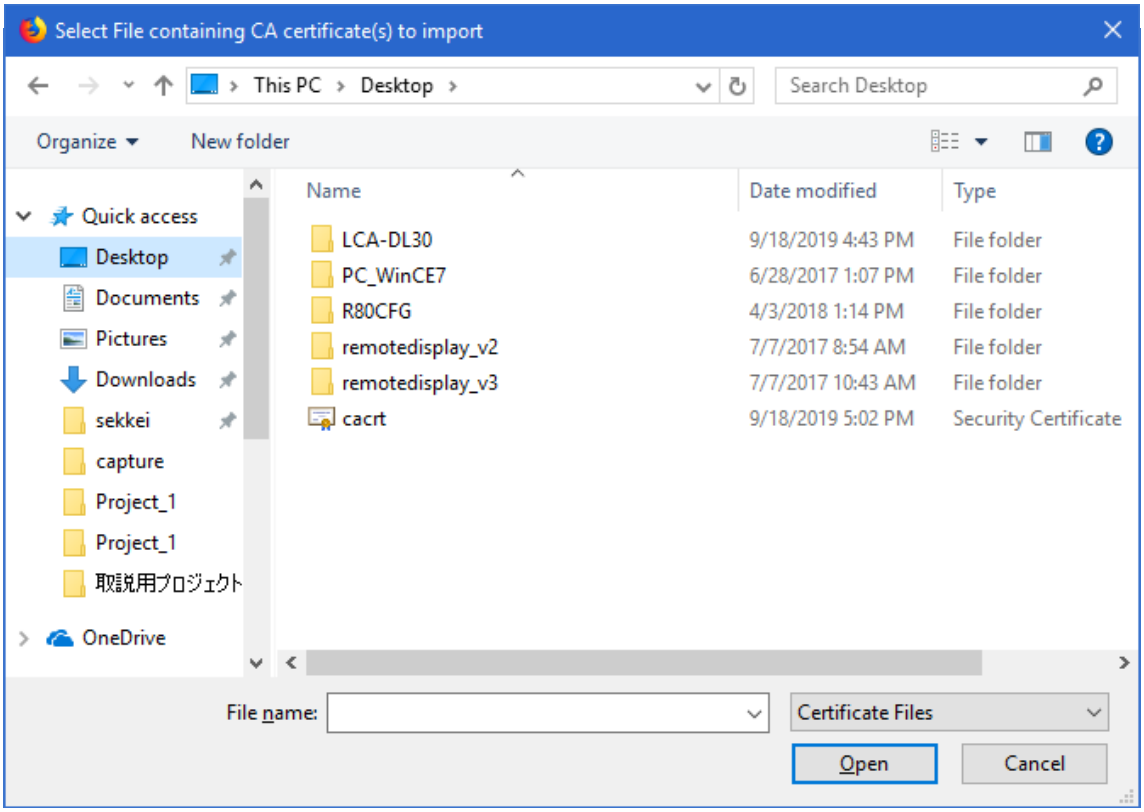


Figure 4.18 File Selector window

(9) Check [Trust this CA to identify websites] and click [OK] to register the certificate for the Local Certification Authority of LCA-DL30 on the Firefox browser.

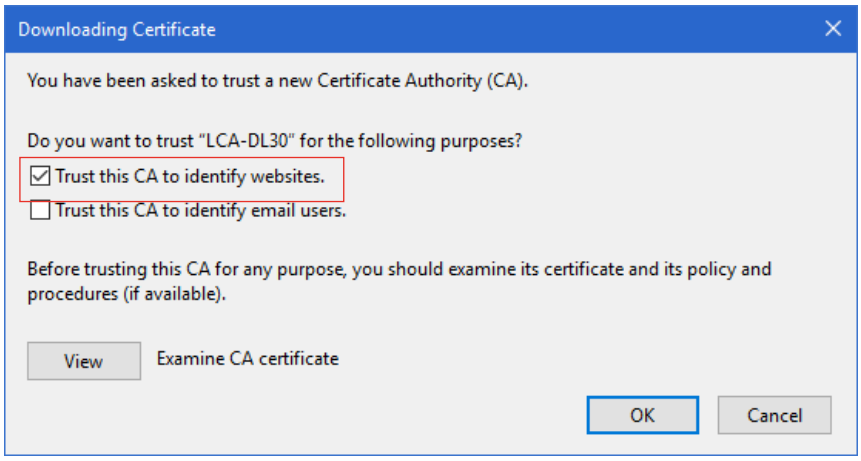


Figure 4.19 Firefox [Downloading Certificate] dialog

(10) Close the Firefox browser.

