Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461 ZVR: 948166612 UID: ATU60778947

CERTIFICATE STATUS TOOL VERSION 3.2.0 (07.06.2016)

The Certificate Status Tool is designed to provide certificate status information based on manually defined trust anchors as well as the EU Trusted Lists of Certification Service Providers (TSL). This status information includes OCSP and CRL-based revocation information. The tool also directly supports querying LDAP services for certificates. Some services are already configured by default (those used by the Austrian Citizen Card, in particular).

1. Installation

This section outlines the installation process and the system requirements for all supported platforms.

1.1. Microsoft Windows

1.1.1. System Requirements

Microsoft Windows is supported starting from version Windows XP. The *Certificate Status Tool* requires a Java Runtime Environment (JRE) ≥1.6. In case the provided Installer is used, a compatible JRE is installed automatically. Alternatively, a JRE can be downloaded from http://www.java.com/en/download.

1.1.2. Installation

Two different versions of the Certificate Status Tool are available for Microsoft Windows: a stand-alone runnable JAR file, as well as an Installer package. The installer package utilises the Microsoft Windows Installer to provide a setup wizard which guides the user through the installation process. As part of this process, the installation directory can be customised. The installer also sets up a JRE for the Certificate Status Tool in order to ensure correct operation. In addition, the installer also creates shortcuts in the start menu.

The provided stand-alone version of the Certificate Status Tool consists of a runnable jar file, which can be double-clicked to start the application (if the correct file association has been configured). Alternatively the jar can be run from the command line by invoking `javaw -jar certtool.jar`. Both versions include the same functionality. All configuration files are created automatically on the first run (these are located in the user's home directory inside .asitCertStatus/).

1.2. Apple OSX

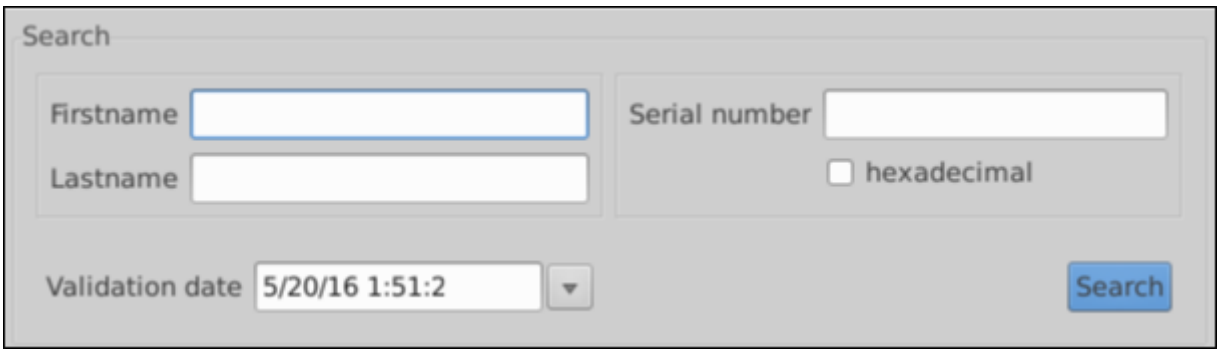
A disk image (*.dmg file) is provided vor Apple OSX. The Certificate Status Tool can be installed by copying the disk image into the /Applications directory. The Certificate Status Tool requires a Java Runtime Environment (JRE) ≥1.6. All configuration files are created automatically on the first run (these are located in the user's home directory inside .asitCertStatus/).

1.3. Linux

No dedicated installer is provided for Linux. Instead, a runnable jar and a start script are provided to run the application. GTK+ version 2 and a Java Runtime Environment (JRE) ≥1.6 are required to run the Certificate Status Tool. The provided downloads are not architecture-independent, therefore the correct package (32 bit or 64 bit) needs to be selected.

2. Search (LDAP)

The Certificate Status Tool integrates an LDAP search functionality. This feature is designed to conveniently search for and directly validate certificates. Both subject names and certificate serial numbers can be used to form a search request. The specified request is sent to all configured LDAP services (see Configuration).



The input fields *Firstname* and *Lastname* shown in the main application window can be used to specify the name of a certificate subject to search for. Alternatively, the serial number can be entered directly into the input field labelled *Serial number* to retrieve information about a specific certificate. A search query is executed by pressing the *Search* button.

