

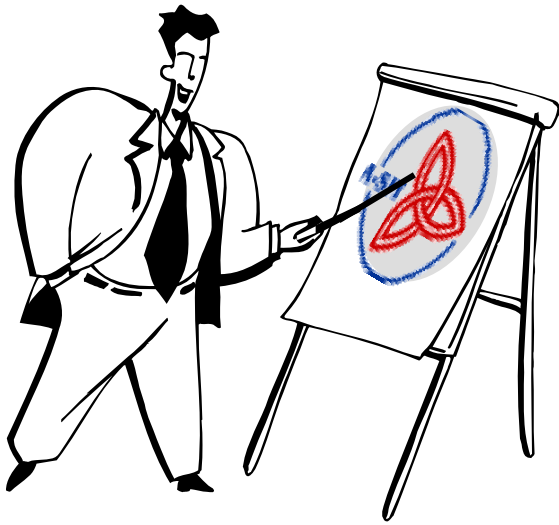
# Signatur- und Zertifikatsprüfung in der Praxis

ADV Tagung

Elektronische Signatur – Der Weg in die  
Praxis

21.11.2006

# Agenda



- Grundlagen zur Signaturprüfung
- Erkennen verschiedener Signaturqualitäten
- Berufsgruppensignaturen

# About A-SIT

- 1999 als gemeinnütziger Verein gegründet

- Mitglieder:

- Bund (BMF)



- OeNB



- TU-Graz

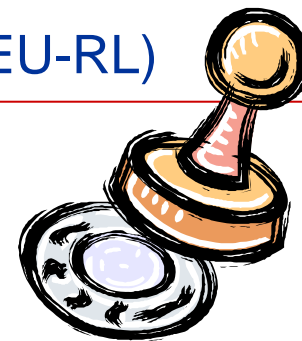


# Aktivitäten

- **Technische Evaluierungen**
  - Bestätigungsstelle nach SigG
  - Akkr. Überwachungsstelle nach ISO/IEC 17020
- **Unterstützung für öffentliche Stellen**
  - Konzept Bürgerkarte
  - Österr. IT-Sicherheitshandbuch
- **Beobachtung bestehender und aufkommender Technologien**
  - Technologiebeobachtung am Standort Graz
  - Mitwirkung in Normungsgremien (W3C, Common Criteria, ETSI, ON, ...)
- **Beiträge zur Stärkung des IT-Sicherheitsbewusstseins**
  - Dokumente und Publikationen
  - Veranstaltungen
- Mehr: [www.a-sit.at](http://www.a-sit.at)



# Bestätigungsstelle (§ 19 SigG, Art. 3 Abs. 4 EU-RL)



- A-SIT ist erste und derzeit einzige österr. Bestätigungsstelle (BGBl II 2000/31)
- Notifizierung bei europ. Kommission  
=> int. Anerkennung
- Aufgaben und Leistungen:
  - Bescheinigungen nach § 18 Abs. 5 SigG
  - Unterstützung der Aufsichtsstelle in technischen Belangen (§ 15 Abs. 3 SigG)
  - Sonst. Bestätigungen, Gutachten
  - Technologiebeobachtung  
=> Empfohlene Algorithmen und Parameter für el. Signaturen (gem. mit RTR GmbH)

# Signaturprüfung – rechtl. Grundlagen (EU)

EU-Richtlinie (1999/93/EC) – Empfehlungen für die sichere Signaturprüfung:

Während des Signaturprüfungsvorgangs ist mit hinreichender Sicherheit zu gewährleisten, dass

- a) die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden,
- b) die Signatur zuverlässig überprüft wird und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
- c) der Überprüfer bei Bedarf den Inhalt der unterzeichneten Daten zuverlässig feststellen kann,
- d) die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden,
- e) das Ergebnis der Überprüfung sowie die Identität des Unterzeichners korrekt angezeigt werden,
- f) die Verwendung eines Pseudonyms eindeutig angegeben wird, und
- g) sicherheitsrelevante Veränderungen erkannt werden können.



# Signaturprüfung – rechtl. Grundlagen (A)



SigG § 18 Abs. 4:

Für die Überprüfung von sicher signierten Daten sind solche technische Komponenten und Verfahren anzubieten, die sicherstellen, dass

1. die signierten Daten nicht verändert worden sind,
2. die Signatur zuverlässig überprüft und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
3. der Überprüfer feststellen kann, auf welche Daten sich die elektronische Signatur bezieht,
4. der Überprüfer feststellen kann, welchem Signator die elektronische Signatur zugeordnet ist, wobei die Verwendung eines Pseudonyms angezeigt werden muss, und
5. sicherheitsrelevante Veränderungen der signierten Daten erkannt werden können.

