InCommon®

InCommon Certificate Manager

SSL Web Service API

InCommon
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

Table of Contents

Version History

1.1. Removed extra error codes.

1. Initial Version

1.2. Added 'SSL' type with 'renewID' field. The 'SSLCollectReponse' type contains 'SSL' field now.

1.3. Fixed variable's name.

1.4. Added 'Invalid ID' return code with 'getCollectStatus' method.

1.5. Added 3 methods (enroll5, getCustomerCertTypes5, enrollWithDCV5)
Added 2 types (CustomerCertTypes5, CustomerCertTypeResponse5)
Changed type (CustomerCertTypes contains Integer array)

1 Introduction

Name	:	EPKIManagerSSLService
Service EPR	:	http://cert-manager.com/ws/EPKIManagerSSL OR http://cert-manager.com/private/ws/EPKIManagerSSL
View WSDL	:	http://cert-manager.com/ws/EPKIManagerSSL?wsdl OR http://cert-manager.com/private/ws/EPKIManagerSSL?wsdl
Service Description	:	The Service allows the Administrator to renew and collect renewed SSL certificates, request, collect, and revoke SSL certificates.

2 Authentication

To access InCommon APIs, you first need to authenticate yourself to the InCommon CM service. You can authenticate via username/password, or via username + client certificate. The SSL Web Service API service uses the SOAP protocol.

- Authentication via Username and Password
- Authentication via Username and a Client Certificate

2.1 Authentication via Username and Password

Prerequisite

- Users should have InCommon CM login credentials and the correct customer login URI
- For the Web Service API, access must be enabled for the customer by InCommon and for each org/dept by admins on the client side.

The URI for the username/password authentication is:

- https://cert-manager.com:443/ws/EPKIManagerSSL

Authentication is performed by sending the AuthData parameter to the web service API. This includes the username, password and Customer URI. After successful authentication, the admin can proceed to the InCommon CM management interface. If authentication is not successful (login and/or password are incorrect, password has expired), the admin will see an error and will be denied access to the Web Service API. The same admin could, however, still authenticate themselves via a client certificate (refer to the next section).

2.2 Authentication via Username and a Client Certificate

Prerequisite

- Admins should have the Customer URI
- For the Web Service API, access must be enabled for the customer by InCommon and for each org/dept by admins on the client side.
- Admins should have 'Certificate Auth' enabled. The authentication certificate must requested and issued via InCommon CM and active at the moment of authentication.

The URI for the username/client certificate authentication is:

- https://cert-manager.com:443/private/ws/EPKIManagerSSL

The certificate must be provided by the admin's client at the time of login. After receiving the authdata parameter (customer URI and login), InCommon CM will verify that the certificate matches the one specified in the 'Certificate Auth' area of the admin's profile. After successful authentication, the admin can proceed to the InCommon CM management interface. If authentication is not successful (username is incorrect, certificate is not correct/revoked), the admin will see an error and will be denied access to the SSL Web Service API. The same admin could, however, still authenticate themselves using the username and password method (see previous section).

3 Remote Functions

3.1 Function for SSL Certificate Renewal

int renew(String renewId)

3.1.1 Arguments

Variable Name	Type	Max. Length (chars)	Description
renewId	String	20	Given by cm in notification letter when SSL certificate was issued.

3.1.2 Return value – 'status code' of operation

Status code	Possible Value(s)
If 'status code' < 0	-3 = internal error; -4 = invalid renewId.
If 'status code' = 0	0 = success.

3.2 Function for SSL Certificate Renewal by SSL ID

int renewById(String renewById)

3.2.1 Arguments

Variable Name	Type	Max. Length (chars)	Description
authData	AuthData		Authentication data for access. See section 3.5.1.1.AuthData type
id	String		This is the SSL identifier previously returned by ***enroll***./**renewById** functions Displayed in SSL Grid as 'Self Enrollment Certificate ID'

3.2.2 Return value - 'status code' of operation

Status code	Possible Value(s)
If 'status code' < 0	-14 = An unknown error occurred; -16 = Permission denied; -40 = Invalid ID; -100 = Invalid auth data; -110 = The certificate type is invalid.
If 'status code' = 0	0 = success.

3.3 Function for Collecting Renewed SSL Certificate

SSLRenewResponse collectRenewed(String renewId, int formatType)

3.3.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
renewId	String	20		Given by cm in notification letter when SSL certificate was issued.
formatType	int	1	0 = X509 PEM Bundle; 1 = X509 PEM Certificate only; 2 = X509 PEM Intermidiate certificate only; 3 = PKCS#7 PEM Bundle; 4 = PKCS#7 DER Bundle.	Format of SSL to be returned.

