LGPKI 登録分局運営の手引　抜粋（英文）

Chapter 1. Introduction

This handbook describes procedures concerning operation of Registration Authority Branches operated by LGWAN participating organizations (below, “Participant Organizations”, based on rules of the Basic Framework for Local Government Public Key Infrastructure (Established April 1, 2006 by the Local Government Wide Area Network Committee).

Chapter 2 Registration Authority Branches

2.1 LGPKI Operation Organization

For Local Government Public Key Infrastructure (below, “LGPKI”), the Local Government Wide Area Network Operation Committee (below, “LGWAN Operation Committee”) provides overall decision-making, and the Local Government Wide Area Network Operation Unit (below, “LGWAN Operation Unit”) operates the Issuing Authority and Registration Authority. (See Figure 2-1)

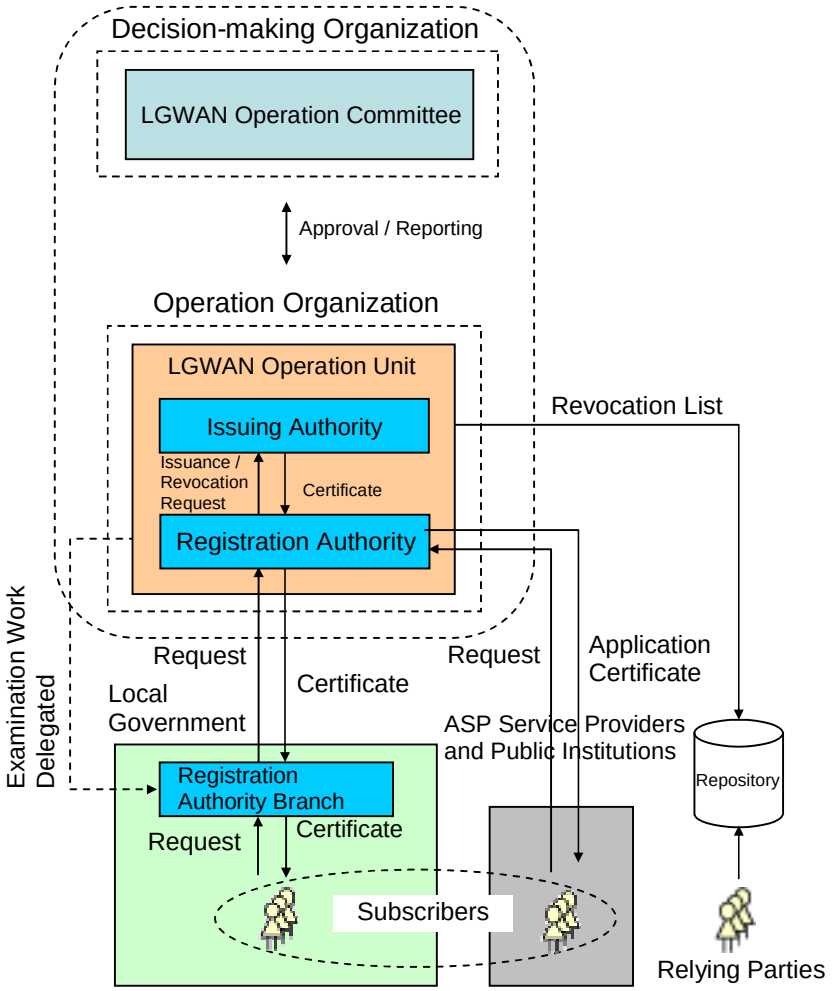


Figure 2-1 LGPKI Organization and Structure

Of the duties performed by the LGWAN Operation Unit, part of its work as the Registration Authority is delegated to Participant Organizations. The organizations which perform this delegated work are called Registration Authority Branches.

Table 2-1 Organization Units & Roles

Organization Unit	Roles
Local Government Wide Area Network Operation Committee	As the organization which decides matters concerning operation of LGPKI, decides and approves the following matters. • CP/CPS for Bridge CA, Application CA, and Organization CA (all referred to below as "CA") • Response when CA private keys are compromised • Emergency response during disasters, etc. • Other important matters concerning operation of each CA
LGWAN Operation Unit	As the operating organization for LGPKI, mainly performs the following work. • Reports on operating status to the Local Government Wide Area Network Operation Committee • Audits the Registration Authority Branches • Operation and maintenance of Certification Authority system • Operation of Registration Authority Branches Receive and examine requests from users for issuance, renewal, and revocation of certificates, and make requests to the Issuing Authority for certificate issuance and revocation. (If the user is a Participant Organization, part of the reception and examination work shall be delegated to the Registration Authority Branch of the Participant Organization) • Operation of the Issuing Authority Issue and revoke certificates, based on requests from Registration Authority Branches.

2.2 Role of Registration Authority Branches

Under delegation from the LGWAN Operation Unit, part of the reception and examination work for requests from users for certificate issuance, renewal, and revocation are done at Registration Branches.
An examination confirms the existence of the organization to which a subscriber belongs ("authentication of organization identity"), confirms the identity of the subscriber who submitted the request (authentication of subscriber identity), and confirms that the information noted in the certificate to be issued is proper without errors ("confirmation of certificate noted items").

2.3 Work of Registration Authority Branches

Registration Authority Branches do the following work: Requests for certificate issuance/renewal/revocation, delivery and elimination of certificates, reports to the LGWAN Operation Unit concerning the Registration Authority Branch, management of documents, and response to audits.

(1) Requests for Certificate Issuance/Renewal/Revocation
Receives requests for certificate issuance/renewal/revocation submitted by subscribers of local governments (identification of applicant, identification of the organization to which the applicant belongs, confirmation of the intention for owning the certificate, confirmation that the information noted in the certificate to be issued is proper), and if there is no problem with the examination, makes a request for issuance/renewal/revocation to the Registration Authority of the LGWAN Operation Unit.
The LGPKI issues the following certificates: (1) Manager certificates and user certificates as certificates issued from an Organization CA, (2) Email certificates, web certificates, and code signing certificates as certificates issued from an Application CA. Each certificate's uses are explained in Table 2-2. For document exchange certificates issued from an Organization CA before February 2008, certificates with PrintableString character codes can be used until the end of March 2008, and certificates with UTF-8String character codes can be used until the end of September 2008 (however, certificates which expire before these dates can only be used until their expiration date).

Table 2-2 Types and Uses of Certificates

Certificate Authority (CA)	Certificate	Uses
Organization CA	Manager certificate	Used by a manager of a local government in electronic signatures on public documents, either between local governments or to residents / companies / etc.
	User certificate	Used to authenticate the user when each system is used. Also used in encryption and electronic by the person in charge of handling documents in the LGWAN electronic document exchange system.
Application CA	Email certificate	Used in email electronic signatures for sending email newsletters to residents and companies. *Only for clients able to sign, and clients able to verify signatures. (See Appendix A)
	Web server certificate	These apply to web servers which handle public notices and request work etc. for residents and companies, used in encryption of SSL communications, etc.
	Code signing certificate	Used in electronic signatures for programs etc. distributed to residents and companies. *Only for signature tools enabling electronic signatures, and browsers enabling electronic signature verification. (See Appendix A)

Registration Authority Branches receive requests for certificate issuance, renewal and revocation from local government subscribers. An outline of each request is shown in Table 2-3. Registration Authority Branches receive requests from subscribers, examine them, submit requests to the LGWAN Operation Unit, and deliver issued certificates.

Table 2-3 Types of Requests Received by Registration Authority Branch

Type of Request	Outline
Issuance Request	This request is made if a certificate is to be newly used, or if a certificate is to be reissued after it was revoked.
Renewal Request	This request is made if use of a certificate is to continue after the certificate's expiration date. A request is possible starting from 6 months before the expiration date.
Revocation Request	This request is made if any of the following apply to a certificate or key storage media being used. • Private key is compromised Examples: Key storage media is lost, stolen, PIN leaked, etc. • Change in certificate noted items Examples: Organization name change, manager name change, etc. • Key storage media defect or damage Examples: Key storage media becomes unusable because it is locked, damaged, etc. • Certificate Use Halted Examples: The work or organization using the certificate was eliminated, etc.
Emergency revocation request	This request is made if the private key of a certificate or key storage media being used is compromised, and the Registration Authority Branch Chief judged it to be an emergency. (LGWAN Operation Unit's reception hours: Weekdays 9:00 - 17:00) The difference from a revocation request is that in the case of standard revocation requests, the revocation list is made available in the public repository in 24 hour intervals after revocations are completed. But when an emergency revocation request was made, the revocation list is made available in the public repository urgently after the revocation was completed.

