# Reference Implementation

**Project Acronym:** PEPPOL

**Grant Agreement number:** 224974

**Project Title:** Pan-European Public Procurement Online

## PEPPOL eSignature Infrastructure
## XKMS Responder Prototype Documentation
## Reference Implementation Library

**Revision: 1.0**


**Authors:**

Frank Schipplick (bremen online services)

Lars Thölken (bremen online services)




| Project co-funded by the European Commission within the ICT Policy Support Programme | | |
|---|---|---|
| Dissemination Level | | |
| P | Public | X |
| C | Confidential, only for members of the consortium and the Commission Services | |

# Revision History

| Revision | Date | Author | Organisation | Description |
|---|---|---|---|---|
| 1.0 | 20100430 | Lars Thölken | bos | First version (pending EC approval) |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

## Statement of copyright

# Contributors

## Organisations

bremen online services (main editor), Germany, http://www.bos-bremen.de

CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione[1]) , Italy, www.cnipa.gov.it

DIFI (Direktoratet for forvaltning og IKT[2]) , Norway, www.difi.no

DILA (Direction de l'Administration Légale et Administrative Of French Prime Minister Office), France

InfoCamere, Italy, www.infocamere.it

## Persons

Adriano Rossi, CNIPA

Ahmed Yacine, DILA

Alexander Funk, bos

Andreas Wall, bos

André Jens, bos

Daniel Eggert, bos

Edgar Thiel, bos

Frank Olthhoff, bos

Jon Olnes, DIFI

Lars Thölken, bos (editor)

Nils Büngener, bos

Piero Milani, InfoCamere



[1] From 29th December 2009, CNIPA will be renamed DigitPA (Legislative Decree 1st December 2009, n. 177)

[2] English: Agency for Public Management and eGovernment

# Table of Contents

# 1 Introduction

## 1.1 Objective

This document provides the documentation of the open source reference implementation PEPPOL XKMS responder. It is written for operators that use and host the reference implementation for themselves and need to maintain and administrate the component.

## 1.2 Scope

This documentation describes a prototype of the XKMS Responder, which is part of the eSignature Infrastucture. The eSignature validation model can be used in many interoperability settings. In the PEPPOL context, it provides eSignature validation for exchange of business documents where eSignatures are required from the legal or the organisational layer in the European Interoperability Framework (EIF 2.0) interoperability model.

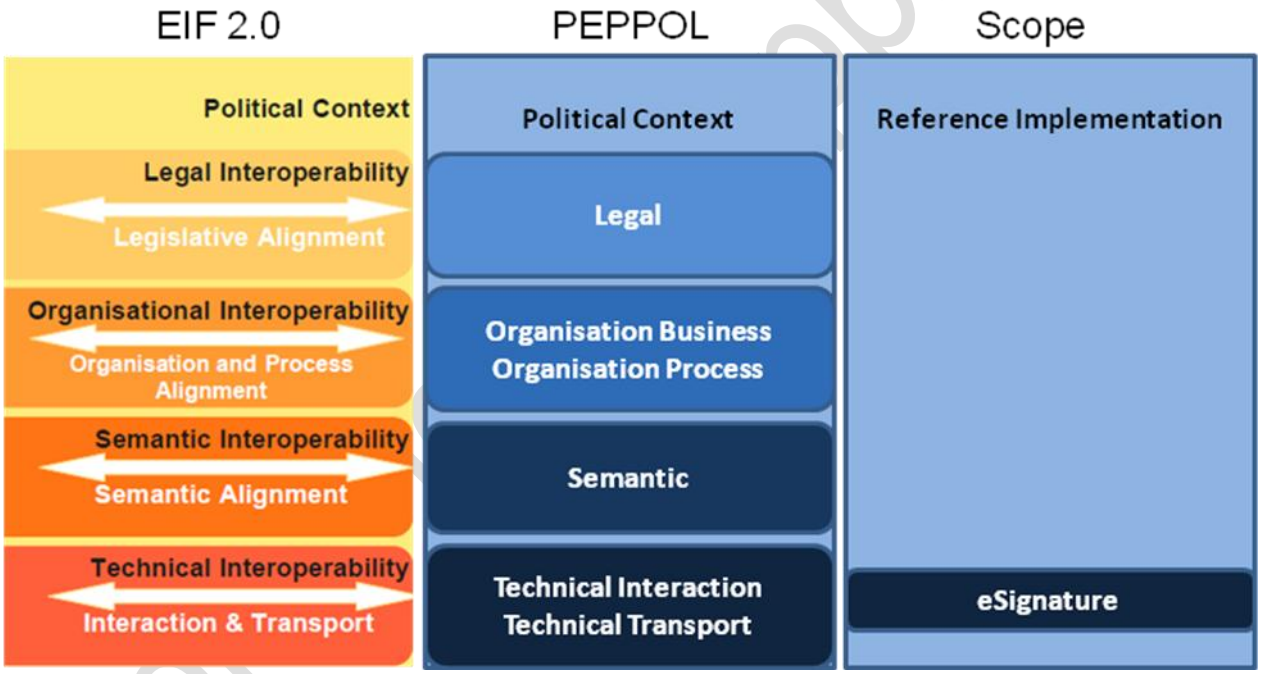


Figure 1: European Interoperability Layer and scope of Reference Implementation

Figure 1a shows which interoperability layers (EIF 2.0 and the PEPPOL specialization) that are in scope for this reference implementation. Figure 1b shows how the generic Reference Architecture for PEPPOL Interoperability (covering all interoperability layers) results in different Implementation models, that again sets the foundation fort he different Implementation Architectures and their (Reference) Implementations.

