1 Introduction

This guide shows how operators of OpenPEPPOL infrastructure services (Access Points, Service Metadata Publishers and Security Token Services) 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 the certificate application form when the application has been approved.

2 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 if cryptographic hardware is encouraged where possible.

3 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

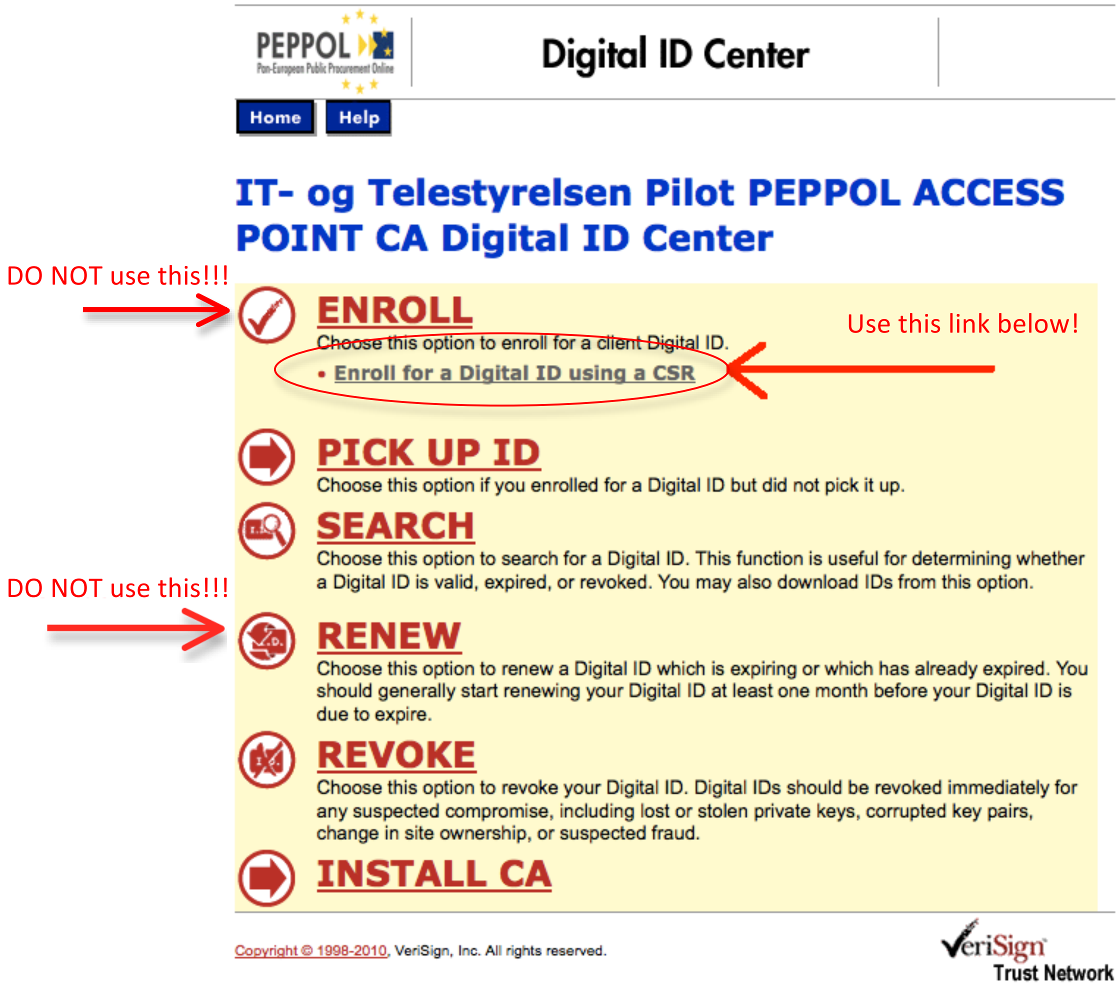
For **PRODUCTION** certificates:

- Access Point CA:
https://onsite.verisign.com/services/DigitaliseringsstyrelsenOpenPEPPOLACCESSPOINTCA/digitalidCenter.htm

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

4 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:



Digital ID Center

Home Help

IT- og Telestyrelsen Pilot PEPPOL ACCESS POINT CA Digital ID Center

DO NOT use this!!!

ENROLL

Choose this option to enroll for a client Digital ID.

- Enroll for a Digital ID using a CSR

Use this link below!

PICK UP ID

Choose this option if you enrolled for a Digital ID but did not pick it up.

SEARCH

Choose this option to search for a Digital ID. This function is useful for determining whether a Digital ID is valid, expired, or revoked. You may also download IDs from this option.

DO NOT use this!!!