4.5.3 Using Certification Authority Certificate

Windows (Chrome, Edge)

(1) Click [Show CA File(S)] on the main screen to display the [Certificate] window.
Click [Install Certificate..] to start the [Certificate Import Wizard].

(2) Follow the same procedure as in "Windows (Chrome, Edge)" on page 10.

Windows (Firefox)

(1) Follow the same procedure from step (4) of "Windows (Firefox)" on page 12.

4.5.4 Installing from DL30-G

First, set the web server protocol of the DL30-G as HTTPS and follow the procedure below.

Windows (Chrome, Edge, Firefox)

To install the certificate created on LCA-DL30 and transferred to the DL30-G, connect to the device over HTTPS to download the file.

(1) Enter “http://<DL30G-IP Address>” to download the Certification Authority certificate file (cacert.crt).

(2) After the file has been downloaded, follow the same procedure as in "4.5.3 Using Certification Authority Certificate" on page 17.

iOS (Safari)

To install the certificate created on LCA-DL30 and transferred to the DL30-G, connect to the device over HTTPS to download the file.

(1) Enter “http://<DL30G-IP Address>” to display the dialog below.

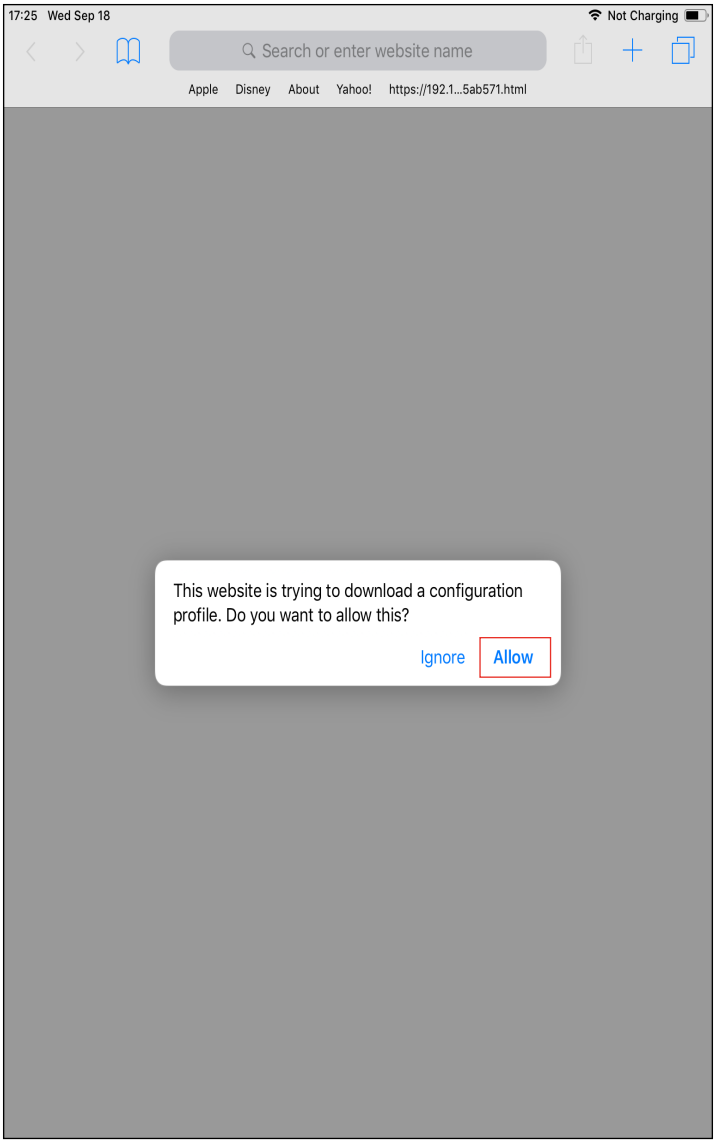


Figure 4.20 iOS Download confirmation dialog

(2) Click [Allow] to download the file.