# Signaturprüfung – rechtl. Grundlagen (A)



## Anforderungen an ZDA (qual. Zertifikate):

- Auf Ersuchen von Gerichten oder anderen Behörden hat ein Zertifizierungsdiensteanbieter die Prüfung der auf seinen qualifizierten Zertifikaten beruhenden sicheren Signaturen vorzunehmen. (SigG § 7 Abs. 6)
- Information des Signators über techn. Komponenten und Verfahren bzw. Methode der Signaturprüfung (SigG § 20 Abs. 3, SigV § 15 Abs. 1 Z. 19)



# Prüfprozess

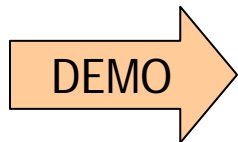
- Prüfen der Signatur



- Prüfen des Zertifikats



- Ggf. Prüfen von Signaturmanifesten



# Screenshot: Signatur-Prüfservice (o.k.)

Link: <https://demo.a-sit.at/pdf-as/>



## PDF Textsignaturen

### Resultat

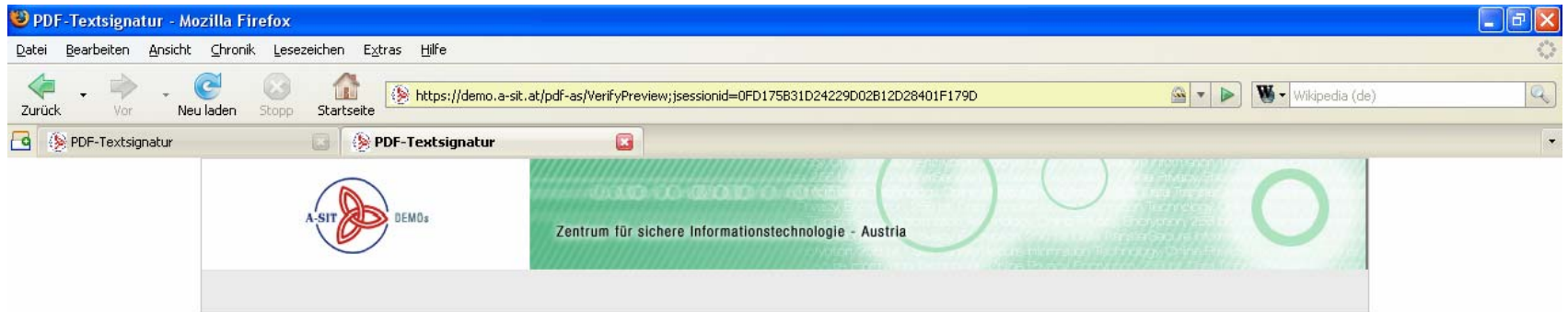
Zertifikat
Signator: C=AT,OU=VSign,O=Hauptverband VC3/B6sterr. Sozialvers.,CN=Daniel Konrad
Aussteller: C=AT,O=Hauptverband österr. Sozialvers.,CN=VSign CA.2
Seriennummer: 17094534195425308268889985453274176889600
Zertifikat: Eine formal korrekte Zertifikatskette vom Signatorzertifikat zu einem vertrauenswürdigen Wurzelzertifikat konnte konstruiert werden. Jedes Zertifikat dieser Kette ist zum in der Anfrage angegebenen Prüfzeitpunkt gültig.
Signatur-Check
Die Überprüfung der Hash-Werte und des Werts der Signatur konnte erfolgreich durchgeführt werden.
Manifest-Check
Für diese Signatur ist kein Signaturmanifest notwendig.

[zurück](#)

Copyright © 2006 A-SIT



# Signatur-Prüfservice (Dokument verändert)



## PDF Textsignaturen

### Resultat

Zertifikat
Signator: serialNumber=792333862198.givenName=Daniel,SN=Konrad,CN=Daniel Konrad,C=AT
Aussteller: CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Seriennummer: 112453
Zertifikat: Eine formal korrekte Zertifikatskette vom Signatorzertifikat zu einem vertrauenswürdigen Wurzelzertifikat konnte konstruiert werden. Jedes Zertifikat dieser Kette ist zum in der Anfrage angegebenen Prüfzeitpunkt gültig.
Signatur-Check
Die Überprüfung der Hash-Werte konnte erfolgreich durchgeführt werden. Beim Überprüfen des Werts der Signatur ist jedoch ein Fehler aufgetreten.
Manifest-Check
Für diese Signatur ist kein Signaturmanifest notwendig.