RENEW

Choose this option to renew a Digital ID which is expiring or which has already expired. You should generally start renewing your Digital ID at least one month before your Digital ID is due to expire.

REVOKE

Choose this option to revoke your Digital ID. Digital IDs should be revoked immediately for any suspected compromise, including lost or stolen private keys, corrupted key pairs, change in site ownership, or suspected fraud.

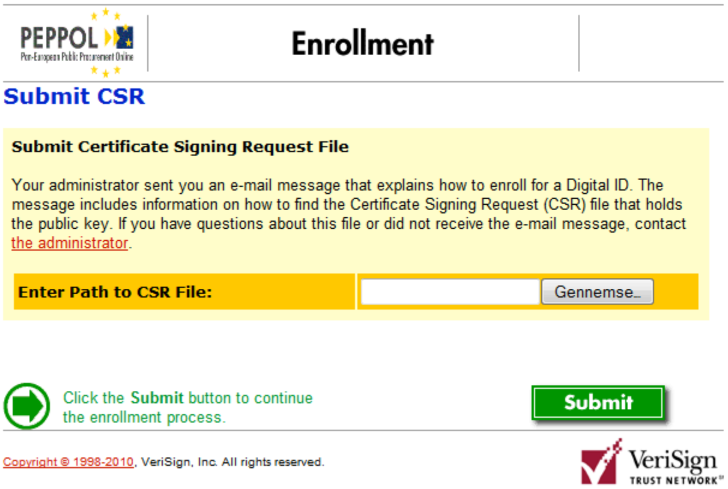
INSTALL CA

Copyright © 1998-2010, VeriSign, Inc. All rights reserved.

VeriSign Trust Network

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:



Submit CSR

Submit Certificate Signing Request File

Your administrator sent you an e-mail message that explains how to enroll for a Digital ID. The message includes information on how to find the Certificate Signing Request (CSR) file that holds the public key. If you have questions about this file or did not receive the e-mail message, contact the administrator.

Enter Path to CSR File:

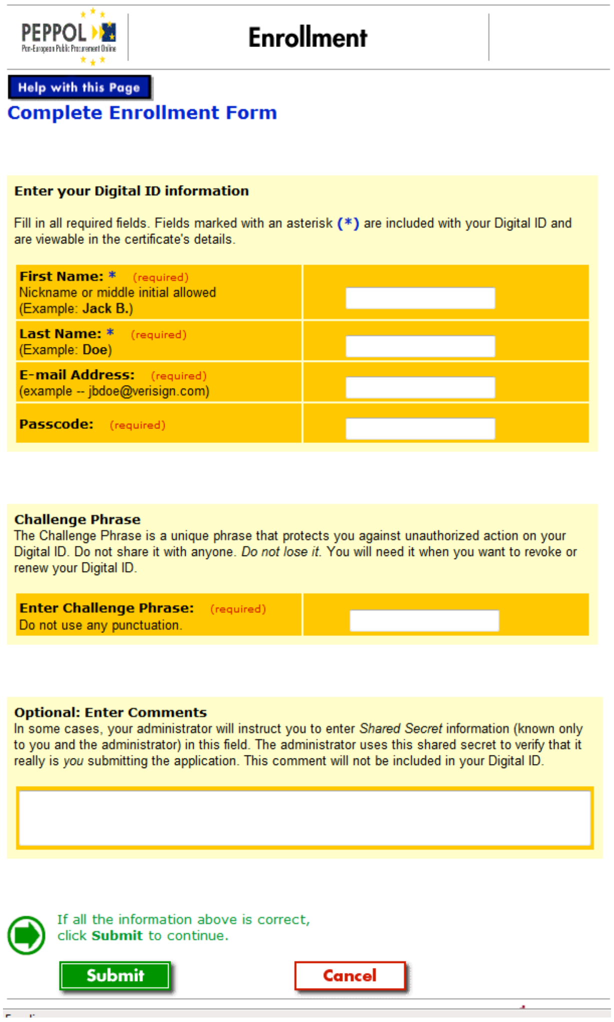
Click the **Submit** button to continue the enrollment process.

Copyright © 1998-2010, VeriSign, Inc. All rights reserved.

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:



Enrollment

Complete Enrollment Form

Enter your Digital ID information

Fill in all required fields. Fields marked with an asterisk **(*)** are included with your Digital ID and are viewable in the certificate's details.

First Name: * (required) Nickname or middle initial allowed (Example: **Jack B.**)	
Last Name: * (required) (Example: **Doe**)	
E-mail Address: (required) (example -- jbdoe@verisign.com)	
Passcode: (required)	

Challenge Phrase
The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. *Do not lose it.* You will need it when you want to revoke or renew your Digital ID.

Enter Challenge Phrase: (required) Do not use any punctuation.	

