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

ZERTIFIKATSSTATUSTOOL VERSION 3.2.0 (07.06.2016)

Das *Zertifikatsstatustool* ermöglicht das einfache Abfragen und Anzeigen von Status- bzw. Widerrufsinformationen von Zertifikaten basierend auf manuell konfigurierbaren Trust-Anchor und der EU *Trusted Lists of Certification Service Providers*. Zusätzlich sind LDAP-Verzeichnisabfragen nach Personen und Seriennummern von Zertifikaten möglich. Die verwendeten LDAP-Verzeichnisdienste sind konfigurierbar, wobei eine Reihe vorkonfigurierter Dienste bereits mitgeliefert wird. Liste der konfigurierten Dienste kann auch zentral über eine Online-Updatefunktion aktualisiert werden – z.B. für eine organisationsweite Konfiguration. Unabhängig davon, kann die Konfiguration auch lokal geändert und erweitert werden.

1. Installation

Im Folgenden werden die Installation sowie die Systemvoraussetzungen aller unterstützen Betriebssysteme beschrieben.

1.1. Microsoft Windows

1.1.1. Systemvoraussetzungen

Microsoft Windows wird ab Version Windows XP unterstützt. Das Zertifikatsstatustool benötigt ein Java Runtime Environment (JRE) ≥1.6. Bei einer Installation über den zur Verfügung gestellten Installer wird automatisch ein kompatibles JRE installiert. Alternativ kann unter www.java.com/de/download ein JRE bezogen werden.

1.1.2. Installation

Für Microsoft Windows werden zwei unterschiedliche Pakete zum Download angeboten: Einerseits als lauffähige JAR-Datei, andererseits in Form eines Installers, welcher es dem Benutzer ermöglicht das Zertifikatsstatustool mit Hilfe eines üblichen Installationswerkzeuges zu installieren. Im Zuge dieses Vorgangs kann der Installationspfad nach Bedarf angepasst werden. Nach erfolgreicher Installation werden automatisch Verknüpfungen im Startmenü (unter *Certificate Status Application*) angelegt. Zusätzlich wird automatisch ein kompatibles JRE installiert, um die einwandfreie Funktion des Zertifikatsstatustools zu garantieren.

Die alternativ zur Verfügungen gestellte JAR-Datei kann (sofern dies konfiguriert wurde) ohne Installation direkt mit einem Doppelklick gestartet werden. Zusätzlich ist es auch möglich diese von der Kommandozeile aus über `javaw -jar certtool.jar` auszuführen. Beide Versionen bieten denselben Funktionsumfang. In jedem Fall werden die Konfigurationsdateien (zu finden im Benutzerverzeichnis unter .asitCertStatus/) automatisch beim ersten Start angelegt.

1.2. Apple OSX

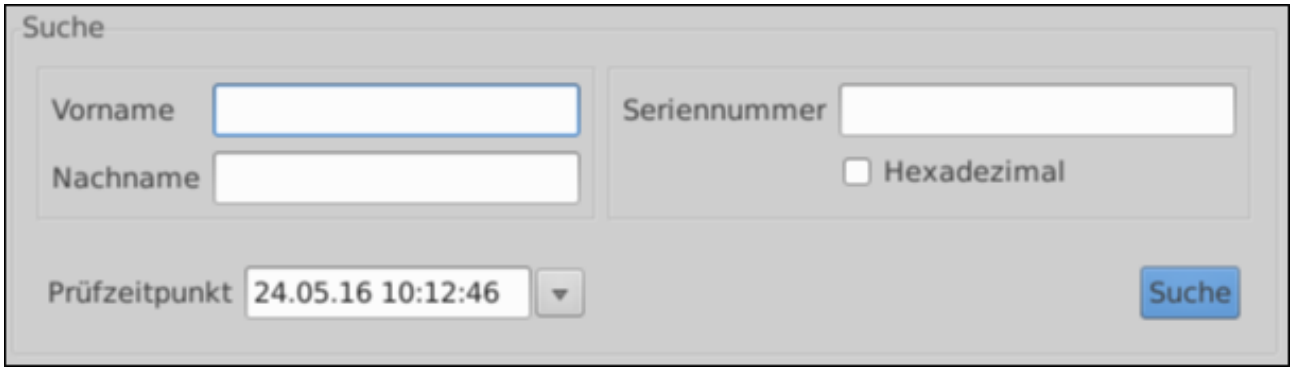
Für OSX wird ein Disk-Image (*.dmg-Datei) zur Verfügung gestellt. Durch Kopieren bzw. Drag and Drop der Datei in das /Applications Verzeichnis wird das Zertifikatsstatustool installiert. Das Zertifikatsstatustool benötigt ein Java Runtime Environment (JRE) ≥1.6. Die Konfigurationsdateien (zu finden im Benutzerverzeichnis unter .asitCertStatus/) werden automatisch beim ersten Start angelegt.

1.3. Linux

Eine Installation unter Linux ist nicht vorgesehen, stattdessen wird das Zertifikatsstatustool inklusive Startscript ausgeliefert. Beim Download ist darauf zu achten die zur Architektur passende Version (32- oder 64-Bit) auszuwählen. Das Zertifikatsstatustool benötigt ein Java Runtime Environment (JRE) ≥1.6, sowie GTK+ in der Version 2. Durch Ausführen das Startscripts wird das Zertifikatsstatustool gestartet.

