LOCAL CERTIFICATION AUTHORITY CREATOR Model: LCA-RGP

USERS MANUAL

Table of Contents

1.	INTRODUCTION	3
	1.1 Overview	3
2.	WEB SERVER CERTIFICATE	4
3.	LOCAL CERTIFICATION AUTHORITY	5
4.	HOW TO USE LCA-RGP	6
	4.1 System requirements	6
	4.2 Installation	
	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-RGP	11
	Windows (Chrome, Edge)	
	Windows (Firefox)	
	4.5.3 Using Certification Authority Certificate	
	Windows (Chrome, Edge)	
	Windows (Firefox)	
	4.5.4 Installing from RGP	
	Windows (Chrome, Edge, Firefox)	
	iOS (Safari)	
	Android (Chrome)	
	4.6 Importing Certificate	
	4.7 Rebuilding Local Certification Authority	
	4.8 Switching Display Language	25

5. LICENSE

26

1. INTRODUCTION

Thank you for downloading our software program.

1.1 Overview

RGPx supports HTTPS for enhancing secure communication. This users manual describes how to create certificates which are indispensable when using HTTPS.

Note: RGP30 Ver. 1.1 or later, or RGP6 Ver 1.0 or later is required to use HTTPS. Update the RGP30 to Ver 1.1 when using Ver 1.0.

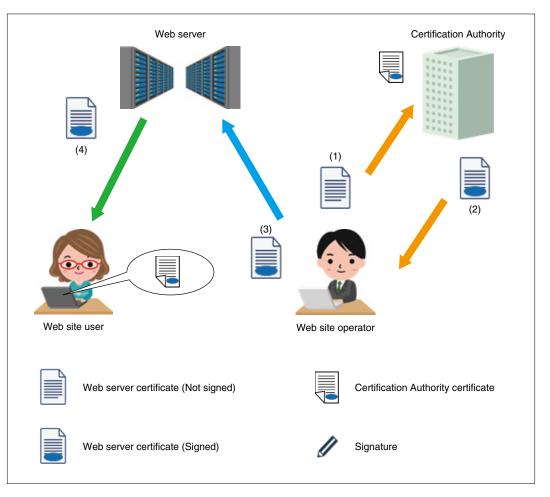
2. WEB SERVER CERTIFICATE

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 server s 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.

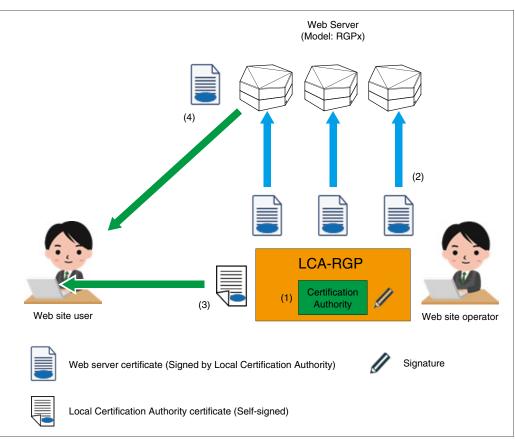
In such a case, it will not be a problem if verification of identity by a third party Certification Authority is omitted.

The Local Certification Authority Creator (model: LCA-RGP) facilitates simplification of such verification.

The software program can be downloaded from the our web site.

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-RGP 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-RGP is not pre-installed in browsers and needs to be manually installed ((3) in the above figure).

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

NOTES

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

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 our web site.

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 our HTTPS server before continuing the installation.

4.3 Creating a Local Certification Authority

Enter the name of your company, organization, etc, and expire date of the certification at an initial startup of LCA-RGP.

Enter the name of your company, organization, etc, to represent the Local Certification Authority.

The dialog to set the expire date of the certification will appear. Enter within 30 to 3653 days.

The confirmation dialog will appear after entering the all contents.

Confirm that the registered organization name and expire date are indicated in "O=" and click [OK].

O: Organization Name	×	DAYS: Expire Date	×
M-SYSTEM		730	
Enter an organization na	ame.	Enter DAYS	
e.g. M-SYSTEM CO.,LTI	D.	(Default: 730)	
	>>	<<	ок
Figure 4.1 Organization	Name entry screen	Figure 4.2 Expire Date s	screen
	LCA-RGP	×	
	0=M-SYSTEM CN=LCA-RGP		
		Authority with the above	
	CN=LCA-RGP Are you sure to create a Certification	1 Authority with the above	
	CN=LCA-RGP Are you sure to create a Certification parameters?		