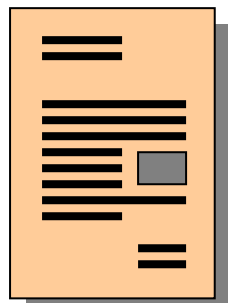
[zurück](#)

Copyright © 2006 A-SIT

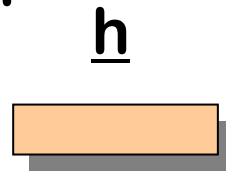


# Verifikation der Signatur

Dokument



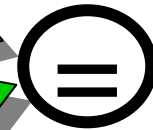
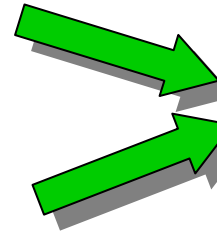
Hash Funktion  
 $h = H(M)$



h

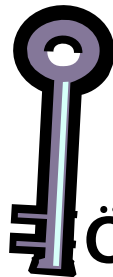


h'



????

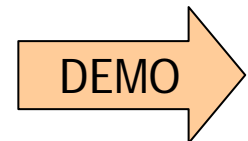
Signatur



Öffentlicher  
Schlüssel

# Verifikation der Signatur

- Aus dem Dokument wird der Hashwert berechnet, und zwar auf identische Weise wie beim Signiervorgang (etwaige Transformationen sind zu beachten)
  - Der verschlüsselte (d.h. signierte) Hashwert wird mit dem öffentlichen Schlüssel des Signators entschlüsselt.
  - Vergleich der Hashwerte
- => Verwendung sicherer Algorithmen und Parameter ist zu beachten



# Screenshot MD5-Kollission

The screenshot displays two PDF files, c1.ps and c2.ps, side-by-side in the GSview application. Both files contain identical text, including membership details for Chaos Computer Club Berlin e.V. and banking information. A PGP log window is overlaid on the files, showing the following data:

Name	Signer	Key ID	Validity	Signed
c1.ps	Annie Yousar <ann@egbg.de>	0x058C998B	●	09.09.2005 15:09:37
c2.ps	Annie Yousar <ann@egbg.de>	0x058C998B	●	09.09.2005 15:09:37

At the bottom of the screenshot, the system tray shows the following information:

Typ: PostScript Geändert am: 30.06.2005 07:59 Größe: 119 KB 119 KB Arbeitsplatz

# Zertifikatsprüfung – die wesentlichen Schritte

- Prüfen der Zertifikatshierarchie



- Prüfen der Gültigkeit

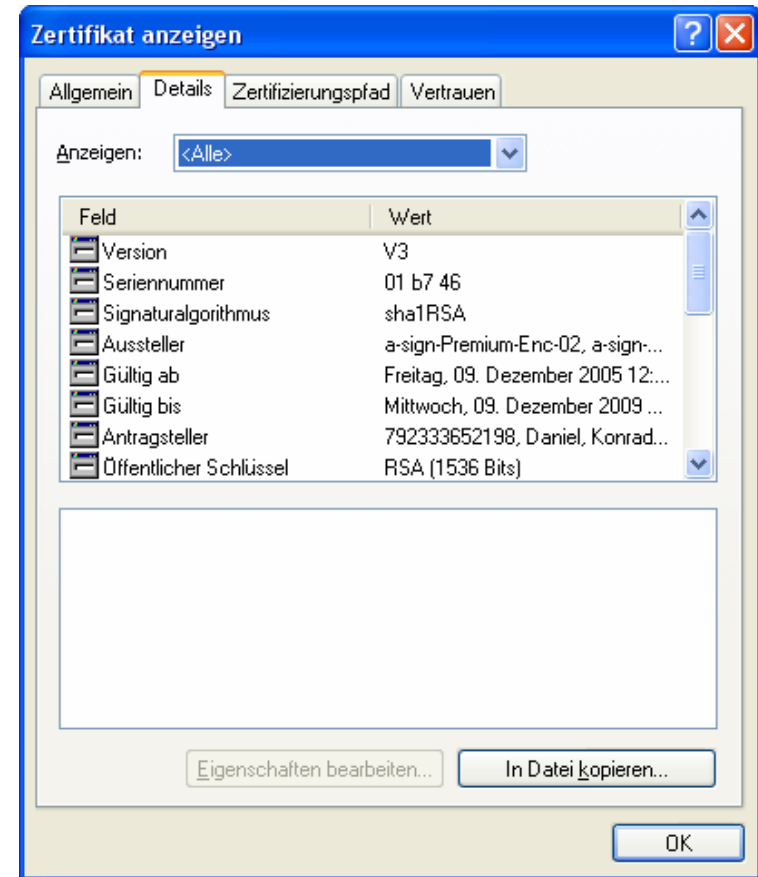


- Prüfen des Widerrufs



# Inhalte eines Zertifikats (X.509, RFC 3280)

- Version
- Seriennummer
- Signaturalgorithmus
- Herausgeber
- Gültigkeit
- Zertifikatsinhaber
- Öffentlicher Schlüssel
- Signatur des ZDA
- Erweiterungen





# Zertifikatserweiterungen

- Können als kritisch bzw. unkritisch markiert sein  
⇒ Kritische Erweiterungen müssen von einer Prüfapplikation interpretiert werden können!
- Kritisch: Typischerweise keyUsage
- Weitere: Hinweise auf Zertifikatspolicies, Widerruflisten-Verteilungspunkte, Zugriff auf Informationen des ZDA (Root-Zertifikat, OCSP), ...

# Wie erkennt man eine sichere Signatur?

- Voraussetzungen für sichere Signaturen:
  - Qualifiziertes Zertifikat



- Sichere Signaturerstellungseinheit (SSCD)



# Kennzeichnungsmöglichkeiten

- Definition über Standards:
  - RFC 3739 – Qualified Certificates Profile
    - Über Erweiterung QC-Statements
  - ETSI TS 101.862 (Qualified Certificates Profile)
    - 2 Möglichkeiten zur Kennzeichnung
      - Über Certificate Policy
      - Über QC-Statements (seit Juli 2005 verpflichtend)

# QC-Statements nach ETSI 101.862

- id-etsi-qcs-QcCompliance
  - Übereinstimmung mit EU-Richtlinie
- id-etsi-qcs-QcLimitValue (optional)
  - Beschränkung des Transaktionswertes
- id-etsi-qcs-QcRetentionPeriod (optional)
  - Archivierungsdauer beim ZDA
- id-etsi-qcs-QcSSCD (optional)
  - Privater Schlüssel auf sicherer Signaturerstellungseinheit

# Kennzeichnung in der Policy

- ETSI TS 101.456 (Policy requirements for certification authorities issuing qualified certificates)
  - qcp-public-with-sscd
    - ZDA stellt nur Zertifikate für Schlüssel auf SSCDs aus
  - qcp-public

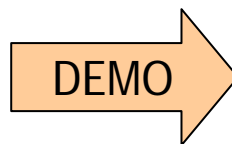
# OIDs

- Hierarchisch organisierter Ordnungsbegriff
- Weltweit eindeutige Kennungen für Objekte
- Aufbau über Baumstruktur
- z.B. {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1)}

# Zertifikat Status Tool

- LDAP-Suche
- Prüfen des Status eines Zertifikats
- Anzeige verschiedener Eigenschaften (qualifiziertes Zertifikat, E-Governmenteigenschaften)

=> [http://demo.a-sit.at/el\\_signatur/zertifikats\\_status](http://demo.a-sit.at/el_signatur/zertifikats_status)



# Screenshot: Zertifikat Status Tool

**A-SIT Zertifikat Status Tool V1.3.0**

Datei Konfiguration Hilfe

**LDAP Suche**

Vorname (z.B. Max)  Nachname (z.B. Muster\*)

Seriennummer   Seriennummer ist hexadezimal

Prüfzeitpunkt (z.B. 01.01.2006 0:00)

**gefundene Zertifikate**

Name	Seriennummer	Aussteller
Daniel Konrad	1709453419542530826888998545327417...	C=AT,O=Hauptverband österr. Sozialvers.,C...
Daniel Konrad	43519	CN=a-sign-Premium-Enc-01,OU=a-sign-Pr...
Daniel Konrad	117454	CN=a-sign-Premium-Enc-02,OU=a-sign-Pr...