(2) Delivery of Certificates
Securely and reliably delivers certificates issued by the Issuing Authority of the LGWAN Operation Unit and completion notices, to local governments and subscribers.

(3) Elimination of Certificates
Certificates issued from an Organization CA (manager certificates and user certificates) are made available in the integration repository[1], and certificate information can be confirmed in the name search screen of the LGWAN electronic document exchange system.
Elimination of certificates is a process which deletes information of manager certificates or user certificates from the integration repository
If a certificate's expiration date is past, the invalid certificate's information remains in the integration repository, so the Registration Authority Branch must periodically check the expiration dates of certificates, submit a request to the LGWAN Operation

[1] Integration repository: System which stores certification information issued by the Certification Authority (certificates, revocation lists, etc.), and makes it available to local governments.

Unit for elimination of the expired certificates, and delete them from the integration repository.

(4) Management of Documents
Manages storage of request documents etc. used in the work of items (1) to (3) above.

(5) Response to Audits
Periodically report to the LGWAN Operation Unit that the work of items (1) to (4) above is being performed properly and smoothly. Also, branches are audited by the LGWAN Operation Unit (only Registration Authority Branches which are selected at its discretion).

2.4 Items Required for Development of Registration Authority Branch

2.4.1 Allocation of Operating Staff of Registration Authority Branch

Participant Organizations must develop and operate Registration Authority Branches, according to rules established by the LGWAN Operation Committee and a handbook shown by the LGWAN Operation Unit.
A Registration Authority Branch shall appoint a Registration Authority Branch Chief, Examination Approver, Examiner, and Receptionist, as shown in Table 2-4 (below, Examination Approver, Examiner, and Receptionist are referred to as "Other Operating Staff").
There are no particular specifications for original positions of people who act as operating staff, but they shall be staff of the Participant Organization.

Table 2-4 Operating Staff Allocated to Registration Authority Branch

Operating Staff	Role
Registration Authority Branch Chief	The Registration Authority Branch Chief is responsible for operation of the Registration Authority Branch, and performs the following work. • Appointment and dismissal of Registration Authority Branch operating staff • Gives policy instructions to Registration Authority Branch operating staff • Final approval for results of examinations of requests from subscribers for certificate issuance, renewal, and revocation • Final approval for submission of requests to the Registration Authority for certificate issuance, renewal, elimination, and revocation • Management of Registration Authority Branch work • Other training of operating staff for the work
Examination Approver	The Examination Approver approves results from the Examiner for examinations of requests for issuance, renewals, and revocations of certificates.

Operating Staff	Role
Examiner	The Examiner examines requests from subscribers for issuance, renewals, and revocations of certificates.
Receptionist	The Receptionist receives requests from subscribers for issuance, renewals, and revocations of certificates, handles communication and coordination with subscribers, and manages storage of documents, etc. Based on instructions of the Registration Authority Branch Chief, communicates and coordinates with the LGWAN Operation Unit, and makes requests to the Registration Authority for certificate issuance, renewal, elimination, and revocation.

As shown in Table 2-5, some second roles are prohibited for operating staff of a Registration Authority Branch, so each Participant Organization shall consider this when assigning staff to match its actual situation.

Table 2-5 Second Roles of Operating Staff: Permitted or Prohibited

Main job \ 2nd role	Registration Authority Branch Chief	Examination Approver	Examiner	Receptionist
Registration Authority Branch Chief		OK	No	No
Examination Approver	OK		No	No
Examiner	No	No		OK
Receptionist	No	No	OK	
	OK: Can perform this second role No: Cannot perform this second role			

2.4.2 Staff Allocation Procedure

- If develop a new Registration Authority Branch
  In the organization, the Registration Authority Branch Chief shall be selected, and the Registration Authority Branch Chief appoints Other Operating Staff.
- If transition from a local government certification authority (See *2.5* Transition from a Local Government Certification Authority)
  The Certification Authority Chief and Other Operating Staff in the certification authority shall be appointed as the Registration Authority Branch Chief and Other Operating Staff.

When operating staff of the Registration Authority Branch are appointed or dismissed, the Registration Authority Branch Chief shall record the operating staff names, appointment dates, and dismissal dates in Appendix C1: Registration Authority Branch Operation Organization Table.

2.4.3 Staff Training

Operating staff of the Registration Authority Branch must thoroughly know its work details.
To this end, the Registration Authority Branch Chief shall himself/herself understand related rules etc., and when appointing Other Operating Staff, must provide required training for Other Operating Staff, which is a role of the Registration Authority Branch Chief.
Related rules etc. apply as shown below. As training for Other Operating Staff, the Registration Authority Branch Chief must have them intensively read and understand these related rules.
In addition to when Other Operating Staff are appointed, also when the Registration Authority's work details change, the Registration Authority Branch Chief must have Other Operating Staff understand such details, and provide them opportunities to receive training at that time.

*Related Rules
Basic Framework for Local Government Public Key Infrastructure, LGPKI Organization Certification Authority CP/CPS, LGPKI Application Certification Authority CP/CPS, LGPKI Registration Authority Branch Operation Handbook, LGPKI Subscriber Handbook (Local Government Version)
Also, LGPKI related documents issued by the Local Government Wide Area Network Operation Committee and the Local Government Wide Area Network Operation Unit

The Registration Authority Branch Chief shall thoroughly learn the work details himself/herself, and record training for other staff, according to Appendix C1: Registration Authority Branch Operation Organization.

2.4.4 Security Management

Participant Organizations must exercise security management for following item, for operations of the Registration Authority Branch involving management of internet computers which make requests for issuance etc. of certificates.

- To handle threats by computer viruses, internet computers shall have antivirus software installed. Antivirus software shall be constantly updated with the latest virus pattern files.

2.5 Transition from Local Government Certification Authority

Participant Organizations which developed a local government certification authority on or before March 31, 2006 shall eliminate its rules and operation organization, as follows.

- Elimination of four types of rules developed based on templates created by the LGWAN Operation Committee (Rules on certification policy decision function, rules on Certification Authority operation functions, audit rules on operation of Certification Authority, and rules on usage of key information etc.)
- Elimination of each operation unit (certification policy decision function, Certification Authority operation function, audit function concerning operation of Certification Authority, and usage unit)

- Cancel appointments of operating staff of Certification Authority (followed by appointment of operating staff of the Registration Authority Branch)

Also, for information of the local government Certification Authority which is shown on web pages aimed at residents and companies, Participant Organizations shall delete such web pages, for concentration on the LGPKI web page (www.lgpki.jp).

2.6 Systems Used in Certificate Issuance Requests Etc.

Requests for issuance etc. of certificates shall use systems provided by the LGWAN Operation Unit.

The flow when requesting certificate issuance etc. is shown in the figure below. When issuing a manager certificate or user certificate, organization information (in the case of a user certificate, organization information and account information) must be registered in advance.

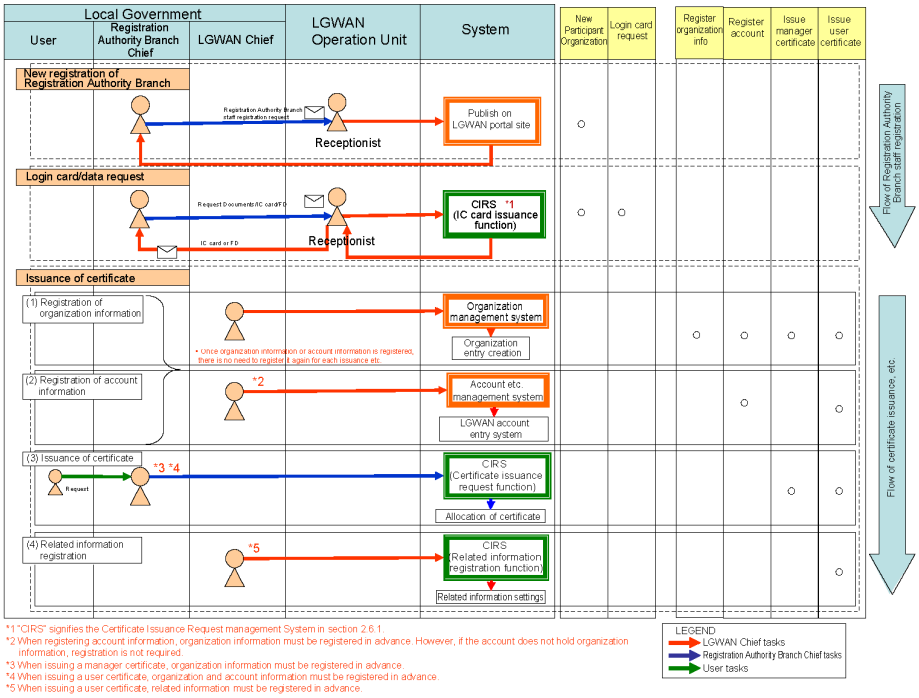


Figure 2-2 Flow of Registration Authority Staff Registration & Certificate Issuance

The figure below shows the Registration Authority Branch's operation flow when deleting account and organization information, and when revoking certificates. When deleting or renewing account information, the certificate must be revoked in advance (in the case of user certificates, including deletion of related information). When deleting or renewing organization information, account information must be deleted in advance.

