Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

Informationen zur Erstellung sicherer elektronischer Signaturen Wirtschaftsuniversität-Wien

Empfohlene Signaturprodukte und Dokumentenformate zur Erstellung sicherer elektronischer Signaturen

1. Verwendete Signaturerstellungseinheit
   Infineon Smartcard IC SLE 66CX320P mit Betriebssystem CardOS M4.01 Verschlüsselungsalgorithmus: RSA/Schlüssellänge: 1024-bit

2. Empfohlene Signaturprodukte, Chipkartenleser und Dokumentenformate
   a.trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH empfiehlt zur Erstellung sicherer elektronischer Signaturen nachfolgend angeführte Signaturprodukte.

Signaturprodukt trustview mit secure viewer v.2.1.0.

(Firma IT-Solutions) zur Erstellung der sicheren elektronischen Signatur

- Verwendung in Verbindung mit Chipkartenreader Signator
- Hashverfahren: SHA-1
- Dokumentenformat
  trustview verwendet 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">Anfrage</Text>
    <Text X="10" Y="58">Senden Sie mir bitte ...:</Text>
    <Vorname X="10" Y="90">Max</Vorname>
    <Nachname X="10" Y="122">Mustermann</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>
```

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

```
      </SignedInfo>
         <SignatureValue>HlX2 … JKHsnbYlenyKQ=</SignatureValue>
       <KeyInfo>
         <X509Data>
           <X509Certificate> +iEtCIZwj … e7Hoqh</X509Certificate>
         </X509Data>
       </KeyInfo>
   </Signature>
</Document>
```

Als Signaturformat im Dokuement wird eine minimale Version der XML-DigSig verwendet:

```
    <Signature>
      <SignedInfo>
       <SignatureMethod Algorithm="rsa-sha1" />
        <Reference URI="#SignedData">
<DigestMethod Algorithm="sha1" />
          <DigestValue>ErcBymw90D … W1wlulQ=</DigestValue>
       </Reference>
     </SignedInfo>
      <SignatureValue>HlX2 … JKHsnbYlenyKQ=</SignatureValue>
      <KeyInfo>
        <X509Data>
         <X509Certificate> +iEtCIrZwj … e7Hoqh</X509Certificate>
       </X509Data>
     </KeyInfo>
    </Signature>
```