InCommon®

InCommon Certificate Manager

SMIME Enroll API

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

Table of Contents

Version History

1.0 Initial version

1.1 Minor fixes (fixed return type for collect function, renamed class CFields to CertFields)

1.2 Improved authentication for all functions.

- Added class 'AuthData' for authentication.

- Added function 'getCollectStatus' to check certificate status.

1.3 Used type Integer instead Long.

1.4 Use Secret Key instead of accessCode.

- Added parameter orgId in enroll method

- Minor improved parameters order in enroll method

- Added new status code (110,111,120), remove old(102,103) and change value for existing(100,101)

- Added utility function getWebServiceInfo()

1.4.1 Added auto revoke description for enroll function.

1.5 Added new functions for enrolling certificates with certain KU/EKU:

- enrollUsingKUTemplates

- getKUTemplates

1.5.1 Added status code 'REJECTED' as return code for 'collect' function. (See 2.2.2)

1.5.2 Added status code 'ORDER_NUMBER_NOT_FOUND' as return error code for 'collect', 'getCollectStatus', 'revoke'functions. (See 2.2.2, 2.3.2, 2.4.2)

1.6 Added new function for revoking certificates by serial number:

1.5revokeBySerialNumber (See 2.4)

1.7 Added new return status code (114) for 'enrollUsingKUTemplates' function.

1.8 Added new API for Device Certificates (See 2.7, 2.8, 2.9)

1.9 API For Device Certificates moved into separate document

1 Introduction

Name	:	EPKIService
Service EPR	:	http://cert-manager.com/ws/EPKIManager OR http://cert-manager.com/private/ws/EPKIManager
View WSDL	:	http://cert-manager.com/ws/EPKIManager?wsdl OR http://cert-manager.com/private/ws/EPKIManager?wsdl
Service Description	:	The Service allows the Administrator to request, collect and revoke client 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 SMIME Enroll API service uses the SOAP protocol.

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/EPKIManager

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/EPKIManager

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 SMIME Enroll 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 Client Certificate Enrollment

3.1.1 General

Integer enroll(AuthData authData, Integer orgId, String secretKey,String username, String email,String CSR)

Previous certificates on the same email will be revoked automatically depending on account settings.

3.1.1.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See description in the section 3.1.3 AuthData Type.
secretKey	string	20		Secret Key is the setting in Client Admin UI > 'Organization' properties > 'Client cert' tab.
orgId	Integer			Organization identifier. Can by obtained from Admin UI > Organization properties > 'Client Cert' tab.
username	string	64		Name to enroll certificate for. This value will be set for the

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
				subject 'CN'.
email	string	128		Valid email address. Domain in email address should match domain from Organization that the secret Key belongs to.
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 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)

3.1.1.2 Return value - Status Code

Status code	Possible Value(s)
If ' status code' < 0	- 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! - 100 = Invalid auth data! - 101 = The 'Access code' argument is invalid. - 120 = Customer configuration is not allowed the desired action

3.1.2 Using Templates

Integer enrollUsingKUTemplates(AuthData authData, Integer orgId, String secretKey,String username, String email,String CSR, List<KUTemplate> kuTemplate)

Previous certificates on the same email will be revoked automatically depending on account settings.

3.1.2.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See description in the section 3.1.3 AuthData Type.
secretKey	string	20		Secret Key is the setting in Client Admin UI > 'Organization' properties >, 'Client cert' tab.
orgId	Integer			Organization identifier. Can by obtained from Admin UI > Organization properties > 'Client Cert' tab.
username	string	64		Name to enroll certificate for. This value will be set for the subject 'CN'.
email	string	128		Valid email address. Domain in email address should match domain from Organization that the secret Key belongs to.
csr	string	32767	Subject: The fields may be in any order (although multiple	Certificate Signing Request (Base-64 encoded with or without the -----BEGIN xxxxx-----

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
			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)	and -----END xxxxx----- header and footer)
List<KUTemplate> kuTemplate	Array of KUTemplate			List of requested 'KU/EKU templates'. List of available KU/EKU templates for your account could be retrieved using 'getKUTemplates()' function.

3.1.3 AuthData type

Name	Description
setLogin(String value)	Set login name for account within InCommon CM. This is login of the Admin with role 'Client Cert' within InCommon CM account.
setPassword(String value)	Set password for account within InCommon CM. This is password of the Admin with role 'Client Cert' within InCommon CM account.
setURI(String value)	URI for logging into account within InCommon CM.

3.1.4 KUTemplate type

Name	Description
getShortName()	Get short name of the cert usage template.

Name	Description
getDescription()	Get description of the cert usage template.
getKeyUsages()	Set of key usages that contains in the template.
getExtKeyUsages()	Set of extended key usages that contains in the template.

