Introduction

This guide shows how operators of OpenPEPPOL infrastructure services (Access Points and Service Metadata Publishers) can obtain a digital certificate from the OpenPEPPOL CAs.

As a prerequisite it is assumed that the operator has already filled out the OpenPEPPOL Transport Infrastructure Agreement Annex 1, submitted it and has been contacted with a one-time passcode to begin the enrollment process. The passcode will be delivered via phone to the technical contact person stated in section 4.6 of the Annex 1 submitted, when the application has been approved.

Generate a key pair and CSR file

The first step consists of creating a 2048 bit RSA key pair locally that contains a private and public key. Thus, the keys are generated locally and only the public key is sent to the CA for inclusion in a certificate.

Key generation is typically performed with tools on the server where the certificate is needed for example using Java keytool, OpenSSL or similar.

As an example, the following OpenSSL command will generate a pair of keys (a private and a public key) together with a certificate signing request (CSR):

```
openssl req -out my-certificate.csr -new -newkey rsa:2048 -nodes -keyout my-private.key
```

Note that the text fields (Country, State, Organisation, etc.) in the CSR file will be ignored – only the part containing the public key will be used.

Further guidance for using OpenSSL can be found at:

- https://www.digitalocean.com/community/tutorials/openssl-essentials-working-with-ssl-certificates-private-keys-and-csrs
- https://www.sslshopper.com/article-most-common-openssl-commands.html

An online CSR file validator tool can be found at: https://ssltools.websecurity.symantec.com/checker/

Note: the private key must be protected well, since compromise will allow an attacker to impersonate the certificate holder within the OpenPEPPOL infrastructure. If the private key is stored on disc it shall be encrypted under a strong password and the file shall be under strict access control; use of cryptographic hardware is encouraged where possible.

Access the relevant Certificate Authority

To enroll for the certificate, go to the relevant web site for the OpenPEPPOL CAs:

For **PILOT** certificates:

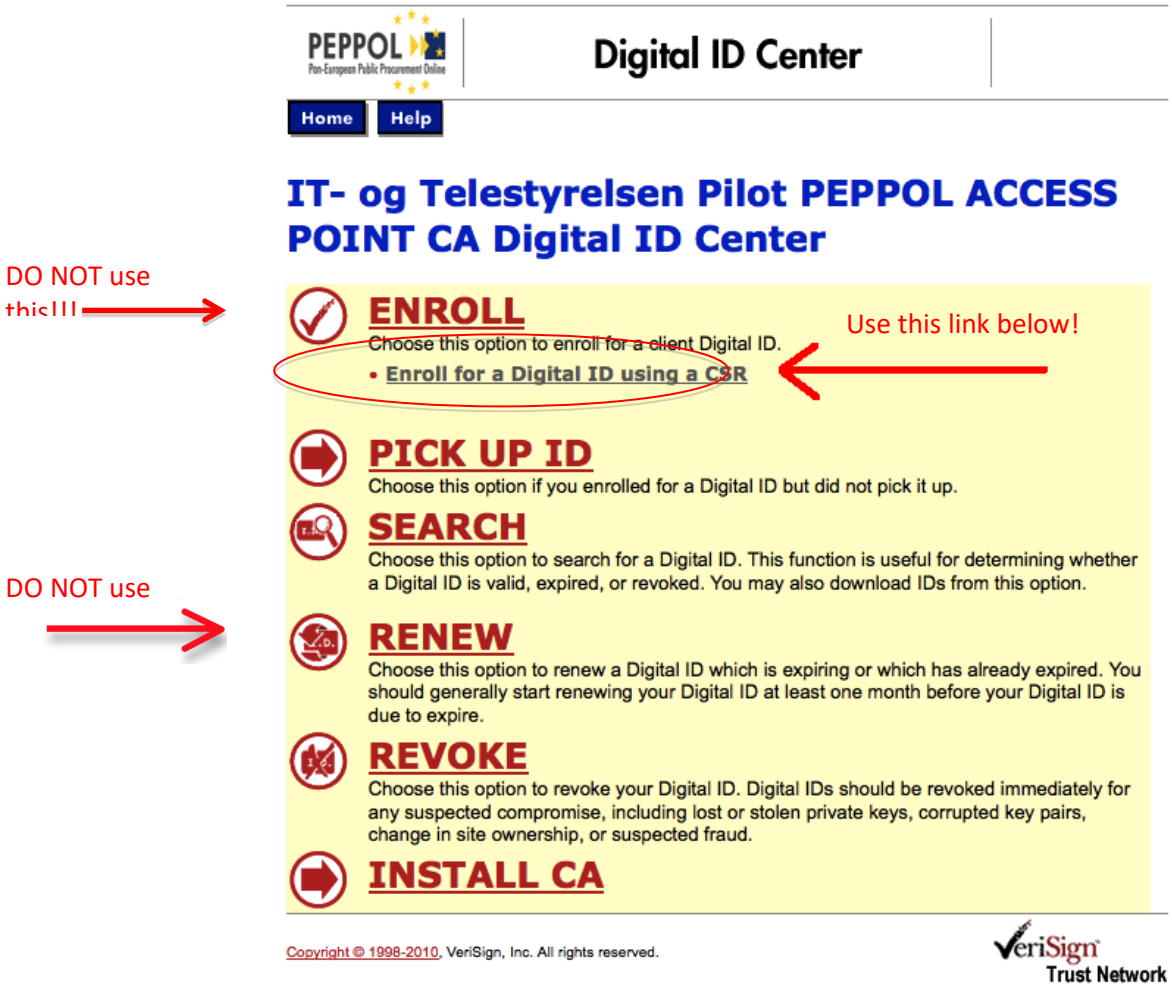
- Access Point CA:
  https://pilotonsite.verisign.com/services/DigitaliseringsstyrelsenPilotOpenPEPPOLACCESSPOINTCA/digitalidCenter.htm
- Service Metadata Publisher CA:
  https://pilotonsite.verisign.com/services/DigitaliseringsstyrelsenPilotOpenPEPPOLSERVICEMETADATAPUBLISHERCA/digitalidCenter.htm

For **PRODUCTION** certificates:

- Access Point CA:
  https://onsite.verisign.com/services/DigitaliseringsstyrelsenOpenPEPPOLACCESSPOINTCA/digitalidCenter.htm
- Service Metadata Publisher CA:
  https://onsite.verisign.com/services/DigitaliseringsstyrelsenOpenPEPPOLSERVICEMETADATAPUBLISHERCA/digitalidCenter.htm

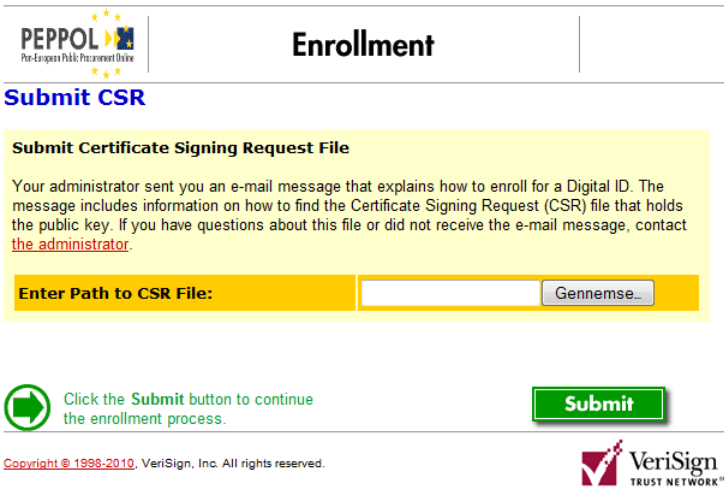
Complete the enrollment process

Below is shown the enrollment process for the Access Point CA; the other CAs are similar (except for the start URL). The first page looks like this:



