InCommon®

InCommon Certificate Manager

Device Certificate Enroll API

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

Table of Contents

1 Introduction

Name	:	EPKIManagerDeviceCert
Service EPR	:	http://cert-manager.com/ws/EPKIManagerDevice OR http://cert-manager.com/private/ws/EPKIManagerDevice
View WSDL	:	http://cert-manager.com/ws/EPKIManagerDevice?wsdl OR http://cert-manager.com/private/ws/EPKIManagerDevice?wsdl
Service Description	:	The Service allows the Administrator to request, collect and revoke Device 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 Device Certificate 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/EPKIManagerDevice

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 Device Certificate Enroll 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/EPKIManagerDevice

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 Device Certificate 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 Device Certificate Revocation

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

3.1.1 Arguments

Variable Name	Type	Max. Length	Description
authData	AuthData	128	Authentication data. See description in the section 3.4.1.1AuthData type
orderNumber	Integer		This is the order number previously returned by function enroll.
reason	String	256	Revocation reason for audit logging. Empty String is also allowed.

3.1.2 Return value - Status code

Status code	Type	Possible value(s)
Status Code	Integer	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; -16 = Permission denied; -20 = The certificate request has been rejected; -21 = The certificate has been revoked; -22 = Still awaiting payment; -24 = Auth data argument is invalid; -25 = DCV not performed; -26 = Organization has incorrect OV status; -31 = The email is not a valid email; -100 = Invalid auth data; -101 = Invalid organization auth data; -105 = Person not found; -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

3.2 Function for Device Certificate Revocation by Serial Number

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

3.2.1 Arguments

Variable Name	Type	Max. Length (chars)	Description
authData	AuthData		Authentication data. See description in the section 3.4.1.1AuthData type
serialNumber	String	64	Certificate serial number.
reason	String	256	Revocation reason for audit logging. Empty String allowed.

3.2.2 Return Value – Status Code

Status code	Possible Value(s)
If ' status code' < 0	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; -16 = Permission denied; -20 = The certificate request has been rejected; -21 = The certificate has been revoked; -22 = Still awaiting payment; -24 = Auth data argument is invalid; -25 = DCV not performed; -26 = Organization has incorrect OV status; -31 = The email is not a valid email; -100 = Invalid auth data; -101 = Invalid organization auth data;

	-105 = Person not found; -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

3.3 Function for Collecting Enrolled Device Certificate

DeviceCertCollectResponse collect(AuthData authData, Integer orderNumber, Integer format)

Variable Name	Type	Description
authData	AuthData	Authentication data. See description in the section 3.4.1.1AuthData type
orderNumber	Integer	Certificate order number.
format	Integer	Allowed formats for downloading of Device Certificate. Allowed Values: 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.

3.3.1 Return Value – DeviceCertCollectResponse

Method Name	Description
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 Device Certificate Enrollment

Integer enroll (AuthData authData, String commonName, Integer orgId, Integer term, String csr, Integer certTypeId, DeviceCertEnrollOptionalFieldsDto optionalFields)

3.4.1 Arguments

Variable Name	Type	Max. Length (chars)	Allowed Values	Description
authData	AuthData			Authentication data. See description in the section 3.4.1.1AuthData type
commonName	String	64		Name to enroll certificate for. This value will be set for the subject 'CN'.
orgId	Integer	128		Organization identifier. Can be obtained from Admin UI > Organization properties > 'General' tab.
term	Integer			Term of the Device certificate in years.