3.3.2 Return value – SSLRenewResponse

SSLRenewResponse - Object that contains collect operation status and SSL Certificate in Byte array if succeed.

Method Name	Possible value(s)
int getErrorCode()	0 = issued; -1 = applied; -2 = certificate error, invalid state; -3 = internal error; -4 = SSL Certificate not exists; -5 = waiting for approval by admin; -6 = admin has declined request.
byte[] getData()	If status code = 0, then certificate in the form of byte array if succeed, *null* otherwise.

3.4 Function for SSL Certificate Replacement

int replace (AuthData data, Integer id, string csr, string reason)

3.4.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 3.5.1.1.AuthData type
id	String			This is the SSL identifier previously returned by function ***enroll***. Displayed in SSL Grid as 'Self Enrollment Certificate ID'
csr	String	32767	Subject: The fields may be in any order, (although multiple street addresses, if present, should be in the correct order). Algorithm OID = rsaEncryption (PKCS#1). Size = 512 to 8192 bits. Attributes: Any attributes MAY be present, but they will be ignored if the subject_ fields are used. Signature Algorithm: md5WithRSAEncryption (PKCS#1).	Certificate Signing Request (Base-64 encoded with or without the -----BEGIN xxxxx----- and -----END xxxxx----- header and footer). Allowed values:
reason	string	256		Reason for the Replacement. The reason will be used for audit logging.
comonName	string		Optional. If tag is present – its value must match corresponding value in CSR.	String of Common Name.
subjAltName	string		Each Subject Alternative Name surrounded by tag. Ignored for Instant SSL. Can be present 0 or more times for Multi-Domain SSL. Its values must match	List of Subject Alternative Names.

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
			corresponding values in CSR.	

3.4.2 Return value - 'status code' of operation

Status code	Possible Value(s)
If 'status code' < 0	-9 = The CSR is not valid Base-64 data; -10 = The CSR cannot be decoded; -11 = The CSR uses an unsupported algorithm; -12 = The CSR has an invalid signature; -13 = The CSR uses an unsupported key size; -14 = An unknown error occurred; -15 = Reason cannot be empty; -16 = Permission denied; -24 = Auth data argument is invalid; -40 = Invalid ID; -100 = Invalid auth data; -101 = Invalid organization auth data; -103 = The type of certificate status is invalid; -105 = Person not found; -106 = EULA is not accepted.
If 'status code' = 0	Operation was successful.

3.5 Functions for SSL Certificate Enrollment

Integer enroll(AuthData data, Integer orgId, String secretKey, String csr, String phrase, String subjAltNames,CustomerCertType certType, Integer numberServers, Integer serverType, Integer term, String comments)

Integer enroll5(AuthData data, Integer orgId, String secretKey, String csr, String phrase, String subjAltNames, CustomerCertType certType, Integer numberServers, Integer serverType, Integer term, String comments)

Integer enrollWithDCV5(AuthData data, Integer orgId, String secretKey, String csr, String phrase, String subjAltNames, CustomerCertType certType, Integer numberServers, Integer serverType, Integer term, String comments, String dcv_email)

Integer enrollWithDCV (AuthData data, Integer orgId, String secretKey, String csr, String phrase, String subjAltNames, CustomerCertType certType, Integer numberServers, Integer serverType, Integer term, String comments, String dcv_email)

Integer enrollWithCustomFields5(AuthData authData, Integer orgId, String secretKey, String csr, String phrase, String subjAltNames, CustomerCertType5 certType, Integer numberServers, Integer serverType, String term, String comments, List<CertCustomFieldDto> certCustomFieldDtos)

Integer enrollWithCustomFields (AuthData data, Integer orgId, String secretKey, String csr, String phrase, String subjAltNames, CustomerCertType certType, Integer numberServers, Integer serverType, Integer term, String comments, List<CertCustomFieldDto> certCustomFieldDto)

Integer enrollWithCustomFields5 (AuthData data, Integer orgId, String secretKey, String csr, String phrase, String subjAltNames, CustomerCertType certType, Integer numberServers, Integer serverType, String term, String comments, List<CertCustomFieldDto> certCustomFieldDto)

Integer enrollV2 (AuthData data, EnrollRequest enrollRequest)