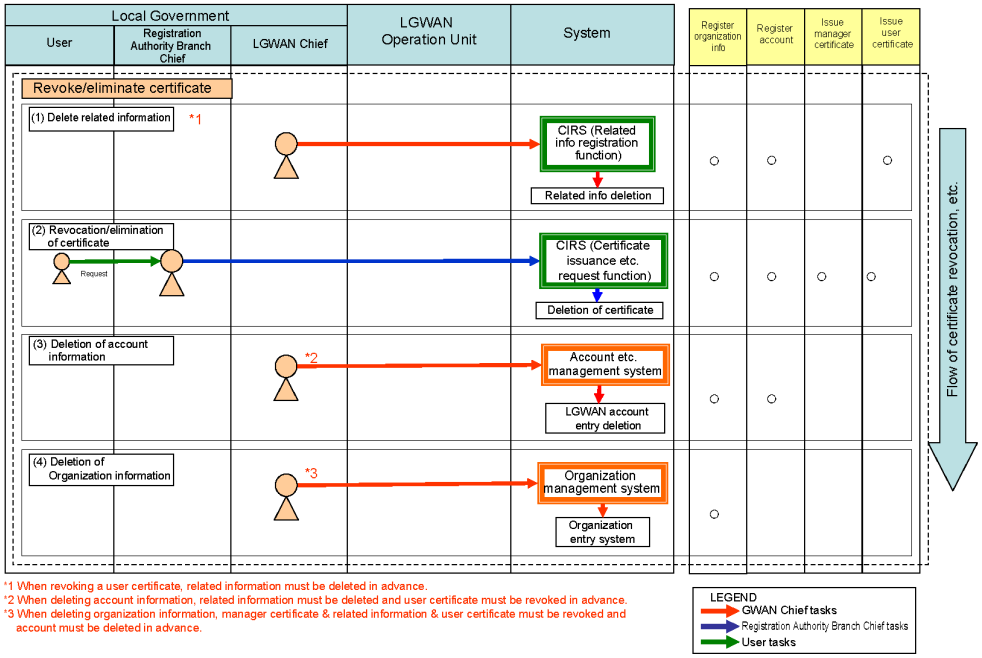


Figure 2-3 Flow of Certificate Revocation, Account Cancellation, and Organization Information Deletion

Next are explanations of the Certificate Issuance Etc Request Management System used by the Registration Authority Branch, the Certificate Issuance Support Standard System used by certificate users, and the Organization Management System and Account Etc. Management System used by the LGWAN Chief.

2.6.1 Certificate Issuance Etc Request Management System

This system performs requests for certificate issuance etc. by the Registration Authority Branch via web browser, and registration/renewal by the LGWAN Chief of related information which becomes the address of the LGWAN electronic document exchange system.
Certificate Issuance Etc Request Management System
(Operating hours: LGWAN Operation Unit operating days, from 8:00 to 22:00)
https://www.cirs.lgwan.jp/main.html
Certificate Issuance Etc Request Management System Operation Procedures (Local Government Authentication Infrastructure Certificate Issuance Etc. Request Function Version)
http://center.lgwan.jp/library/index.html#K-3-1
In order to use this system, a login card or login data (which is operator identification information) must be issued in advance.

(1) Certificate Issuance Etc. Request
Requests certificate issuance/renewal/revocation/elimination, obtains issued certificates (download), searches for requested certificates, etc. The Registration Authority Branch Chief's login card or login data is required in order to use these functions.

(2) LGWAN Electronic Document Exchange System Related Information Registration & Renewal

Registration, renewal, deletion, etc. of related information (address information of the person in charge of document handling, email address for notification of document arrival, etc.) required to use the LGWAN electronic document exchange system, for already issued user certificates.

Registration of this related information enables selecting the name of the user certificate as "sender" or "recipient" in the LGWAN electronic document exchange system.

*About Login Card and Login Data

The LGWAN Chief's login card or login data must be issued in order to use this function. The role of the LGWAN Chief here is work to register related information required when using the LGWAN electronic document exchange system (which is an LGWAN basic service). This is not work of the Registration Authority Branch, thus it is arranged that the person who performs this procedure shall be the LGWAN Chief (who is the person responsible for LGWAN participation), separate from the Registration Authority Branch Chief.

However, if the situation is that management of related information is being done by a Registration Authority Branch unit or document management unit etc., thus the title "LGWAN Chief" does not apply, then without sticking to this title, the manager actually managing related information in the organization shall manage the login card or login data.

(3) Registration Authority Branch Staff Change

Changes the registered details of Registration Authority Branch staff registration requests. The login card or login data of the Registration Authority Branch Chief is required in order to use this function.

2.6.2 Certificate Issuance Support Standard System

This is a system which performs work related to certificate users generating key pairs[2] in key storage media, creation of Certificate Signing Request files (below, "CSR"), and storage in key storage media the certificates issued by the LGWAN Operation Unit. In Participant Organizations, programs provided by the LGWAN Operation Unit shall be installed in a computer and used.

In addition to certificates, for login data used by the Registration Authority Branch, this also performs the work of key pair generation in login data storage media, creation of login data issuance request files, and storing in login data media storage the login data issued by the LGWAN Operation Units.

When this system is used to create a CSR and request issuance of a certificate, postal delivery of key storage media between the Registration Authority Branch and LGWAN Operation Unit becomes unnecessary in order to do the work to store in key storage media the certificate issued on the certificate user side. (In the case of login data, postal delivery of a floppy disc is required)

The Certificate Issuance Support Standard System's program and user guide shall be downloaded from the LGWAN portal site, and installed.

URL: http://center.lgwan.jp/library/index.html#K-3-3

[2] Key Pair: Two corresponding keys used in public key encryption methods – A "private key" which is generally not published, and a "public key" which is generally published

* Version 2.0 or later of the Certificate Issuance Support Standard System's program shall be used. If an old version of the program was being used, the latest version program shall be obtained by download from the LGWAN portal site.

2.6.3 Organization Management System

System for the LGWAN Chief to add/change/delete organization information via a web browser.
Organization Management System
(Operating hours: LGWAN Operation Unit operating days, from 8:00 to 22:00)
https://reg.lis.lgwan.jp/lis_org_main.html
In order to use this system, a login card or login data (operator identification information) must be issued in advance.

2.6.4 Account Etc. Management System

This system is for the LGWAN Chief and person in charge of data entry to add/change delete via a browser the user account and group member information registered in the system user authentication information.
Account Etc. Management System
(Operating hours: LGWAN Operation Unit operating days, from 8:00 to 22:00)
https://reg.lis.lgwan.jp/lis_acc_main.html
In order for a person in charge of data entry to use this system, a user ID and password must be issued to that person in advance.
In order for the LGWAN Chief to use this system, the Chief must receive a login card or login data (operator identification information) in advance.

2.7 Entries of Certificate Subject Identifiers

2.7.1 Certificate Storage Method in Integration Repository

Subjects of certificates Application CA and Organization CA shall be expressed in the X.500[3] Distinguished Name format.
Identifiers of manager certificates and user certificates issued by an Organization CA shall be comprised of a Directory Information Tree (below, "DIT") with no inconsistencies overall, and stored in the integration repository.

The DIT structure in the LGPKI is Level 1: country, and Level 2: LGPKI container or Local Governments container. For Level 3, each CA is allocated in an LGPKI container or below, with prefectures containers allocated in Local Governments containers or below. For Level 4 or below, there are only Local Governments containers or below, and tree composition adopts a levels structure which shows each organization's structure in units of local government, chief, committee, bureau, and section. Also, for storage in the directory tree, local government container subdirectories and below are comprised of an English named tree and a Japanese named tree with exactly the same structure, for end users' and application's convenience. Table 2-6 shows the DIT structure.

[3] X.500: Directory service standard specification established by the ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union). A single global namespace can be built, enabling easy data search, etc.