The asterisk (*****) character can be used as a placeholder to construct fuzzy queries. To issue an exact search, the entered terms should be enclosed in quotation marks (**"**). Doing so makes it possible to query for subjects having only the specified name(s) (as opposed to including subjects with additional first and/or last names).

2.1. Examples

- Search for a known name: In case the full name of a subject is known, it should be entered as is. For example: first name *Max*, last name *Mustermann*. The Certificate Status Tool automatically transforms this into a query for *Max*Mustermann*. The results encompass all

certificates issued to subjects whose names start with *Max* and end with *Mustermann* such as *Maximilian Mustermann*.

- Search for partial last names such as: first name *Max*, last name *Must**. This results in a query for *Max*Must**. The results encompass all certificates issued to subjects whose first names start with *Max* and whose last names contain *Must*.
- Exact search for *Max Mann*: Both first and last name need to be enclosed in quotation marks; first name *"Max"*, last name *"Mann"*.
- Search for a certificate with a known serial number. The complete serial number should be entered into the *Serial number* input field. In case the hexadecimal representation of a serial number is entered, the corresponding checkbox needs to be ticked.

2.2. Hints

Some LDAP services (such as the A-Trust LDAP service) manage serial numbers as a numeric field. Numeric fields do not support the use of placeholders.

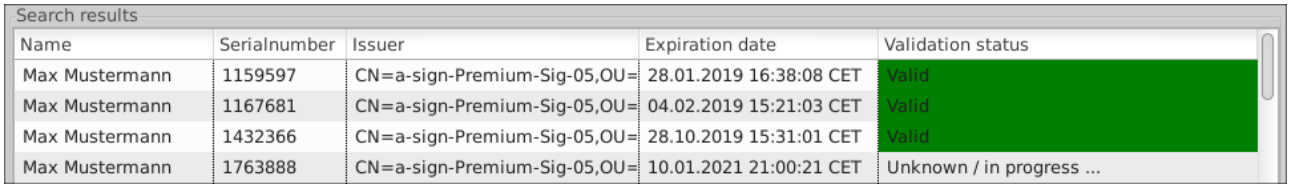
LDAP services are case-insensitive.

Note: The time an LDAP query takes to complete depends on the number of results and the network connection. To shorten this time, queries should be specified as precisely as possible. Issuing an exact search further speeds up this process.

The list of configured LDAP services is shown in the configuration dialogue and can be edited at any time (see Configuration).

2.3. Search Results

Search results are shown in table below the input form.