2. Suche (LDAP)

Das Zertifikatsstatustool bietet die Möglichkeit in Verzeichnisdiensten nach Zertifikaten zu suchen. Dies kann entweder durch Angabe der Zertifikatsseriennummer, oder den Namen von Personen erfolgen.



Im Feld *Vorname* und *Nachname* kann der Name des Antragstellers von gesuchten Zertifikaten angegeben werden. Alternativ kann mit einer Eingabe im Feld *Seriennummer* nach einem Zertifikat mit der angegebenen Seriennummer gesucht werden. Ein Klick auf den Button *Suche* startet eine Suchanfrage.

Grundsätzlich wird in beiden Feldern das übliche Platzhalterzeichen (*****) unterstützt. Bei Suchanfragen wird das Platzhalterzeichen automatisch zwischen Vorname und Nachname gesetzt, damit z.B. auch Zertifikate von Personen mit einem zweiten Vornamen automatisch gefunden werden. Durch diese Voreinstellung würden bei der Suche nach *Max Muster* im Vornamenfeld alle Zertifikate von Personen gefunden, deren Nachname mit *Muster* beginnt.

Indem Namen in Anführungszeichen (**"**) gesetzt werden, können exakte Suchanfragen gestartet werden.

2.1. Beispiele

- Suche nach bekannten Namen: Wenn der vollständige Name einer Person bekannt ist, sollte dieser eingegeben werden. Zum Beispiel: Vorname *Max*, Nachname *Mustermann* - das Zertifikatsstatustool sucht automatisch nach *Max*Mustermann.*
  In diesem Beispiel werden alle Personen gefunden, deren Vorname mit *Max* beginnt und deren Nachname mit *Mustermann* endet, d.h. auch *Maximilian Mustermann* o.ä.
- Suche nach allen Personen deren Nachname mit einer bestimmten Zeichenkette beginnt, z.B. Vorname: *Max*, Nachname: *Must** - das Programm sucht automatisch nach *Max*Must** In diesem Beispiel werden alle Personen gefunden deren Vorname mit *Max* beginnt und deren Nachname *Must* enthält!
- Exakte Suche nach *Max Mann*. Indem Vorname und/oder Nachname in doppelte Anführungszeichen gesetzt wird (*"Mann"*), wird eine exakte Suche gestartet. Standardmäßig würde nach *Max*Mann* gesucht werden, daher würde auch *Max Mustermann*; gefunden werden.
- Suche nach allen Personen deren Name auf eine bestimmten Zeichenkette endet: Hierzu darf nur der Nachname (z.B. *Mustermann*) spezifiziert werden. In diesem Beispiel würde die Suche nach dem Nachnamen *Mustermann* alle Personen mit dem Nachnamen *Mustermann* zurückliefern, da das Programm automatisch nach **Mustermann* sucht.
- Suche nach einem Zertifikat mit einer bekannten Seriennummer: Die Eingabe von *123456* im Feld *Seriennummer* würde nach einem Zertifikat mit der Seriennummer 123456 suchen. Durch Setzen des Häkchens "hexadezimal" wird die Eingabe als Hexadezimalzahl interpretiert.

2.1.1. Hinweise

Manche LDAP-Dienste verwalten die Seriennummer als numerisches Feld. Bei solchen Feldern wird serverseitig das Verwenden von Platzhaltern nicht unterstützt (z.B. beim LDAP-Dienst der A-Trust).

LDAP-Dienste unterscheiden grundsätzlich nicht nach Groß- und Kleinschreibung.

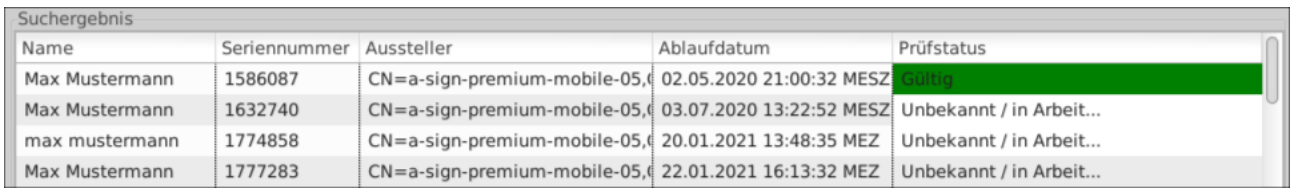
Bitte beachten Sie weiters, dass eine LDAP-Abfrage, abhängig von der Anzahl der Ergebnisse und der Geschwindigkeit der Internetverbindung eine längere Zeit in Anspruch nehmen kann. Versuchen Sie bitte daher, die Suchparameter so exakt wie möglich zu definieren.

Es müssen zumindest insgesamt drei Buchstaben in den Feldern Vorname und Nachname oder ein Zeichen in das Feld Seriennummer eingegeben werden, um über die Maßen langwierige Suchanfragen zu verhindern.

Die Liste der konfigurierten LDAP-Dienste kann im Menüpunkt *Konfiguration → Bearbeiten* angepasst werden (siehe Konfiguration).