Optional: Enter Comments
In some cases, your administrator will instruct you to enter *Shared Secret* information (known only to you and the administrator) in this field. The administrator uses this shared secret to verify that it really is *you* submitting the application. This comment will not be included in your Digital ID.

If all the information above is correct, click **Submit** to continue.

Step 3: Fill-out enrollment form

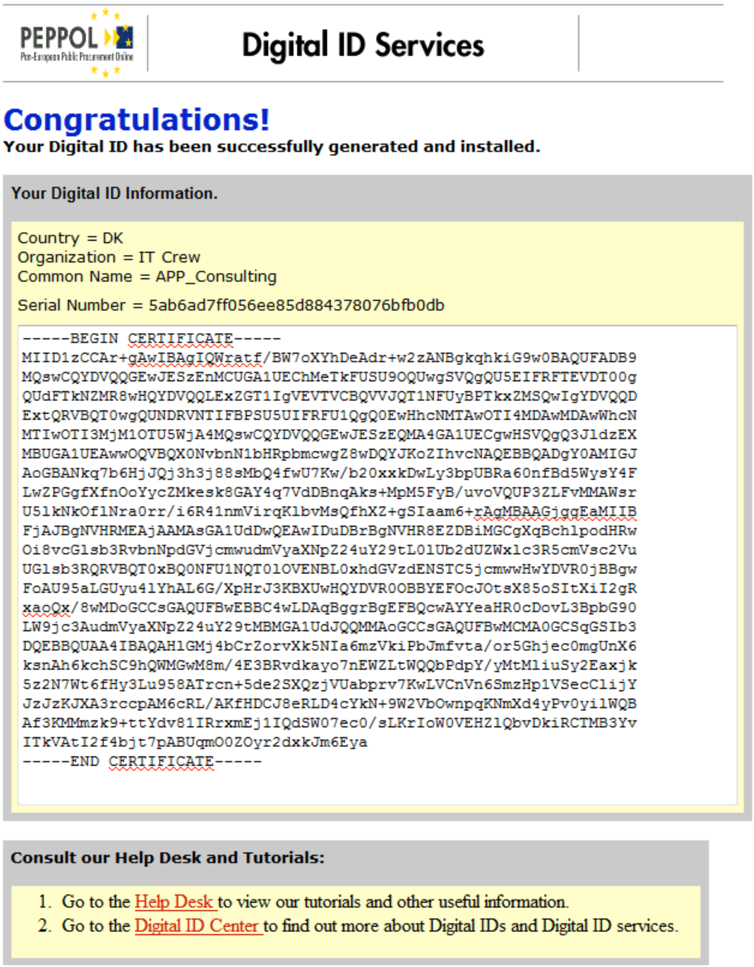
Fill out the above form in the following way:

- Enter in the “First Name” field the first name that was specified in the certificate application form.
- Enter in the “Last Name” field the last name that was specified in the certificate application form.
- Enter in the “E-mail Address” field the e-mail address that was specified in the certificate application form. 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 the certificate application form 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 PIN codes are specific to a specific CA, so be sure to use the correct PINs with the corresponding CA.**

- 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:



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
MTIwOTI3MjM1OTU5WjA4MQswCQYDVQQGEwJESzEQMA4GA1UECgwHSVQgQ3J1dzEX
MBUGA1UEAwwOQVBQX0NvbnN1bHRpbmcwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBANkq7b6HjJQj3h3j88sMbQ4fwU7Kw/b20xxkDwLy3bpUBRa60nfBd5WysY4F
LwZPGgfXfnOoYycZMkesk8GAY4q7VdDBnqAks+MpM5FyB/uvoVQUP3ZLFvMMAWsr
U5lkNkOflNra0rr/i6R41nmVirqKlbvMsQfhXZ+gSIaam6+rAgMBAAGjggEaMIIB
FjAJBgNVHRMEAjAAMAsGA1UdDwQEAwIDuDBrBgNVHR8EZDBiMGCgXqBchlpodHRw
Oi8vcGlsb3RvbnNpdGVjcmwudmVyaXNpZ24uY29tL01Ub2dUZWxlc3R5cmVsc2Vu
UGlsb3RQRVBQT0xBQ0NFU1NQT01OVENBL0xhdGVzdENSTC5jcmwwHwYDVR0jBBgw
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.

5 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.

6 Updating SML with 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 serialnumber 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

7 How to get help

Please contact:

Sven Rostgaard Rasmussen

E-mail: svrra@digst.dk

Phone: +45 3392 8000

8 Other info

The OpenPEPPOL certificates will expire two years from the issuance date. It is the responsibility of the operator of OpenPEPPOL APs, SMPs and STSs 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.