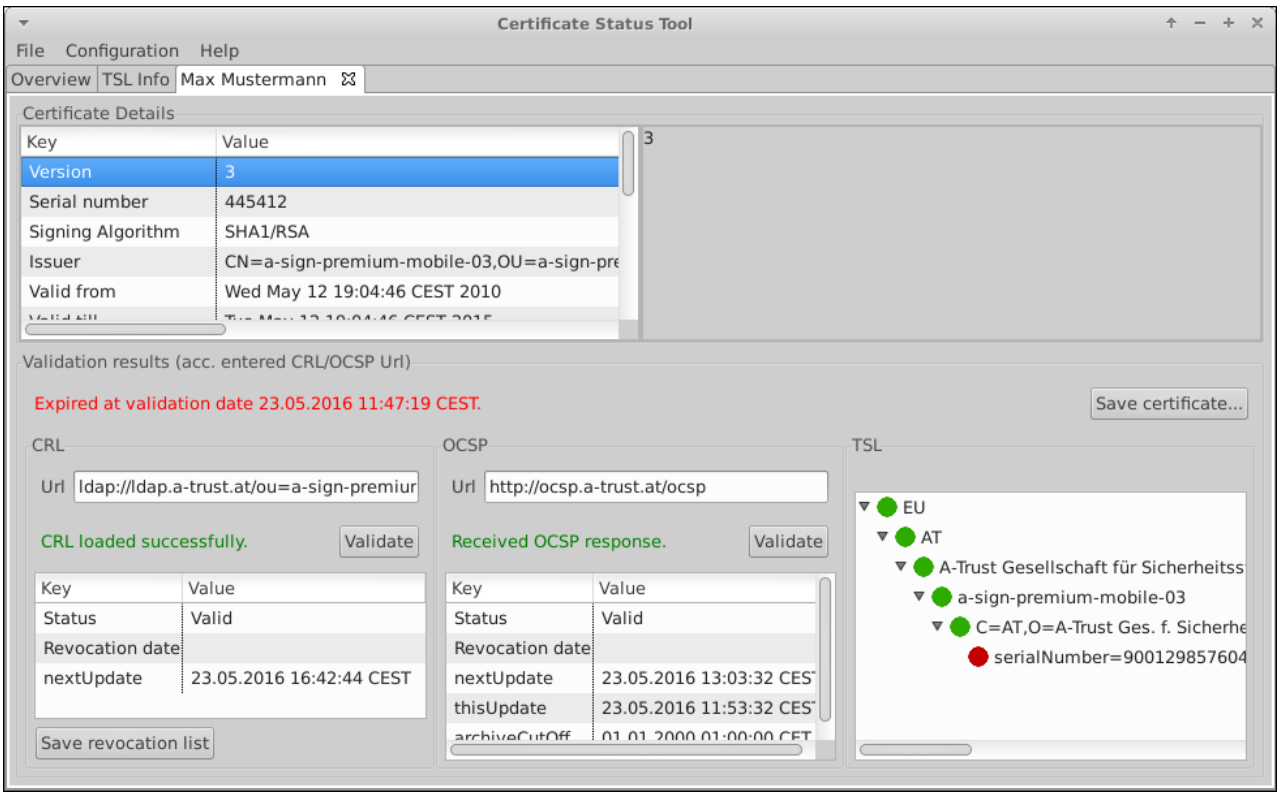


The first column indicates the name of the subject (common name, CN). The second column shows the serial number and the next columns indicate the issuer of the certificate (Issuer Distinguished Name, IssuerDN) and the expiration date. In case automatic validation is enabled, the validation status is also present.

3. Certificate Details and Status

Double clicking on a search result (see searching for certificates) or opening a certificate using *File → Open certificate…* opens a new tab containing the details of the selected certificate. The certificate's validity is verified based on the validation date specified in the application's main screen. Furthermore, CRL distribution points and OCSP responders are queried for revocation information. Please note that it does not make sense to try and validate a certificate for some future point in time since OCSP and/or CRL information may not be available.

Whether a certificate is considered valid, depends on (manually configurable) trust anchors (see Configuration). As trust anchors are always configured manually, even revoked issuer certificates can be used for validating certificates.
In addition to verification based on trust anchors, the EU trusted lists of certification service providers are used to determine a certificate's validity. Therefore, the results based on manually configured trust anchors can differ from the results based on the trusted lists of certification service providers.



As can be seen above, the certificate's details are shown and can be explored by selecting individual rows from the corresponding table.
Below this certificate information, the validity status is shown based on the configured validation date.

3.1. CRL Info

Detailed information about the CRL distribution point used for the current certificate are also presented:

- **Status:** Indicates whether the certificate has been revoked.
- **Revocation Time:** In case the certificate has been revoked, the revocation time is shown here.
- **nextUpdate:** Indicates the latest possible date, at which the certificate authority will issue a new CRL. After this date the current CRL will become invalid.

The current CRL can also be saved to a file by clicking the *Save revocation list* button. The CRL distribution point information is extracted from the certificate (if present). Otherwise, manually configured CRL distribution points are used (see Configuration). Alternatively, the URL to a CRL distribution point can be entered manually.

3.2. OCSP Info

In addition to CRL information, the OCSP status of the current certificate is also queried, providing in the following information:

- **Status:** Indicates whether the certificate has been revoked.
- **Revocation Time:** Shows the revocation date and time in case the certificate was revoked.
- **nextUpdate:** Indicates the latest possible date, at which the certificate authority issues newer status information.
- **thisUpdate:** Indicates the time at which the currently displayed information is valid.
- **archiveCutOff:** The archiveCutOff value indicates the earliest date for which OCSP information is available.

The OCSP responder URL is extracted from the certificate if present. Otherwise, manually configured OCSP responders are used (see Configuration). Alternatively, the URL to an OCSP responder can be entered manually.