**Details und Status**

Zertifikat (SubjectDN): serialNumber=810907919940,givenName=Daniel,SN=Konrad,CN=Daniel Konrad,C=AT

Zertifikat (IssuerDN): CN=a-sign-Premium-Sig-01,OU=a-sign-Premium-Sig-01,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT

E-Government OID: keine

zeitliche Gültigkeit: Der Prüfzeitpunkt liegt innerhalb des Gültigkeitszeitraumes.  
Gültig von: 07.07.2004 15:38:06 CEST bis: 31.12.2006 15:38:06 CET

Art des Zertifikates: qualifiziertes Zertifikat

Schlüsselverwendung: gemäß RFC 3280: digitalSignature nonRepudiation

Zertifikatsstatus: **Das Zertifikat ist zum Prüfzeitpunkt widerrufen. Das Zertifikat wurde widerrufen, da das Service eingestell wurde. [reasoncode: cessationOfOperation (5)] (Information lt. Zertifikat und Konfiguration)**

Widerrufszeitpunkt: **09.02.2006 16:22:17 CET (Information lt. Zertifikat und Konfiguration)**

Begrenzung des Transaktionswertes: nicht angegeben

(c) 2006 A-SIT



# OIDs der öffentlichen Verwaltung

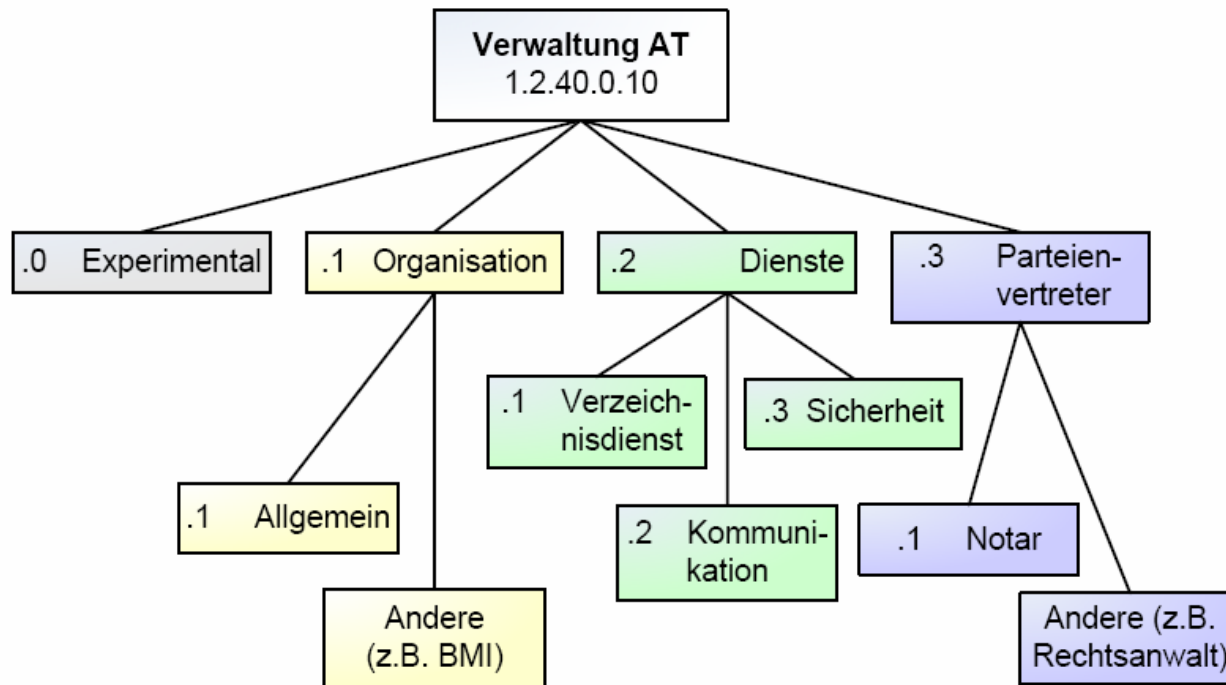


Abbildung 1 – OID-Baum der Verwaltung

Quelle: [http://www.cio.gv.at/it-infrastructure/oid/OID-1\\_0\\_6-20060227.pdf](http://www.cio.gv.at/it-infrastructure/oid/OID-1_0_6-20060227.pdf)