2.2. Suchergebnisse

Das Ergebnis von Suchanfragen wird unterhalb der Eingabefelder in tabellarischer Form dargestellt.


Suchergebnis

Name	Seriennummer	Aussteller	Ablaufdatum	Prüfstatus
Max Mustermann	1586087	CN=a-sign-premium-mobile-05,(	02.05.2020 21:00:32 MESZ	Gültig
Max Mustermann	1632740	CN=a-sign-premium-mobile-05,(	03.07.2020 13:22:52 MESZ	Unbekannt / in Arbeit...
max mustermann	1774858	CN=a-sign-premium-mobile-05,(	20.01.2021 13:48:35 MEZ	Unbekannt / in Arbeit...
Max Mustermann	1777283	CN=a-sign-premium-mobile-05,(	22.01.2021 16:13:32 MEZ	Unbekannt / in Arbeit...

In den Spalten werden der Reihe nach Name des Antragstellers, die Seriennummer des Zertifikats, der Aussteller, das Ablaufdatum, sowie das Prüfergebnis angezeigt. Letzteres wird jedoch nur

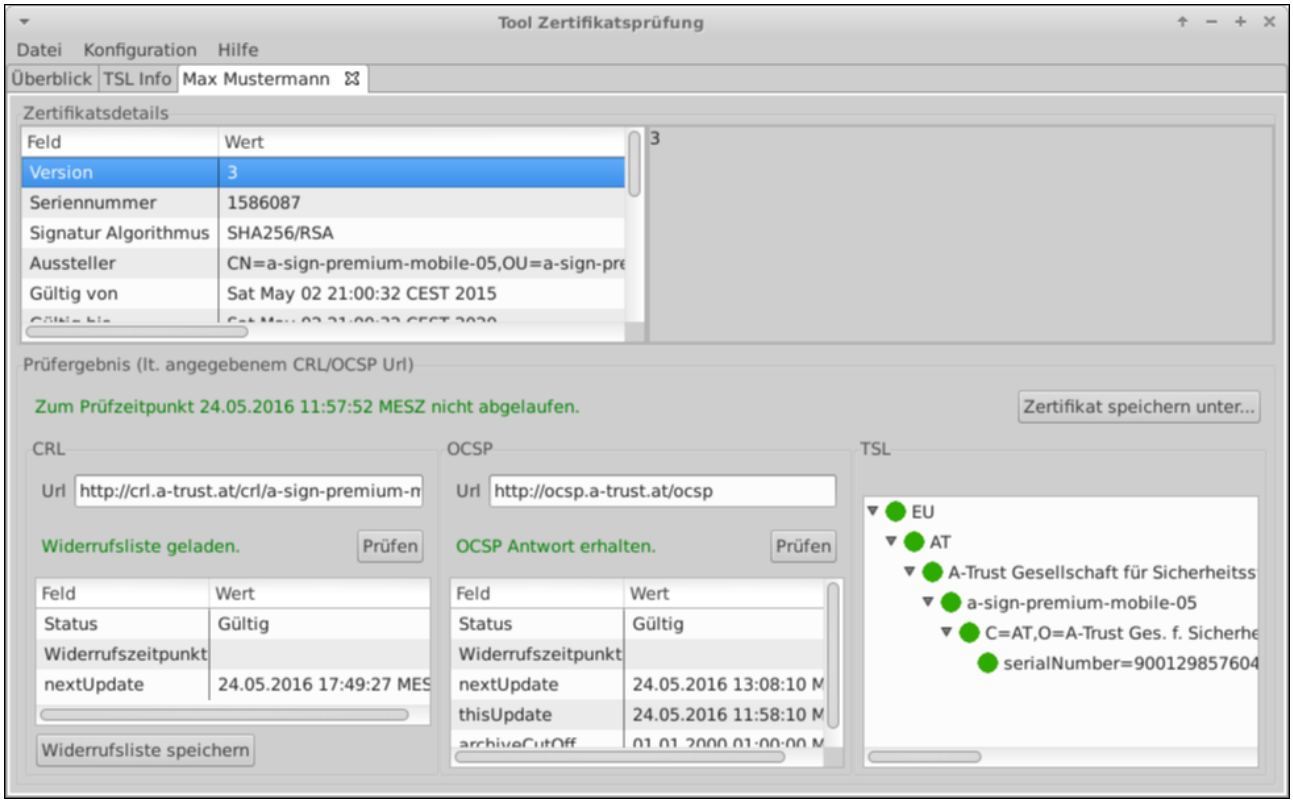
angezeigt, falls die automatische Zertifikatsprüfung aktiviert ist. Diese Einstellung kann über den Menüpunkt Konfiguration → Einstellungen geändert werden.

Ein Doppelklick auf ein Suchergebnis öffnet die Detailansicht, welche ausführliche Informationen über das ausgewählte Zertifikat enthält (siehe Statusabfrage und Details von Zertifikaten).