Table 2-6 DIT Structure

C = JP	Level 1	Country code
O = Local Governments	Level 2	Local government organization (alphabet)
L = XXX Area	Level 3	Prefecture (alphabet)
OU = XXX	Level 4	Local government name (alphabet)
OU = XXX	Level 5	Local government (prefecture/city office, committee, etc., in alphabet)
OU=XXX	Level 6	Local government organization name (bureau, in alphabet)
OU=XXX	Level 7 or lower	Local government organization name (section/office, in alphabet)
...	...	
CN=XXX	Leaf (Level 4 or lower)	Name (job title etc., in alphabet)
...	...	
L=XXX (*Note)	Level 3	Prefecture (alphabet)
OU=XXX	Level 4	Local government name (alphabet)
OU=XXX	Level 5	Local government (Prefecture/city office, committee, etc., in alphabet)
OU=XXX	Level 6	Local government organization name (bureau, in alphabet)
OU=XXX	Level 7 or lower	Local government organization name (section/office, in alphabet)
...		
CN=XXX	Leaf (Level 4 or lower)	Name (job title etc., in alphabet)
...		
O=LGPKI	Level 2	LGPKI CA group
OU=Bridge CA	Level 3	Bridge CA
OU=Application CA G2	Level 3	Application CA G2
OU=XXX Area CA	Level 3	Organization CA (prefecture)
OU=Organization CA U8 (*Note)	Level 3	Organization CA
...	...	
O=Local government	Level 2	Local government organization (in Japanese)
L=XXX prefecture	Level 3	Prefecture (in Japanese)
OU=XXX prefecture	Level 4	Local government name (in Japanese)
OU=XXX	Level 5	Local government organization name (bureau name etc., in Japanese)
OU=XXX	Level 6	Local government organization name (section/office name etc., in Japanese)
OU=XXX	Level 7 or below	Local government organization name (organization name etc. of section/office or below, in Japanese)
...		
CN=XXX	Leaf (Level 4 or lower)	Title (job title etc., in Japanese)
...	...	
L=XXX prefecture (*Note)	Level 3	Prefecture (in Japanese)
OU=XXX prefecture	Level 4	Local government name (in Japanese)
OU=XXX	Level 5	Local government organization name (bureau name etc., in Japanese)
OU=XXX	Level 6	Local government organization name (section/office name etc., in Japanese)
OU=XXX	Level 7 or lower	Local government organization name (name etc. of organization below section/office, in Japanese)
...	...	
CN = XXX	Leaf (level 4 or lower)	Title (job title etc., in Japanese)
...	...	

(*Note): Certificates issued since February 2008 are stored in this container.

2.7.2 Certificate Subject Identifiers of Web Server Certificates and Code Signing Certificates

For issuance of web server certificates and code signing certificates, after the subscriber generates a key pair when a certificate issuance request is made, a CSR must be created and sent to the Registration Authority Branch. The key pair made in such a case shall be generated by an RSA encryption algorithm (1024 bit key length), and the identifier set in the certificate subject must be attached to the CSR. Usually, this identifier shall be specified in the same format as the certificate noted item specified in English in the certificate request documents.
If the CSR cannot be created with the same identifier structure as the certificate noted item specified in the certificate issuance request documents, due to a technical reason of the web server or key information etc. generation software (subject which can be set in CSR is a standardized format, etc.), then the identifier specified by the CSR creator shall be translated and created. The LGWAN Operation Unit shall use the identifier specified in the CSR unchanged for creating the web server certificate and code signing certificate.

Table 2-7 shows examples of translations of identifiers.

Table 2-7 CSR Subject Setting by Translation: Examples

Attribute format and attribute value specified by web server or software for generating key information etc.: Example		Translation	Value setting example	Note
C	Country	Specifies the country code unchanged.	JP	
ST or S	Prefecture	Not specified. If cannot be abbreviated, specifies the prefecture to which each local government belongs.		
L	City/town/village	Specifies the prefecture to which each local government belongs.	xxxxx	
O	Organization name	Local Governments is the fixed specification.	Local Governments	
OU (*1)	Unit name	Specifies the local government name. Optionally, also possible to specify the server management organization name.	xxxxx Prefecture Soumubu IT Suishinshitsu	
CN (*1)	Web server	Specifies the server's Fully Qualified Domain Name (FQDN).	www.pref.xxxxx.lg.jp	Web server certificate
	Code administrator name	Specifies the local government name, and CodeAdmin which shows the code administrator (*2). Optionally, also possible to specify the organization name and application name.	CodeAdmin of xxxxx Prefecture {organization name} {application name}	Code signing certificate

(*1) The English expressions of OU and CN have a 64 character limit, so if they exceed 64 characters, they shall be changed to be within 64 characters. Also, the English expressions of local government names shall use the characters specified in the "LGPKI Organization Name List". The LGPKI organization name list shall be obtained by download from the LGWAN portal site.

(*2) The Code administrator shall have the fixed expression CodeAdmin, unless there is a special reason not to.

2.7.3 Name of Code Signing Certificate

In the case of a code signing certificate, when a resident/company/etc. downloads a program etc. electronically signed by a signature tool, it shall be shown similar to the screen in Figure 2-2, thus the CN shall take this into account.

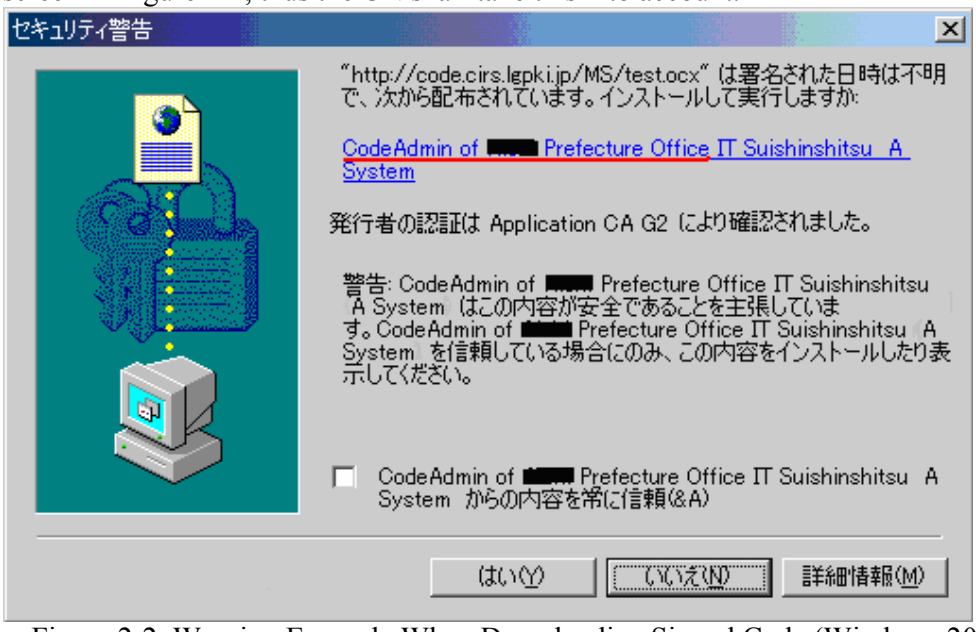


Figure 2-2 Warning Example When Downloading Signed Code (Windows 2000)

Chapter 4 Certificate Related Work

This chapter explains parts of the work done by Registration Authority Branches as specified in 2.3 Work of Registration Authority Branches: (1) Requests for Certificate Issuance/Renewal/Revocation, (2) Distribution of Certificates, (3) Elimination of Certificates.

Information is entered in order to do certificate issuance etc. in the Certificate Issuance Etc Request Management System. When issuing a manager certificate, information of organizations 1 to 7 refers to organization information registered in the Organization Management System. When issuing a user certificate, in addition to organization information registered in the Organization Management System, name information refers to information registered in the Account Etc. Management System. Therefore, certificate issuance cannot be done with organization information and account information which is not registered in the Organization Management System nor in the Account Etc. Management System, so organization information (in the case of a user certificate, organization information and account information) must be registered in advance.

However, if a manager certificate or user certificate is to be issued in a name without organization information such as its chief, then registration of organization information is not required. (refer to 2.6 Systems Used in Certificate Issuance Requests Etc.)

4.1 How to Request Certificate Issuance, Renewals, and Revocations

Certificates are issued, renewed, and revoked by the following two methods.

- Participant Organization creates a CSR and makes a request, then stores the issued certificate in key storage media.
- Based on the certificate noted information requested by the Participant Organization, the LGWAN Operation Unit creates a CSR, stores it in key storage media, and issues the certificate.