Figure 4.3 Confirmation dialog

*1 The [Organization Name] dialog only appears at the initial startup of LCA-RGP. To change the organization name, rebuild the Certification Authority. See "4.7 Rebuilding Local Certification Authority" on page 25.

PARAMETER ITEM	DESCRIPTION
Organization Name	Enter the company/organization name as the name of the Local Certification Authority of LCA-RGP. Available characters First character : A-Z, a-z, " _ (underline)" Second and after: A-Z, a-z, 0-9, " _ (underline)", " , (comma)", " . (period)", " - (hyphen)", " (blank)"
Expire Date	Enter the expire date of the certificate within 30 to 3653 days.

(3) When the Local Certification Authority has been created, the LCA-RGP main screen as shown below appears.

Confirm that the entered name is displayed for "O" in the [Certification Authority] frame.

🔮 LCA-RGP	🙎 LCA-RGP — 🗆 🗙							
New CA(<u>N</u>)	Import(<u>I</u>) Language(L) Versior	Ś					
Certifica	tion Authority		Certifica	te				
🖾 Show	CA File(<u>S</u>)		1 New C	ertificate(<u>C</u>)				
Name O CN	Value M-SYSTEM LCA-RGP		CN	Domains	IP Ad	dresses		

Figure 4.4 Main Screen

4.4 Creating and Transferring Web Server Certificate

In order to create a Web server certificate for RGPx 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 RGPx

Create Certificate ×					
Domain Name m-system.ddns.jp	IP Address 192.168.0.1				
Add Edit Del Enter DNS of the unit. e.g. www.m-system.co.jp	Add Edit Del Enter IP Address of the unit. (Loopback address is added automatically.) e.g. 192.168.0.1				
CN RGP30-1 Enter the unit name. e.g. RGP-STATION1	OK Cancel				

4.5 [Create Certificate] window

PARAMETER ITEM	DESCRIPTION
Domain Name	Enter the domain name of RGPx for accessing the device via the internet using alphanumer- ic characters (Japanese domain name not allowed). Up to 8 domain names can be registered.
IP Address	Enter the IP address of RGPx for accessing the device via the internet or LAN using alphanu- meric 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)"

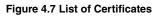
(3) As the confirmation dialog appears, click [Yes] to display the [Transfer] window.

Transfer					
Transfer files to the target unit.					
IP Address	192.168.35.245 ~				
Port					
(Default: 30559)	30559 ≑				
Account					
User					
USEI					
Password					
ок	Abort Cancel				
	Abort Cancel				

Figure 4.6 [Transfer] window

- (4) Enter the IP Address or Domain Name, and the user name and password of the RGP 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.

🔮 LCA-RGP					- [Х
New CA(<u>N</u>)	New CA(<u>N</u>) Import(<u>I</u>) Language(<u>L</u>) Version(<u>V</u>)						
Certifica	tion Authority		Certifica	ite			
🗐 Show	CA File(<u>S</u>)		📩 🔁 New (Certificate(<u>C</u>)			
Name	Value		CN	Domains	IP Addre	ses	
0	M-SYSTEM		RGP30-1	m-system.ddns.jp	192.168.0	D.1	
CN	LCA-RGP						



(6) When two or more RGP 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-RGP 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 RGPx web server while 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.

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 RGP 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 RGP 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-RGP

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].

08	Certificate	×
Ge	eneral Details Certification Path	
	Certificate Information	-
	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.	
	Issued to: LCA-RGP	
	Issued by: LCA-RGP	
	Valid from 7/16/2016 to 7/9/2046	
,	Install Certificate Issuer Statement	
	ОК	

Figure 4.8 [Certificate] window when [General] tab is selected

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

÷	Certificate Import Wizard	×
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	 Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: 	
	Browse	
	<u>N</u> ext Cano	el:

Figure 4.9 [Certificate Store] screen

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

Select Certificate Store	×
Select the <u>c</u> ertificate store you want to use.	
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates	^ ~
Show physical stores	
OK Cancel	

Figure 4.10 [Select Certificate Store] dialog

(4) 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-RGP, 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...].

