

InCommon®



InCommon Certificate Manager

Software Version 2.8.23

SMIME Enroll API

Release Date: 23rd June, 2011

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

Table of Contents

Version History	4
1 Introduction	5
2 Remote Functions	5
2.1 Function for Client Certificate Enrollment	5
2.1.1 General.....	5
2.1.1.1 Arguments.....	5
2.1.2 Using Templates.....	6
2.1.2.1 Arguments.....	7
2.1.3 AuthData type.....	8
2.1.4 KUTemplate type.....	8
2.1.5 KeyUsage type.....	9
2.1.6 ExtKeyUsage type.....	9
2.1.7 Return value – 'status code' of operation.....	9
2.2 Function for Checking if Certificate is Available	10
2.2.1 Arguments.....	10
2.2.2 Return value – status of certificate availability.....	10
2.3 Function for Collecting Enrolled Client Certificate	11
2.3.1 Arguments.....	11
2.3.2 Return value – SMIMECollectResponse.....	11
2.4 Function for Client Certificate Revocation	12
2.4.1 Arguments.....	12
2.4.2 Return value – Status code.....	12
2.5 Function for loading list of available KUTemplates for your account.	13
2.5.1 Arguments.....	13
2.5.2 Return value – List of KUTemplate	13

2.6 Utility Function for Getting Short Information about Web Service (name, version, etc.).....13

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:

- revokeBySerialNumber (See 2.4)

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

1 Introduction

Name : EPKIService

Service EPR : http://CM-host/ws/EPKIManager

View WSDL : http://CM-host/ws/EPKIManager?wsdl

Service Description : The Service allows the Administrator to request, collect and revoke client certificates.

2 Remote Functions

2.1 Function for Client Certificate Enrollment

2.1.1 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.

2.1.1.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See description in the section 2.1.3 AuthData Type .
secretKey	string	20		Secret Key is the setting in Client Admin UI > 'Organization' properties > 'Client cert' tab.
orgId	Integer			Organization identifier. Can be 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.

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
				Domain in email address should match domain from organization that the secret Key belongs to.
csr	string	32767	<p>Subject:</p> <p>The fields may be in any order (although multiple street addresses, if present, should be in the correct order).</p> <p>Algorithm OID =</p> <p>rsaEncryption</p> <p>(PKCS#1).</p> <p>Size = 512 to 8192 bits.</p> <p>Attributes:</p> <p>Any attributes MAY be present, but will be ignored if the subject_ fields are used.</p> <p>Signature Algorithm:</p> <p>md5WithRSAEncryption</p> <p>(PKCS#1)</p>	<p>Certificate Signing Request</p> <p>(Base-64 encoded with or without the -----BEGIN xxxxx----- and -----END xxxxx----- header and footer)</p>

2.1.2 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.

2.1.2.1 Arguments

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

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
				the section 2.1.3 AuthData Type .
secretKey	string	20		Secret Key is the setting in Client Admin UI > 'Organization' properties >, 'Client cert' tab.
orgId	Integer			Organization identifier. Can be 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	<p>Subject:</p> <p>The fields may be in any order (although multiple street addresses, if present, should be in the correct order).</p> <p>Algorithm OID =</p> <p>rsaEncryption</p> <p>(PKCS#1).</p> <p>Size = 512 to 8192 bits.</p> <p>Attributes:</p> <p>Any attributes MAY be present, but will be ignored if the subject_ fields are used.</p>	<p>Certificate Signing Request</p> <p>(Base-64 encoded with or without the</p> <p>-----BEGIN xxxxx-----</p> <p>and</p> <p>-----END xxxxx-----</p> <p>header and footer)</p>

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
			Signature Algorithm: md5WithRSAEncryption (PKCS#1)	
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.

2.1.3 AuthData type.

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

2.1.4 KUTemplate type

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

2.1.5 KeyUsage type

Name	Description
getCode()	Get internal identifier of the key usage

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

2.1.6 ExtKeyUsage type

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

2.1.7 Return value – 'status code' of operation

Status code	Possible Value(s)
If 'status code' < 0	<ul style="list-style-type: none"> - 2 = The 'Access code' 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! - 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 - 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.

2.2 Function for Checking if Certificate is Available.

Integer `getCollectStatus (AuthData authData, Integer orderNumber)`

2.2.1 Arguments

Variable Name	Type	Allowed values	Description
authData	AuthData		Authentication data for access. See description in the section 2.1.3 AuthData Type .
orderNumber	Integer	Any order number previously returned to your account.	This is the order number previously returned by function enroll.

2.2.2 Return value – status of certificate availability

Value	Description
Status Code	1 = Certificate available 0 = Certificate being processed by Comodo -1 = The 'Order number' argument is invalid. -2 = The certificate with 'Order number' not found. -14 = An unknown error occurred! -20 = CSR rejected - 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 desired action

2.3 Function for Collecting Enrolled Client Certificate.

SMIMECollectResponse `collect (AuthData authData, Integer orderNumber)`

2.3.1 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 2.1.3 AuthData Type .

2.3.2 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 Comodo -1 = The 'Order number' argument is invalid. -2 = The certificate with 'Order number' not found. -20 = Certificate rejected -14 = An unknown error occurred! -16 = Permission denied! -20 = The certificate request has been rejected! -21 = The certificate has been revoked! -22 = Still awaiting payment! -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

SMIMECollectResponse	Possible value(s)
	-120 = Customer configuration is not allowed the desired action
String certificate	If status code = 1, then - certificate in Base-64 if succeed, null otherwise.

2.4 Function for Client Certificate Revocation

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

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

2.4.1 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		Authentication data. See description in the section 2.1.3 AuthData Type .

2.4.2 Return value – Status code

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

Status code	Possible Value(s)
	-16 = Permission denied! -20 = The certificate request has already been Rejected! -21 = The certificate has already been Revoked! -26 = The certificate is currently being Issued! - 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 desired action

2.5 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)

2.5.1 Arguments

Variable Name	Type	Max. Length	Description
authData	AuthData		Authentication data. See description in the section 2.1.3 AuthData Type .

2.5.2 Return value – List of KUTemplate

Refer to section [2.1.4 KUTemplate types](#) for details.

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

String getWebServiceInfo()