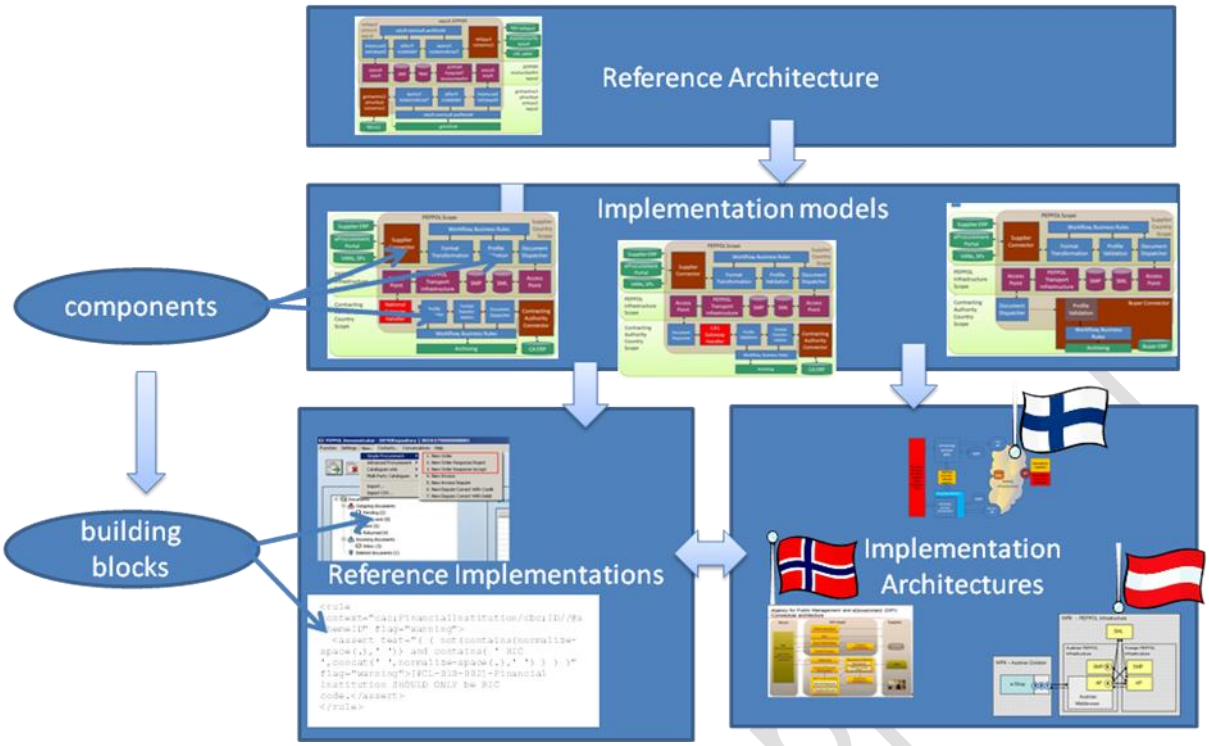


Figure 1b: PEPPOL Architecture-Implementation Model

## 1.3 Target Audience: Administrators

This annex document deals with the server component PEPPOL XKMS responder, and shall enable server administrators to install, configure and host the component. General abilities in administering server applications are expected to use the documentation successfully.

## 1.4 XKMS Responder Version

This documentation refers to the version 1.0 of the PEPPOL XKMS responder, released in May 2010.

# 2 Server Component PEPPOL XKMS Responder

The PEPPOL XKMS Responder provides functionality for handling X.509 certificates for various software applications or platforms. It enables certificate validation and creates the required certificate chain necessary for validation.

The PEPPOL XKMS responder uses certificate validation methods following the PEPPOL specification as given in "PEPPOL Deliverable D1.1 Requirements for Use of Signatures in Public Procurement Processes", approved by the European Commission, version 1.3 of Novermber 6th 2009.

The responder extracts the certificate information from the certificates and validates it according to the configured validation method. The validation results are returned to the server components and can be visualised for the users by appropriate applications, such as the PEPPOL-Signer or an eProcurement platforms. The PEPPOL XKMS responder offers the following configuration categories:

- Issuer management
- Trusted anchor management
- Properties management
- Configuration import and export

The issuer management provides information on validation methods and validation chains. In case certificates should not be further validated or are the highest instance in the validation chain they can be configured as trusted anchor certificates. These are treated as trustworthy that is, no further validation is performed.

With the "Properties management" proxy settings can be configured and a private signature key for the XKMS-responses can be chosen. Configuration import and export offers updating and saving configuration versions. The configuration file (XML) contains all issuer and trusted anchor certificates as well as technical data for connecting configurations of the bound trust centres with directory services and their respective validation methods. All of the above is currently (at time of delivery) in the configuration file.

The screenshots in this chapter use testing data as examples in the screens regarding to a special CA or configuration setting.

## 2.1 Hardware and software requirements

The current version of the XKMS responder is tested with the described software and hardware and technical support is provided. For cryptographic operations, the crypto provider Bouncy Castle is used (http://www.bouncycastle.org).

### Hardware requirements

X86 compatible platforms with AMD or Intel processors a clock rate of 2GHz are recommended. At least 2GB RAM is required.

### Network connection

The network communication between distributed server components, as well as to the database should at least provide a connection speed of 100MBit/s. Only TCP/IP networks are supported.

### Databases

The basic configuration of the database usually requires 50MB memory (100 MB recommended) for certificates, settings, cache, etc.

| | |
|---|---|
|  | **Attention**: The character encoding must be ISO 8859-1 |

### 2.1.1 Processor and operating-system combinations

The following table shows all combinations of processors and operating systems currently supported by the XKMS Responder on the server side. Please note that JDKs and processors that are given for some components.

| Application server | Operating system | DBMS |
|---|---|---|
| JBoss 4.2.X from version 4.2.2<br>JBoss Enterprise Application Platform 4.2<br>SUN JDK 1.5.0_X from version 1.5.0_10, recommended 1.5.0_16 | SUSE Linux Enterprise Server 10 on x86<br>Windows 2003 Server<br>Red Hat Enterprise 5 | Oracle 10gR2<br>MySQL 5<br>(both cluster capable) |

Table 1: Supported application servers, processors and operating systems

**Note concerning the Oracle database:** versions 10.2.0.1, 10.2.0.2 and 10.2.0.3 are supported on delivery time of the XKMS responder:

| | |
|---|---|
|  | **Note**: For the use of other software please contact bremen online services to confirm its technical support. |

### 2.1.2 Supported software

The supported software can be downloaded at the listed web pages:

- JBoss 4.2.X: http://sourceforge.net/projects/jboss/files/JBoss/JBoss-4.2.2.GA/
- Java JDK 5: http://java.sun.com/javase/downloads/index_jdk5.jsp
- MySQL 5: http://dev.mysql.com/downloads/
- SUSE Linux Enterprise Server 10: http://www.suse.com
- Oracle 10gR2 : http://www.oracle.com
- Red Hat Enterprise 5: http://www.redhat.com/

### 2.1.3 Requirements (software)

The current XKMS responder supports various operating systems (on the client and server side), application servers, JREs and databases. For future versions the policy to support will be:

- If a software is newly supported in the current the XKMS responder release (3.x) it is also supported in the following release (3.x+1)
- Software of preceding releases (e.g. 3.x-1, 3.x-2, 3.x-3) that is no longer supported in release 3.x+1, is announced to be discontinued in 3.x.
- First time installations must always use the most current software version.