3. Statusabfrage und Details von Zertifikaten

Der Status eines Zertifikates wird automatisch durch einen Doppelklick auf das Zertifikat im Suchergebnis (siehe Suche) geprüft. Alternativ kann ein Zertifiakt über *Datei → Zertifikat öffnen…* aus einer Datei geladen und überrüft werden. Das Ergebnis bezieht sich dabei auf jenen Zeitpunkt, der als Prüfzeitpunkt angegeben wurde. Zusätzlich werden CRL– und OCSP-Informationen abgefragt sowie eine Verifikation basierend der EU *Trusted Lists of Certification Service Providers* (TSL) (siehe TSL) durchgeführt. Bitte beachten Sie, dass es nicht sinnvoll ist, Prüfungen für zukünftige Zeitpunkte durchzuführen, da insbesondere CRL– und/oder OSCP-Informationen nicht verfübar sein könnten.

Ob ein Zertifikat als gültig angesehen wird, hängt von mehreren Faktoren ab. Tatsächlich werden zwei voneinander getrennte Verifikationsprozesse ausgeführt: Zum einen werden die manuell konfigurierbaren Trust Anchor (siehe Konfiguration) herangezogen; nachdem diese immer manuell konfiguriert werden können, ist es auch möglich bereits abgelaufene Ausstellerzertifikate für eine Verifikation heranzuziehen.
Zusätzlich wird unabhängig davon eine Verifikation auf Basis der EU Trusted Lists of Certification Service Providers durchgeführt. Daher kann es zu widersprüchlichen Resultaten kommen.



Wie in der obigen Abbildung ersichtlich, werden Zertifikatsdetails in Form einer interaktiven Tabelle dargestellt. Durch einen Klick auf eine Zeile, kann der Wert eines Attributs im Detail eingesehen werden. Unterhalb dieser Tabelle wird der Gültigkeitsstatus des Zertifikats angezeigt.

3.1. CRL Informationen

Sofern CRL Informationen verfügbar sind werden diese im Detail angezeigt:

- **Status:** Gibt Aufschluss über den Widerrufsstatus des Zertifikats.

- **Widerrufszeitpunkt:** Falls das Zertifikat Widerrufen wurde, wird der Widerrufszeitpunkt hier angezeigt.
- **nextUpdate:** Gibt den spätestmöglichen Zeitpunkt an, zu dem vom Zertifizierungsdiensteanbieter eine neue Widerrufsliste herausgegeben wird. Gleichzeitig endet damit auch die Gültigkeit der aktuellen Widerrufsliste.

Weiters kann die verwendete Widerrufsliste durch einen Klick auf den Button *Widerrufsliste speichern* lokal gespeichert werden. Zusätzlich kann auch manuell eine URL angegeben werden, über die eine Widerrufsliste bezogen werden soll.

3.2. OCSP Informationen

- **Status:** Gibt Aufschluss über den Widerrufsstatus des Zertifikats.
- **Widerrufszeitpunkt:** Falls das Zertifikat widerrufen wurde, scheint hier der Widerrufszeitpunkt auf.
- **nextUpdate:** Gibt den spätestmöglichen Zeitpunkt an, ab dem neue Statusinformationen verfügbar sein werden.
- **thisUpdate:** Gibt den Zeitpunkt an, für den die erhaltene Statusinformation gültig ist.
- **archiveCutOff:** Gibt den frühestmöglichen Zeitpunkt an, für den Widerrufsinformationen verfügbar sind.

Die zur Prüfung verwendete CRL– und OCSP-URL wird aus dem zu prüfenden Zertifikat ausgelesen. Sollten im Zertifikat keine URLs gegeben sein, werden die URLS (falls vorhanden) aus der Konfiguration entnommen. Zusätzlich ist es auch hier möglich, manuell eine OCSP-URL einzugeben.

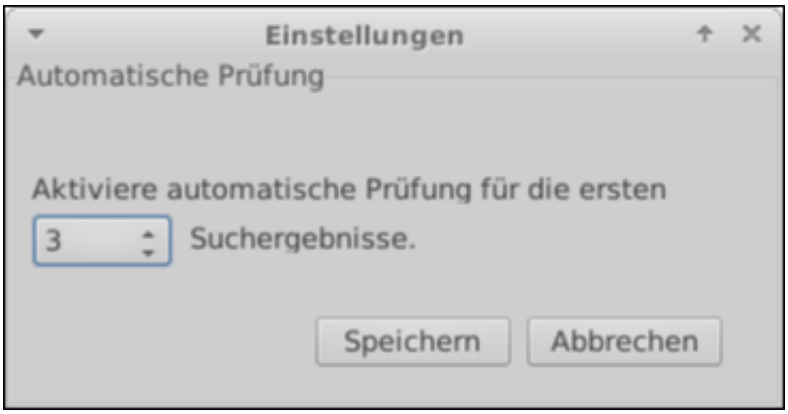
3.3. TSL-basierte Verifikation

Parallel zur Verifikation auf Basis manuell konfigurierter Trust-Anchor, wird auch TSL-basierte Verifikation unterstützt. Um die Gültigkeit eines Zertifikats basierend auf TSL-Informationen zu ermitteln, werden folgende Schritte durchgeführt:

1. Der Status der EU Toplevel-TSL wird auf Basis festgelegter EU-Trust-Anchor ermittelt.
2. der Vertrauensstatus des Landes, für welches das zu Prüfende Zertifikat ausgestellt wurde, wird auf Basis der Toplevel-TSL ermittelt.
3. Die Gültigkeitsperiode des zu prüfenden Zertifikats wird (ohne CRL– und OCSP-Status) ermittelt.
4. Die Ausstellerinformation wird aus dem Zertifikat ausgelesen.
5. Die Gültigkeitsperiode des Ausstellerzertifikat wird ermittelt (inklusive CRL– und OCSP-Status).
6. Der Vertrauensstatus des Ausstellerzertifikats wird auf Basis der EU Trusted Lists of Certification Service Providers und der darin deklarierten vertrauenswürdigen Services geprüft.
7. Ein Service wird als gültig bzw. vertrauenswürdig angesehen, wenn zumindest eines der zugehörigen Zertifikaten gültig bzw. vertrauenswürdig ist.
8. Ein Serviceprovider wird als gültig bzw. vertrauenswürdig anerkannt, wenn zumindest einer der zugehörigen Services gültig bzw. vertrauenswürdig ist.

Aus dieser Prüfstrategie ergibt sich eine Vertrauenskette ausgehend von der EU Toplevel-TSL bis hin zum zu prüfenden Zertifikat. Ein grüner Indikator signalisiert, dass ein Glied der Kette vertrauenswürdig/gültig ist, wohingegen rot Ungültigkeit bzw. nicht gegebener Vertrauenswürdigkeit entspricht. Knoten, welche Zertifikaten entsprechen, können mittels Doppelklick im Detail betrachtet werden. Die entsprechenden Zertifikatsdetails werden in einem separaten Fenster angezeigt. Dort besteht die Möglichkeit das angezeigte Zertifikat zu speichern.

3.1. Automatische Zertifikatsprüfung



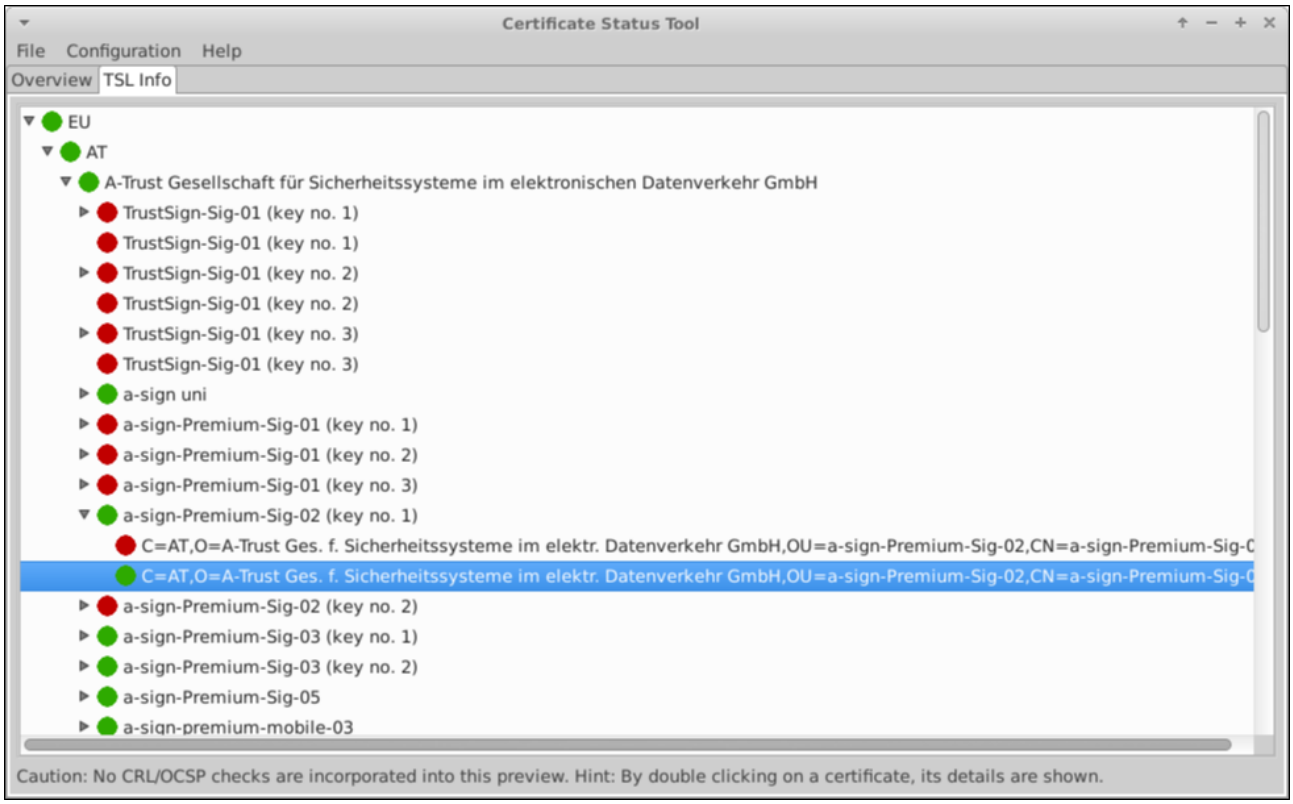
Durch einen Klick auf Konfiguration → Einstellungen kann ausgewählt werden, ob eine automatische Prüfung der ersten 3/10/20 Suchergebnisse erfolgen soll. Dabei wird zu den Suchergebnissen der Prüfstatus des Zertifikates angezeigt, sobald dieser ermittelt wurde. Standardmäßig ist die automatische Prüfung nicht aktiviert.

