



Zentrum für sichere Informationstechnologie – Austria 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

Homepage: www.a-sit.at
E-Mail: office@a-sit.at

Bescheinigung nach §18(5) SigG:

Signatursoftware trustview, Version 2.1.0

Antragsteller:
IT Solution GmbH
Neubaugasse 12-14
1070 Wien

1. Beschreibung der bescheinigten Komponente

Die bescheinigte Komponente ist die Signatursoftware trustview, Version 2.1.0 (nachstehend trustview genannt). Trustview ist eine Software zur vertrauenswürdigen Anzeige und zur Bereitstellung der zu signierenden Daten sowie zur Signaturprüfung von elektronisch signierten XML Dokumenten¹.

Gegenstand dieser Bescheinigung sind die Funktionen von trustview zur vertrauenswürdigen Anzeige und zur Bereitstellung der zu signierenden Daten.

Hersteller von trustview ist die IT Solution GmbH, Neubaugasse 12-14, 1070 Wien.

1.1. Lieferumfang

Die Software wird vom Hersteller auf einer geschlossenen CD per persönlicher Übergabe oder per Postversand direkt an den Endkunden oder an einen OEM (Original Equipment Manufacturer) ausgeliefert. Der OEM fügt den vollständigen Lieferumfang von trustview seiner eigenen OEM CD hinzu, oder bietet den vollständigen Lieferumfang von trustview über einen authentifizierten Server zum Download via HTTPS an. Zum Lieferumfang von trustview gehören:

- Das Installationsprogramm setup.exe.
- Trustview 2.1.0, bestehend aus trustview.exe und w-form.dll.
- Optionale Zertifikate von Wurzel- und Zwischenzertifizierungsstellen.
- Optionale Zertifikatswiderrufslisten von Zertifizierungsdiensteanbietern.
- Das Integritätscheckprogramm ueberpruefung.exe.
- Das Installations- und Benutzerhandbuch, Version 1.0.3 vom 27.09.2002.

Trustview wird in einer festen Konfiguration ausgeliefert und in dieser Form installiert.

1.2. Technische Einsatzumgebung

Trustview ist für den Einsatz auf Arbeitsplatzrechnern im Büro oder Heimbereich vorgesehen und kommt auf folgenden Betriebssystemen zum Einsatz:

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows ME

¹ Spezifikation des XML Dokumentenformats siehe Anhang A.

- Microsoft Windows NT 4.0
- Microsoft Windows 2000
- Microsoft Windows XP

Trustview benötigt mindestens folgende Hardware: PC mit CPU der Pentium Klasse (ab Pentium 60MHz), 8 MB RAM, 200 MB Festplatte, Grafikkarte mit min. 640x480 Pixel Bildschirmauflösung, min. 15 Bit Farbtiefe.

Zur Erstellung elektronischer Signaturen bedient sich trustview einer Signaturkarte und eines Chipkartenterminals.

Folgende Schnittstellen zur Signaturerstellungskomponente werden unterstützt:

- Kartenleser mit serieller Schnittstelle/T=1 Protokoll
- Siemens Sign@tor USB Schnittstelle
- Andere Leser über PC/SC Schnittstelle/T=1 Protokoll

Trustview unterstützt Signaturkarten mit folgenden Betriebssystemen:

- G+D StarCOS 2.3
- TeleSec TCOS 2.0
- Siemens Sicrypt
- Setec SetCOS 4.3
- Siemens CardOS M4.01 (nur bei Verwendung mit Siemens Sign@tor)

1.3. Funktionsumfang

Folgende Funktionen² von trustview sind für diese Bescheinigung relevant:

- **F.IntAut_G.1 - Dokumentdarstellung:** Trustview stellt dem Benutzer das zu signierende Dokument wie auch signierte Dokumente und Prüfergebnisse im Fenster von trustview sicher dar. Alle anzuzeigenden Daten befinden sich funktional in einem statischen, nicht veränderbaren Zustand. Trustview kennt nur diesen Modus der Anzeige.
- **F.IntAut_G.2 - Bildschirmoperationen:** Trustview ermöglicht dem Benutzer, die Überprüfung der Korrektheit der Darstellung durch geeignete Bildschirmoperationen (Wasserzeichen, Screenwiper und Zoomfunktion) zu unterstützen. Nachdem der Benutzer sich von der Korrektheit der Anzeige überzeugt hat, hat er die Möglichkeit den eigentlichen Signaturvorgang explizit auszulösen.
- **F.IntAut_G3 - Korrektheit der Darstellung:** Trustview überprüft die Korrektheit der Darstellung durch Vergleiche verschiedener Hashwerte, die zum Dokument berechnet wurden. Diese Hashwerte berechnet er mit SHA-1 aus verschiedenen Repräsentationen der zu signierenden Daten: zum einen aus deren interner XML Darstellung, zum anderen aus den Informationen der Bildschirmdarstellung.
- **F.IntAut_G4 - Signaturhashwert:** Trustview generiert mit dem Hash-Algorithmus SHA-1 den zum zu signierenden Dokument gehörigen Hashwert h.
- **F.IntAut_G.5 - Übertragung Signaturhashwert zum Token:** Trustview überträgt den Hashwert zur Signaturerstellungskomponente (z.B. Kartenleseterminal mit Signaturkarte des Benutzers). Das geschieht entweder mit Hilfe der zertifizierten Schnittstelle (USB) des Siemens Sign@tors (bestehend aus Siemens Sign@tor Terminal und Siemens Sign@tor Software) oder über die serielle Schnittstelle einer laut den Vorgaben eines Zertifizierungsdiensteanbieters vertrauenswürdig installierten Signaturerstellungskomponente.
- **F.IntAut_G.6 – Empfang der Signatur vom Token:** Trustview empfängt von der Signaturerstellungskomponente mit dem verschlüsselten Hashwert (SHA-1) die

² Die Funktionen sind den Sicherheitsvorgaben zur Zertifizierung von trustview entnommen. Die Sicherheitsvorgaben sind Teil des Zertifizierungsberichtes. Kopien des Zertifikats und des Zertifizierungsberichtes sind beim Hersteller oder bei der Zertifizierungsstelle (TÜV Informationstechnik GmbH, Am Technologiepark 1, D-45307 Essen, <http://www.tuvit.de/XS/ASP/content.020112&zerttyp=1/sprache.DE/SX/>) erhältlich.

Signatur (RSA) und das Signaturzertifikat des Benutzers. Er verbindet diese Informationen (Dokumentzusätze) mit dem zu exportierenden Dokument. Signatur und Signaturzertifikat werden dem Benutzer angezeigt. Die Signatur wird anhand des vorgegebenen Hashwertes verifiziert.

- **F.IntAut_G.7 – Signatur hinzufügen oder verwerfen:** Trustview erlaubt dem Benutzer, die Signatur zu verwerfen oder zu bestätigen. Nach Bestätigung der Signatur durch den Benutzer wird diese dem Dokument anschließend hinzugefügt, andernfalls vernichtet.

2. Erfüllung der Anforderungen des SigG³ und der SigV⁴

Trustview, Version 2.1.0 erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach §18(1) SigG⁵
- Anforderungen nach §18(2) SigG⁶
- Anforderungen nach §7(1) SigV⁷ ⁸;
- Anforderungen nach §7(2) SigV⁹ und
- Anforderungen nach §9(2) SigV¹⁰.

Trustview, Version 2.1.0 ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Darstellung der zu signierenden Daten.
- Komponenten und Verfahren zum Erzeugen des Hashwertes aus dem Dokument.

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist zwei Jahre nach der Ausstellung gültig.

4. Einsatzbedingungen

- (1) Trustview wird auf Arbeitsplatzrechnern im Büro oder im Heimbereich eingesetzt und ist dort nur bestimmten Personen zugänglich. Manipulationen an der Hardware und Software des Arbeitsplatzrechners, auf dem trustview installiert ist, sind zu verhindern. Der Arbeitsplatzrechner ist zudem mit einem Zugriffsschutz zu versehen, der nicht autorisierte Benutzer von der Verwendung von trustview oder Manipulation an trustview oder der benötigten Software fernhält.
- (2) Trustview und seine Umgebung sind vertrauenswürdig installiert. Der Benutzer muss sich mit dem vom Hersteller bereitgestellten Tool bei der Installation und später regelmäßig vergewissern, dass er nur die bescheinigte Version von trustview verwendet.
- (3) Die Systemzeit des Betriebssystems des Arbeitsplatzrechners, auf dem trustview installiert ist, ist korrekt.

³ Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 152/2001 vom 21. Dezember 2001.

⁴ Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000 vom 2. Februar 2000.

⁵ Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen (...).

⁶ Die bei der Erstellung einer sicheren Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, dass die zu signierenden Daten nicht verändert werden; sie müssen es weiters ermöglichen, dass dem Signator die zu signierenden Daten vor Auslösung des Signaturvorgangs dargestellt werden. (...)

⁷ Die Signatoren dürfen für die Erstellung sicherer elektronischer Signaturen nur solche Hashverfahren (...) einsetzen, die im Anhang 2 Punkt 2. (...) genannt sind.

⁸ Folgende Hashverfahren werden als sicher anerkannt (...) b) Funktion SHA-1. Diese Hashverfahren sind bis 31.12.2005 für den Einsatz bei elektronischen Signaturen als sicher anzusehen. (...)

⁹ Die von den Signatoren eingesetzten technischen Komponenten und Verfahren zur Erstellung sicherer elektronischer Signaturen müssen die vollständige Anzeige der zu signierenden Daten ermöglichen. Für die zu signierenden Daten dürfen nur die vom Zertifizierungsdiensteanbieter empfohlenen Formate verwendet werden. Die Spezifikation dieser Formate muss allgemein verfügbar sein. Können in einem Format auch dynamische Veränderungen oder unsichtbare Daten codiert werden, so dürfen die betreffenden Codierungen nicht verwendet werden. Der Zertifizierungsdiensteanbieter hat die Anwender anzuweisen oder ihnen Methoden bereitzustellen, um dynamische Veränderungen oder unsichtbare Daten auszuschließen.

¹⁰ (...) bei den übrigen technischen Komponenten und Verfahren muss die Evaluationsstufe E 2 mit der Mindeststärke der Sicherheitsmechanismen „hoch“ eingehalten sein. (Anmerkung: Die Evaluationsstufe EAL 3 nach Common Criteria entspricht der Evaluationsstufe E 2 nach ITSEC)

- (4) Zur Erzeugung der sicheren elektronischen Signatur sind sichere Signaturerstellungseinheiten zu verwenden, welche die Anforderungen von SigG und SigV erfüllen. Die sichere elektronische Signatur muss ausschließlich auf der Signaturerstellungseinheit erstellt werden. Die Signaturerstellungseinheit muss mit dem privaten Signaturschlüssel des identifizierten und authentisierten Benutzers den von trustview gelieferten Hashwert des Dokumentes mit dem RSA-Algorithmus nach PKCS#1 verschlüsseln und das Signaturzertifikat des Signators liefern.
- (5) Zur Verbindung von trustview mit der Signaturerstellungseinheit ist ein Kartenleser zu verwenden, der die Anforderungen von SigG und SigV erfüllt. Die Identifikation und Authentisierung des Signators gegenüber der Signaturerstellungseinheit muss durch PIN-Eingabe über den verwendeten Kartenleser erfolgen. Der Kartenleser muss direkt am benutzten Arbeitsplatzrechner angeschlossen sein. Der Signator muss sich von der unmittelbaren Verbindung des Kartenlesers mit dem Arbeitsplatzrechner vergewissern können, da diese sicherheitsrelevant ist.

5. Algorithmen und zugehörige Parameter

Zum Erzeugen des Hashwertes aus dem Dokument wird von trustview das SHA-1 Hashverfahren mit 160 Bit bereitgestellt. Dadurch sind die Anforderungen gemäß Anhang 2 Punkt 2 SigV erfüllt.