**Server side operating systems**

Supported in the enterprise or professional versions.

- **RedHat Enterprise**: supported is only the quarterly update (QU) of the supported RedHat Enterprise version that is current when the latest the XKMS Responder is released.
- **SUSE Linux Enterprise Server**: supported is only the latest version with belonging service pack, current when the latest the XKMS Responder is released.
- **Windows**: basically the latest service packs and security updates are supported

**Client side operating systems**

- **openSUSE:** only the latest version is supported.
- **Windows:** basically the latest service packs and security updates are supported. In case different versions of a Windows operating system are available, only the professional or premium version is supported, since usually their security updates are provided over the longest period of time.

**Application server**

- **JBoss:** Only the current JBoss version is supported. We strongly recommend using the enterprise edition. The currently supported version is listed in the table in chapter 2.2. In order to have up-to-date information on future version-changes of the JBoss, chapter 4.1 lists announcements and discontinued server platforms combinations with the respective the XKMS Responder releases.

**JDK/SDK**

- **JDK:** Changes of versions are not performed automatically. In order to have up-to-date information on future version-changes of JDKs, chapter 4.1 should be read, which lists announcements and discontinued server platforms combinations with the respective the XKMS Responder releases. A change of version can only be performed after the application server provider has been upgraded.

**Databases**

- **Oracle DB:** There is no automatic change to a more current version. However, support ends, when the provider stops support. In future new versions are only supported on request. In order to have up-to-date information on future version-changes of the Oracle database, chapter 4.1 lists announcements and discontinued server platforms combinations with the respective the XKMS Responder releases.
- **MySQL:** There is no automatic change to a more current version. However, support end, when the provider stops support. In future new versions are only supported on request. In order to have up-to-date information on future version-changes of the MySQL database, chapter 4.1 lists announcements and discontinued server platforms combinations with the respective the XKMS Responder releases.

## 2.2 Installation

In the current version of the PEPPOL XKMS responder, a VMware image with a standard installation setup of the XKMS responder is provided. The installation covers only the installation of this image. For details, see VMware documentation at: http://www.vmware.com/support/pubs/server_pubs.html.

On the image, the directory /home/xkms/scripts contains a file “readme.txt” with instructions to start the responder.

## 2.3 Configuration

The PEPPOL XKMS responder enables the validation of certificates and the creation of the certificate chains required for validation. It is used to extract the certificate information from the certificates and to verify this certificate information on the basis of a configured validation method. The validation results

thereby obtained are returned to the server components and can be displayed to the user via the corresponding applications.

After the XKMS server has been started, the configuration page is available from the URL http://localhost:8080/PeppolWebAdmin/WebAdmin in the web browser (Mozilla Firefox recommended).

The system overview is the starting point of the configuration. On the administration page, the following overview is displayed:


Figure 2: Administration application of the PEPPOL XKMS responder (detail)

On initial use, no configuration is stored in the database of the PEPPOL XKMS responder. Hence, you must load a configuration file. The administration page offers the following configuration options:

- Administration of properties
- Administration of issuers
- Administration of trusted anchor certificates

It is necessary to activate the appropriate link in order to check and administrate the respective sub-function. Some frequently reocurring administration tasks in conjunction with the PEPPOL XKMS responder are:

- Importing own CA certificates
- Activating and deactivating issuer entries
- Configuration of signing certificate.

The following sections explain the individual links for administrating the sub-functionalities.

### 2.3.1 Load and save configuration

Initially, no configuration is stored in the database of the PEPPOL XKMS responder. A configuration file must be loaded. This file contain all trusted anchor certificates and issuer certificates, valid at the time of delivery, as well as technical data concerning the connection configuration of the trust centres connected by default (including directory services and their validation methods).

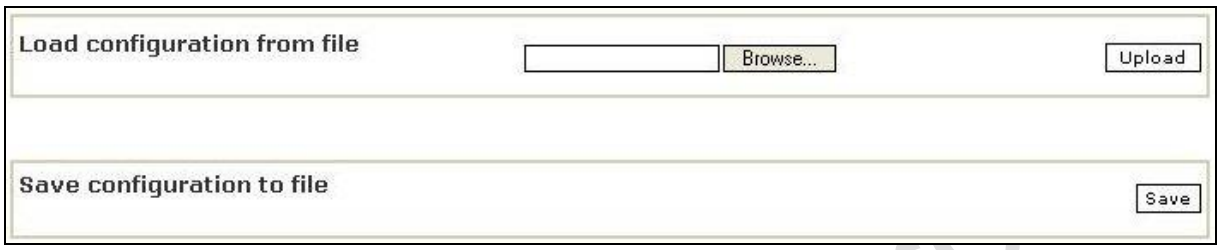


Figure 3: Load and save area of the configuration

The XML file containing the configuration will be supplied by the WP1 member in charge and handed over. To load the configuration, scroll down on the administration page to the section labelled “Load configuration from file” (see Fig. 44). To store a changed configuration use the button “Save” in the section “Save configuration to file”. A file chooser dialog will appear to select the target directory and filename.

### 2.3.2 Administration of XKMS responder properties

In the first section the administrator can set proxy settings and select a private signature key for the responder (if necessary).

**Administration of proxy settings**

To route the external connections of the PEPPOL XKMS responder via a proxy, first configure this proxy.

- **Proxy host**: Enter the host name or the IP address of the proxy here.
- **Proxy port**: Enter the port number. Valid port numbers are 1 to 65535.
- **Username/password**: If the proxy server is set up with authentication, the corresponding user data must be entered here.
- **Proxy exceptions**: Enter the hosts here, which can be reached without the configured proxy. A detailed explanation is at the end of this list. An entry is only valid in this field, if a proxy is configured in the above field "Proxy host".

**General properties**

- **Timeout for HTTP connections**: The timeout value is entered as a number of seconds from 1 to 30. A value of 30 is mostly correct, 0 is not allowed. All communication with issuers using validation method OCSP is executed with HTTP. The timeout that you can set here effects these entire HTTP requests (see chapter 3.6.3 for more information on OCSP).

**Proxy exceptions**

It is possible to list the hosts, which can be reached without the configured proxy. Several addresses can be listed separated by a semicolon. IP addresses may be generic, that is, parts of the IP address can be substituted by asterisks stepwise form, right to left. Example:

| Valid proxy exceptions: | Invalid proxy exceptions: |
|---|---|
| 10.20.30.40 | 10.20 |
| 10.20.30.40; 10.20.30.41 | 10.20.* |
| 10.20.30.* | 10.20.*.50 |
| 10.20.30.*; 10.20.30.41 | |
| 10.20.*.* | |
| www.hostname.de | |

Table 2: Proxy exceptions

An entry is only valid in this field. If a proxy is configured in the above field "Proxy host". The values localhost and 127.0.0.1 are valid but are used by default as proxy exceptions. Click "Apply" when you have completed all entries. The figure below shows the dialog.