(3) After the file has been downloaded, go back to the Home screen, and tap the gear icon for Settings. Click [Profile Downloaded] to display the downloaded Profile.

Figure 4.21 iOS Settings Screen

(4) Tap the downloaded profile to display the [Install Profile] window.
Tap [Install] at the right top of the window to start the installation of the profile on the terminal.
If a security warning appears during the installation, tap [Install] again to continue the installation.

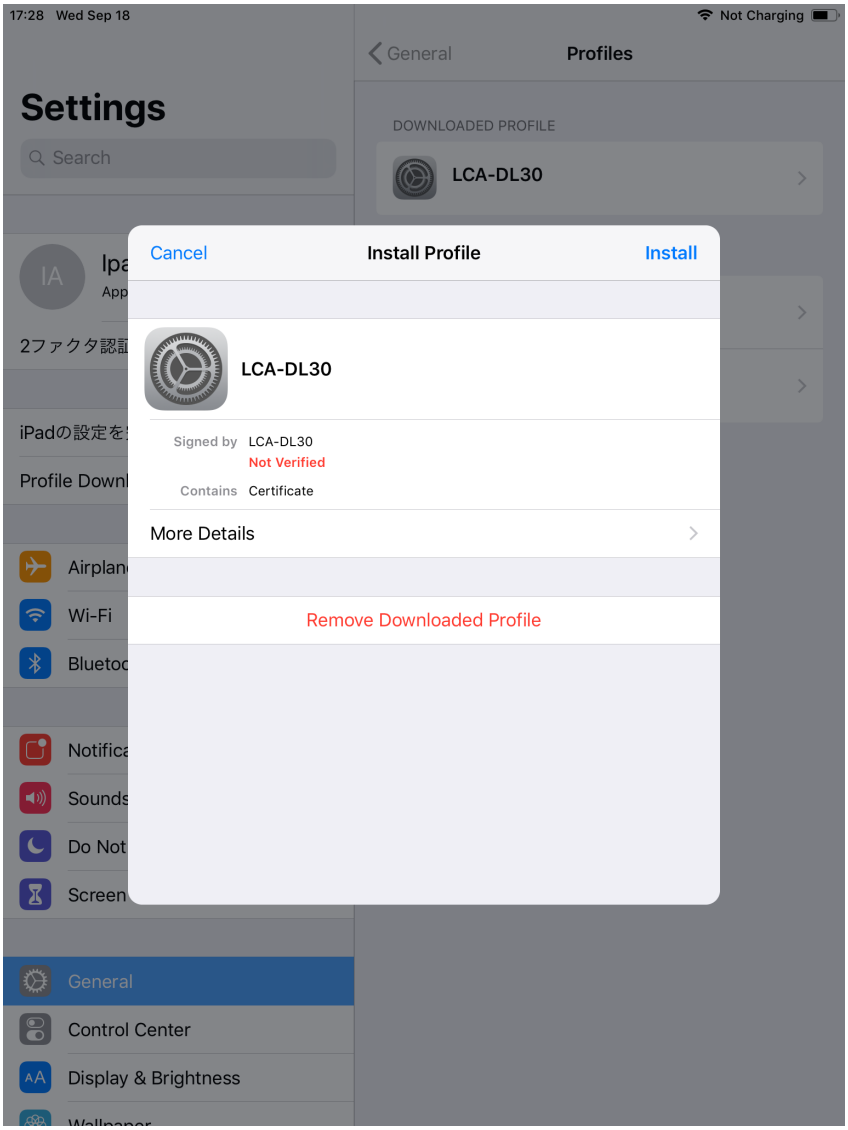


Figure 4.22 iOS [Install Profile] window

(5) When the installation has been completed, tap [Settings] > [General] > [About] > [Certificate Trust Settings] to open the [Certificate Trust Settings] screen.
Check [ENABLE FULL TRUST FOR ROOT CERTIFICATES] to enable trust for the downloaded certificate.