3.3. TSL-Based Validation Results

In addition to validating certificates based on manually configured trust anchors, TSL-based validation is also supported. Such a validation process is performed automatically and works as follows:

1. The EU's toplevel TSL validity status is evaluated based on predefined EU trust anchors.
2. The validity status of the country matching the certificate issuer is evaluated based on the EU toplevel TSL.
3. The validity period of certificate itself is validated (excluding CRL and OCSP info).
4. The issuer information is extracted from the to-be-validated certificate.
5. The issuer certificate is validated (including CRL and OCSP info).
6. The issuer status is evaluated against the EU trusted lists of certification service providers and their services.
7. The identified service is considered valid if at least one of its certificates is still valid.
8. The corresponding service provider itself is considered valid, if at least one of its services is still valid.

This results in a chain of trust which is visualised accordingly. Green indicates a valid (and thus trusted) node, red indicated an invalid (or not trustworthy) node. Any node corresponding to a certificate can be double-clicked on to display the underlying certificate's details. These details are displayed in a separate dialogue window, presented in the same manner as the current certificate under evaluation. This dialogue also allows for saving a certificate to a file.

3.4. Automatic Certificate Validation

It is possible to automatically validate certificates returned form an LDAP query. The number of automatically validated certificates can configured from the menu bar using *Configuration → Preferences*. The status of certificates validated this way is incorporated into the search results and displayed accordingly.

Hint: Validating certificates takes some time, especially if the TSL information is being updated in the background. In such cases, timeouts can occur (see TSL for more information).

3.5. Notes on Selected Certificate Details

Some selected certificate properties are discussed below:

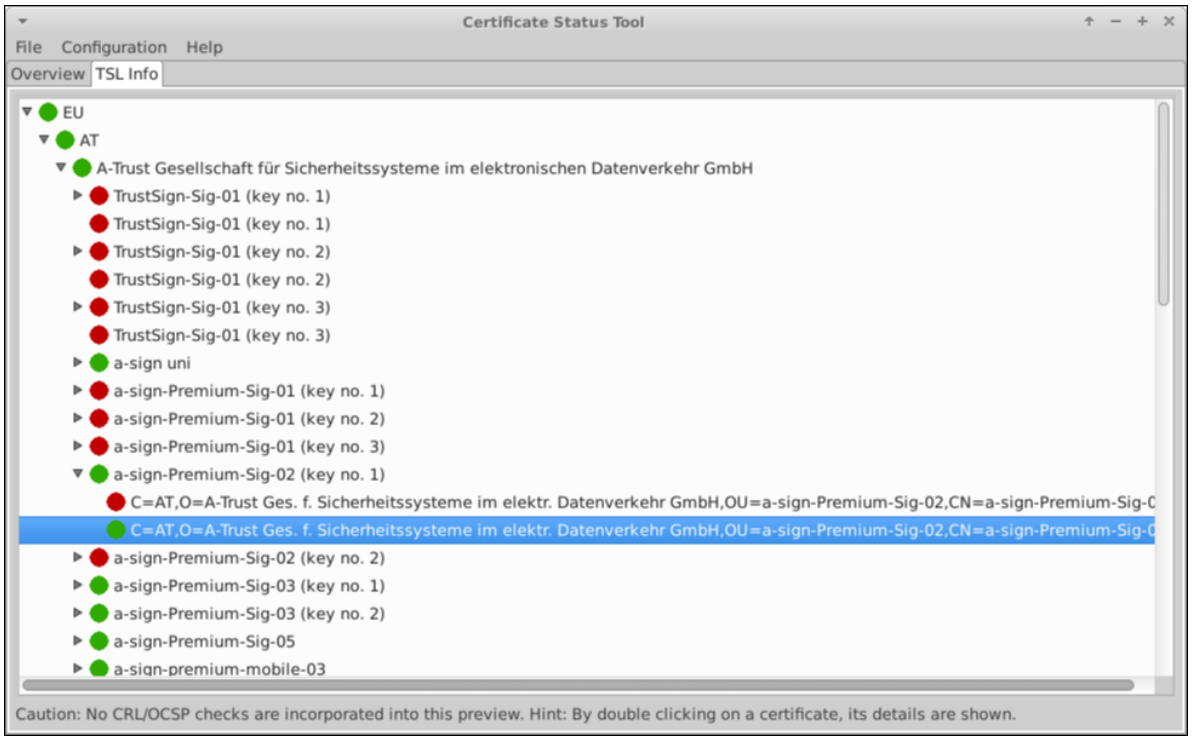
- **Issuer:** corresponds to the name of the certificate issuer (IssuerDN)
- **E-Government OID:** If present in the certificate, this field displays the Austrian E-Government Object Identifier. In case no E-Government OID exists, the message "The certificate does not contain any eGovernment OID" is shown instead. These Object Identifiers are only defined for the public administration sector [OID].
- **Certificate Type:** This field contains the value *simple certificate* or *qualified certificate*. The latter indicates that the certificate features at least one of the configured OIDs representing a qualified certificate (see Configuration). If applicable, additional information such as *E-Card Verwaltungssignatur-Zertifikat*, for example, is shown. (This is also configurable.)
- **Key Usage:**Displays the certificate's key usage according to RFC3280.
- **Limit on the Value of Transaction:** According to [SigG] a qualified certificate can be used to authorise transactions up to a specified limit. If a transaction exceeding this limit is issued using the certificate at hand, the certificate service provider is not liable for any potential losses.