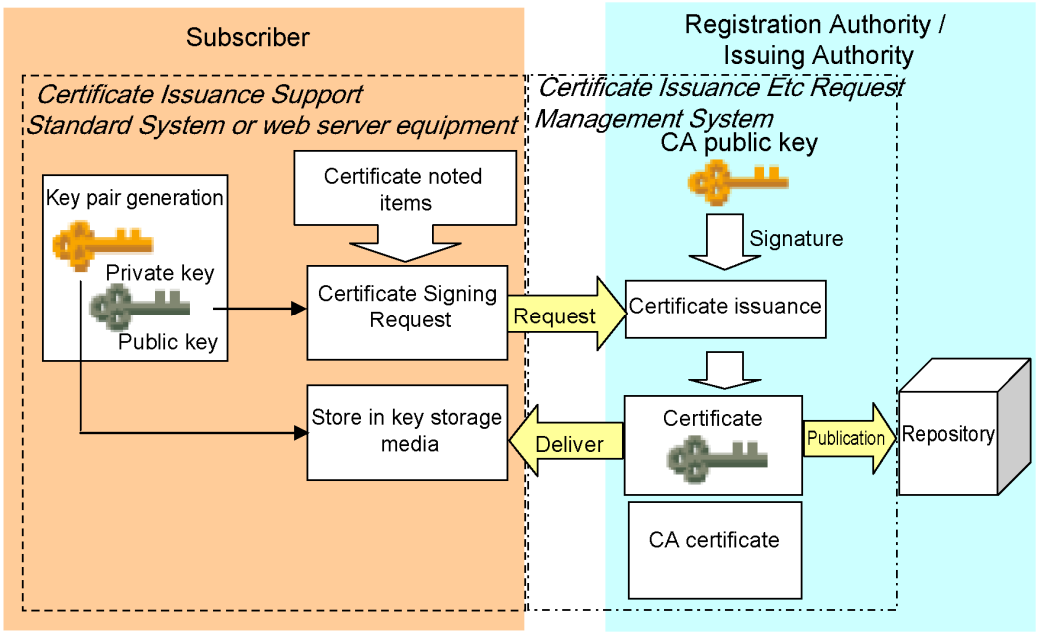
In this handbook, for convenience, the first method shall be called “CSR Request”, and the second “Standard Request”. (For details, refer to Table 4-1 and Figure 4-1)

Also, for a CSR Request or a Standard Request, one can make an “Individual Request” which requests one certificate, or a “Batch Request” which requests multiple certificates together.

Table 4-1 Differences Between a CSR Request and a Standard Request

Procedure	CSR Request	Standard Request
Request from subscriber to Registration Authority Branch	Attach a certificate signing request (below, "CSR") created using the web server equipment or Certificate Issuance Support Standard System, and submit it along with the certificate issuance request.	Create the certificate issuance request documents, and make request.
Reception and examination by Registration Authority Branch	Authenticate the applicant and the organization to which it belongs, confirm the intention for owning the certificate, and confirm that the information noted in the certificate to be issued is proper. Enter the CSR in the Certificate Issuance Etc Request Management System, and confirm that the CSR's content is the same as the content noted in the request documents.	Authenticate the applicant and the organization to which it belongs, confirm the intention for owning the certificate, and confirm that the information noted in the certificate to be issued is proper.
Request from the Registration Authority Branch to the LGWAN Operation Unit	Enter the CSR in the Certificate Issuance Etc Request Management System, and make request.	Enter certificate noted items into the Certificate Issuance Etc Request Management System, make request, and send the IC card etc. by post.
Reception of certificate issued by the LGWAN Operation Unit	Download certificate issued from the Certificate Issuance Etc Request Management System.	Receive postal delivery of IC card which stores the certificate, PIN information, etc.
How to distribute certificates to users from the Registration Authority Branch	Store the downloaded certificate in a floppy disc, and deliver to the applicant along with the certificate issuance request documents for the expiration and serial number noted in the issuance notice box.	Deliver the following to applicant: IC card, PIN information, and the certificate issuance request documents for the expiration and serial number noted in the issuance notice box.
Use of certificate	Subscriber uses web server equipment or Certificate Issuance Support Standard System to store the certificate in the web server equipment or key storage media, and uses the certificate.	Subscriber uses the certificate by the IC card and PIN information.
Types of certificates which can be requested	Manager certificate User certificate Email certificate Web server certificate Code signing certificate	Manager certificate User certificate Email certificate

(1) CSR Request (Subscriber generates key pair)



(2) Standard Request (Registration Authority Branch generates key pair)

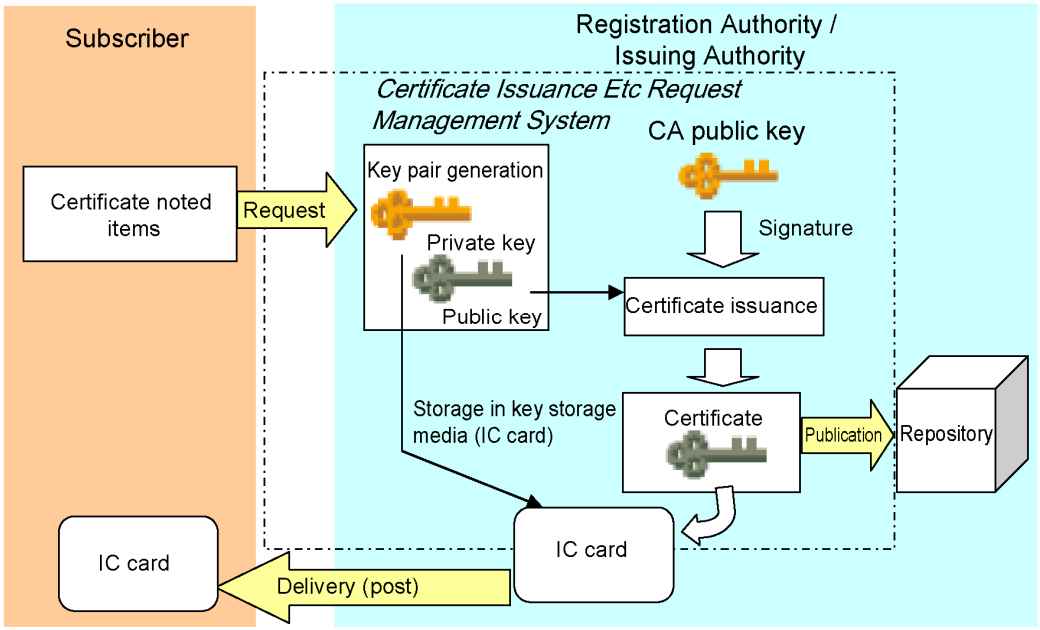


Figure 4-1 Differences Between CSR Request and Standard Request

4.2 Procedures in Registration Authority Branch for Certificate Issuance, Renewal, and Revocation

4.2.1 Flow of Procedures

Figure 4-1 shows the flow of procedures in a Registration Authority Branch for certificate issuance, renewal, and revocation.
The Receptionist receives request documents from a subscriber (applicant), the Examiner examines them, the Examination Approver approves the examination results, and the Registration Authority Branch Chief gives the final request approval. If the Registration Authority Branch Chief approved the request, instruction is given to the Recipient to do the procedures for a request to the LGWAN Operation Unit. After the process is completed in the LGWAN Operation Unit, the Receptionist performs the processes required for delivery etc. of the certificate to the subscriber (applicant).

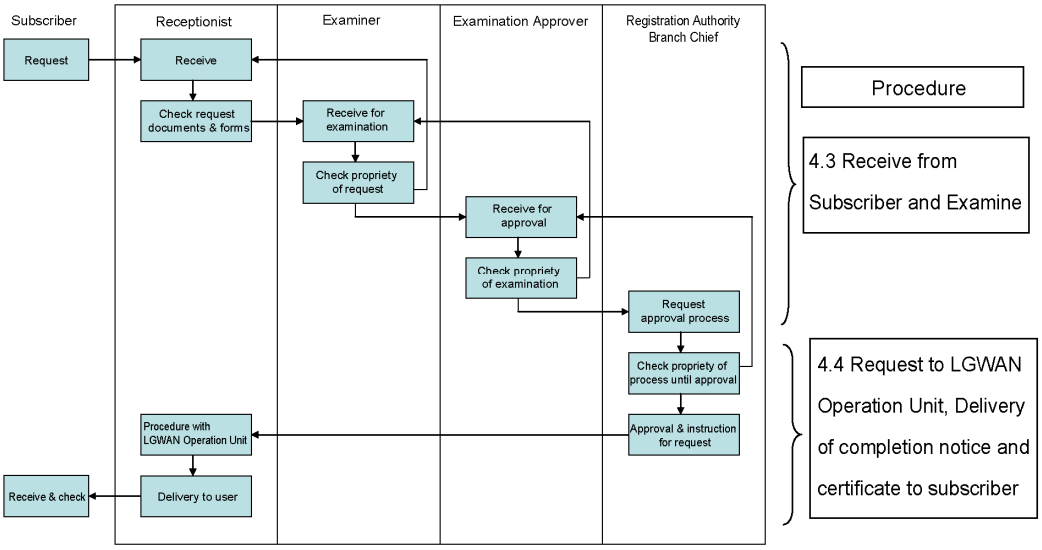


Figure 4-2 Procedures from Request until Delivery

4.2.2 Records of Procedures

For reception and examination work in an Registration Authority Branch, the Appendix C2: Process Record Form must be used to confirm and record the work details necessary to verify that the work is properly operating based on the rules and handbook etc. complied with.
Also, for management of the status of deliveries to subscriber and to prevent forgotten deliveries, Appendix C3: Request Management Book shall be used to record reception and delivery dates, and records must be managed from request reception until delivery.
For the Registration Authority Branch, if there is a system etc. in the government office which enables work confirmation as described above and recording of each certificate's reception date and delivery date, it may not be necessary to use the

attached form, but when the LGWAN Operation Unit audits the Registration Authority Branch, the records shall be inspected as necessary.