🛺 Certificate		×
General Details Certific	ation Path	
Show: <all></all>	~	
Field	Value V3 00 8f ef 1e 08 ca 48 71 d7 sha256RSA thm sha256 LCA-RGP, M-SYSTEM, Osaka, JP Saturday, July 16, 2016 3:34: Monday, July 9, 2046 3:34:00 I CA-RGP M-SYSTEM Osaka 1P	
	OK	

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].

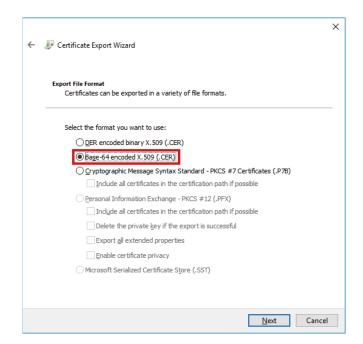


Figure 4.12 [Export File Format] screen of [Certificate Export Wizard]

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

		×
~	😺 Certificate Export Wizard	
	File to Export	
	Specify the name of the file you want to export	
	<u>F</u> ile name:	
	Browse	
	<u>N</u> ext Cance	I

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.

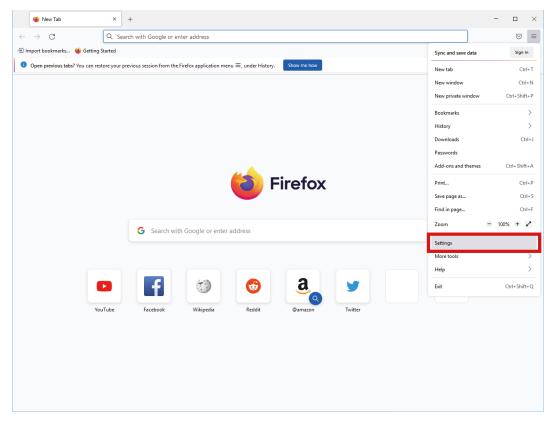


Figure 4.14 Firefox browser

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

	1 Settings	× +		-		×
\leftarrow	→ C	Firefox about:preferences	ŝ		\bigtriangledown	≡
		\wp Find in Settings				^
	🚱 General	General				
	Home	Startup				
	Q Search	Open previous windows and tabs				
	-	Always check if Firefox is your default browser				
	Privacy & Security	Sirefox is not your default browser Make Default				
	Sync					
		Tabs				
		Ctrl+Iab cycles through tabs in recently used order				
		✓ Open links in tabs instead of new windows				
		When you open a link, image or media in a new tab, switch to it immediately				
		Confir <u>m</u> before closing multiple tabs				
		Show tab previews in the Windows taskbar				
		Language and Appearance				
		Fonts and Colors				
		Default font Default (Times New Roman) v Size 16 v Advanced				
		<u>C</u> olors				
	ඩ් Extensions & Themes					
	⑦ Firefox Support	Zoom				
		Default zoom 100% V				~

Figure 4.15 Firefox [Options] screen

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

	🕄 Settings	× +			-		×
\leftarrow	→ C	Firefox about:preferences#privacy		4		\bigtriangledown	≡
			₽ Find in Settings				^
:	③ General 合 Home	Allow Firefox to send backlogged crash reports on your behalt	Eern more				
	၃ Search	Security					
	Privacy & Security	Deceptive Content and Dangerous Software Protection					
	Sync	Block dangerous and deceptive content Learn more					
	• - ,	Block <u>d</u> angerous downloads					
		✓ Warn you about unwanted and uncommon software					
		Certificates Query OCSP responder servers to confirm the current validity of certificates	f View <u>C</u> ertificates Security <u>D</u> evices				
		HTTPS-Only Mode					
		HTTPS provides a secure, encrypted connection between Firefox a websites support HTTPS, and if HTTPS-Only Mode is enabled, the connections to HTTPS. Learn more					
		Enable HTTPS-Only Mode in all windows	Manage Exceptions				
		Enable HTTPS-Only Mode in private windows only					
	은 Extensions & Themes	O Don't enable HTTPS-Only Mode					
	③ Firefox Support						