3.6. Handling of Certificate Extensions

Some of a certificate's most relevant properties are defined through extensions. Not all extensions may be known to an application processing a certificate. According to RFC3280 special attention needs to be paid to so-called *critical* extensions. In particular, certificates featuring unknown critical extensions need to be rejected. The Certificate Status Tool informs the user whenever an unknown extension is encountered and stops processing the certificate featuring this extension.

4. EU Trusted Lists of Certification Service Providers

The Certificate Status Tool also supports validating certificates against the *Trusted Lists of Certification Service Providers* (TSL) issued by the European Commission (see Certificate Details and Status).
In order to provide insights about the state and structure of the EU TSL, the Certificate Status Tool features an interactive visualisation of the tree based on the EU toplevel TSL.



The TSL tree is composed of the following levels:

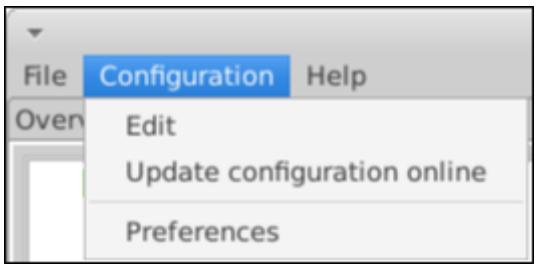
1. Country
2. Service provider
3. Service
4. Certificate

The algorithm determining the validity of individual nodes is described as part of the certificate details and status topic. Nodes of the TSL tree can be collapsed and expanded as desired. Additionally, nodes representing certificates can be double-clicked to inspect the underlying certificate's details. These details are shown in a separate window, which also enables saving the certificate to a file.

The TSL information is updated on every launch of the Certificate Status Tool. However, TSL-based validations are performed on (potentially out-of-date) information cached from the previous run, until the update has been completed. Depending on bandwidth and processing power such an update can take a few minutes. Furthermore, updates are not designed to be cancellable. Therefore, updates are always completed, which may delay exiting the Certificate Status Tool. This approach guarantees accurate and consistent information.

5. Configuration

Various aspects of the certificate Validation Process can be configured. For example, LDAP directories and revocation services are customisable. The main configuration dialogue can be launched using the menu *Configuration → Edit*.



As shown in the above figure, the configuration menu consists of the following entries:

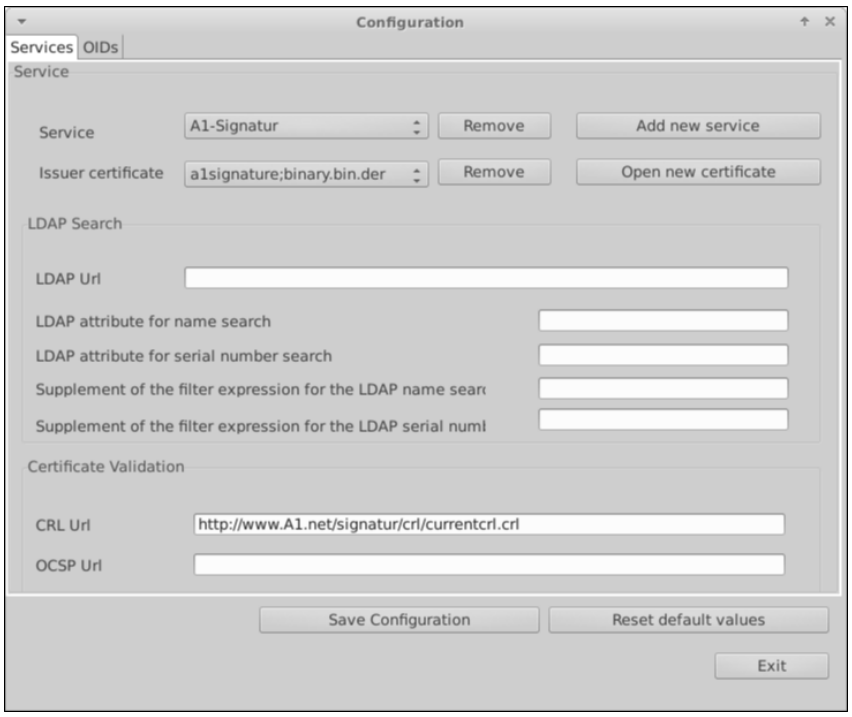
- **Edit**: Launches the main configuration dialogue.
- **Online Update**: Automatically downloads the most recent default configuration from the Internet (including trust anchors).
- **Preferences**: Used to enable and adapt automatic certificate validation settings.

5.1. Configuration Files

The configuration consists of local settings (the file *localconfig.properties*) and default settings (*defaultconfig.properties*). Configuration changes are stored as part of the local settings. By design, the default configuration is never altered. This enables resetting custom configuration values to their defaults. By manually editing the value of the *RemoteConfigurationURL* entry in the default settings configuration file, the distribution point for the default configuration can be customised.

5.2. Changing the Configuration

The main configuration dialogue enables the configuration of LDAP services and their corresponding OCSP responders and CRL distribution points as depicted in the figure below. Additionally, OIDs identifying qualified certificates can be specified.



5.2.1. Service Configuration

Selecting a service from the drop-down menu of all configured services populates all input fields with the values configured for this service and displays The trust anchors associated with the service. The following properties can be configured:

- **Issuer certificates:** Represents the trust anchors associated with a service. By pressing *Open new certificate* a certificate can be imported as a trust anchor for the currently selected service. An import copies the configured certificate into the directory *.asitCertStatus/certificates* in the user's home directory. In order to enable OCSP requests and a verification of certificates issued by a service provider, this provider has to be configured as a service, and its issuer certificate has to be imported.

  Hint: Multiple issuer certificates can be provided in order to support back-up certificates. In case the configured primary certificate gets revoked, the verification process can still commence based on additional certificates (if configured).

- **LDAP Url:** Specifies the URL of an LDAP directory to be queried. The URL must start with ldap://. In case no URL is specified, a service is not considered for queries.

- **LDAP attribute for name search:** The string of the LDAP pattern which specifies the field indicating subject names can be specified here. In most cases *cn=* is correct.

- **Supplement of the filter expression for the LDAP name search:** Contains the string which is appended to the subject name query string. If, for example, *Meier* is specified and the name search starts with *Max Mustermann* the resulting query string will be *cn=MaxMustermannMeier*. In most cases, this field should be left empty. The Austrian eCard, however, mandates *:SER**, since an LDAP query must also contain a filter for serial numbers, which are specified by the *SER* field.

- **LDAP attribute for serial number:** Specifies the string of the LDAP pattern which denotes the field indicating a certificate serial number. In most cases *serial=*, or *serialNumber=* is correct.

- **Supplement of the filter expression for the LDAP serial number search:** Contains the string which is appended to the serial number query string.

- **CRL Url:** Used to specify the URL to a CRL distribution point used for the configured service. Delta-CRLs cannot be used. The URL must start with ldap:// or http://. By default, any certificate is inspected for CRL distribution points during its verification. If no distribution points are specified in the certificate, the URL specified here is used.

- **OCSP Url:** Used to configure the URL to an OCSP responder. As with CRL distribution points, the configured responder is only used as a fallback. OCSP responder URLs must start with http://.

Any changes made can be saved by pressing the *Save configuration* button.