4.3 Receive from Subscriber and Examine

4.3.1 Receptionist Work

The Receptionist shall do the following reception work regarding the documents submitted by a subscriber.
(1) Assign a Registration Authority Branch Reception Number, and Create a Process Record Form
In the Request Management Book, assign a Registration Authority Branch Reception Number to each request, and create a process record form. The Receptionist shall write the assigned number on the received request form.

(2) Confirmation of Request Documents
Certificate issuance/renewal/revocation request documents (below, "Request Documents") and attachments shall be checked to see if they are insufficient or improperly filled out, based on the Process Record Form's checklist. Also, if a floppy disc is attached, it shall be checked for viruses.
Table 4-2 shows the documents required for each request.

Table 4-2 Request Documents Required

Request Documents	CSR Request	Standard Request
Issuance request	Certificate Issuance Request Form CSR saved in floppy disc	Certificate Issuance Request Form
Renewal request	Certificate Renewal Request Form CSR saved in floppy disc	Certificate Renewal Request Form
Revocation request	Certificate Revocation Request Form	

If there was a problem as a result of this checking, then create an Appendix C5: Request Non-Acceptance Notice, and add it to the Request Documents.

4.3.2 Examiner Work

The Examiner receives examination requests from the Receptionist, does the following examination work, and records the examination results in the Process Record Form.
(1) Examination of Applicant
For an applicant which submitted Request Documents, do a face-to-face confirmation (if the applicant is not known personally, compare the applicant's identity and job position document, etc.), or phone to check based on the organization's predetermined telephone number list etc., and thereby confirm the applicant's identity, authenticate the organization to which the applicant belongs, and confirm the intention to own the certificate.

(2) Examination of Certificate Noted Items
The following shall be confirmed for certificate noted items of the Request Documents.
(For Issuance or Renewal)

- No errors in the Request Documents regarding the certificate content.
- In the case of a manager certificate or user certificate, the Organization and Name entered are actually existing organization name, job position name, and manager name.
- In the case of an email certificate, the email address should in principle be in the lg.jp domain name.
- In the case of a web server certificate, the common name (CN) is in the FQDN (Fully Qualified Domain Name) format, and in principle is the lg.jp domain name.
- In the case of a code signing certificate, the organization name (English letters) entered in Organization, and the group name (English letters) entered in Name actually exist in the organization.

(For Revocation)

- The certificate content of the Request Documents has the same information as the certificate content of the certificate issuance Request Documents when the certificate to be revoked was issued.
- The reason for revocation in the Request Documents is valid, referring to Table 4-3.

Table 4-3 Validity of Reason for Revocation

Reason for Revocation Request	Specific Information
Private key compromise	Private key storage media lost, stolen, PIN disclosed, etc.
Change in certificate noted item	Organization name change, manager name change, etc.
Key storage media defect or damaged	Key storage media unusable due to lock or damage, or other problem
Certificate use halted	Work using the certificate ended, organization eliminated, etc.

If there was a problem as a result of the examination, create an Appendix C5: Request Non-Acceptance Notice, and attach it to the Request Documents.

4.3.3 Examination Approver Work

The Examination Approver receives an examination approval request from the Examiner, checks the results of the examination done by the Examiner, and enters the examination results in the Process Record Form.
If the Examiner Approver recognizes that the results of the examination done by the Examiner are proper, the Examiner Approver approves them, and makes a request to Registration Authority Branch Chief for approval of the request process. If there is an improper point, it shall be pointed out to the Examiner, and a re-examination or improved examinations requested.
If there were problems as a result of the examination approval, a Request Documents Non-Acceptance Notice shall be created and attached to the Request Documents.

4.3.4 Work of Registration Authority Branch Chief

The Registration Authority Branch Chief receives the request from the Examination Approver for approval of the request process, checks the series of processes from reception until examination approval and examination results, and judges whether or not to approve the request. The result of this decision is entered in the Process Record Form.
If the request is approved, the Receptionist is instructed to follow procedures for the request to the LGWAN Operation Unit.
If the request is not approved, this is pointed out to the Examination Approver, and a review of the examination process requested.
If it becomes not accepted during the period from reception until examination approval, the Request Non-Acceptance Notice shall be signed and stamped by the Registration Seal of the Registration Authority Branch Chief, and the Receptionist instructed to follow the request non-acceptance procedure.

4.3.5 Request Non-Acceptance Process

If the request from the subscriber was not accepted, the Receptionist takes copies of the Request Documents Non-Acceptance Notice and Request Documents. The original Request Documents Non-Acceptance Notice and Request Documents shall be given to the applicant, and copies of the Request Documents Non-Acceptance Notice and Request Documents stored in the Registration Authority Branch.
The completion date shall be entered in the Request Management Book, with "Non-acceptance" entered as the reason in the delivery column.

4.4 Request to LGWAN Operation Unit, Delivery of Completion Notice and Certificate to Subscriber

After the Registration Authority Branch approved the certificate issuance/renewal/revocation request from the subscriber, the Branch requests that the LGWAN Operation Unit does a certificate issuance/renewal/approval to the Registration Authority Branch.
For the request for LGWAN Operation Unit issuance/renewal/approval to the Registration Authority Branch, the Certificate Issuance Etc Request Management System is used by the Receptionist to enter the request, and by the Registration Authority Branch Chief for approval.
After that, the process result is confirmed, and when completed, a completion notice is delivered to the subscriber. Also, in the case of an issuance or renewal request, the issued certificate is also delivered to the user.
Only in the case of a web server certificate, it is recommended that by advance consultation, issue a certificate from a test environment CA by a generated CSR of the web server equipment, and confirm that the issued certificate can be incorporated in the web server equipment.

4.4.1 Advance Consultation (Web Server Certificate Only)

(1) Entry and Confirmation of Request Data
The Receptionist downloads the Advance Consultation Certificate Issuance Request Sheet from the LGWAN portal site, enters the required items, and attaches the CSR.

(2) Approval of Request Data
The Registration Authority Branch Chief checks the Advance Consultation Certificate Issuance Request Sheet entered by the Receptionist, approves it if there are no problems, and gives instruction to send the Advance Consultation Certificate Issuance Request Sheet. →(4)
If there is a problem, send it to the Receptionist as rejected. →(3)

(3) Deletion of Rejected Data
If rejected in step (2), the Receptionist tells the subscriber the rejection cause etc.

(4) Send to the LGWAN Operation Unit
The Receptionist attaches the Advance Consultation Certificate Issuance Request Sheet to an email, and sends it.
Advance consultation email address: info@lasdec.lgwan.jp
*Clearly write "Server Certificate Advance Consultation" at the start of the email's subject.

(5) Issuance of Certificate
After the LGWAN Operation Unit receives the Advance Consultation Certificate Issuance Request Sheet, the web server certificate is issued from the test environment CA, and sent by email. The following is attached to the email: web server certificate, certificate issuance list (text list), and self-signed certificate of the test environment CA (TESTAppCA.cer).

(6) Delivery of Certificate
The Receptionist securely delivers a floppy disc storing the certificate to the subscriber, either in person or by taking measures to ensure that it does not pass into the hands of a person other than the subscriber.

The floppy disc storing the certificate shall be stored in a lockable storage cabinet, except for taking it out in order to deliver it to the subscriber, and managed in a way that there is no loss, theft, etc.

4.4.2 CSR Request

(1) Entry and Confirmation of Request Data
The Receptionist enters the CSR requested in the Advance Consultation Certificate Issuance Request Sheet, confirms that there are no differences between its content and the certificate noted items of the Request Documents, and enters it in the Process Record Form.

(2) Approval of Request Data
In the Certificate Issuance Etc Request Management System, the Registration Authority Branch Chief checks the data entered by the Receptionist, and does the approval process if is are no problem. If there is a problem, the Chief does the rejection process.
If the approval process was done, the *Reception Number Notice* screen is displayed, so this screen shall be printed, and passed to the Receptionist along with a Process Record Form on which the process details are noted.