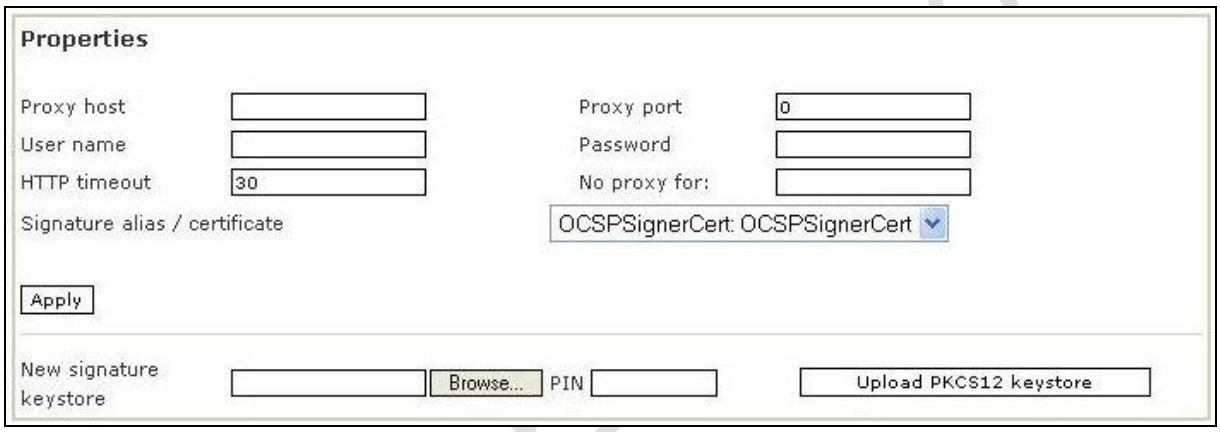


Figure 4: Proxy configuration

**Settings for the signature**

In the lower part of the properties box, upload the PKCS#12 keystore which is used to sign the messages of the PEPPOL XKMS responder. Click the "Browse" button next to the “New signature keystore” entry to select a PKCS#12 file. Thereafter, enter the PIN for the respective keystore. The figure below shows an example.

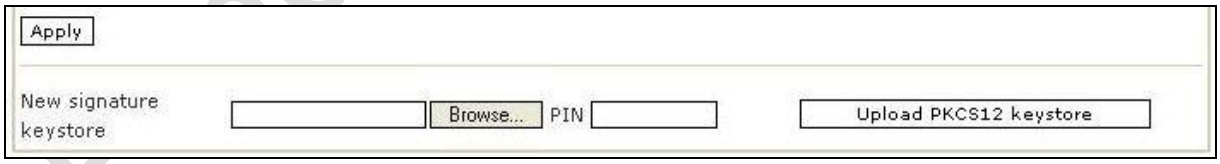


Figure 5: Add certificate

### 2.3.3 Administration of issuers

The "Issuers" link brings a section with a list of all certificate service providers that are currently stored. The list is organised as a table. The columns of the table have the following meanings:

- **Name**: This refers to the issuer's name. This name is implemented as a link, which leads to the detail information stored for this issuer.
- **Signature Level**: This refers to the quality of the certificates. This column can contain the following values: unknown, low, lcp, ncp, ncpplus, qcp, qcpplus

- **Validation method**: This column shows one of the following validation methods: None, OCSP, CRL, LDAP, LDAP + CRL and XKMS; for further details, see below.
- **Status**: The status can be changed by clicking on the value. The status can change between "Active" and "Inactive".

**Explanations for the "Validation method" column**

The values in the "Validation methods" column have the following meanings.

- **OCSP**: Online Certificate Status Protocol. OCSP is a certificate validation method, which enables positive validation of the current status of a certificate within the scope of signature validation. The validation result is signed and contains the following information: The certificate is valid, revoked, not yet activated, or unknown. OCSP offers the following advantages compared to CRL: positive validation, very up-to-date due to the avoidance of static lists, smaller data volume.
- **CRL**: Certificate Revocation List. CRLs are static revocation lists, which contain information about withdrawn or revoked certificates. The revocation lists are provided by the certification service providers (CSPs) and must be available in regularly updated form for performing so-called negative validation of the PEPPOL XKMS responder.
- **LDAP**: Lightweight Directory Access Protocol. This is a simplified DAP protocol for access to standardised directory systems according to X.500 in which certificate data is stored. Refer also to http://www.ietf.org/rfc/rfc2251.txt.
- **XKMS**: Redirects requests to another XKMS responder, capable of validating certificate in question.

**Explanations concerning the "Status" column**

- **Inactive**: Certificates of issuers whose status are "Inactive" are not validated.
- **Active:** If an issuer is set "Active", the certificates of this issuer are validated**.**

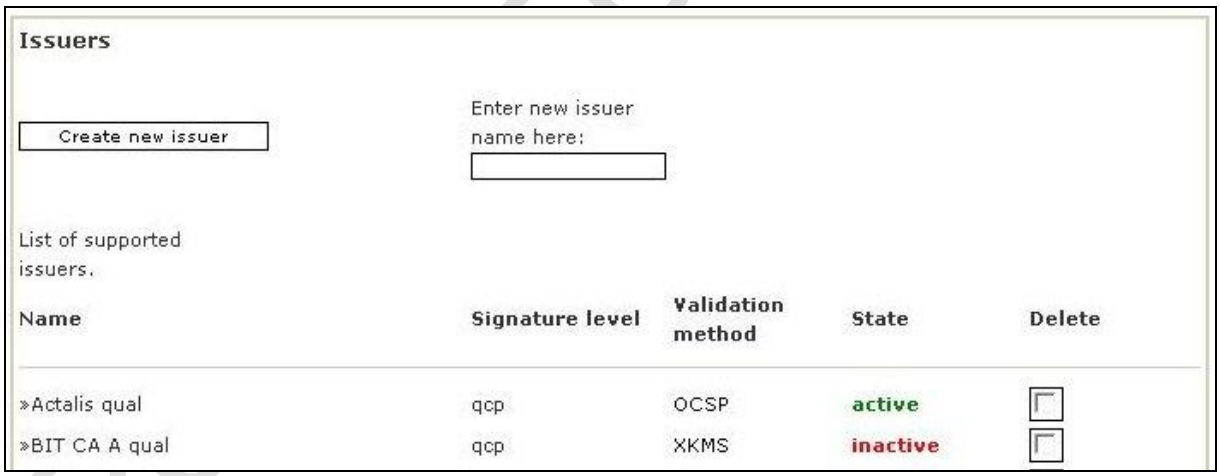


Figure 6: Part of the area "Issuers"

**Edit or display issuer**

When clicking on a name in the list of issuers, you can edit or display this issuer's data.

