



Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
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

GROBSPEZIFIKATION V.0.7.1 ZUM A-SIT ZERTIFIKAT STATUS TOOL (4.093)

Autor – Thomas.Aichinger@a-sit.at, 08.06.2006

Kurzfassung - Grobspezifikation einer Applikation, welche das einfache Abfragen und Anzeigen von Status- bzw. Widerrufsinformationen von Zertifikaten (insbesondere jene, welche bei Bürgerkarten eingesetzt werden) ermöglicht. Es soll eine Suche nach Personen und Seriennummern über eine Reihe (vorkonfigurierter) Zertifizierungsdienste möglich sein. Die Liste der Zertifizierungsdienste ist erweiterbar.

Inhaltsverzeichnis

Inhaltsverzeichnis	1
1. Kurzbeschreibung	2
2. Funktionsweise	2
2.1. Abfrage	2
2.2. Konfiguration	3
2.2.1. automatisch	3
2.2.2. benutzerdefiniert	3
3. Funktionen im Detail	3
3.1. Suchparameter	3
3.2. Statusinformation	4
3.3. Konfigurierbare „Koordinaten“ der Zertifizierungsdienste	4
4. Plattform	5
5. Referenzen	5

1. Kurzbeschreibung

Als Ergänzung zu den vorhandenen Bürgerkartentools soll ein Tool zum Abfragen von Zertifikatsstatusinformationen entwickelt werden.

Mit diesem Tool kann der Status von Zertifikaten der konfigurierten Zertifizierungsdienste auf einfache Weise bestimmt und angezeigt werden. Mittels Seriennummer und/oder Personendaten (Vorname, Nachname) wird das Zertifikat übergreifend in den öffentlichen Verzeichnissen der ZDAs bzw. in den Widerrufslisten gesucht.

Der Prüfzeitpunkt, für welchen die Statusinformation angezeigt werden soll, kann angegeben werden.

Zu dem gewählten Zertifikat wird der Status bzw. die Widerrufsinformationen (Grund, Zeitpunkt) angezeigt. Weiters werden die Art des Zertifikates (qualifiziert, einfaches Zertifikat, und ggf. Zusatzinformationen) und auf Wunsch das Zertifikat selbst angezeigt.

Die Verzeichnisdienste, Widerrufslisten und Root-Zertifikate der bestehenden Bürgerkarten sind vorkonfiguriert, weitere können über eine Online-Update Funktion nachgeladen werden.

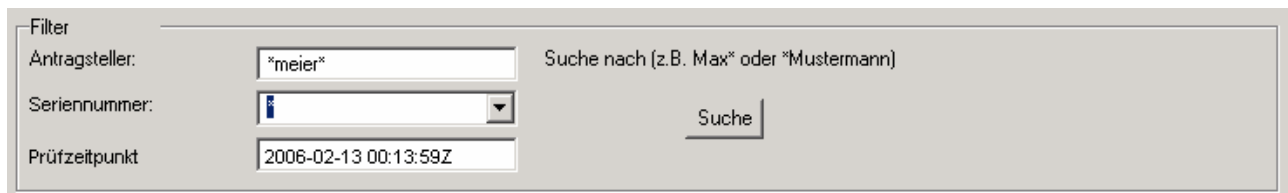
2. Funktionsweise

2.1. Abfrage

1) Starten des Tools

2a) Suche nach Personen (Antragsteller), Unterstützung der LDAP-Wildcards) oder

2b) Suche nach Seriennummer (zur Auswahl: hexadezimale oder dezimale Eingabe)



Filter

Antragsteller: Suche nach (z.B. Max* oder *Mustermann)

Seriennummer:

Prüfzeitpunkt:

Für die Prüfung von Zertifikaten (nicht für die Prüfung von Seriennummern) kann der Prüfzeitpunkt angegeben werden, auf welchen sich die angezeigte Statusinformation bezieht.