This Reception Number is assigned to each approval by the Certificate Issuance Etc Request Management System, so even if multiple request data are approved at the same time, only one Request Number is output. →(3)

If the rejection process was done, a check mark shall be placed for request not accepted in the Process Record Form, and it shall be passed to the Receptionist. →(4)

(3) Confirmation of Request Status
The Receptionist checks the process status of requested data, using the Request Status Confirmation Screen of the Certificate Issuance Etc Request Management System. (LGWAN Operation Unit's reception is not automated, so it may take a little time until reception.)
After reception at the LGWAN Operation Unit, if it is suspended or not accepted, then this can be checked on the Request Status Confirmation Screen, so this shall be reported to the Registration Authority Branch Chief, and the procedure for re-request etc. considered.

In the case of an issuance or renewal request, after the certificate issuance/renewal process at the LGWAN Operation Unit is completed, its status becomes "Waiting to obtain file". When the certificate is obtained, the status becomes "Complete".

(4) Deletion of Rejected Data
If rejected in step (2), the Receptionist deletes the rejected request data, and tells the subscriber the rejection cause, etc.

(5) Certificate Issuance/Renewal Notice Creation
The Receptionist checks the request status in the Certificate Issuance Etc Request Management System, and if it became "Waiting to obtain file", obtains the certificate, and stores it in a floppy disc.
The Receptionist also checks the expiration date and serial number of the certificate issued in the Certificate Issuance Etc Request Management System, and after entering the expiration date and serial number in the issuance notice box of the certificate issuance/renewal Request Documents, requests approval by the Registration Authority Branch Chief.
The Registration Authority Branch Chief checks the contents of the Request Documents, then signs the Request Documents, and approves it by stamping the registration seal of the Registration Authority Branch Chief.

(6) Delivery of Certificate
The Receptionist takes a copy of the approved Request Documents and securely delivers them to the subscriber in person along with the certificate stored in a floppy disc, or if this is not possible in person, delivers by taking measures to ensure that they do not pass into the hands of a person other than the subscriber. The original Request Documents shall be stored in the Registration Authority Branch, and in the Request Management Book, "Complete" shall be circled in this request's delivery status box and the delivery date etc. entered.

The floppy disc storing the certificate shall be stored in a lockable storage cabinet, except for taking it out in order to deliver it to the subscriber, and managed in a way that there is no loss, theft, etc.

4.4.3 Standard Request

(1) Entry and Confirmation of Request Data
Certificate noted items noted in Request Documents are entered into the Certificate Issuance Etc Request Management System by the Receptionist, who also writes them on the Process Record Form.

(2) Approval of Request Data
The Registration Authority Branch Chief checks the request data entered by the Receptionist in the Certificate Issuance Etc Request Management System, and does the approval process if there is no problem. If there is a problem, the Chief does the rejection process.
If the approval process was done, the *Reception Number Notice* screen is displayed, so this screen shall be printed, and passed to the Receptionist along with a Process Record Form on which the process details are noted. →(3)
The Reception Number is assigned to each approval by the Certificate Issuance Etc Request Management System, so even if multiple request data are approved at the same time, only one Request Number is output.

If the rejection process was done, a check mark shall be placed for "Request not accepted" in the Process Record Form, and it shall be passed to the Receptionist. →(7)

(3) Send IC Card Etc. to the LGWAN Operation Unit
After the approval process is done by the Registration Authority Branch Chief, the Receptionist posts the following to the LGWAN Operation Unit (LGWAN-PKI Receptionist) by general certified registered mail: paper on which the Reception Number Notice screen was printed, IC card, reply envelopes and postage stamps (the address shall be accurately written as noted below).
Participant Organizations shall individually procure IC cards, based on the Local Government Wide Area Network Connection Specification, and the Local Government Wide Area Network Connection Specification (Attachments).
LGWAN Connection Specification http://center.lgwan.jp/library/index.html#F-1-1-2
LGWAN Connection Specifications (Related Documents) http://center.lgwan.jp/library/index.html#F-1-1-3

Items Required in Certificate Issuance/Renewal Requests
(1) Reception Number Notice (screen displayed in the Certificate Issuance Etc. Management System printed on paper)
(2) One IC card for each certificate to be issued
(3) Two return envelopes and postage stamps
The IC card and PIN information (security number for using the IC card) shall be sent separately for security, so two are required. The postage stamps shall be equivalent to the postage for two general certified registered mails.
* IC cards and floppy discs shall be packed in padded envelopes, protective packaging materials, etc., to prevent damage during delivery.
* The address written on the return envelopes shall be return address information for delivery items (IC cards, etc.) of Registration Authority Branch staff registration/change/transfer Request Documents

Contact: Local Authorities Systems Development Center
LGWAN-PKI Receptionist
25 Ichiban-cho, Chiyoda-ku
Tokyo 102-8419, Japan

(4) Issuance of Certificate
After receiving the Reception Number Notice, the LGWAN Operation Unit shall check its contents, issue the certificate if there is no problem, place the issued IC card and required documents etc. in the enclosed return envelopes, and return them.

(5) Reception of Certificate
The Receptionist shall check the following returned items. Remember that the IC card and PIN information are returned in separate envelopes

- Copy of Reception Number Notice
- IC card (Certificate stored in card. If not accepted, nothing stored in the card.)
- Certificate issuance list (none if not accepted)
- PIN information (none if not accepted)
- Fingerprint information (none if not accepted)

If not accepted, check the not accepted reason in the Certificate Issuance Etc Request Management System, and do a request again.

(6) Confirmation of Certificate
The Receptionist shall check the following for certificates etc. sent from the LGWAN Operation Unit.

- Quantity of IC cards sent equals the quantity of IC cards returned
- The certificates were issued as requested (the name printed on each IC card surface is the same as the certificate noted items of the Request Documents)
- The serial number printed on each IC card surface matches the certificate issuance list.
- IC cards are usable with the PIN information sent

(7) Deletion of Rejected Data
If request data was rejected in step (2), the Receptionist deletes the rejected request data, and tells the subscriber the rejection cause, etc.

(8) Certificate Issuance/Renewal Notice Creation
The Receptionist checks the expiration date and serial number of the certificate issued in the Certificate Issuance Etc Request Management System, enters the expiration date and serial number in the issuance notice box of the certificate issuance/renewal Request documents, then requests approval by the Registration Authority Branch Chief.
The Registration Authority Branch Chief checks the content of the Request Documents, then signs the Request Documents, and approves them by stamping the registration seal of the Registration Authority Branch Chief.

(9) Delivery of IC Card and Issuance Notice
The Receptionist takes a copy of the Request Documents, and securely delivers them to the subscriber in person along with the IC card and PIN information list (IC card and PIN information list are enclosed in separate envelopes), or if this is not possible in person, delivers by taking measures to ensure that they do not pass into the hands of a person other than the subscriber. The original Request Documents shall be stored in the Registration Authority Branch, and in the Request Management Book, “Complete” circled in this request’s delivery status box and the delivery date etc. entered.

After receiving the IC card and PIN information list from the LGWAN Operation Unit, they shall be stored in a lockable storage cabinet, except for taking it out in order to deliver it to the subscriber, and managed in a way that there is no loss, theft, etc.

4.4.4 Revocation Request

There are two kinds of revocation requests: standard revocation requests and emergency revocation requests. (Refer to Table 2-3 Types of Requests Received by Registration Authority Branch)
An emergency revocation request can be made when a private key is compromised, and the Registration Authority Branch Chief judged it to be an emergency. The request method is done in the Certificate Issuance Etc Request Management System, same as for standard revocation requests, and the LGWAN Operation Unit is contacted by telephone.
If the Certificate Issuance Etc Request Management System cannot be used due to system troubles etc., the emergency revocation request shall be received by fax. Also, in the case of a standard revocation notice done for manager certificates and document exchange certificates issued before February 2008, a fax request is done in the same way (until end of September 2008).

◆ **Revocation Request by Certificate Issuance Etc Request Management System**
(1) Entry and Confirmation of Request Data
Based on the Request Documents, the Receptionist searches in the Certificate Issuance Etc Request Management System for the certificate to be revoked, makes a revocation request, and enters it in the Process Record Form.
The revocation reason of the Certificate Issuance Etc Request Management System shall be entered based on correspondence table 4-4.