### 2.3.3.1 Add issuer

The **"Create new issuer"** button is located at the beginning of the list on the "Administration of issuers". This button brings a dialog, in which another certification service provider can be added to the list of issuers. Add the name of the new issuer and click on “Create new issuer”. Initially, the dialog looks like this:

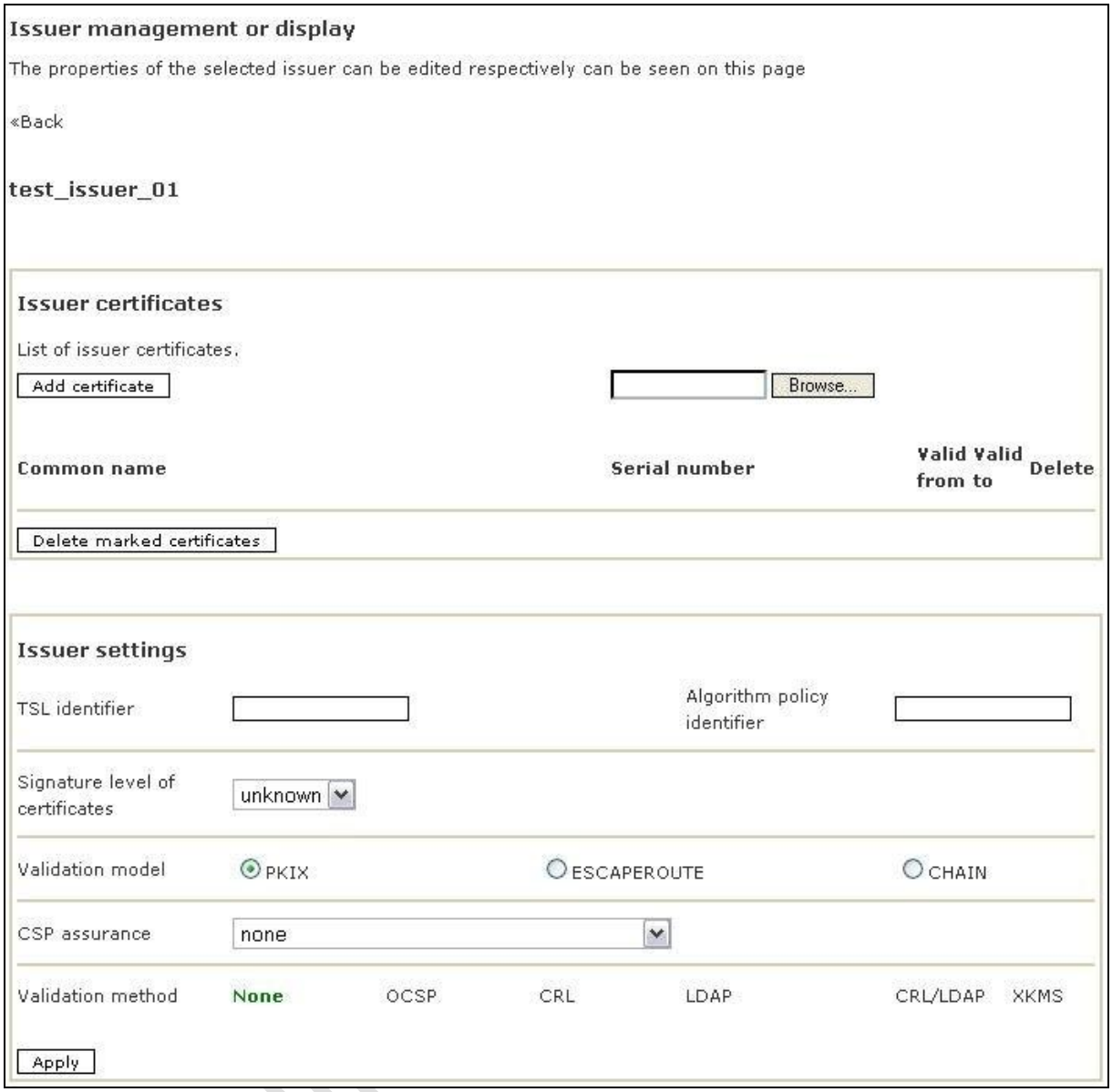


Figure 7: Create new issuer

**Add certificate**

To add an issuer certificate, click on the “Choose” button and select the certificate file (usually with “.cer” or “.crt” extension). After approving the selection click “Add certificate”. The certificate will be added to the list.

**Issuer settings**

The fields have the following meanings:

- **TSL Identifier:** The identifier for the Trustservice Status List, supported in future releases.
- **Algorithm Policy Identifier:** The identifier for algorithm policies list, supported in future releases.

**Signature level of certificates**: Select one of the following values from the selection list: “low”, “lcp”, “ncp”, “ncpplus”, “qcp” or “qcpplus”. Note that the default value "unknown" is not valid! The meanings of the different qualities of a certificate are explained in D1.1 part 7: eID and e-signature Quality Classification.

**Explanation**

- **“low”**: Low confidence in certificate but certificate policy exists or quality assessment is possible by other means.
- **“lcp” (medium level):** Certificates governed by a certificate policy in compliance with the ETSI TS 102 042 standard for LCP or a similar standard.
- **“ncp” (high level):** Certificates governed by a certificate policy in compliance with the ETSI TS 102 042 standard for NCP or a similar standard.
- **“ncpplus” (high level +):** Certificates governed by a certificate policy in compliance with the ETSI TS 102 042 standard for NCP+ or a similar standard. (Use of a SSCD is mandated in the CP.)
- **“qcp” (very high level):** Certificates governed by a certificate policy in compliance with the ETSI TS 101 456 standard for QCP or a similar standard.
- **“qcpplus” (very high level +):** Certificates governed by a certificate policy in compliance with the ETSI TS 101 456 standard for QCP+ or a similar standard. (Use of a SSCD is mandated in the CP. Thus, this level supports qualified signatures according to the EU Directive on electronic signatures.)
- **Explanation of abbreviations:**
  - LCP = Lightweight Certificate Policy
  - NCP = Normalized Certificate Policy
  - QCP = Qualified Certificate Policy
  - SSCD = Secure Signature Creation Device
- **Validation method**: Click one of the following validation methods: XKMS, OCSP, LDAP, CRL, LDAP + CRL or none. Depending on your selection, the dialog will be expanded to include those fields, which must be filled in for the respective validation method.