# Wichtige E-Government OIDs

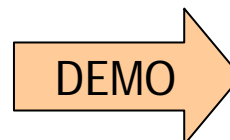
- Verwaltungseigenschaft – 1.2.40.0.10.1.1.1
- Dienstleistereigenschaft – 1.2.40.0.10.1.1.2
- Notarseigenschaft – 1.2.40.0.10.3.1
- Rechtsanwaltseigenschaft – 1.2.40.0.10.3.2
- Ziviltechnikereigenschaft – 1.2.40.0.10.3.3

# Berufsgruppensignaturen

- Notare
  - Beurkundungssignatur:
    - Qualifiziertes Zertifikat
      - Notareigenschaft
      - Daten des Amtssiegels
      - im el. Verzeichnis f. Beurkundungs- und Notarsignatur zu führen
    - Amtssiegel muss auch im Unterschriftenvermerk angebracht werden
  - Notarsignatur
    - Qualifiziertes Zertifikat
      - mit Notareigenschaft
      - im el. Verzeichnis f. Beurkundungs- und Notarsignatur zu führen

# Berufsgruppensignaturen (Fortsetz.)

- **Rechtsanwälte (el. Anwaltssignatur)**
  - Qualifiziertes Zertifikat
    - Rechtsanwaltseigenschaft
- **Ziviltechniker**
  - Beurkundungssignatur
    - Qualifiziertes Zertifikat
      - Ziviltechnikereigenschaft
      - Daten des Siegels
    - Siegel muss auch im Unterschriftsvermerk angebracht werden
  - Ziviltechnikersignatur
    - Qualifiziertes Zertifikat
      - Ziviltechnikereigenschaft



# Screenshot: Verwaltungseigenschaft

The screenshot shows the 'A-SIT Zertifikat Status Tool V1.3.0' window. The 'LDAP Suche' section contains search criteria: Vorname (Daniel), Nachname (Konrad), and Prüzzeitpunkt (21.11.2006 10:23:50 CET). The 'gefundene Zertifikate' table lists one certificate: Oswald Kessler, SN 80524, issued by CN=a-sign-corporate-light-02,OU=a-sign-co... The 'Details und Status' section shows the SubjectDN, IssuerDN (circled in red), E-Government OID (Verwaltungseigenschaft (1.2.40.0.10.1.1.1)), validity period, and certificate type (einfaches Zertifikat).

**A-SIT Zertifikat Status Tool V1.3.0**

Datei Konfiguration Hilfe

**LDAP Suche**

Vorname (z.B. Max)  Nachname (z.B. Muster\*)

Seriennummer   Seriennummer ist hexadezimal

Prüzzeitpunkt (z.B. 01.01.2006 0:00)

**gefundene Zertifikate**

Name	Seriennummer	Aussteller
Oswald Kessler	80524	CN=a-sign-corporate-light-02,OU=a-sign-co...
Daniel Konrad	1709453419542530826888998545327417	C=AT O=Hauptverband österr. Sozialvers. C...

**Details und Status**

Zertifikat (SubjectDN): serialNumber=202828344996,CN=Oswald Kessler,OU=Sektion IV, SU-ZMR,O=Bundesministerium für Inneres,C=AT

Zertifikat (IssuerDN): CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT

E-Government OID: Verwaltungseigenschaft (1.2.40.0.10.1.1.1)

zeitliche Gültigkeit: Der Prüzzeitpunkt liegt innerhalb des Gültigkeitszeitraumes.  
Gültig von: 25.05.2005 10:10:54 CEST bis: 25.05.2010 10:10:54 CEST

Art des Zertifikates: einfaches Zertifikat

Schlüsselverwendung: gemäß RFC 3280: digitalSignature keyEncipherment dataEncipherment

Zertifikatsstatus: Für das Zertifikat scheint zum Prüzzeitpunkt kein Widerruf auf. (Information lt. Zertifikat und Konfiguration)

Widerrufszeitpunkt:

Begrenzung des Transaktionswertes: nicht angegeben

(c) 2006 A-SIT

# Danke für Ihre Aufmerksamkeit!

---

Kontakt:

A-SIT, Zentrum für sichere  
Informationstechnologie - Austria  
Daniel Konrad

Weyringergasse 35  
1040 Wien

Tel: +43 (0)1-5031963-50

Fax: +43 (0)1-5031963-66

[daniel.konrad@a-sit.at](mailto:daniel.konrad@a-sit.at)

[www.a-sit.at](http://www.a-sit.at), [www.buergerkarte.at](http://www.buergerkarte.at)