3.5.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 3.5.1.1 AuthData Type.
orgId	Integer			Organization identifier. Can be obtained from Admin UI – 'Settings' - 'Organization' tab.
secretKey	String	20		Secret Key for SSL is setting in Client Admin UI. 'Settings' – 'Organization' – 'Add/Edit Organization' dialog, 'SSL' tab.
csr	String	32767	Subject:	Certificate Signing Request

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
			The fields may be in any order (although multiple street addresses, if present, should be in the correct order). Algorithm OID = rsaEncryption (PKCS#1). Size = 512 to 8192 bits. Attributes: Any attributes MAY be present, but will be ignored if the subject_ fields are used. Signature Algorithm: md5WithRSAEncryption (PKCS#1)	(Base-64 encoded with or without the -----BEGIN xxxxx----- and -----END xxxxx----- header and footer)
phrase	String	64		Pass phrase for revocation.
subjAltNames	String		Subject Alternative Names splitted with ",".	List of Subject Alternative Names.
certType	CustomerCertType			Certificate types available for the ordering customer. See description in section 3.9.2 for more details.
numberServers	Integer			Number of servers.
serverType	Integer			Server type of the SSL certificate. See description below in section 3.5.1.2 Server Type.
term(for enroll and enrollWithDCV) term(for enroll5 and enrollWithDCV5)	Integer Integer		Term in years. Term in days.	Term of the SSL certificate. Term of the SSL certificate.
comments	String	256		The message that will be

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
				attached to the certificate.
certCustomFieldDto	List<CertCustomFieldDto>			Zero or more CertCustomFieldDto's
enrollRequest	EnrollRequest			Enrollment request. See description below in section EnrollRequest type
certCustomFieldDto	List<CertCustomFieldDto>			Zero or more CertCustomFieldDto's
enrollRequest	EnrollRequest			Enrollment request. See description below in section 3.5.1.2. EnrollRequest type

3.5.1.1 AuthData type

Method Name	Description
setLogin(String value)	Set login name for account within cm. This is the login of the Admin with role 'MRAO Admin, RAO SSL Admin' or 'DRAO SSL Admin' within cm account.
setPassword(String value)	Set password for account within cm. This is the login of the Admin with role 'MRAO Admin, RAO SSL Admin' or 'DRAO SSL Admin' within cm account.
setURI(String value)	URI for logging into account within cm.

3.5.1.2 EnrollRequest type

Method Name	Description
setOrgId(Integer orgId)	Setter for organization identifier. Can be obtain from Admin UI - Organization properties 'Client Cert' tab.
setSecretKey(String secretKey)	Setter for Secret Key. Secret Key for SSL is setting in Client Admin UI 'Organization' properties, tab 'SSL Certificates'.
setCsr(String csr)	Setter for Certificate Signing Request (Base-64 encoded with or without the

Method Name	Description
	-----BEGIN xxxxx----- and -----END xxxxx----- header and footer).
setPhrase(String phrase)	Setter for Pass phrase. Pass phrase is used for revocation.
setSubjAltNames(String subjAltNames)	Setter for list of Subject Alternative Names. Allowed value is Subject Alternative Names splitted with ','
setCertType(CustomerCertType certType)	Setter for the CustomerCertType. See description in section 3.7.2. for details.
setNumberServers(Integer numberServers)	Setter for the Number of servers.
setServerType(Integer serverType)	Setter for the Server type. See allowed values in section 3.3.1.2 Server Type
setTerm(String term)	Setter for the Term of the SSL certificate in years.
setComments(String comments)	Setter for the Comments - the message that will be attached to the certificate.
setCustomFields(List customFields)	Setter for list of Custom Fields - zero or more CertCustomFieldDto's.
setDcv(String dcv)	Setter for Domain Control Validation email.
setExternalRequester(String externalRequester)	Setter for External Requester email(s). If there is more than one email, values must be separated by commas.

3.5.1.3 CertCustomFieldD to type

Method Name	Description
setCustomFieldDto(CustomFieldDto customFieldDto)	Setter for CustomFieldDto. See description in guide for *EPKIManagerCustomField* service its type CustomFieldDto.
setValue(String value)	Setter for Value of certificate custom field. Max length 256 chars.