**Add issuer with the OCSP validation method**

The following dialog is displayed for issuers with the OCSP validation method.


Figure 8: Configuration of an issuer with the OCSP validation method

The properties have the following meanings.

- **URL**: This is the URL of the trust center where the certificates are validated.
- **Subtype**: The subtype indicates the validation logic. The following options are available:
  - **Common PKI**: OCSP server according to Common PKI -> positive and negative validation.

- **RFC**: OCSP server according to RFC2560 -> same validation logic as CRL, however, the only validation performed is negative validation (i.e. a check is performed whether the certificate is revoked).

- **Use cache**: The relay provides a cache in which certificate validation results are available for a defined period of time. If this cache is to be used, activate the "yes" option here.
- **Cache timeout**: This indicates the number of seconds during which the above-mentioned cache has to be available.
- **Check response signature**: The responses from the trust centers are digitally signed; this signature is validated if "yes" is activated.

**Add issuer with the LDAP validation method**

The following dialog is displayed for issuers with the LDAP validation method.

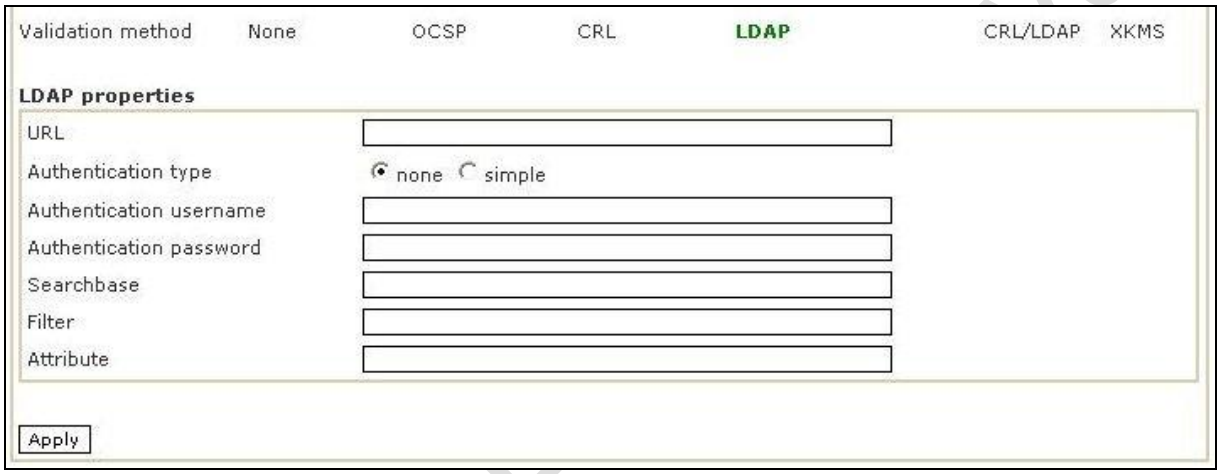


Figure 9: Configuration of an issuer with the LDAP validation method

The properties have the following meanings.

- **URL**: This is the real URL of the trust centre where the certificates are validated.
- **Authentication type**: This authentication is at present requested by no LDAP server in the case of the trust centres, which are supported by default. In the event that authentication is required, please enter the authentication type in this box. There are three types of authentication:
  - "none" (no authentication, the field can remain blank)
  - "simple" (for more detailed information, please refer to the LDAP specification for authentication)
- **Authentication username**: Please enter the user name for authentication here.
- **Authentication password**: Please enter the password for authentication here.
- **Searchbase**: Search base for LDAP validations, also server root, root directory or searchbase. Enter an LDAP-compliant string here. This string typically consists of the following parts: "o=Originator, c=country-code".
- **Filter**: In the case of certificates, this can, for example, be the e-mail address. The entry must comply with LDAP conventions.
- **Attribute**: The value of this attribute is disclosed by the manufacturer. It is the name of the attribute under which the user's certificate can be found.

**Add issuer with the CRL validation method**

The following dialog is displayed for issuers with the CRL validation method.

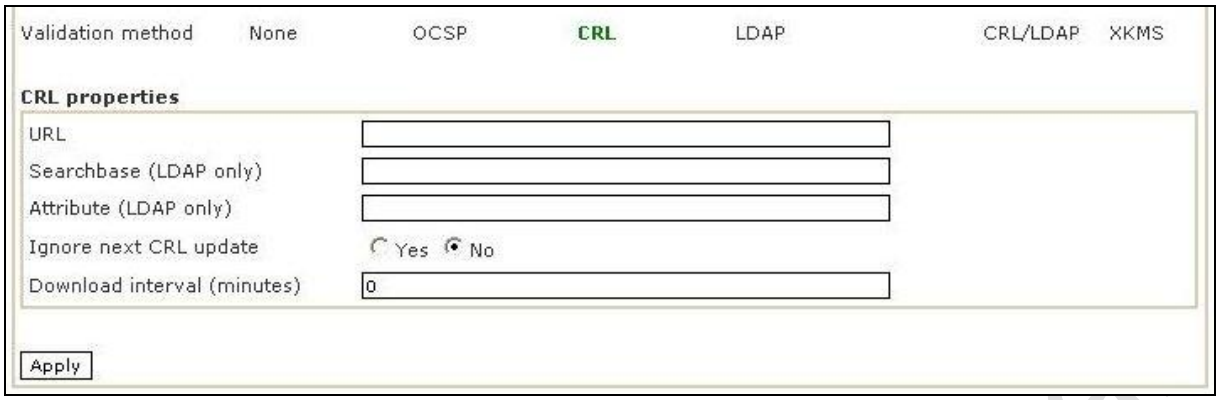


Figure 10: Configuration of an issuer with the CRL validation method

The properties have the following meanings.