3) Anzeige der Suchergebnisse in einer Liste (sortiert nach ZDA, dann nach Seriennummer)

Name	Aussteller
Alexander Tampermeier 135	CN=TrustMark-VSC-01,OU=TrustMa
Alexander Tampermeier 179	CN=TrustMark-VSC-01,OU=TrustMa
Alexander Tampermeier 184	CN=TrustMark-VSC-01,OU=TrustMa
Alexander Tampermeier 198	CN=TrustMark-VSC-01,OU=TrustMa
Alexander Tampermeier 247	CN=TrustMark-VSC-01,OU=TrustMa
Alexander Tampermeier 4671	CN=TrustMark-VSC-01,OU=TrustMa
Alfred Schmidmeier 108484	CN=a-sign-Premium-Enc-02,OU=a-sign-Pn
Alois MEIER 2230	CN=TrustMarkToken-Enc-01,OU=Tr
Andreas Meier 109654	CN=a-sign-Premium-Enc-02,OU=a-sig
Angelika Meier 12240	CN=TrustMarkToken-Enc-01,OU=Tr
Anton Hintermeier 117393	CN=a-sign-Premium-Enc-02,OU=a-sig
Anton Hintermeier 97923	CN=a-sign-Premium-Enc-02,OU=a-sig

Die Sortierung kann durch Anklicken der Tabellen-Überschrift geändert werden.

- 4) ggf. Auswahl des gewünschten Zertifikates
- 5) Anzeige der Statusinformationen (siehe Kapitel 3.2)
- 6) ggf. Anzeige des OID gemäß [OID]
- 7) Auf Wunsch: Anzeige des Zertifikats im Zertifikatsviewer, lokales Abspeichern möglich.

2.2. Konfiguration

2.2.1. Automatisch

In der Applikation wird ein Menüpunkt vorgesehen, mit welchem die automatische Update-Funktion aufgerufen werden kann (Online Update).

Beim Online-Update werden die Konfigurationsdatei sowie die Aussteller-Zertifikate der Zertifizierungsdienste aktualisiert. A-SIT stellt dazu auf seiner Homepage die erforderlichen Dateien bereit.

2.2.2. Benutzerdefiniert

Die Konfiguration kann durch Editieren einer lokalen Konfigurationsdatei (JAVA-Properties-File) und das Hinzufügen von Aussteller-Zertifikaten erweitert werden.

3. Funktionen im Detail

3.1. Suchparameter

Grundsätzlich kann nach Namen und/oder Seriennummern gesucht werden. Bei der Seriennummer kann zwischen dezimaler und hexadezimaler Eingabe umgeschaltet werden. Übliche Platzhalterzeichen (z.B. *) können vor, nach und im Namen verwendet werden.

Es wird immer über alle konfigurierten Zertifizierungsdienste gesucht.

Bei A-TRUST und Hauptverband: Zertifikate werden anhand des Namens und/oder der Seriennummer im LDAP-Verzeichnis gesucht.

Bei der A1 Signatur: Hier wird überprüft, ob die angegebene Zertifikatsseriennummer in der aktuellen Widerrufsliste aufscheint. Es ist keine Zertifikatssuche möglich (Anm. Es gibt keinen durchsuchbaren Verzeichnisdienst).

Es kann weiters der Zeitpunkt angegeben werden (default: aktueller Zeitpunkt) auf welchen sich die Statusinformation bei der Zertifikatsprüfung beziehen soll (z.B. Bestimmung ob das Zertifikat zu einem bestimmten Zeitpunkt in der Vergangenheit widerrufen war). Bei der Prüfung der Seriennummern bleibt das Feld „Prüfzeitpunkt“ unberücksichtigt.

3.2. Statusinformation

Die ZDAs bieten unterschiedliche Dienste (LDAP, CRL, OCSP) an. Die verwendbare Statusinformation ist daher von der Art der bereitgestellten Dienste bzw. der daraus extrahierbaren Informationen abhängig.