Figure 4.16 Firefox [Privacy & Security] screen

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

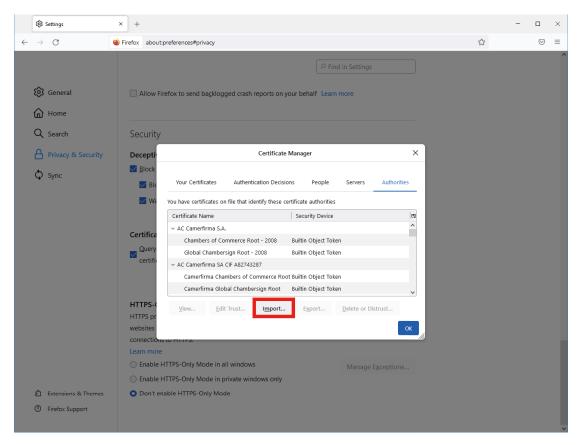


Figure 4.17 Firefox [Certificate Manager] window

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

🍅 Select File contai	ining CA cert	ificate(s) to import						Х
← → ~ ↑	→ This PC	> Desktop > Certificate			ٽ ×	Search Certificate		P
Organize 🔻 🛛 N	lew folder					:== :==	-	?
📌 Quick access		lame	Date modified	Туре	Size			
Curce access	E	acacert	7/16/2016 3:37 PM	Security Certificate	2 K	В		
🛄 This PC								
💣 Network								
	File <u>n</u> ame:				\sim	Certificate Files		\sim
						<u>O</u> pen	Cancel	

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-RGP on the Firefox browser.

Downloading Certificate	×
You have been asked to trust a new Certificate Authority (CA).	
Do you want to trust "LCA-DL8" for the following purposes? Trust this CA to identify websites. Trust this CA to identify email users.	
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).	
View Examine CA certificate	
OK Cancel	

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 11.

Windows (Firefox)

(1) Follow the same procedure from step (4) of "Windows (Firefox)" on page 13.

4.5.4 Installing from RGP

Windows (Chrome, Edge, Firefox)

(1) To download the certificate created on LCA-RGP and transferred to the RGPx, connect to the certificate download site (http://192168.0.1/SSL when the IP address of the RGPx is initial setting) for RGPx and click "Certificate_file".

After the file has been downloaded, follow the same procedure as in "4.5.3 Using Certification Authority Certificate" on page 18.

Enter the Login ID and password of user account setting transferred by RGP-designer.

iOS (Safari)

(1) To download the certificate created on LCA-RGP and transferred to the RGPx, connect to the certificate download site (http://192168.0.1/SSL when the IP address of the RGPx is initial setting) for RGPx and click "Certificate_file".



Figure 4.20 iOS Download confirmation dialog

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

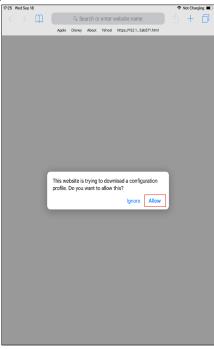


Figure 4.21 Message screen

(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.

7:27 Wed Sep 18		🗢 Not Charging 🔳
	Wi-Fi	
Settings		
Q Search	Wi-Fi	
	✓ aterm-8c075f-g	₽ \$ (j)
Ipad A1474	CHOOSE A NETWORK	
Apple ID, iCloud, iTunes & App St	044665954724	ê 🗢 🚺
2ファクタ認証を有効にする 🛛 👌	aterm-392baf-aw	€ ≈ (j
	aterm-8c075f-gw	a ≈ (j)
iPadの設定を完了する 🚺 🗦	aterm-codesys-a	a ≈ (i)
Profile Downloaded >	aterm-d2e775-a	a ≈ (j)
	BUFFALO-25F3C0	a ≈ (j)
Airplane Mode	Extender-A-DB68	a 🗟 (j)
Wi-Fi aterm-8c075f-g	Extender-G-DB68	a 🕈 (j)
Bluetooth On	GENEDEV-1	₽ \$ (Ì)
Notifications	IB10W1-AP181	ê ╤ (Ì)
	msystem2-musen	a ? (j)
Sounds	rgp6-ap111	€ ╤ (j)
Do Not Disturb	RGP6-N-R-13-14	ê 🗢 🚺
Screen Time	RGP6-N-R-13-15	₽ ≎ (j)
6 General	RGP6-NJ-BR2-16	₽ ≎ (j
Control Center	s-syoltd	₽ ╤ (j)
AA Display & Brightness	SCADALINX-INET	₽ ङ ()
	test-ssid-rgp	≜ ≈ (j

Figure 4.22 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.