Hinweise: Bitte beachten Sie, dass die automatische Prüfung der Zertifikate einige Zeit in Anspruch nehmen kann. Besonders, wenn im Hintergrund aktuelle TSL-Informationen abgerufen werden (siehe TSL), kann es einige Zeit dauern, bis Ergebnisse angezeigt werden.

4. EU Trusted Lists of Certification Service Providers

Das Zertifikatsstatustool unterstützt Zertifikatsprüfung auf Basis der von der europäischen Kommission herausgegebenen TSL (siehe Statusabfrage und Details von Zertifikaten).

Um zusätzliche Informationen über den Status und die Struktur der EU TLS bereitzustellen, verfügt das Zertifikatsstatustool über eine interaktive Visualisierung der TSL-Struktur.



Die TSL Baumstruktur besteht (ausgehend von der EU Toplevel-TSL) aus folgenden Ebenen:

1. Land

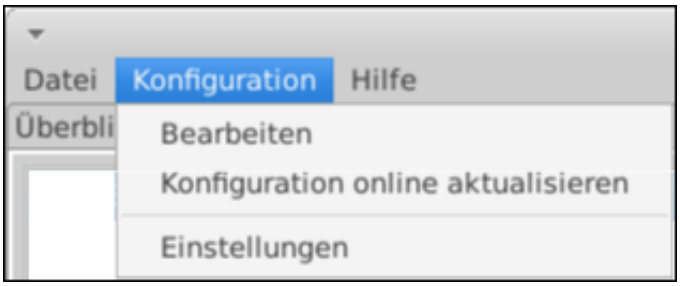
2. Service Provider
3. Service
4. Zertifikat

Der Algorithmus zu Ermittlung des Gültigkeits– bzw. Vertrauensstatus' einzelner Knoten ist unter TSL-basierte Verifikation beschrieben. Knoten, welchen ein Zertifikat zu Grunde liegt, können mittels Doppelklick im Detail betrachtet werden. Die entsprechenden Zertifikatsdetails werden in einem neuen Fenster angezeigt, von dem aus das Zertifikat auch gespeichert werden kann.

Um stets über aktuelle TSL-Informationen zu verfügen wird bei jedem Programmstart ein Update durchgeführt. Besonders beim ersten Start des Zertifikatsstatustools kann dies einige Zeit in Anspruch nehmen. Tatsächlich wird jedoch bei jedem Programmstart eine vollständige Validierung aller Information durchgeführt. Währenddessen kann es zu Verzögerungen oder Timeouts während Zertifikatsprüfungen kommen. TSL-Updates sind nicht darauf ausgelegt, unterbrochen zu werden. Daher ist auch keine Möglichkeit vorgesehen diesen Prozess zu unterbrechen. Aus diesem Grund kann sich auch das Beenden des Zertifikatsstatustools verzögern.

5. Konfiguration und Online-Update

Das Zertifikatsstatustool kann für die Suche in LDAP-Verzeichnissen und die Prüfung von bestimmten Widerrufsdiensten vorkonfiguriert werden.



Die in der obigen Abbildung dargestellten Menüpunkte haben folgende Funktionen:

- **Bearbeiten:** Hier können die konfigurierten Dienste eingesehen bzw. bearbeitet werden.
- **Konfiguration online aktualisieren:** Die Auswahl dieses Menüpunkts führt eine Online-Aktualisierung aller konfigurierten Dienste durch. Im Zuge dessen werden auch alle Trust Anchor aktualisiert. Dieser Vorgang überschreibt alle Einstellungen!
- **Einstellungen:** Hier kann die automatische Signaturprüfung aktiviert bzw. konfiguriert werden.