Android (Chrome)

(1) Download the Certification Authority certificate following the same procedure for iOS and open the downloaded certificate.

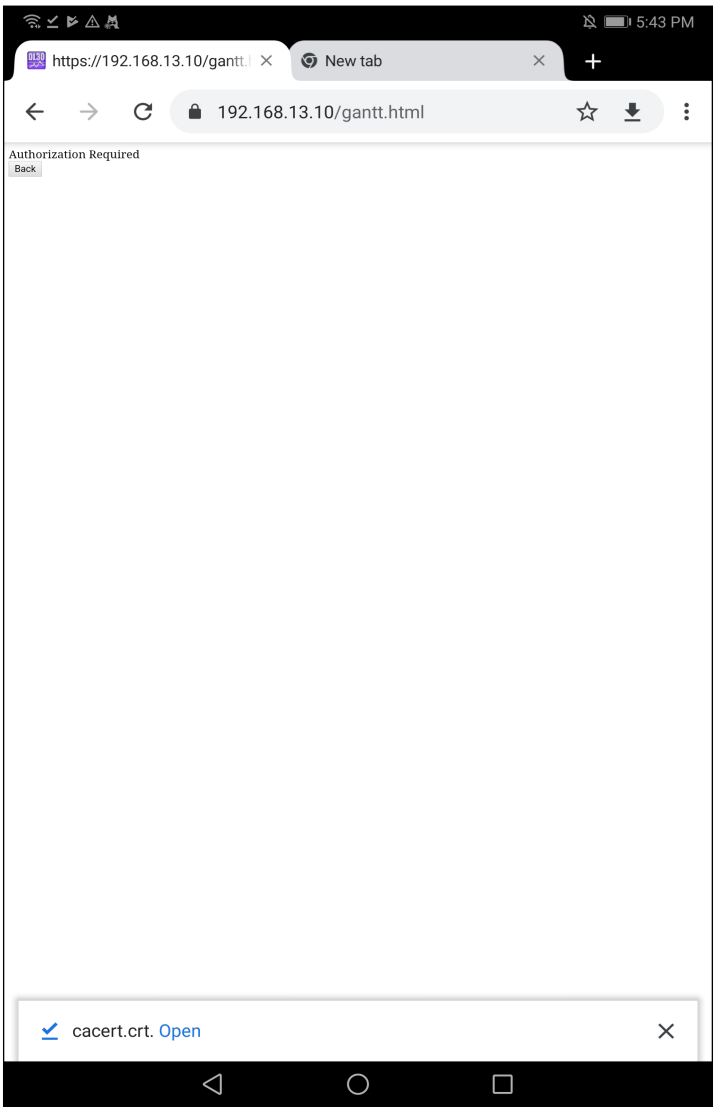


Figure 4.23 Android cacert.crt opening screen

(2) As the Certificate Installer starts, enter the certificate name and click [OK] to register the certificate.

