

AusCERT CA

Certificate Services Manager

SSL Web Service API
Version 1.3



AusCERT

Table of Contents

1 Introduction.....	4
2 Remote Functions.....	4
2.1 Function for SSL Certificate Renewal.....	4
2.1.1 Arguments.....	4
2.1.2 Return value – 'status code' of operation.....	4
2.2 Function for Collecting Renewed SSL Certificate.....	4
2.2.1 Arguments.....	4
2.2.2 Return value – SSLRenewResponse.....	5
2.3 Function for SSL Certificate Enrollment.....	5
2.3.1 Arguments.....	6
2.3.1.1 AuthData type.....	7
2.3.1.2 Server Type.....	7
2.3.2 Return value – 'status code' of operation.....	9
2.4 Function for Checking if Certificate is Available.....	10
2.4.1 Arguments.....	10
2.4.2 Return value – status of certificate availability.....	10
2.5 Function for Collecting Enrolled SSL Certificate.....	11
2.5.1 Arguments.....	11
2.5.2 Return value – SSLCollectResponse.....	11
2.5.3 SSL type.....	12
2.6 Function for SSL Certificate Revocation.....	12
2.6.1 Arguments.....	12
2.6.2 Return value – 'status code' of operation.....	13
2.7 Function for loading list of available certificate types for customer.....	13
2.7.1 Arguments.....	13

2.7.2 Return value.....13

2.7.2.1 CustomerCertType – type for saving information about available customer certificate type.....14

2.8 Utility Function for Getting Short Information about Web Service (name, version, etc.).....14

1 Introduction

Name : EPKIManagerSSLService

Service EPR : <http://csm-host/ws/EPKIManagerSSL>

View WSDL : <http://csm-host/ws/EPKIManagerSSL?wsdl>

Service Description : The Service allows the Administrator to renew and collect renewed SSL certificates, request, collect, and revoke SSL certificates.

2 Remote Functions

2.1 Function for SSL Certificate Renewal

int renew(String renewId)

2.1.1 Arguments

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

2.1.2 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.

2.2 Function for Collecting Renewed SSL Certificate

SSLRenewResponse collectRenewed(String renewId, int formatType)

2.2.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
renewId	String	20		Given by CSM in notification letter when SSL certificate

				was issued.
formatType	int	1	0 = X509 PEM Bundle; 1 = X509 PEM Certificate only; 2 = X509 PEM Intermediate certificate only; 3 = PKCS#7 PEM Bundle; 4 = PKCS#7 DER Bundle.	Format of SSL to be returned.

2.2.2 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, <i>null</i> otherwise.

2.3 Function 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)

2.3.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 2.3.1.1 AuthData Type .
orgId	Integer			Organization identifier. Can be obtained from Admin UI – Organization properties “SSL Cert” tab.
secretKey	String	20		Secret Key for SSL is setting in Client Admin UI 'Organization' properties, tab 'SSL Certificates'.
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 = rsaEncryption (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 (PKCS#1)</p>	<p>Certificate Signing Request (Base-64 encoded with or without the</p> <p>-----BEGIN xxxxx-----</p> <p>and</p> <p>-----END xxxxx-----</p> <p>header and footer)</p>
phrase	String	64		Pass phrase for revocation.
subjAltNames	String		Subject Alternative Names splitted with ",".	List of Subject Alternative Names.
certType	CustomerCertificateType			Certificate types available for the ordering customer.

				See description in section 2.7.2 for more details.
numberServers	Integer			Number of servers.
serverType	Integer			Server type of the SSL certificate. See description below in section 2.3.1.2 Server Type .
term	Integer		Term in years.	Term of the SSL certificate.
comments	String	256		The message that will be attached to the certificate.

2.3.1.1 AuthData type

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

2.3.1.2 Server Type

Server Type	Description
1	AOL
2	Apache/ModSSL
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 (Javasoftware / 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
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

2.3.2 Return value – 'status code' of operation

Status code	Possible Value(s)
If 'status code' < 0	<p>-3 = The 'User name' argument is invalid.</p> <p>-7 = Country is not a valid ISO-3166 country!</p> <p>-9 = The CSR is not valid Base-64 data!</p> <p>-10 = The CSR cannot be decoded!</p> <p>-11 = The CSR uses an unsupported algorithm!</p> <p>-12 = The CSR has an invalid signature!</p> <p>-13 = The CSR uses an unsupported key size!</p> <p>-14 = An unknown error occurred!</p> <p>-16 = Permission denied!</p> <p>-31 = The email is not a valid email.</p> <p>-32 = The two phrase should be the same!</p> <p>-33 = The Comodo certificate type is invalid!</p> <p>-34 = The secret key is invalid!</p> <p>-35 = The server type is invalid!</p> <p>-36 = The term is invalid for customer type!</p> <p>- 100 = Invalid authentication data for customer</p> <p>- 101 = Invalid authentication data for customer organization</p> <p>- 110 = Domain is not allowed for customer</p>

	- 111 = Domain is not allowed for customer organization - 120 = Customer configuration is not allowed the requested action
If 'status code' > 0	SSL identifier. It will be used for certificate collecting/revoking.

2.4 Function for Checking if Certificate is Available

Integer `getCollectStatus(AuthData data, Integer id)`

2.4.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 2.3.1.1 AuthData Type .
id	Integer		Any SSL identifier previously returned to your account.	This is the SSL identifier previously returned by function enroll .

2.4.2 Return value – status of certificate availability

Possible Value(s)
1 = Certificate available 0 = Certificate being processed by Comodo -14 = An unknown error occurred! -16 = Permission denied! - 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

2.5 Function for Collecting Enrolled SSL Certificate

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

2.5.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 2.3.1.1 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 Intermediate certificate only; 3 = PKCS#7 PEM Bundle; 4 = PKCS#7 DER Bundle.	Allowed formats for downloading of SSL.

2.5.2 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()	1 = Certificate Available 2 = Certificates Attached 0 = Being processed by Comodo -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!

	<ul style="list-style-type: none"> - 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
SSL getSSL()	If status code = 2, then the special object with the certificate in Base-64 if succeed, <i>null</i> otherwise. See section 2.5.3. 'SSL' type .

2.5.3 SSL type

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

2.6 Function for SSL Certificate Revocation

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

2.6.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 2.3.1.1 AuthData Type .
id	Integer		Any SSL identifier previously returned to your account.	This is the SSL identifier previously returned by function enroll .
reason	String	256		Revocation reason for audit logging. Empty String allowed.

2.6.2 Return value – 'status code' of operation

Possible Value(s)
0 = Successful
-14 = An unknown error occurred!
-16 = Permission denied!
- 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

2.7 Function for loading list of available certificate types for customer.

CustomerCertTypeResponse `getCustomerCertTypes(AuthData data)`

2.7.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data for access. See section 2.3.1.1 AuthData Type .

2.7.2 Return value.

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

Field Name	Possible Value(s)
CustomerCertType[] getTypes()	If customer does not have available certificate type – result array will be empty.
int getStatusCode()	0 = Successful -14 = An unknown error occurred! -16 = Permission denied!

2.7.2.1 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”
int[] getTerms	List of available terms for this customer certificate type.

**2.8 Utility Function for Getting Short Information about Web Service (name, version, etc.).
String getWebServiceInfo()**