Step 1: Start page of the Access Point CA

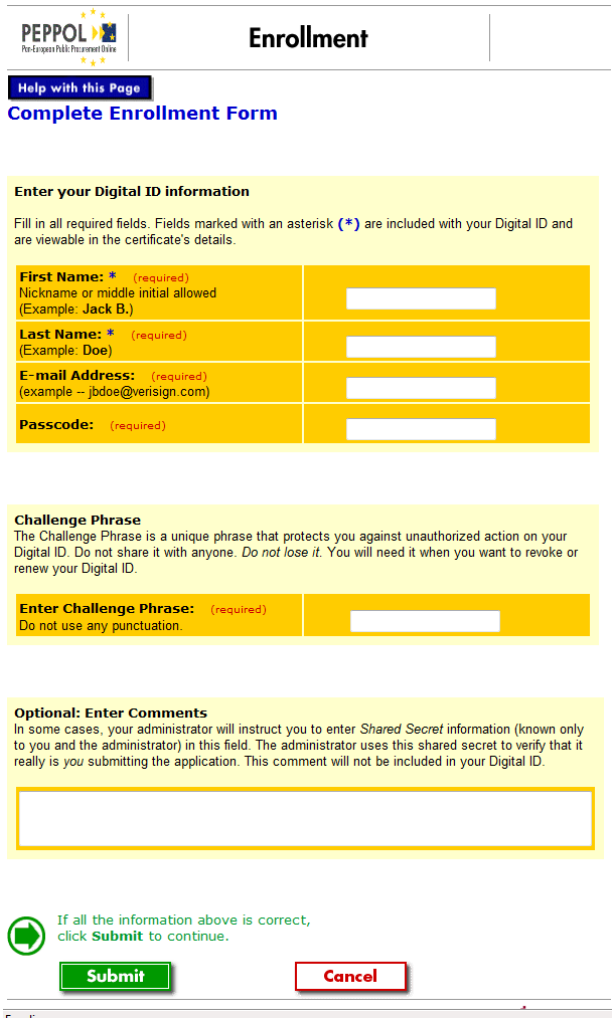
Click on the link titled "**Enroll for a Digital ID using a CSR**" (marked with the red arrow in the figure above) and the following screen appears:



Step 2: Submit CSR file

Enter the path for the previously generated .CSR file and press the "Submit" button to upload it.

The next page will look like this:



Step 3: Fill-out enrollment form

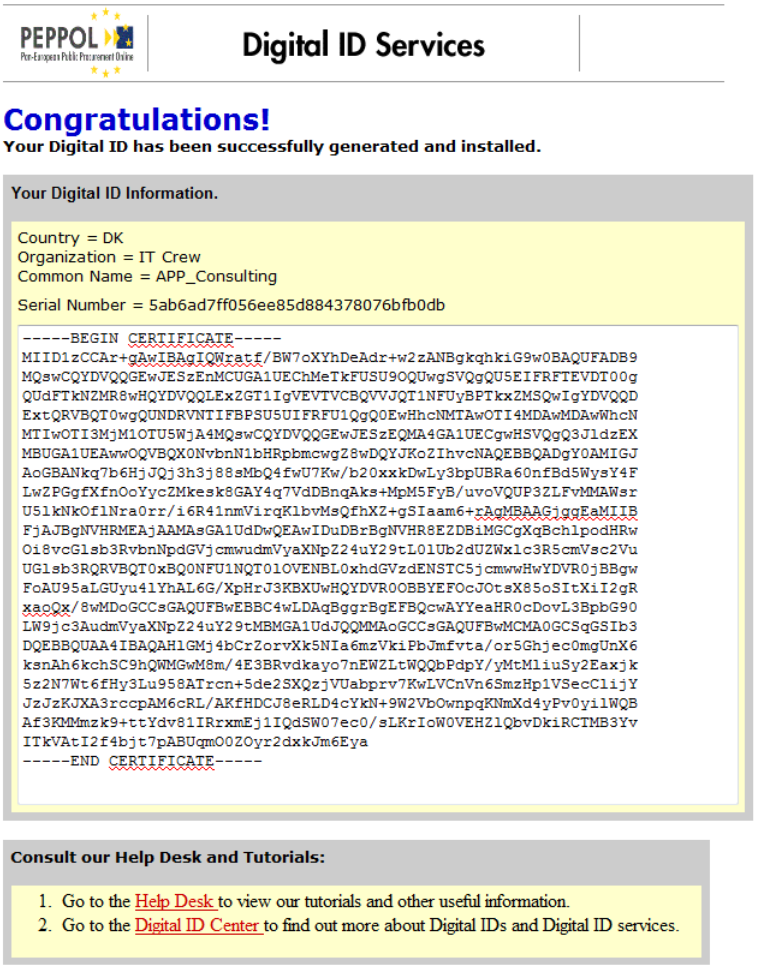
Fill out the above form in the following way:

- Enter in the “First Name” field the first name that was specified in section 4.6 in Annex 1 of the Transport Infrastructure Agreement.
- Enter in the “Last Name” field the last name that was specified in in section 4.6 in Annex 1 of the Transport Infrastructure Agreement.
- Enter in the “E-mail Address” field the e-mail address that was specified in section 4.6 in Annex 1 of the Transport Infrastructure Agreement. Note: no emails will be sent to this address, but it is important that the entered e-mail address exactly matches the value given in Annex 1, under “technical contact person”.

- Enter in the “Passcode” field the passcode (number) received on the phone (via call or SMS) from the CA administrator. **Note: the Passcodes are specific to a specific CA, so be sure to use the correct Passcodes with the corresponding CAs.**
- Enter in the “Enter Challenge Phrase” field, a challenge phrase (chosen by yourself) that is used e.g. for revoking the certificate. Make sure it is recorded somewhere appropriate where it can be quickly found.

Then press the “Submit” button.

If the enrollment is successful, the following page will appear:


PEPPOL Pan-European Public Procurement Online

Digital ID Services

Congratulations!

Your Digital ID has been successfully generated and installed.

Your Digital ID Information.

Country = DK
Organization = IT Crew
Common Name = APP_Consulting

Serial Number = 5ab6ad7ff056ee85d884378076bfb0db

```
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIQWratf/BW7oXYhDeAdr+w2zANBgkqhkiG9w0BAQUFADB9
MQswCQYDVQQGEwJESzEnMCUGA1UEChMeTkFUSU9OQUwgSVQgQU5EIFRFTEVDT00g
QUdFTkNZMR8wHQYDVQQLExZGT1IgVEVTVCBQVVJQT1NFUyBPTkxZMSQwIgYDVQQD
ExtQRVBQT0wgQUNDRVNTIFBPSU5UIFRFU1QgQ0EwHhcNMTAwOTI4MDAwMDAwWhcN
MTIwOTI3MjM1OTU5WjA4MQswCQYDVQQGEwJESzEQMA4GA1UECgwHSVQgQ3JldzEX
MBUGA1UEAwwOQVBQX0NvbnN1bHRpbmcwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBANkq7b6HjJQj3h3j88sMbQ4fwU7Kw/b20xxkDwLy3bpUBRa60nfBd5WysY4F
LwZPGgfXfnOoYycZMkesk8GAY4q7VdDBnqAks+MpM5FyB/uvoVQUP3ZLFvMMAWsr
U5lkNkOflNra0rr/i6R41nmVirqKlbvMsQfhXZ+gSIaam6+rAgMBAAGjggEaMIIB
FjAJBgNVHRMEAjAAMAsGA1UdDwQEAwIDuDBrBgNVHR8EZDBiMGCgXqBchlpodHRw
Oi8vcGlsb3RvbnNpdGVjcmwudmVyaXNpZ24uY29tL0lUb2dUZWxlc3R5cmVsc2Vu
UGlsb3RQRVBQT0xBQ0NFU1NQT0lOVENBL0xhdGVzdENSTC5jcmwwHwYDVR0jBBgw
FoAU95aLGUyu41YhAL6G/XpHrJ3KBXUwHQYDVR0OBBYEFOcJOtsX85oSItXiI2gR
xaoQx/8wMDoGCCsGAQUFBwEBBC4wLDAqBggrBgEFBQcwAYYeaHR0cDovL3BpbG90
LW9jc3AudmVyaXNpZ24uY29tMBMGA1UdJQQMMAoGCCsGAQUFBwMCMA0GCSqGSIb3
DQEBBQUAA4IBAQAHlGMj4bCrZorvXk5NIa6mzVkiPbJmfvta/or5Ghjec0mgUnX6
ksnAh6kchSC9hQWMGwM8m/4E3BRvdkayo7nEWZLtWQQbPdpY/yMtMliuSy2Eaxjk
5z2N7Wt6fHy3Lu958ATrcn+5de2SXQzjVUabprv7KwLVCnVn6SmzHp1VSecClijY
JzJzKJXA3rccpAM6cRL/AKfHDCJ8eRLD4cYkN+9W2VbOwnpqKNmXd4yPv0yilWQB
Af3KMMmzk9+ttYdv81IRrxmEj1IQdSW07ec0/sLKrIoW0VEHZlQbvDkiRCTMB3Yv
ITkVAtI2f4bjt7pABUqmO0ZOyr2dxkJm6Eya
-----END CERTIFICATE-----
```