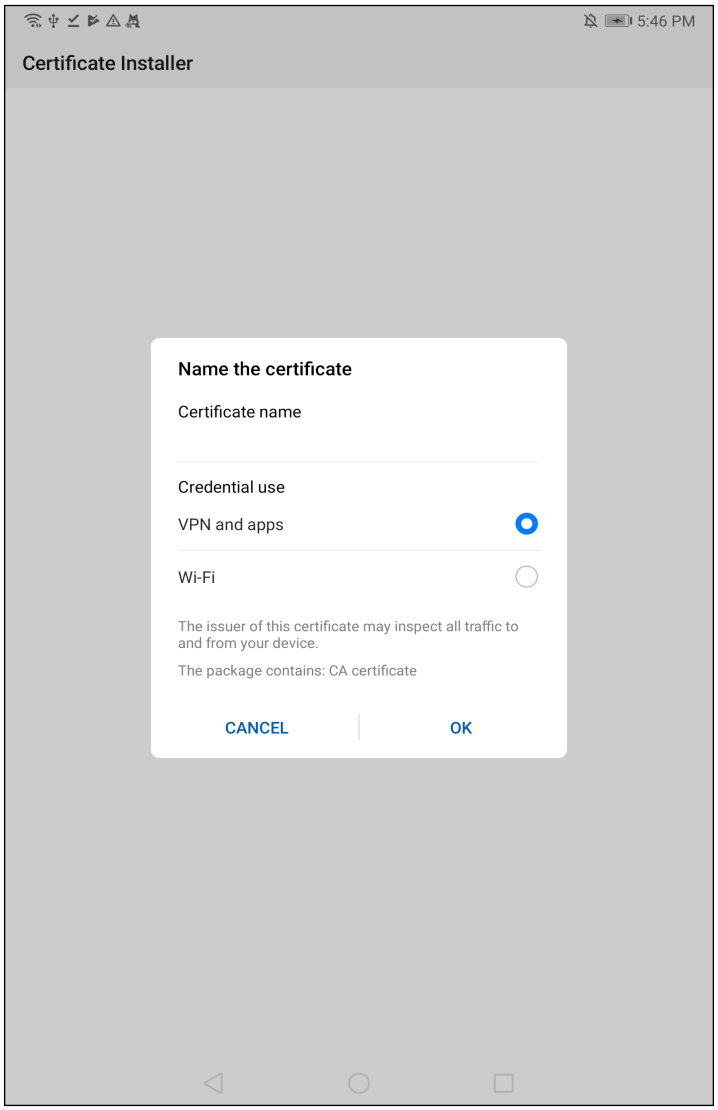


Figure 4.24 Android Certificate Installer

4.6 Importing Certificate

Certificate for your web server can also be signed by a third party Certification Authority as in the same manner as when normally opening a web site using HTTPS without using the Local Certification Authority of LCA-DL30.

(1) Click [Import(I)] on the LCA-DL30 main screen to display the [Import] dialog.

(2) Specify the file name and key/password and click [OK] to transfer the certificate and the secret key to the DL-30.

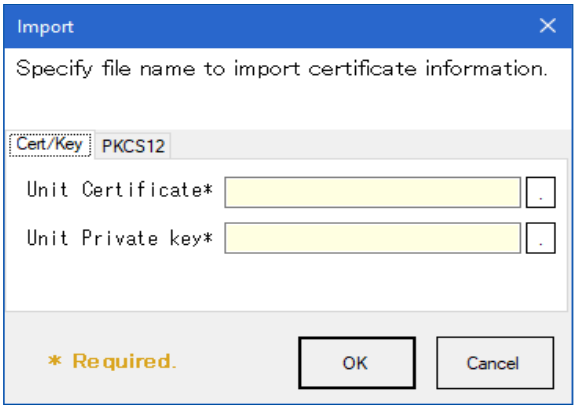


Figure 4.25 File importing dialog for DER format

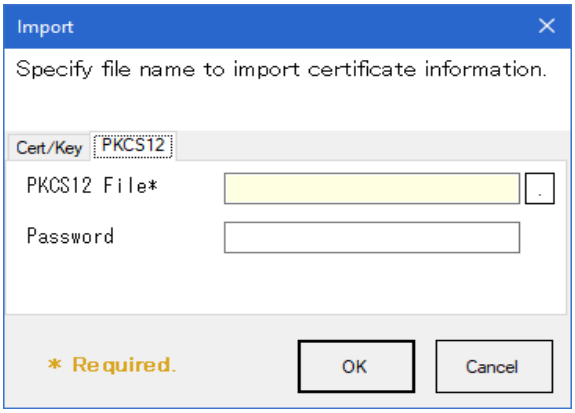


Figure 4.26 File importing dialog for PKCS12 format

Compatible file formats: DER (.crt, .key, .der)
PKCS12 (.pfx, .p12)

NOTES

- We are unable to answer any questions about certificates signed by third-party Certificate Authorities or the import of such certificates.

