

## 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://pilotsite.verisign.com/services/DigitaliseringsstyrelsenPilotOpenPEPPOLACCESSPOINTCA/digitalidCenter.htm>
- Service Metadata Publisher CA:  
<https://pilotsite.verisign.com/services/DigitaliseringsstyrelsenPilotOpenPEPPOLSERVICEMETADATAPUBLISHERCA/digitalidCenter.htm>

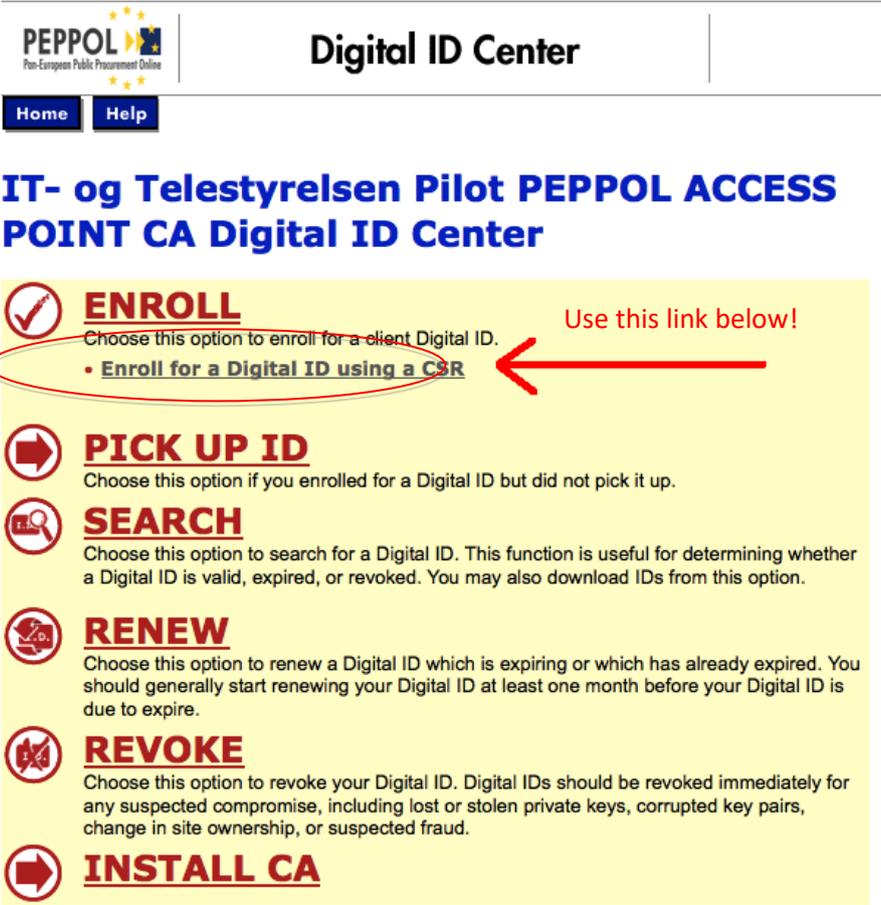
For **PRODUCTION** certificates:

- 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:



The screenshot shows the 'Digital ID Center' interface. At the top, there is a header with the PEPPOL logo and the text 'Digital ID Center'. Below the header are 'Home' and 'Help' buttons. The main heading is 'IT- og Telestyrelsen Pilot PEPPOL ACCESS POINT CA Digital ID Center'. A yellow box contains several options: 'ENROLL', 'PICK UP ID', 'SEARCH', 'RENEW', 'REVOKE', and 'INSTALL CA'. The 'ENROLL' option is circled in red, and a red arrow points to it from the text 'DO NOT use this!!!'. Another red arrow points to the sub-link 'Enroll for a Digital ID using a CSR' with the text 'Use this link below!'. A third red arrow points to the 'SEARCH' option with the text 'DO NOT use'. At the bottom of the page, there is a copyright notice and the VeriSign Trust Network logo.

DO NOT use this!!! →

Use this link below! →

DO NOT use →

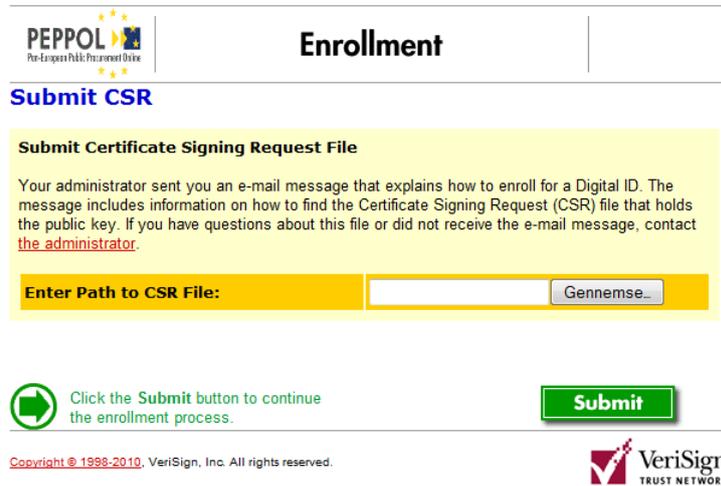
Copyright © 1998-2010, VeriSign, Inc. All rights reserved.

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:



The screenshot shows the PEPPOL Enrollment page. At the top left is the PEPPOL logo. The main heading is "Enrollment". Below it is a blue link "Submit CSR". A yellow box contains the text: "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." Below this is a form with a label "Enter Path to CSR File:", an input field, and a "Gennemse..." button. At the bottom left is a green arrow icon with the text "Click the Submit button to continue the enrollment process." At the bottom right is a green "Submit" button. The footer includes "Copyright © 1998-2010, VeriSign, Inc. All rights reserved." and the VeriSign Trust Network logo.

**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**

[Help with this Page](#)

**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.

<b>First Name:</b> * (required) <small>Nickname or middle initial allowed                      (Example: Jack B.)</small>	<input type="text"/>
<b>Last Name:</b> * (required) <small>(Example: Doe)</small>	<input type="text"/>
<b>E-mail Address:</b> (required) <small>(example -- jbdoe@verisign.com)</small>	<input type="text"/>
<b>Passcode:</b> (required)	<input type="text"/>

**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.

<b>Enter Challenge Phrase:</b> (required) <small>Do not use any punctuation.</small>	<input type="text"/>
---	----------------------

**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.

Submit
Cancel

**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”.





## 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](mailto: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](mailto: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.