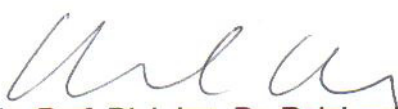
6. Prüfstufe und Mechanismenstärke


Es liegt das Deutsche IT-Sicherheitszertifikat TUVIT-DSZ-CC-9207-2002¹¹ für das „Softwareprodukt trustview, Version 2.1.0 der IT Solution GmbH, Wien“ vor, ausgestellt durch die Zertifizierungsstelle der TÜV Informationstechnik GmbH¹² am 25.10.2002. Trustview wurde nach den Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1 (ISO 15408) evaluiert und erfüllt die Vertrauenswürdigkeitsanforderungen der Stufe **EAL 3**, erweitert um die Komponenten **ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.2, AVA_VLA.4**. Die Stärke der Funktionen des Evaluationsgegenstandes wird mit „hoch“ (SOF-Hoch) bewertet. Der Zertifizierungsbericht TUVIT-DSZ-CC-9207-2002¹³ vom 24.10.2002 enthält die Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

Wien 23.01.2003

A-SIT Zentrum für sichere Informationstechnologie - Austria


o. Univ.-Prof. Dipl.-Ing. Dr. Reinhard Posch
Wissenschaftlicher Gesamtleiter


Manfred Holzbach
Geschäftsführender Vorstand

¹¹ Im Internet unter <http://www.tuvit.de/XS/ASP/content.020112&zerttyp=1/sprache.DE/SX/> verfügbar.

¹² Am Technologiepark 1, D-45307 Essen

¹³ Im Internet unter <http://www.tuvit.de/XS/ASP/content.020112&zerttyp=1/sprache.DE/SX/> verfügbar.

Anhang A – XML Dokumentenformat

Trustview benutzt XML als Dokumentenformat. Die zu signierenden 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 1 - Beispiel eines signierten XML-Dokuments

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>`

Die Positionierungskordinaten entsprechen dem Pixel Offset am Bildschirm wobei sich die Koordinate X=0/Y=0 in der linken oberen Ecke der Anzeige befindet. Trustview überprüft ob sich einzelne Elemente bei der Darstellung überschneiden. Binäre Daten (z.B. Bitmap im Image Tag, Hashwert oder Signatur) müssen immer Base64 kodiert angegeben werden. Jedes XML Dokument muss zwingend einen Datum Tag besitzen.

Als Signaturformat im Dokument wird eine minimale Version der XMLDSig-Spezifikation¹⁴ verwendet:

```
<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> +iEtCIRZwj ... e7Hoqh</X509Certificate>
    </X509Data>
  </KeyInfo>
</Signature>
```

Abbildung 2 - XML Signatur eines von trustview signierten Dokumentes

Die verwendete XMLDSig enthält:

- einen Hinweis auf den Signaturalgorithmus: „SignatureMethod“
- einen Hinweis auf den Hashalgorithmus: „DigestMethod“
- die Referenz auf die signierten Daten: „Reference“ (Angabe der ID des Tags von dem von Anfang bis Ende der angegebene Hashwert „DigestValue“ berechnet wird)
- den Hashwert der zu signierenden Daten: „DigestValue“
- die Signatur: „SignatureValue“
- das Signaturzertifikat: „X509Certificate“

Die Signatur erfolgt ebenfalls gemäß XMLDSig: Erst wird der Hashwert der zu signierenden Daten gebildet (Hashwertberechnung über den Inhalt des im Feld „Reference“ angegebenen XML Tags). Dieser Hashwert wird in den nach XMLDSig vorgegebenen „SignedInfo“ Tag im Sub-Tag „DigestValue“ eingefügt. Anschließend wird der Hashwert über den Inhalt des „SignedInfo“ Tags berechnet und nach RSA verschlüsselt.

Das angegebene Format ist strikt einzuhalten. Auch etwaige zusätzliche Zeichen („Whitespace“) wie sie üblicherweise in XML Dokumenten z.B. zwischen Tags gestattet werden sind untersagt. Widerspricht ein Dokument in mindestens einem Punkt dieser Spezifikation, so wird es von trustview abgelehnt.

¹⁴ <http://www.w3.org/TR/xmlsig-core/>