- **URL**: This is the address where the CRLs for the validation can be downloaded from.
- **Searchbase**: If you have selected a LDAP protocol under "URL", you must specify a search base for LDAP validations; this is also referred to as server root, root directory or searchbase. Enter an LDAP-compliant string here. This is typically made up of the following parts: "o=originator, c=country-code".
- **Attribute**: The value of this attribute is disclosed by the issuer and refers to the access to the CRL.
- **Ignore next CRL update:** If you accept the default, i.e. "No", the CRL will be automatically replaced according to the settings of the certification authority. The "NextUpdate" attribute which is contained in the CRL is evaluated for this purpose. If you select "Yes" here, you must enter a time interval in minutes in the next field in order to define the time intervals at which the CRL will be replaced, i.e. downloaded from the server of the certification authority. Some CRLs of certain issuers become invalid the moment you download them. In this case the update should be ignored. Fill in "Yes" and set the interval to for example 30 minutes.
- **Download interval (minutes):** The default setting is 60 minutes. The interval is set at 40 minutes for most issuers. Contact the issuer you wish to add in order to find out which entry is advisable here. Important: This interval becomes only effective if you have selected "Yes" for next above.

**Add issuer with the LDAP + CRL validation methods**

The properties which are displayed for this selection are made up of the above-described properties for issuers with LDAP and issuers with CRL.

**Add issuer with XKMS validation method**

The following dialog is displayed for issuers with the XKMS validation method.

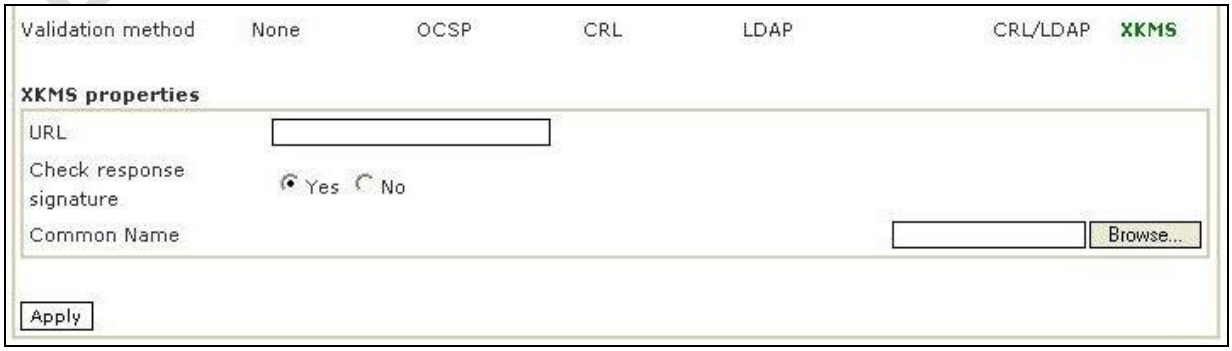


Figure 11: Configuration of an issuer with the XKMS validation method

The properties have the following meanings.

- **URL**: This is the URL of the responsible XKMS responder for these certificates.
- **Check response signature**
  - **Yes**: The signature of the received XKMS response will be checked. You have to configure a certificate at the following “Choose” button.
  - **NO**: The signature of the received XKMS response is not checked.
- **Common Name**: The SubjectName of the choosen certificate (if a certificate for validating is configured)
- **“Choose” Button**: Will open a file dialog to configure a certificate for validating.

After having entered the issuer properties, click the “Apply” button to save your changes.

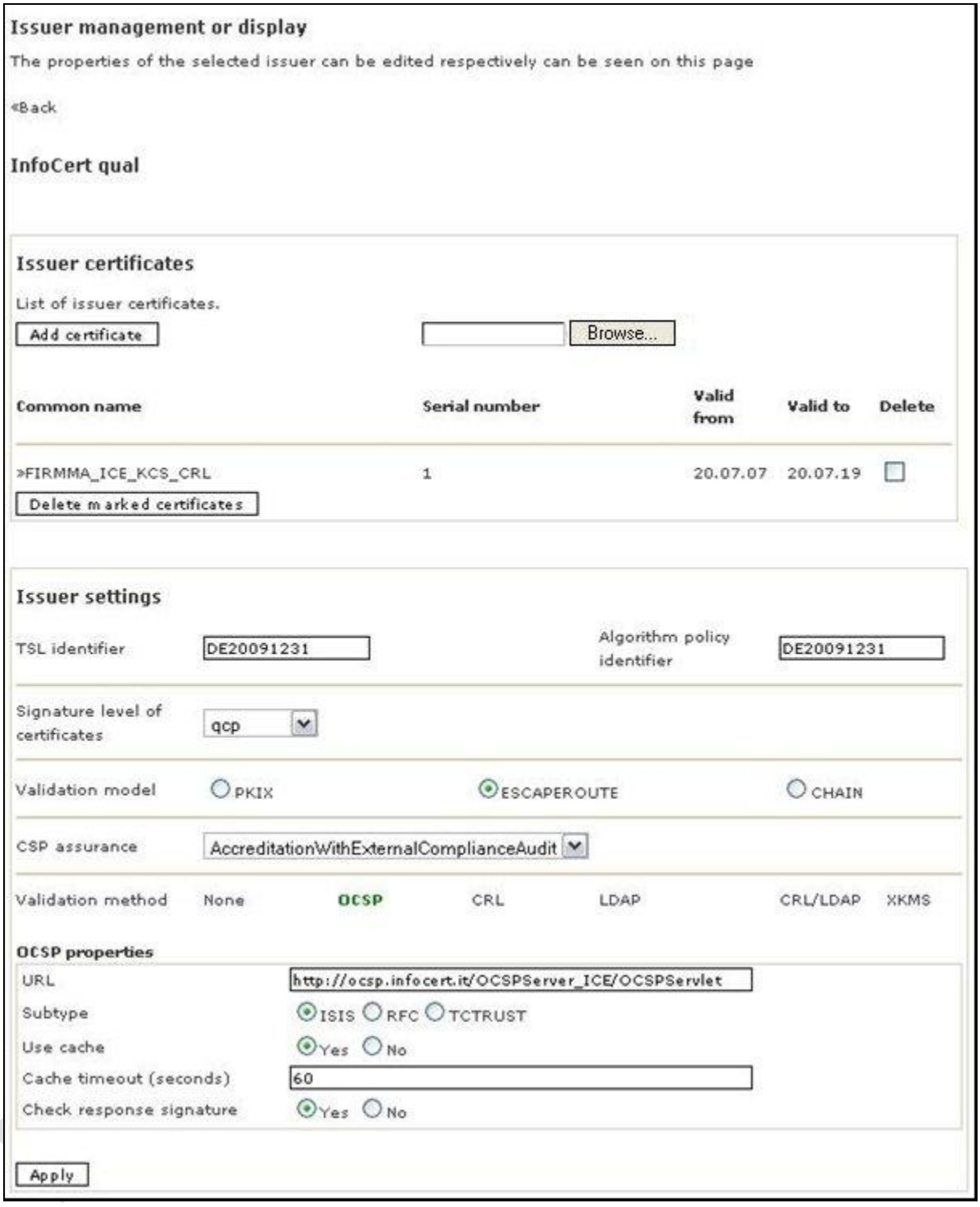


Figure 12: Edit or display issuer

**View of the issuer certificate**

The table below the issuer name contains the entries in the "Name" column as links, which you can use in order to access the view of the selected certificate details. This view offers the following options:

- Display certificate details
- Delete certificate

- Apply settings; this brings you back to the "Upload certificate" dialog.