3.5.1.4 Server Type

Server Type	Description
1	AOL
2	Apache/ModSSL

Server Type	Description
3	Apache-SSL (Ben-SSL, not Stronghold)
4	C2Net Stronghold
33	Cisco 3000 Series VPN Concentrator
34	Citrix
5	Cobalt Raq
6	Covalent Server Software
7	IBM HTTP Server
8	IBM Internet Connection Server
9	iPlanet
10	Java Web Server (Javasoft / Sun)
11	Lotus Domino
12	Lotus Domino Go!
13	Microsoft IIS 1.x to 4.x
14	Microsoft IIS 5.x and later
15	Netscape Enterprise Server
16	Netscape FastTrack
17	Novell Web Server
18	Oracle
19	Quid Pro Quo
20	R3 SSL Server
21	Raven SSL
22	RedHat Linux
23	SAP Web Application Server

Server Type	Description
24	Tomcat
25	Website Professional
26	WebStar 4.x and later
27	WebTen (from Tenon)
28	Zeus Web Server
29	Ensim
30	Plesk
31	WHM/cPanel
32	H-Sphere
-1	OTHER

3.5.1.5 CertCustomFieldDto

Name	Description
CustomFieldDto customFieldDto	Custom field
String value	Requested value

3.5.1.6 CustomFieldDto

Name	Description
Integer id	Custom field identifier
String name	Custom field name
String certType	Custom fields type, must be “SSL” for SSL Certificate enrollment
Boolean mandatory	Mandatory or not
String state	Custom field state [ACTIVE | INACTIVE]

3.5.2 Return value – 'status code' of operation

Status code	Possible Value(s)
If 'status code' < 0	-3 = The 'User name' argument is invalid. -7 = Country is not a valid ISO-3166 country! -9 = The CSR is not valid Base-64 data! -10 = The CSR cannot be decoded! -11 = The CSR uses an unsupported algorithm! -12 = The CSR has an invalid signature! -13 = The CSR uses an unsupported key size! -14 = An unknown error occurred! -16 = Permission denied! -31 = The email is not a valid email. -32 = The two phrase should be the same! -33 = The Comodo certificate type is invalid! -34 = The secret key is invalid! -35 = The server type is invalid! -36 = The term is invalid for customer type! -41 = Subject Alternative Names are not allowed for selected Certificate Type -60 = Custom field 'id' is invalid! -61 = Invalid or missing custom field value -62 = Missing mandatory custom field! - 100 = Invalid authentication data for customer - 101 = Invalid authentication data for customer Organization - 110 = Domain is not allowed for customer

Status code	Possible Value(s)
	- 111 = Domain is not allowed for customer Organization - 120 = Customer configuration is not allowed the requested action -139 = External Requester is required; -140 = External Requester has invalid format; -141 = Some of External Requester emails doesn't meet organization constraints.
If 'status code' > 0	SSL identifier. It will be used for certificate collecting/revoking.

3.6 Function for Checking if Certificate is Available

Integer getCollectStatus(AuthData data, Integer id)

3.6.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 3.5.1.1 AuthData Type.
id	Integer		Any SSL identifier previously returned to your account.	This is the SSL identifier previously returned by function ***enroll***.

3.6.2 Return value – status of certificate availability

Possible Value(s)
0 = Cert is being processed by InCommon 1 = Cert is available for collection -14 = An unknown error occurred! -16 = Permission denied! -23 = Certificate is waiting for approval! - 40 = Invalid ID

Possible Value(s)
- 100 = Invalid authentication data for customer -101 = Invalid authentication data for customer organization -110 = Domain is not allowed for customer -111 = Domain is not allowed for customer organization - 120 = Customer configuration is not allowed the requested action -136 = The certificate request has been rejected by CA; -137 = The certificate request is invalid.

3.7 Function for Collecting Enrolled SSL Certificate

SSLCollectResponse collect(AuthData data, Integer id, int formatType)

3.7.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 3.5.1.1 AuthData Type.
id	Integer		Any SSL identifier previously returned to your account.	This is the SSL identifier previously returned by function ***enroll***.
formatType	int	1	0 = X509 PEM Bundle; 1 = X509 PEM Certificate only; 2 = X509 PEM Intermidiate certificate only; 3 = PKCS#7 PEM Bundle; 4 = PKCS#7 DER Bundle.	Allowed formats for downloading of SSL.

3.7.2 Return value – SSLCollectResponse

SSLCollectResponse - Object that contains collect operation status and SSL Certificate in Base-64 if succeed.

Method Name	Possible Value(s)
int getStatusCode()	0 = when certificate is not ready -14 = An unknown error occurred! -16 = Permission denied! -20 = CSR rejected -21 = The certificate has been revoked! -22 = Still awaiting payment! - 40 = Invalid ID - 100 = Invalid auth data! - 120 = Customer configuration is not allowed the desired action -136 = The certificate request has been rejected by CA; -137 = The certificate request is invalid.