5.1. Konfigurationsdateien

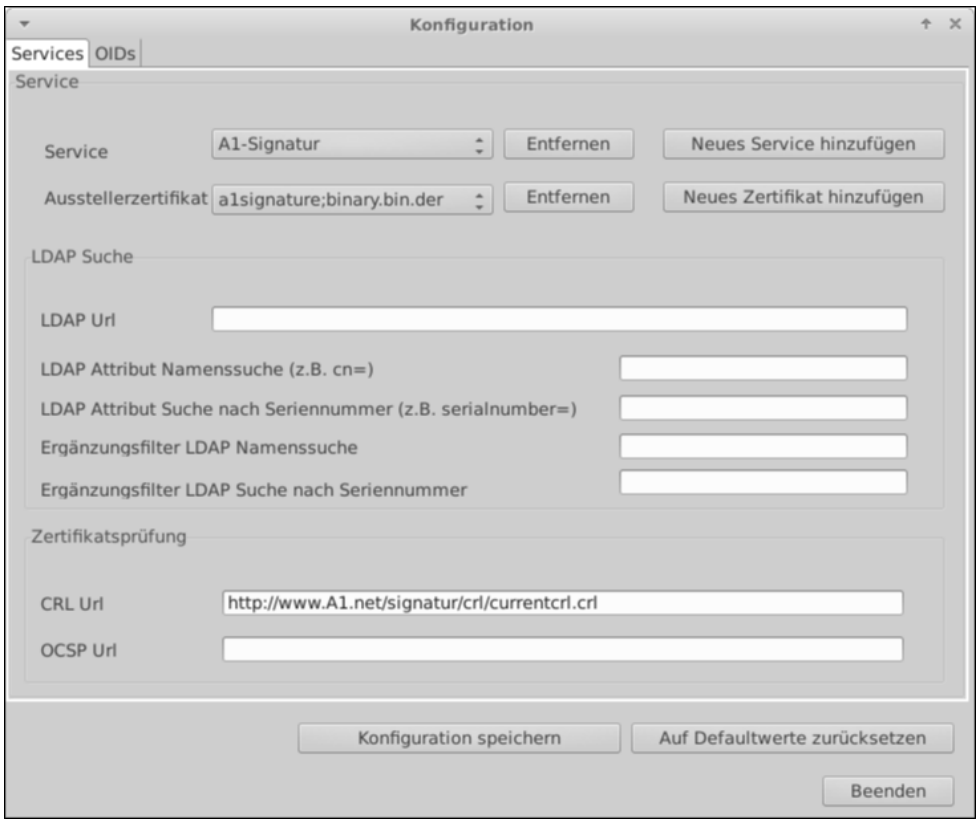
Die Konfiguration besteht aus einer lokalen Komponente (Datei localConfig.properties im Verzeichnis .asitCertStatus ausgehend vom Benutzerverzeichnis), welche über den Menüpunkt *Bearbeiten*; angepasst werden kann, sowie einer Default-Konfiguration, welche alle vorkonfigurierten Einträge enthält. Die Default-Konfiguration kann z.B. für eine organisationsweite zentrale Konfiguration verwendet werden. Sie wird beim Online-Update vom Server geladen und lokal als Kopie abgespeichert. Die Quelle des Online-Updates kann in der Default-Konfiguration angepasst werden. Das Vorhandensein aller Standardwerte ermöglicht es, die Konfiguration jederzeit zurückzusetzen und etwaige Änderungen zu verwerfen.

5.2. Konfiguration Anpassen

Ein umfassender Konfigurationsdialog kann über den Menüpunkt *Konfiguration → Bearbeiten* erreicht werden.

5.2.1. Konfigurieren von Diensten

Der erste Tab des Konfigurationsdialogs ermöglicht die Verwaltung von Trust Anchor und Verzeichnisdiensten.



Die einzelnen konfigurierten Dienste werden in der Liste rechts von *Service* angezeigt.

Für jeden einzelnen Dienst können folgende Eigenschaften definiert werden (bitte beachten Sie, dass zumindest das Ausstellerzertifikat und ein Name angegeben werden müssen):

- **LDAP Url:** Hier wird die URL des LDAP-Verzeichnisdienstes angegeben. Diese muss mit ldap:// beginnen. Wird keine LDAP-URL spezifiziert, so wird dieser Dienst nicht für die Suche herangezogen.
- **Ausstellerzertifikat:** Hier scheinen die mit dem Dienst assoziierten Zertifikate (Trust Anchor) auf. Zertifikate können über den Button *Neues Zertifikat hinzufügen* importiert werden. Dabei werden die Dateien in das Verzeichnis *.asitCertStatus/certificates* im Benutzerverzeichnis kopiert. Um die Prüfung von Zertifikaten mittels OCSP zu ermöglichen, muss das Ausstellerzertifikat des zu prüfenden Zertifikats vorhanden sein. Zusätzliche Zertifikate (sogenannte Backup-Zertifikate) sind optional. Im Falle eines Ausfalls des Hauptsystems, werden neue Zertifikate mit einem Backup-Zertifikat ausgestellt. Um einen reibungslosen Ablauf bei der Zertifikatsprüfung zu gewährleisten, wird empfohlen, Backup-Zertifikate (falls vorhanden) hinzuzufügen. Um ein Ausstellerzertifikat zu löschen, markieren Sie den Eintrag des jeweiligen Zertifikates in der Liste und klicken Sie auf *Entfernen*.
- **LDAP Attribut Namenssuche:** Hier wird die Bezeichnung des LDAP-Feldes, welches den Namen zu suchender Personen enthält eingegeben, gefolgt von dem Zeichen =. In den meisten Fällen wird liefert *cn*= die gewünschten Resultate.
- **Ergänzungsfilter LDAP-Namenssuche:** Hier kann ggf. eine Zeichenkette angegeben werden, welche an den Suchstring angehängt werden soll, wenn nach dem Namen eine Person gesucht wird. Beispiel: würde hier *Meier* angegeben, so würde eine Suche nach dem Namen *Max Mustermann* den LDAP-Suchfilter *cn=MaxMustermannMeier* erzeugen. In den meisten Fällen kann dieses Feld leer gelassen werden. Im Fall der E-Card Verwaltungsignatur ist es jedoch notwendig *SER** angegeben, da im Namensfeld zusätzlich die Zeichenkette *SER:* und die Zertifikatsseriennummer kodiert sind.
- **LDAP Attribut Seriennummernsuche:** In diesem Feld kann die Bezeichnung des LDAP-Feldes, welches die Seriennummer des zu suchenden Zertifikates enthält, festgelegt

werden. Diese muss von dem Zeichen = gefolgt werden. In vielen Fällen führt*serialNumber*= oder *serial*= zum gewünschten Ergebnis.