Aus der Kombination der Antworten der abgefragten Services wird die Statusantwort generiert, welche dem Benutzer angezeigt wird:

Diese kann daher lauten:

- „Das Zertifikat war zum Prüfzeitpunkt nicht widerrufen.“
- "Das Zertifikat ist zum Prüfzeitpunkt widerrufen." Anschließend wird der Grund für den Widerruf (sofern vom Widerrufsdiensnt angegeben) angezeigt.
- "Unbekannt": Der Status des Zertifikates kann nicht bestimmt werden. Dieser Fall sollte nur bei Fehlkonfigurationen des Online-Services auftreten.
- "Das Zertifikat ist zum Prüfzeitpunkt noch nicht gültig.": Der Prüfzeitpunkt liegt vor dem Gültigkeitszeitraum des Zertifikates.
- "Das Zertifikat ist zum Prüfzeitpunkt bereits abgelaufen.": Der Prüfzeitpunkt liegt nach dem Gültigkeitszeitraum des Zertifikates.
- "Aus dem Zertifikat konnten keine Daten eines Widerrufsservices gelesen werden. Keine CRL oder OCSP Url angegeben.": Für das Zertifikat ist kein Prüfservice vorkonfiguriert und auch im Zertifikat selbst konnte keine Angabe eines Prüfservices gefunden werden. Der Status des Zertifikates kann daher nicht bestimmt werden.
- "Die Seriennummer ist auf keiner der konfigurierten Widerrufslisten."
- "Die Seriennummer ist auf einer der konfigurierten Widerrufslisten." unter Angabe von Widerrufszeitpunkt und –grund.
- "Die Seriennummer ist auf mehreren der konfigurierten Widerrufslisten." unter Angabe der Widerrufszeitpunkte und –gründe.

Verwendete Informationsquellen der Zertifizierungsdienste:

LDAP: Zertifikat zu Seriennummer / Name existiert / oder existiert nicht.

OCSP: good (nicht revoked), revoked, unknown. Widerrufszeitpunkt und –grund, soweit diese Informationen zur Verfügung gestellt werden.

CRL: nicht widerrufen, widerrufen. Widerrufszeitpunkt und -grund, soweit diese Informationen zur Verfügung gestellt werden.

3.3. Konfigurierbare „Koordinaten“ der Zertifizierungsdienste

Die Konfigurationsdaten werden in zwei lokalen Konfigurationsdateien (Standard JAVA-„Properties“- Dateien abgelegt.

Für jeden Zertifizierungsdienst gibt es (pro Issuer-Zertifikat) folgende Einträge:

- Issuer-Zertifikat: CN („primary key“), Filename
- Verzeichnisdienst: none | LDAP-URL
- CRL: none | URL
- OCSP: none | URL
- Typ: optional zusätzliche Beschreibung
- Friendly Name (muss nicht eindeutig sein)

Es gibt zwei Konfigurationsdateien - eine benutzerdefinierbare und eine, welche die vorkonfigurierten Zertifizierungsdienste enthält. Die benutzerdefinierbare Datei ergänzt bzw. „overrult“ (falls sie sich auf einen bereits vorhandenen Zertifizierungsdienst – CN des Issuer Zertifikates bezieht) die vorkonfigurierten Einträge. Die vorkonfigurierte Datei kann mit Hilfe der Online-Update Funktion aktualisiert werden.

4. Plattform

Die Applikation wird als Standalone-Applikation unter JAVA 1.5 entwickelt.

Als Security-Provider (Zertifikatshandling, OCSP, ...) wird JCE 3.14 verwendet.

Für den Betrieb ist eine Online-Verbindung zu den konfigurierten ZDAs (Verzeichnisdienst, Widerrufsliste, OCSP, ...) erforderlich.

5. Referenzen

Folgende Standards/Normen werden verwendet:

[LDAP] „LDAP standards and documents“, abgerufen am 13.02.2006 unter <http://www.mozilla.org/directory/standards.html>

[OCSP] „RFC 2560“, June 1999, abgerufen am 13.02.2006 unter <ftp://ftp.rfc-editor.org/in-notes/rfc2560.txt>

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

[RFC3280] „RFC 3280“, April 2002, abgerufen am 13.02.2006 unter <ftp://ftp.rfc-editor.org/in-notes/rfc3280.txt>

[x509ext – 1.0.3] Arno Hollosi, „X.509 Zertifikatserweiterungen für die Verwaltung“, 2005-02-21, abgerufen unter <http://www.quetesiegel.gv.at/criteria/X509ext-1.0.3-20050221.pdf>