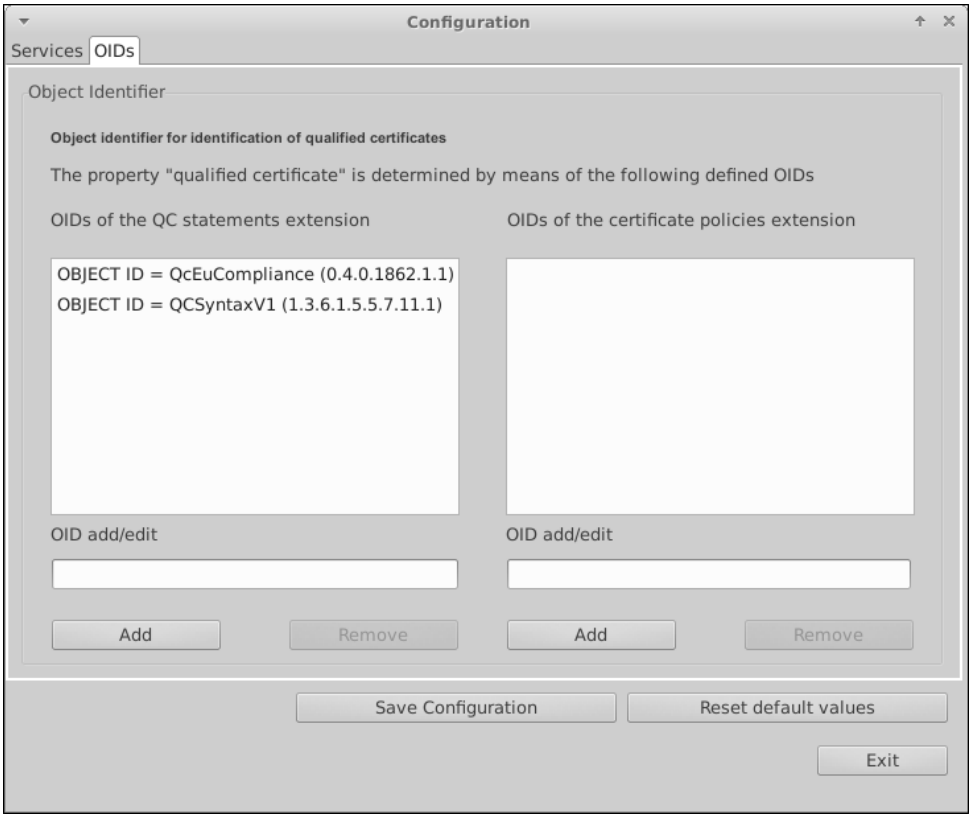
The configuration can be reset to its defaults at any time by pressing the *Reset default values* button.

The buttons *Add new Service* and *Remove* can be used to add/remove services. The *Remove* button next to a certificate is used to remove individual trust anchors.

Hint: If an LDAP service is configured attribute names for name and serial number must be provided as well.

5.2.2. OID Settings

The OID tab of the configuration editor allows for defining OIDs which are considered to indicate qualified certificates.



OIDs can either be declared as QC statements or as certificate polcies extensions.

Certificates may contain certain OIDs which mark them as qualified certificates. Any certificate having at least one of the specified OIDs (either as part of the *qualified certificate statements extensio*n or in the *certificate policies extensions*) are considered qualified certificates. Note: In both cases these data are set by the certificate issuer and will thus not be checked. New OIDs can be added by simply filling out the corresponding input field and pressing the *Add* button. By selecting an already specified OID it can be edited in the same way.

6. End User License Agreement

7. References

[ETSI] ETSI, “ETSI TS 101 862 Qualified Certificate Profile”, Version 1.3.3, Jänner 2006

[OID] Bundeskanzleramt, IKT-Strategie des Bundes, "Object Identifier der öffentlichen Verwaltung", 2006-02-27, abgerufen am 08.05.2006 unter http://www.cio.gv.at/it-infrastructure/oid/OID-1_0_6-20060227.pdf

[RFC 3280] Network Working Group, P. Housley, W. Polk, W. Ford, D. Solo, "Request for Comments: 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002

[SigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19.August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 164/2005 vom 30. Dezember 2005.

[SigV] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV, BGBl. II Nr. 30/2000 vom 2. Februar 2000) in der Fassung BGBl. II Nr. 527/2004 vom 30. Dezember 2004.