Table 4-4 Revocation Reason Correspondence Table

Request Situation	Revocation Reason of Certificate Issuance Etc Request Management System
Private key compromised (Key storage media: loss, theft, PIN leaked, etc.)	Key compromise
Certificate noted items changed	Change content
Private key storage media defect or damage	Replacement
Use of certificate ended	Operation ended

(2) Approval of Request Data
The Registration Authority Branch Chief checks the request data entered by the Receptionist in the Certificate Issuance Etc Request Management System, and does the approval process if there is no problem. If there is a problem, the Chief does the rejection process.
If the approval process was done, a check mark is entered for approval on the Process Record Form, and it is passed to the Receptionist. →(3)
If the rejection process was done, a check mark is entered for request not accepted on the Process Record Form, and it is passed to the Receptionist. →(4)

(3) Confirmation of Request Status
The Receptionist checks the process status of requested data, using the Request Status Confirmation Screen of the Certificate Issuance Etc Request Management System. (LGWAN Operation Unit's reception is not automated, so it may take a little time until reception. In case of emergency revocation, a phone call must be placed to the LGWAN-PKI receptionist (03-5214-0423) of the LGWAN Operation Unit.)
When the certificate revocation process is complete at the LGWAN Operation Unit, the status becomes "Complete".
After reception at the LGWAN Operation Unit, if it is suspended or not accepted, then this can be checked on the Request Status Confirmation Screen, so this shall be reported to the Registration Authority Branch Chief, and the procedure for re-request etc. considered.

(4) Deletion of Rejected Data
If rejected in step (2), the Receptionist deletes the rejected request data, and tells the subscriber the rejection cause, etc.
(5) Certificate Revocation Notice Creation
The Receptionist checks the request status in the Certificate Issuance Etc Request Management System, and if it has become "Complete", confirms the revocation date in the Certificate Issuance Etc Request Management System, writes the revocation date on the certificate revocation Request Documents, then requests approval by the Registration Authority Branch Chief.
The Registration Authority Branch Chief checks the content of the Request Documents, then signs the Request Documents, and approves them by stamping the registration seal of the Registration Authority Branch Chief.

(6) Delivery of Certificate Revocation Completion Notice
The Receptionist takes a copy of the approved Request Documents and securely delivers them to the subscriber in person, or if this is not possible in person, delivers by taking measures to ensure that they do not pass into the hands of a person other than the subscriber. The original Request Documents shall be stored in the Registration Authority Branch, and in the Request Management Book, "Complete" shall be circled in this request's delivery status box and the delivery date etc. entered.

◆ Emergency Revocation by Fax Request
(1) Sending of Certificate Revocation Request Documents
The Registration Authority Branch Chief shall stamp the registration seal on the Appendix B4: Emergency Revocation by Fax Request Sending Form, and instruct the Receptionist to fax it.
The Receptionist shall fax the Emergency Revocation Sending Form and certificate revocation Request Documents to the LGWAN Operation Unit reception contact (03-5214-0427), and shall telephone to 03-5214-0423.
After the revocation request by fax, the LGWAN Operation Unit Examiner shall telephone the main phone number of the local government, and confirm that the emergency revocation request is from that organization. If this can be confirmed, it shall execute the revocation process.

(2) Confirmation of Revocation Completion
After the revocation process is completed, the LGWAN Operation Unit reception contact shall telephone to the Receptionist, so the Receptionist shall report to the Registration Authority Branch Chief.
After receiving a report that the revocation process is complete, the Registration Authority Branch Chief shall telephone the Certification Authority System Chief of the LGWAN Operation Unit (System Chief's name and phone number shall be provided separately), to tell him that completion of the emergency revocation process was confirmed.

(3) Execution of Standard Certificate Revocation Procedure
In order to rigorously perform the revocation process, after the emergency revocation process is completed, when the Certificate Issuance Etc Request Management System becomes usable, the standard certificate revocation procedure shall be followed. At that time, the status of the certificate for which emergency revocation was done is still valid, so the standard revocation process shall be done from that status.

◆ **Revocation Requests for Manager Certificates and Document Exchange Certificates Issued Before February 2008**

(1) Sending of Certificate Revocation Request Documents
The Registration Authority Branch Chief shall stamp the registration seal on the Appendix B4: Emergency Revocation by Fax Request Sending Form, and instruct the Receptionist to fax it. In the notes section, it shall be noted that this is a standard revocation request.
The Receptionist shall fax the Emergency Revocation Sending Form and certificate revocation Request Documents to the LGWAN Operation Unit reception contact (03-5214-0427), and shall telephone to 03-5214-0423.
After the revocation request by fax, the LGWAN Operation Unit Examiner shall telephone the main phone number of the local government, and confirm that the emergency revocation request is from that organization. If this can be confirmed, it shall execute the revocation process.

(2) Confirmation of Revocation Completion
After the revocation process is completed, LGWAN Operation Unit reception contact shall telephone to the Receptionist, so the Receptionist shall report to the Registration Authority Branch Chief.

4.4.5 Revocation Due to Duplicate Public Key

A certificate may be revoked for reasons other than revocation based on a revocation request from the Registration Authority Branch.
When a request is made to issue an email certificate (CSR request), web server certificate, or code signing certificate, if the public key is found to be a duplicate[4] of the public key of a certificate already issued or being requested from the Application CA or for which the request, the certificate already issued certificate being requested becomes a "Compromised public key", and must be revoked.

[4] Occurs with a probability of approximately 0.5^{1024} (0.5 raised to the 1024th power).

(1) Response (Request Side) When there is a Duplicate Public Key
When the Registration Authority Branch made a certificate issuance request, if the Certificate Issuance Etc Request Management System displays a message that a duplicate public key was found, then the Registration Authority Branch shall telephone[5] to the LGWAN Operation Unit's LGWAN-PKI Receptionist (03-5214-0423). In the LGWAN Operation Unit, the non-acceptance process shall be done for that request, so the Registration Authority Branch Chief shall complete the non-acceptance process in the Certificate Issuance Etc Request Management System.

(2) Response (Certificate Owner Side) When there is a Duplicate Public Key
The LGWAN Operation Unit shall tell the Registration Authority Branch which requested issuance of the original certificate with the discovered duplicate public key, that a duplicate public key occurred, and the private key is compromised.
If that certificate issuance is being requested, then the Registration Authority Branch shall do the non-acceptance process, or revoke it if already issued. This revocation procedure is the same as in 4.4.4 Revocation Request.

4.5 Certificate Elimination Request

A certificate issued from an Organization CA (manager certificates and user certificates) is published in the integration repository, and its certificate information can be checked in the name search screen of the LGWAN electronic document exchange system.
If its expiration date is past, information of a manager certificate or user certificate remains in the integration repository, so the Registration Authority Branch shall periodically check the expiration dates of manager certificates and user certificates, and send an elimination request for expired manager certificates and user certificates to the LGWAN Operation Unit, and they must be deleted from the integration repository. Elimination requests are not required for manager certificates and document exchange certificates issued before February 2008.

(1) Related Information Delete Request (User Certificates Only)
The Receptionist shall search for user certificates past their expiration date, and send a request to the LGWAN manager (person responsible for management of related information) for deletion of related information by the person in charge of document handling.

(2) Entry and Confirmation of Request Data
For certificates past their expiration date, the Receptionist shall make elimination requests in the Certificate Issuance Etc. Management System.

(3) Approval of Request Data
The Registration Authority Branch Chief shall check request data entered by the Receptionist into the Certificate Issuance Etc. Management System, and do the approval process if there is no problem. If there is a problem, the rejection process shall be done.

[5] Depending on how the requested CSR was made etc., the Certificate Issuance Etc Request Management System may detect a duplicate public key, even though the private key is not compromised. It must be determined whether it is compromised or not, so the LGWAN Operation Unit must be contacted.

If the rejection process was done, a check mark for non-acceptance shall be placed in the Certificate Issuance Etc. Management System, and it shall be passed to the Receptionist. →(5)

(4) Confirmation of Request Status
The Receptionist shall confirm the process status of requested data, using the Request Status Confirmation Screen of the Certificate Issuance Etc. Management System.

(5) Deletion of Rejected Data
If rejected in step (3), the Receptionist shall delete the rejected request data, and tells the subscriber the rejection cause, etc.

(6) Certificate Elimination Completion Process
The Receptionist shall check the request status, using the Certificate Issuance Etc. Management System.

Chapter 5 Management of Documents

This Chapter explains some of the work done by Registration Authority Branches, as determined in 2.3 Work of Registration Authority Branches, (4) Management of Documents.
As document evidence in order to show that the work of the Registration Authority Branch is being done properly and smoothly, the documents shown in Table 5-1 used in the Registration Authority Branch must be stored.
The storage period shall be for a minimum 5 years from the certificate's expiration date. After that, continued storage, disposal, etc. shall be decided according to document storage rules etc. of the Participant Organization.