4.7 Rebuilding Local Certification Authority

Normally, there is no need to rebuild the Local Certification Authority which has been automatically created at initial startup of LCA-DL30 after installation.
However, if need arises, rebuilt the Local Certification Authority by clicking [New CA(N)] on the main screen and following the procedure in "4.3 Creating a Local Certification Authority" on page 7.

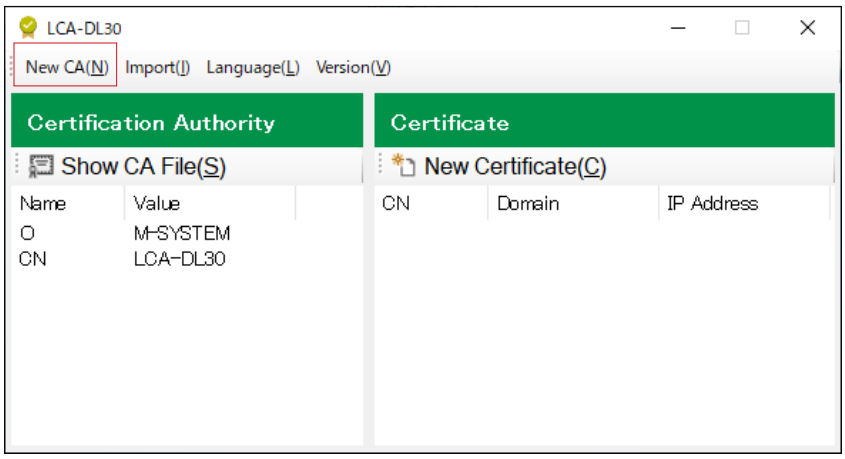


Figure 27 Rebuilding Local Certification Authority

In that case, the certificate for the new Local Certification Authority must be manually installed on the browser/OS of the terminal of the user again. See "4.5 Installing Local Certification Authority Certificate" on page 10.

4.8 Switching Display Language

The display language of LCA-DL30 is automatically selected depending on the language of your OS.
Japanese is selected for Japanese OS and English is selected for OS non-Japanese OS.
In order to manually switch the display language, click [Language(L)] on the main screen to display the language switching dialog.
Restart LCA-DL30 to apply the change.

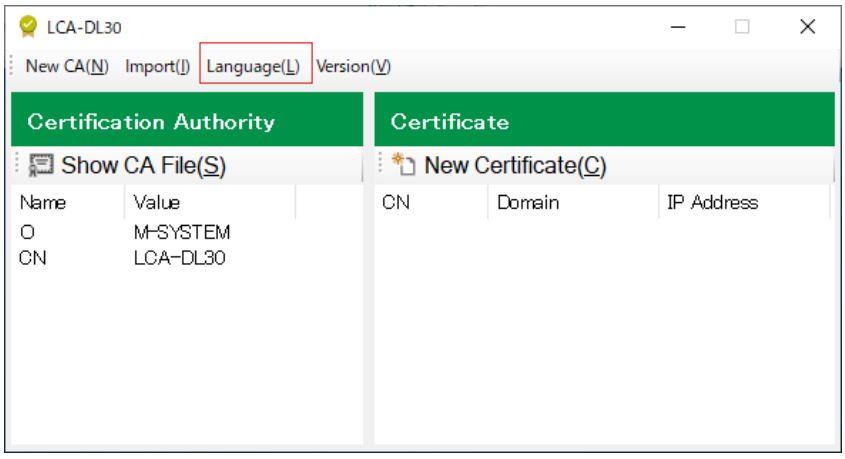


Figure 28 Switching Display Language

5. LICENSE

The LCA-DL30 uses OpenSSL v1.0.1r (dual license of OpenSSL and Original SSLeay).

The LCA-DL30 contains software to which the following Camellia license is applicable.

OpenSSL License

==========

Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)." The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence].

camellia.c ver 1.2.0

Copyright (c) 2006, 2007
NTT (Nippon Telegraph and Telephone Corporation). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer as the first lines of this file unmodified.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY NTT "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL NTT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.