Informationen zur Erstellung sicherer elektronischer Signaturen

Empfohlene Signaturprodukte und Dokumentenformate zur Erstellung sicherer elektronischer Signaturen

1. Verwendete Signaturerstellungseinheiten
   Dabei handelt es sich um die Chipkarte, die in Verbindung mit dem User Zertifikat Premium ausgegeben wird:

   - Philips Smart Card Controller P8WE5032VOG mit Betriebssystem Starcos SPK 2.3. – mit Starcert 1.84
     Verschlüsselungsalgorithmus: RSA/Schlüssellänge: 1024-bit

   - Philips Smart Card Controller P8WE5032VOG mit Betriebssystem Starcos SPK 2.3 – mit Starcert 2.2.
     Verschlüsselungsalgorithmus: RSA/Schlüssellänge: 1024-bit

2. Empfohlenes Signaturprodukt, Chipkartenleser und Dokumentenformat
   Zur Erstellung sicherer elektronischer Signaturen wird nachfolgend angeführtes Signaturprodukt empfohlen.

   Signaturprodukt trustview mit secure viewer v.2.1.0.
   (Firma IT-Solutions) zur Erstellung der sicheren elektronischen Signatur

   - Verwendung in Verbindung mit Chipkartenreader Kobil Kaan Professional und 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>
      </SignedInfo>
          <SignatureValue>HlX2 ... JKHsnbYlenyKQ=</SignatureValue>
       <KeyInfo>
          <X509Data>
             <X509Certificate> +iEtCIZwj ... e7Hoqh</X509Certificate>
          </X509Data>
       </KeyInfo>
   </Signature>
</Document>
```

Als Signaturformat im Dokument 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>
```