- **Ergänzungsfilter LDAP-Seriennummernsuche:** Analog zur LDAP-Namenssuche kann hier ein zusätzlicher String angegeben werden, welcher bei der Suche nach Seriennummern an den Suchstring angehängt wird.
- **CRL Url:** In diesem Feld kann eine URL zur aktuellen Widerrufsliste angegeben werden. Es darf sich dabei nicht um eine Delta-CRL handeln. Die URL muss mit ldap:// oder http:// beginnen.
- **OCSP Url:** Hier kann die URL eines OCSP Services angegeben werden. Die URL muss mit http:// beginnen.

Änderungen werden nach dem Speichern (Button *Konfiguration speichern*) wirksam.

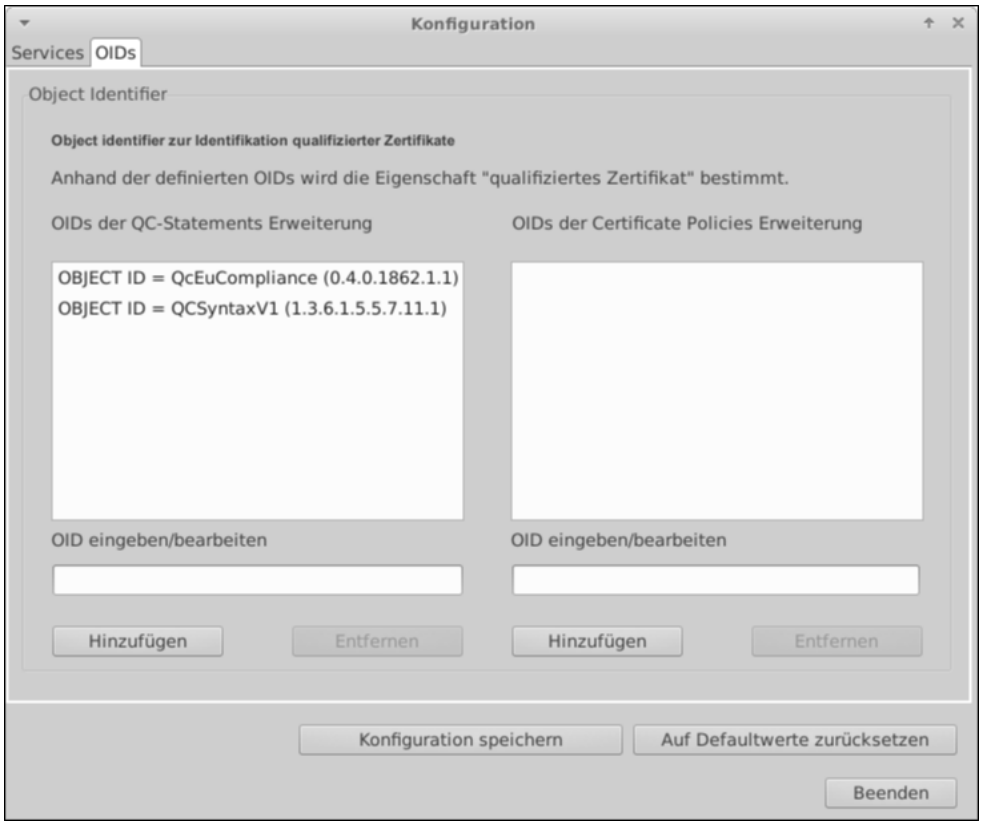
Mit einem Klick auf *Auf Defaultwerte zurücksetzen* können die Einstellungen aus der zentralen Konfigurationsdatei für das aktuelle Service geladen werden.

Mit dem Button *Neues Service hinzufügen* wird ein neues Service in der Liste angelegt, mit dem Button *Entfernen* wird das momentan in der Liste markierte Service gelöscht.

Hinweis: Wird ein LDAP-Service konfiguriert, muss zumindest das LDAP-Attribut für die Namenssuche und die Seriennummernsuche definiert werden.

5.2.2. OID Einstellungen

über den Tab *OIDs* können OIDs konfiguriert werden, welche Zertifikate als qualifizierte Zertifikate ausweisen.



Zertifikate, welche zumindest einen der hier angegebenen OIDs in der *Qualified Certificate Statements*-Zertifikatserweiterung bzw. in der *Certificate Policies*-Zertifikatserweiterung enthalten, werden als qualifizierte Zertifikate betrachtet. Bitte beachten Sie, dass es sich dabei um eine Angabe des Zertifikatsausstellers handelt, welche nicht überpüft wird. Neue OIDs können im entsprechenden Feld eingegeben werden und mit einem Klick auf den zugehörigen *Hinzufügen*-Button hinzugefügt werden. Bestehende OIDs können auf dieselbe Art bearbeitet werden,

nachdem sie ausgewählt wurden. Durch einen Klick auf den entsprechenden *Entfernen*-Button können ausgewählte OIDs auch entfernt werden.

Änderungen werden sofort wirksam. Die Änderungen werden jedoch nur dann permanent gespeichert, wenn der Button *Konfiguration Speichern* betätigt wird.

6. Lizenzbedingungen

7. Referenzen

[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.