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)
certTypeId	Integer			Identifier for Device certificate type. When not specified, default type is used.
optionalFields	DeviceCertEnrollOptionalFieldsDto			Optional fields for the Device certificate. Optional parameter

3.4.1.1 AuthData type

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

3.4.1.2 Return Value – Status Code

Status code	Possible Value(s)
If ' status code' < 0	0 = SUCCESSFUL; -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; -24 = Auth data argument is invalid; -25 = DCV not performed; -26 = Organization has incorrect OV status; -31 = The email is not a valid email; -32 = The passphrase is empty; -33 = The certificate type is invalid; -34 = The secret key is invalid; -35 = The Server type is invalid; -36 = The term is invalid for certificate type; -37 = The cert type name is invalid; -38 = Unable to enroll device certificate as some required fields are empty; -39 = The cert type ID is invalid; -100 = Invalid auth data; -101 = The 'Access code' argument is invalid;

	-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); -116 = Can't change person properties; -120 = Customer configuration is not allowed the desired action.
If 'status code' > 0	SSL identifier. It will be used for certificate collecting/revoking.

3.5 Function for Retrieving All Ids of KU/EKU for Device Cert Enroll Process

DeviceCertTypeIdsResponse getDeviceCertTypeIds (AuthData authData)

3.5.1 Arguments

Variable Name	Type	Description
authData	AuthData	Authentication data. See description in the section 3.4.1.1AuthData type

3.5.2 Return value - DeviceCertTypeIdsResponse

Status code	Possible Value(s)
If ' status code' < 0	0 = SUCCESSFUL; -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; -24 = Auth data argument is invalid; -25 = DCV not performed; -26 = Organization has incorrect OV status; -31 = The email is not a valid email; -32 = The passphrase is empty; -33 = The certificate type is invalid; -34 = The secret key is invalid; -35 = The Server type is invalid; -36 = The term is invalid for certificate type; -37 = The cert type name is invalid; -38 = Unable to enroll device certificate as some required fields are empty; -39 = The cert type ID is invalid; -100 = Invalid auth data; -101 = The 'Access code' argument is invalid; -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);

	-116 = Can't change person properties; -120 = Customer configuration is not allowed the desired action.
If 'status code' > 0	List of all retrieving Ids will be used for certificate enroll.

3.6 Function for Retrieving Certificate Type Information by its ID

DeviceCertTypeResponse getDeviceCertType (AuthData authData, Integer certTypeId)

Variable Name	Type	Description
authData	AuthData	Authentication data. See description in the section 3.4.1.1AuthData type
certTypeId	Integer	Identifier for Device certificate type. When not specified, default type is used.

3.6.1 Return value - DeviceCertTypeResponse

Status code	Possible Value(s)
If ' status code' < 0	0 = SUCCESSFUL; -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; -24 = Auth data argument is invalid; -25 = DCV not performed;

	-26 = Organization has incorrect OV status; -31 = The email is not a valid email; -32 = The passphrase is empty; -33 = The certificate type is invalid; -34 = The secret key is invalid; -35 = The Server type is invalid; -36 = The term is invalid for certificate type; -37 = The cert type name is invalid; -38 = Unable to enroll device certificate as some required fields are empty; -39 = The cert type ID is invalid; -100 = Invalid auth data; -101 = The 'Access code' argument is invalid; -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); -116 = Can't change person properties; -120 = Customer configuration is not allowed the desired action.

3.7 Function for Retrieving Custom Fields for Customer

getDeviceCustomFields (String customerLoginUri, String uriExtension)

Variable Name	Type	Description
customerLoginUri	String	Customer login URI.
uriExtension	String	URI extension.

3.7.1 Return value - DeviceCertCustomFieldResponse

Status code	Possible Value(s)
If ' status code' < 0	0 = SUCCESSFUL; -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; -24 = Auth data argument is invalid; -25 = DCV not performed; -26 = Organization has incorrect OV status; -31 = The email is not a valid email; -32 = The passphrase is empty; -33 = The certificate type is invalid; -34 = The secret key is invalid; -35 = The Server type is invalid; -36 = The term is invalid for certificate type; -37 = The cert type name is invalid; -38 = Unable to enroll device certificate as some required fields are empty;

	-39 = The cert type ID is invalid; -100 = Invalid auth data; -101 = The 'Access code' argument is invalid; -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); -116 = Can't change person properties; -120 = Customer configuration is not allowed the desired action.
If 'status code' > 0	List of custom fields will be used for certificate enroll.

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

String getWebServiceInfo()