#### 2.3.3.1.1 Administration of trusted anchor certificates

The overview (which can be accessed via the link of the same name on the main administration page of the PEPPOL XKMS responder) shows all certificates, which were defined as so-called "trusted anchors".

**Meaning of trusted anchor certificates**

Validation methods and validation chains are published via the configurations in the PEPPOL XKMS responder. Certificates (which are not further validated) or certificates, which constitute the highest instance in a chain, can be configured as so-called trusted anchor certificates. Trusted anchor certificates are considered to be trustworthy, i.e. no further validation is carried out.

The software certificates of the server components, which you create at a later point in time, for instance, can be configured as trusted anchors. Certain issuer certificates also have to be defined as so-called trusted anchors because no further validation is possible.

**The "Trusted anchor certificate management" dialog**

The "Trusted anchor certificate management" dialog lists the existing trusted anchor certificates in a table and offers the option of adding further trusted anchor certificates. The date of a trusted anchor certificate that has expired is shown in red; see the example in the figure below:

Trusted anchor certificates

List of trusted anchors.

Add certificate | Browse...

| Common name | Serial number | Valid from | Valid to | Delete |
|---|---|---|---|---|
| »S-TRUST Qualified Root CA 2008-001:PN | 238711914426349127017336825542203409125 | 01.01.08 | 31.12.12 | |
| »ChamberSign Qualified CA 2 2006:PN | 55118 | 27.10.06 | 27.04.11 | |
| »D-TRUST Qualified CA 1 2006:PN | 47457 | 27.04.06 | 27.04.11 | |
| »S-TRUST Qualified Root CA 2009-001:PN | 313361942446221017759042062853284723 53 | 01.01.09 | 31.12.13 | |
| »QuoVadis Root Certification Authority | 985026699 | 19.03.01 | 17.03.21 | |
| »ChamberSign Qualified CA 1 2006:PN | 55117 | 27.10.06 | 27.04.11 | |
| »Swisscom Diamant CA 1 | 289807302858559253261008283882982509 13 | 25.04.06 | 25.04.16 | |
| »S-TRUST Qualified Root CA 2006-001:PN | 297023384592669574518635044825222184674 | 01.01.06 | 31.12.10 | |
| »ChamberSign Qualified CA 1 2007:PN | 288692 | 06.11.07 | 31.10.12 | |
| »D-TRUST Qualified CA 2 2006:PN | 47458 | 27.04.06 | 27.04.11 | |
| »S-TRUST Qualified Root CA 2008-002:PN | 260701990535702880117417416763096039037 | 01.01.08 | 31.12.12 | |
| »D-TRUST Qualified CA | 277 | 13.09.01 | 13.09.07 | |
| »D-TRUST Qualified Root CA 2 2006:PN | 47456 | 27.04.06 | 27.04.11 | |
| »LISIT Servizio di certificazione per la Firma Digitale | 1 | 02.09.04 | 02.09.16 | |

Figure 13: Trusted anchor certificate management

When you click the column headings, the entries in the lines of the selected column can be sorted in ascending or descending order.

The entries in the "Common name" column are links, which lead to a detail view of the trusted anchor certificates. The dialog titled "View of the trusted anchor certificate" shows important properties of the certificate. Deleting a trusted anchor certificate is possible in this detail view only. Additionally, a "Details" button is available, which enables the static display of all displayable details of the certificate in a new browser window.

# 3 Requirements for Integration of Certificate Authorities into the PEPPOL XKMS Responder

To enable the PEPPOL XKMS-Responder to validate certificates of a certain Certificate Authority (CA), technical information about the CA and its certificates is required. This chapter provides assisting guidelines to gather information that helps to configure the XKMS responder.

In this chapter provides a list of certificates and documents requested for the configuration. The second part provides a questionnaire that should be filled out by the respective certificate authority.

| | |
|---|---|
|  | *The PEPPOL XKMS-Responder validates only X509V3 certificates according to PKIX!* |

## 3.1 Needed Certificates and signed documents/objects

To configure and test the PEPPOL XKMS-Responder we need the following:

1. Two "End Entity Certificates" (EE Certificates), no test certificates
2. Root Certificates
3. CA Certificates
4. Sub CA Certificates (if applicable)
5. CRL and OCSP Signer Certificates and those of their Certificate Chain
6. One signature card of the respective CA (if possible)
7. Signed documents (office documents, PDF, signed with own signature creation software), signed according to at least one of the following formats
   - PKCS#7
   - PDF inline
   - XADES Basic / XadES Timestamp / CAdES BES

## 3.2 Questionnaire for Certificate Authority

### 3.2.1 General information about CA

- How are the certificate chains structured (Root, CA, Sub-CA, EE)?
  - How is it structured regarding person related certificates and what level of signature is used (according to EU-Directive)?
  - How is it structured for OCSP/CLR certificates?
- Which mechanisms for validation are supported (e.g. OCSP according to RFC, LDAP/CRL, CRL)?
  - How are the mechanisms for person related certificates?
  - How are the mechanisms for the CA Certificate, Sub CA Certificate?

- How are the mechanisms for the OCSP or the CRL Certificate?

- What are the serveradresses/URL for all of the certificates mentioned in 1.2
  - What are the URLs of the services?
  - If LDAP: Which version of LDAP is used? What binding? How is the directory structured?
  - If CRL: How is the file structured? Notice: DELTA-CRL is not sufficient for negativ testing and will not be supported by the PEPPOL XKMS Responder.

### 3.2.2 Technical information about certificate profiles and certificate structure

- Which encoding is used?
- How is the building of certificate chains done?
  - Is there a "Key Authority Identifier"?
  - Is the building of certificate chains possible by allocating issuer to subject?

### 3.2.3 Additional information

- Information concerning the Certificate Policy
- Explanation of the practice in producing certificates (Certificate Practice Statement = CPS; for example according to RFC 3647)
- Is Certificate Suspension possible in the member state and CA in question?
- Further information that appears to be noteworthy: .....

# 4 Index of figures



# 5 Index of tables