3.7.3 SSL type

Method Name	Description
String getRenewID()	Given by cm when SSL certificate was issued. This code may be used for renewing the certificate.
String getCertificate()	The certificate in Base-64

3.8 Function for SSL Certificate Revocation

Integer revoke(AuthData data, Integer id, String reason)

3.8.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 3.5.1.1 AuthData Type.
id	Integer		Any SSL identifier previously returned to your account.	This is the SSL identifier previously returned by function

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
				enroll.
reason	String	256		Revocation reason for audit logging. Empty String allowed.

3.8.2 Return value – 'status code' of operation

Possible Value(s)
-14 = An unknown error occurred! -16 = Permission denied! - 40 = Invalid ID - 100 = Invalid auth data! - 120 = Customer configuration is not allowed the desired action

3.9 Function for Loading List of Available Certificate Types for Customer.

CustomerCertTypeResponse getCustomerCertTypes (AuthData authData)

CustomerCertTypeResponse5 getCustomerCertTypes5 (AuthData authData)

CustomerCertTypeResponse getCustomerCertTypesByOrg (AuthData authData, Integer orgId)

CustomerCertTypeResponse5 getCustomerCertTypesByOrg5 (AuthData authData, Integer orgId)

3.9.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 3.5.1.1 AuthData Type.

3.9.2 Return value.

CustomerCertTypeResponse - Object that contains array available customer certificate types (see description of CustomerCertType below).

CustomerCertTypeResponse5 - Object that contains array available customer certificate types (see description of CustomerCertType5 below).

Field Name	Possible Value(s)
CustomerCertType[] getTypes() CustomerCertType5[] getTypes()	If customer does not have available certificate type - result array will be empty. If customer does not have available certificate type - result array will be empty.
int getStatusCode()	-14 = An unknown error occurred! -16 = Permission denied!-

3.9.2.1 CustomerCertType – type for saving information about available customer certificate type.

Variable Name	Description
int getId()	The service customer cert type identifier.
String getName()	Name of this certificate type. For example “InstantSSL”
String[] getTerms	List of available terms for this customer certificate type (In Years).

For backward compatibility during the certificate enrollment process, one can specify the number of years instead of the number of days.

3.9.2.2 CustomerCertType5 - type for saving information about available customer certificate type

Variable Name	Description
String[] getTerms	List of available terms for this customer certificate type (In Days).

3.10 Function for changing SSL Certificate External Requester

Integer updateRequesterExt(AuthData data, Integer id, String[] requesterExt)

3.10.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description

authData	AuthData			Authentication data for access. See section 3.5.1.1.AuthData type
id	Integer		Any SSL identifier previously returned to your account.	This is the SSL identifier previously returned by function ***enroll***.
requesterExt	String[]		Array of email addresses	Array of email addresses for external requester(s)

3.10.2 Return Value - 'status code' of Operation

CustomFieldResponse – object which contains collection of **CustomFieldDto** objects. See section 3.5.1.4 for the details.

Possible Value(s)
0 = SUCCESSFUL;
-14 = An unknown error occurred;
-16 = Permission denied;
-31 = External Requester is invalid;
-100 = Invalid auth data;
-101 = Invalid organization auth data;
-106 = EULA is not accepted;
-110 = Domain is not allowed for customer;
-111 = Domain is not allowed for organization;
-112 = KU/EKU template is not allowed for customer;
-113 = KU/EKU template is not allowed any more;
-114 = Client Cert Type is not available for organization;
-115 = Domain is not DCV validated (while 'Enforce DCV for S/MIME' is ON);
-120 = Customer configuration is not allowed the desired action.

3.11 Function for getting possible Custom Fields

Integer getCustomFields(AuthData data)

3.11.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 3.5.1.1.AuthData type

3.11.2 Return Value - 'status code' of Operation

Possible Value(s)
0 = SUCCESSFUL; -14 = An unknown error occurred; -16 = Permission denied; -31 = External Requester is invalid; -100 = Invalid auth data; -101 = Invalid organization auth data; -106 = EULA is not accepted; -110 = Domain is not allowed for customer; -111 = Domain is not allowed for organization; -112 = KU/EKU template is not allowed for customer; -113 = KU/EKU template is not allowed any more; -114 = Client Cert Type is not available for organization; -115 = Domain is not DCV validated (while 'Enforce DCV for S/MIME' is ON); -120 = Customer configuration is not allowed the desired action.

3.12 Utility Function for Getting Short Information about Web Service (name, version, etc.).

String getWebServiceInfo()