◀ Safari 16:12 Tue Dec 14	4	Ceneral	Profile	奈 98% ■
Settings		DOWNLOADED PROFILE		
IA Ipad A2 Apple ID, iCl	152 loud, iTunes & App St	LCA-RGP		>
電話番号を確認	1 >			
	Cancel	Install Profile	Install	
Profile Downloade				
Airplane Mc	LCA-RGP			
🛜 Wi-Fi	Signed by LCA-RGP			
Bluetooth	Not Verified Contains Certificate	1		
	More Details		>	
Notification				
Sounds				
Screen Time				
General				
Control Cer				
AA Display & B				
Home Screen	& Dock			
(1) Accessibility				
Wallpaper				
Siri & Search				
Touch ID & Pa	asscode			
Demana				

Figure 4.23 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.

<u>ि ×</u>	25	1	
Operation of the second sec			
← → C ③ 192.168.35.16/SSL	☆	<u>+</u>	÷
		_	
Certificate file download page.			
Certificate file			
M-SYSTEM CO.,LTD.			
✓ cacert.crt。開<			×

Figure 4.24 Android cacert.crt screen

(2) Open the downloaded certificate.

()(; <	⋫≙ặ								12 II	D I 5:43	3 PM
🔛 h	ttps://192	2.168.1	3.10/ç	gantt.) ×	Ner	w tab		×	+		
÷	\rightarrow	G		192.168.	.13.10/ថ្	gantt.h	tml		☆	ŧ	:
Authoriza Back	tion Requi	red									
											_
⊻	cacert	.crt 0	pen							2	×
			<	1		0					

Figure 4.25 Android cacert.crt opening screen

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

፨ቀጚ⊳∿₩				逸 💌 5:46 PM
Certificate Install	er			
	Name the certificat	e	_	
	Certificate name			
	Credential use			
	VPN and apps		0	
	Wi-Fi		\bigcirc	
	The issuer of this certifica and from your device.	te may inspect all tr	affic to	
	The package contains: CA	A certificate		
	CANCEL	ок		

Figure 4.26 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-RGP.

- (1) Click [Import(I)] on the LCA-RGP 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 RGPx.

Import		\times
Import certificate in name.	formation by specifying the t	file
Cert/Key PKCS12		
Unit Certificate*		
Unit Private key*		
* D 1 1		_
* Required.	OK Cancel	

Figure 4.27 File importing dialog for DER 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.

Import	×
Import certificate name.	information by specifying the file
Cert/Key PKCS12	
PKCS12 File*	
Password	
* Required.	OK Cancel

Figure 4.28 File importing dialog for PKCS12 format

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-RGP 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.

♀ LCA-RGP - × New CA(N) Import(I) Language(L)									
Certification Authority		Certificate							
🖾 Show CA File(<u>S</u>)		1 New Certificate(<u>C</u>)							
Name O CN	Value M-SYSTEM LCA-RGP		CN RGP30-1	Domains m−system.ddns.jp	IP Add 192.16	Iresæs 8.0.1			

Figure 29 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-RGP 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-RGP to apply the change.

♀ LCA-RGP — — × New CA(N) Import() Language(L) Version(V)									
Certification Authority			Certificate						
🗐 Show CA File(<u>S</u>)		1 New Certificate(<u>C</u>)							
Name O CN	Value M - SYSTEM LCA-RGP		CN RGP30-1	Domains m-system.ddns.jp	IP Adı 192.10	dresses 58.0.1			

Figure 30 Switching Display Language

5. LICENSE

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

The LCA-RGP 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 WAR-RANTIES, 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 CON-TRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUEN-TIAL 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 OTHER-WISE) 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, Ihash, 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, IN-CLUDING, 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 (INCLUD-ING, 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 POS-SIBILITY OF SUCH DAMAGE.