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. Empfohlene Signaturprodukte, Chipkartenleser und Dokumentenformate
Datakom empfiehlt zur Erstellung sicherer elektronischer Signaturen nachfolgend angeführte Signaturprodukte.

2.1. Signaturprodukt „proSIGN mit WYSIWYS-Viewer“ (secure viewer) v. 2.0 (Firma Infonova) zur Erstellung der sicheren elektronischen Signatur

- Verwendung in Verbindung mit Chipkartenreader Cardman 2020 (USB)
- Hashverfahren: SHA-1
- Empfohlenes Dokumentenformat: XML
  - Dateien nach XML 1.0 Spezifikation abrufbar unter http://www.w3.org/TR/2000/REC-xml-20001006
  - Namespaces nach http://www.w3.org/TR/1999/REC-xml-names-19990114

Hinweis: nicht unterstützt werden derzeit: Referenzen, Binaries bzw. Processing Instructions!

Textdatei im XML-Format (transformiert):

```
<?xml version="1.0" encoding="UTF-8" ?>
- <simpletext:text xmlns:simpletext="http://aida.infonova.at/simpletext"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://aida.infonova.at/simpletext aida://aida.infonova.at/simpletext">
    Das ist ein Beispieltext
    <simpletext:br />
    <simpletext:br />
 </simpletext:text>
```

Textdatei im XML-Format (und signiert):

```
<?xml version="1.0" encoding="UTF-8" ?>
- <aida:eDocument xmlns:aida="http://aida.infonova.at"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://aida.infonova.at aida:eDocument">
   - <aida:signedContent>
      - <simpletext:text xmlns:simpletext="http://aida.infonova.at/simpletext"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="http://aida.infonova.at/simpletext
            aida://aida.infonova.at/simpletext">
          Das ist ein Beispieltext
          <simpletext:br />
          <simpletext:br />
        </simpletext:text>
    </aida:signedContent>
   - <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
      - <dsig:SignedInfo>
          <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
              c14n-20010315" />
          <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        - <dsig:Reference
            URI="#xmlns(aida=http://aida.infonova.at)%20xmlns(dsig=http://www.w3.org
            /2000/09/xmldsig%23)%20xpointer(here()/ancestor::aida:eDocument%5b1%5
            d/child::aida:signedContent%5b1%5d)">
            <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <dsig:DigestValue>M/5KW9Y3tfW9l/BPJNOv6QW/LPM=</dsig:DigestValue>
          </dsig:Reference>
- <dsig:Reference
URI="#xmlns(aida=http://aida.infonova.at)%20xmlns(dsig=http://www.w3.org/2000/09/xmldsig%23)%20xpointer(here()/ancestor::dsig:Signature%5b1%5d/child::dsig:KeyInfo)">
            <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <dsig:DigestValue>+QBTd3HNBapB6bfZGxeQG//C8u8=</dsig:DigestValue>
          </dsig:Reference>
        - <dsig:Reference
            URI="#xmlns(aida=http://aida.infonova.at)%20xmlns(dsig=http://www.w3.org
            /2000/09/xmldsig%23)%20xpointer(here()/ancestor::dsig:Signature%5b1%5d
            /child::dsig:Object/child::aida:properties/child::aida:signedProperties)">
            <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <dsig:DigestValue>Kx7o+MDx7E71z9vJ5hWM8Ek4bJw=</dsig:DigestValue>
          </dsig:Reference>
       </dsig:SignedInfo>

          <dsig:SignatureValue>Sp6sLRKKpZKbtXBR03tU4EGTLIP810hDgjh0iOYUwheRqkHj
          0lTb+EXPBTmNKRX9
          opXHF893Z40R9h0OopGlcejkXADqRKbLHyK+ZiX2V4n/l74G1Nc+OMUuFk69DJj6
          eMC2a07MwbZnfkPyG6HRb6UBFH9/Y/Rn8T1NnRNbQDs=</dsig:SignatureValue>
      - <dsig:KeyInfo>
        - <dsig:X509Data>

              <dsig:X509Certificate>MIIDuTCCAyKgAwIBAgICAP4wDQYJKoZIhvcNA
              QEFBQAwgYAxCzAJBgNVBAYTAkFU.....
```

```
        .....nEQzQAUSSWgHJVoQvhoVsq22spQ2g2TI79oYvhy0YkeIhl)kICNRukXP
                </dsig:X509Certificate>
            </dsig:X509Data>
        </dsig:KeyInfo>
      - <dsig:Object>
        - <aida:properties xmlns:aida="http://aida.infonova.at">
          - <aida:signedProperties>
              <aida:transformDataID>simpletextTrafo1</aida:transformDataID>

                  <aida:documentHash>igaPsC9kPUX6gZgrEtSDXxdHQoA=</aida:d
                  ocumentHash>
            </aida:signedProperties>
            <aida:unsignedProperties />
          </aida:properties>
        </dsig:Object>
    </dsig:Signature>
</aida:eDocument>
```

2.2. 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 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>
```