A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5
DVR-Nummer: 1065181 - FN: 195738 a
www.a-trust.at

Empfehlungen für sichere Signaturen

Die von der A-Trust empfohlenen Komponenten und Formate für sichere Signaturen behandeln eine qualitätsgesicherte Arbeitsumgebung des Zertifikatsinhabers.

Das Hauptaugenmerk der A-Trust Empfehlung wurde auf die Merkmale des Merkblattes der österreichischen Bestätigungsstelle gelegt, deren Hauptaspekte sich in drei Themenkreise zusammenfassen lassen:

- PIN Eingabe
- Hashverfahren
- Vertrauenswürdige Anzeige und Dokumentenformate

Diese Liste wird stets aktuell gehalten und stellt die jeweils am Markt verfügbaren und von der A-Trust empfohlenen Produkte zur Erstellung sicherer Signaturen dar. Die A-Trust Empfehlung umfaßt die Kompatibilität der angeführten Komponenten mit den Smart Card - und Zertifikats.-Produkten der A-Trust, sowie die Korrektheit der Zertifizierungen und Bescheinigungen.
(D.h.: Das die angeführten Produkte schon im Rahmen der Evaluierungen auf das Zusammenwirken mit A-Trust Produkten geprüft wurden.)

PIN Eingabe

Die PIN (Personal Identification Number) ist eine Ziffernfolge, die auch als Aktivierungsdaten für die Signaturerstellung bezeichnet wird. Die A-Trust empfiehlt Kartenlesegeräte mit eigenem Nummerneingabefeld für die sichere PIN Eingabe.

Folgend finden Sie die von der A-Trust empfohlenen Kartenlesegeräte:

- Kobil KAAN Professional (Kobil Systems GmbH)

Hashverfahren

Unter Hashverfahren versteht man mathematische bzw. kryptografische Verfahren. Die angeführten Produkte wurden auf die einwandfreie Implementierung dieser Verfahren geprüft.

Hinweis: Diese Produkte können häufig deckungsgleich mit denen der sicheren Anzeige sein!

Folgend finden Sie die von der A-Trust empfohlenen Produkte:

- trustview secure viewer (IT Solution GmbH)
- MBS Modul zur Erstellung sicherer Signaturen (BDC. EDV Consulting GesmbH)

A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5
DVR-Nummer: 1065181 - FN: 195738 a
www.a-trust.at

Vertrauenswürdige Anzeige und Dokumentenformate

Unter vertrauenswürdiger Anzeige versteht man Produkte, die gewährleisten, dass nur die dem Signator dargestellten Daten auch tatsächlich signiert werden. Es werden auch die empfohlenen Dokumentenformate, die von diesen Produkten sicher angezeigt werden können, angeführt.

Folgend finden Sie die von der A-Trust empfohlenen Produkte:

- **trustview secure viewer (IT Solution GmbH)**

Hinweis: Das genannte Produkt ist auch für die sichere Signaturprüfung geeignet

trustview benutzt XML als Dokumentenformat. Die zu signierenden bzw. zu prüfenden Dokumente entsprechen folgender Spezifikation:

```
<?xml version="1.0" encoding="UTF-8" ?>
  <Document Height="520" Width="640">
     <Data Id="SignedData">
      <Text X="10" Y="10">Bestätigung</Text>
      <Text X="10" Y="58">Ich bestätige hiermit ... Angaben:</Text>
      <Vorname X="10" Y="90">Rainer</Vorname>
      <Nachname X="10" Y="122">Gundacker</Nachname>
      <Datum X="10" Y="170">31.01.2002 09:28.41 GMT+00</Datum>
   </Data>
     <Signature>
        <SignedInfo>
         <SignatureMethod Algorithm="rsa-sha1" />
           <Reference URI="#SignedData">
            <DigestMethod Algorithm="sha1" />
           <DigestValue>ErcBymw90D … W1wlulQ=</DigestValue>
         </Reference>
      </SignedInfo>
           <SignatureValue>HIX2 … JKHsnbYlenyKQ=</SignatureValue>
        <KeyInfo>
           <X509Data>
              <X509Certificate> +iEtCIZwj … e7Hoqh</X509Certificate>
           </X509Data>
        </KeyInfo>
   </Signature>
</Document>
```

Abbildung: signiertes Beispiel XML Dokument von trustview

Das XML Dokument selbst kann vier verschiedene Arten von XML Tags enthalten:

- Text Tags mit Positionierungsattributen (X/Y Koordinate)
  Beispiel: <Text X="10" Y="10">**Bestätigung**</Text>
- Daten Tags mit Positionierungsattributen (X/Y Koordinate)
  Beispiel: <Vorname X="10" Y="90">**Rainer**</Vorname>
- Image Tags mit Positionierungsattributen (X/Y Koordinate)
  Beispiel: <Image X="450" Y="20">**Qk3EJwJk ... AAA==**</Image>
  Image Tags enthalten immer eine Bitmap (Windows BMP Format) als Daten
- einen Datum Tag mit Positionierungsattributen (X/Y Koordinate)
  Beispiel: <Datum X="10" Y="170">**31.01.2002 09:28.41 GMT+00**</Datum>

- **MBS Modul zur Erstellung sicherer Signaturen (BDC. EDV Consulting GesmbH)**

Characterset

Das MBS Modul zur Erstellung sicherer Signaturen benutzt als Characterset ein eingeschränktes ISO 8859-1.
Als erlaubte Zeichen sind folgende spezifiziert:

Zeichen	Hexwert
Linefeed	0x0a
Space	0x20
#	0x23
-	0x2d
.	0x2e
0-9	0x30-0x39
A-Z	0x41-0x5a
a-z	0x61-0x7a
Ä	0xc4
Ö	0xd6
Ü	0xdc
ß	0xdf
ä	0xe4
ö	0xf6
ü	0xfc

Wien, am 22. Februar 2002