Consult our Help Desk and Tutorials:

1. Go to the Help Desk to view our tutorials and other useful information.
2. Go to the Digital ID Center to find out more about Digital IDs and Digital ID services.

Now select the text starting with “-----BEGIN CERTIFICATE-----” and ending with “----END CERTIFICATE-----“ and copy to a text editor. Save the file as a file with “.CER” extension.

On a Windows PC the content of the certificate can be examined by simply double-clicking on the .cer file.

Install the certificate

Once the certificate has been stored, it must be installed on the server(s). Since this step is system-specific it will not be described in detail.

As a specific example, a guide for the Oxalis system can be found here:
https://github.com/difi/oxalis/blob/master/doc/keystore.md

In many situations, the CA certificates are needed to install the PEPPOL certificate in order to build a full trust chain. Note that the "Install CA" certificate link on the enrollment pages does not provide a full chain. Files with the full chain can be requested from the below contact.

Updating the SML with a new SMP certificate

If a new SMP certificate is issued for replacing an existing SMP certificate, the following procedure must be followed to update the existing SML registrations currently linked to the old SMP certificate:

1. In the SML database, the existing registrations are linked to the old certificate and these registrations need to be updated when changing certificate in order to support updates or removals of old SML entries with the new certificate.
2. You need to send details for the old and new certificate to SUPPORT CEF-EDELIVERY-SUPPORT@ec.europa.eu and request the update for a specific time.
3. The information you need to provide is CN, O, C and serial number from the old and the new SMP certificate.

Example:

Old certificate SMP certs:

- Owner: CN=SMP_2000000099, O=Test Corporation, C=FI
- Serial number: 598fd3b554462bec874c213ffdcf3bbc

New certificate SMP certs:

- Owner: CN=SMP_2000000123, O=Test Corporation, C=FI
- Serial number: 5a48fe06e6b6768b5f22d3a96fb1a7eb

How to get help

Please contact:

Thomas Gundel

E-mail: tg@itcrew.dk

Other info

The OpenPEPPOL certificates will expire two years from the issuance date. It is the responsibility of the operator of OpenPEPPOL Aps and SMPs to renew their certificates before they expire. An expired certificate may cause transactions to be rejected by other OpenPEPPOL parties and thus lead to errors and downtime. It is advised to create automatic calendar reminders to ensure renewal in due time or establish some other process that ensures renewal.