3.1.5 KeyUsage type

Name	Description
getCode()	Get internal identifier of the key usage
getName()	Get internal human like name of the key usage.

3.1.6 ExtKeyUsage type

Name	Description
getCode()	OID of the extended key usage.
getName()	Name of the extended key usage.

3.1.7 Return value – 'status code' of operation

Status code	Possible Value(s)
If ' status code' < 0	- 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! - 100 = Invalid auth data! - 101 = The 'Access code' argument is invalid. - 111 = Domain is not allowed for Organization

Status code	Possible Value(s)
	- 112 = KU/EKU template is not allowed for customer - 113 = KU/EKU template is not allowed any more - 114 = KU/EKU template is not available for Organization - 120 = Customer configuration is not allowed the desired action
If 'status code' > 0	Order number. It will be used for certificate collection/revoking.

3.2 Function for Checking if Certificate is Available.

Integer getCollectStatus (AuthData authData, Integer orderNumber)

3.2.1 Arguments

Variable Name	Type	Allowed values	Description
authData	AuthData		Authentication data for access. See description in the section 3.1.3 AuthData Type.
orderNumber	Integer	Any order number previously returned to your account.	This is the order number previously returned by function enroll.

3.2.2 Return value – status of certificate availability

Value	Description
Status Code	1 = Certificate available 0 = Certificate being processed by InCommon -1 = The 'Order number' argument is invalid. -2 = Order number not found. -14 = An unknown error occurred! -16 = Permission denied! - 100 = Invalid auth data! - 101 = Invalid authentication data for customer Organization - 120 = Customer configuration is not allowed the desired action

3.3 Function for Collecting Enrolled Client Certificate.

SMIMECollectResponse collect (AuthData authData, Integer orderNumber)

3.3.1 Arguments

Variable Name (case insensitive)	Type	Allowed values	Description
orderNumber	Integer	Any order number previously returned to your account.	This is the order number previously returned by function enroll.
authData	AuthData		Authentication data. See description in the section 3.1.3 AuthData Type.

3.3.2 Return value – SMIMECollectResponse

SMIMECollectResponse - Object that contains collect operation status and Client Certificate in Base-64 if succeed.

SMIMECollectResponse	Possible value(s)
int statusCode	1 = Certificates attached 0 = Being processed by InCommon -1 = The 'Order number' argument is invalid. -2 = Order number not found. -14 = An unknown error occurred! -16 = Permission denied! -20 = CSR rejected -21 = The certificate has been revoked! -22 = Still awaiting payment! -100 = Invalid auth data! -101 = Invalid Organization auth data! -120 = Customer configuration is not allowed the desired action
String certificate	If status code = 1, then - certificate in Base-64 if succeed, null otherwise.

3.4 Function for Client Certificate Revocation

Integer revoke (AuthData authData, Integer orderNumber, String reason)

Integer revokeBySerialNumber (AuthData authData, String serialNumber, String reason)

Integer revokeAllByPerson (AuthData data, String email, String org, String dep)

3.4.1 Arguments

Variable Name	Type	Max. Length	Description
orderNumber	Integer		This is the order number previously returned by function enroll.
serialNumber	String		The serial number of the certificate to be revoked, with 16 hex format.
reason	String	128	Revocation reason for audit logging. Empty String is also allowed.
authData	AuthData	128	Authentication data. See description in the section 3.1.3 AuthData Type.
email	String	128	The email of the of the client
org	String	128	The name of the Organization on which a person assigned to.
dep	String	128	The name of the Department (if available) on which a person assigned to.

3.4.2 Return value – Status code

Status code	Possible Value(s)
Status Code	0 = Successful -1 = The 'Order number' argument is invalid. -2 = Order number not found. -3 = The 'Serial number' argument is invalid. -4 = Serial number not found. -14 = An unknown error occurred!

Status code	Possible Value(s)
	-16 = Permission denied! -20 = The certificate request has been rejected! -21 = The certificate has been revoked! -26 = The certificate is currently being Issued! - 100 = Invalid auth data! - 101 = Invalid Organization auth data! - 120 = Customer configuration is not allowed the desired action

3.5 Function for Loading List of Available KUTemplates for Your Account

Ask support to add or change specific template to your account.

List<KUTemplate> getKUTemplates (AuthData authData)

3.5.1 Arguments

Variable Name	Type	Max. Length	Description
authData	AuthData		Authentication data. See description in the section 3.1.3 AuthData Type.

3.5.2 Return value – List of KUTemplate

Refer to section 3.1.4 KUTemplate types for details.

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

String getWebServiceInfo()