PersoSim

Anpassungen von TA Trust Points innerhalb einer bestehenden Personalisierung

PersoSim erlaubt es dem Benutzer im Rahmen seiner Tests verschiedene Personalisierungen zu verwenden. Zu diesem Zweck stellt PersoSim bereits 10 Standardprofile mit Personalisierungen bereit, die ein breites Spektrum an Möglichkeiten hierfür abdecken. Neben gewöhnlichen Personalisierungen wie sie auf der überwiegenden Mehrheit ausgegebener Personalausweise vorzufinden sind, finden sich in den Profilen auch solche, die weniger häufig anzutreffende aber nichtsdestotrotz zulässige Sonderfälle sowie deren Kombinationen abdecken. Eine genaue Liste der angebotenen Profile und ggf. ihrer Besonderheiten findet sich auf der PersoSim Projektseite[1]. Jedes einzelne dieser Profile enthält eine zulässige Personalisierung. Eine vollständige und erfolgreiche Verifikation der Profile ist jedoch aufgrund abweichender Signaturen nur innerhalb der Test-PKI möglich.

Um den Austausch und Transfer von Profilen zu vereinfachen kommen hierfür im Umfeld von PersoSim XML-Dateien zum Einsatz. Dieses Format stellt auch den einfachsten und bevorzugten Weg dar, um Änderungen an den Profilen vorzunehmen.

Diese Anleitung beschreibt wie sich speziell Trust Points innerhalb einer bestehenden Personalisierung für die Terminal Authentication ändern lassen. Als Trust Points werden im Folgenden alle, einen bestimmten Terminaltyp (AT, IS, ST) authentifizierenden, Zertifikate bezeichnet. Die Menge dieser Trust Points in Bezug auf einen bestimmten Terminaltyp selbst wird hingegen als Trust Anchor bezeichnet.

Im Folgenden ist beschrieben wie sich grundsätzlich Änderungen an Profilen vornehmen lassen insbesondere aber die an Trust Points.

Ausgangspunkt für alle Änderungen ist jeweils eine XML-Datei zu einem bestehenden Standard-Profil. Im Folgenden wird hierfür beispielhaft das Profil 1 verwendet.
Dieses enthält bereits einen TA Trust Anchor für ein AT Terminal, in dem ein einziger Trust Point abgelegt ist.

Der Trust Anchor wird durch das Element `TrustPointCardObject`

```
<de.persosim.simulator.cardobjects.TrustPointCardObject id="continuousId">
      ...
</de.persosim.simulator.cardobjects.TrustPointCardObject>
```

unterhalb des Pfads

1 http://www.persosim.de

```
<de.persosim.simulator.perso.Profile01 id="1">
/<masterFile>
/<children>,
```

dargestellt, siehe auch:

```
<de.persosim.simulator.perso.Profile01 id="1">
      ...
  <mf id="12">
    <children id="13">
          ...
      <de.persosim.simulator.cardobjects.TrustPointCardObject id="77">
          ...
      </de.persosim.simulator.cardobjects.TrustPointCardObject>
          ...
    </children>
          ...
  </mf>
</de.persosim.simulator.perso.Profile01>
```

Das bereits vorhandene Trust Anchor Element selbst sieht aus wie folgt:

```
<de.persosim.simulator.cardobjects.TrustPointCardObject id="77">
        <parent class="de.persosim.simulator.cardobjects.MasterFile"
          reference="12"/>
        <children id="78"/>
        <lifeCycleState>CREATION</lifeCycleState>
        <currentCertificate id="79">
          ...
        </currentCertificate>
        <identifier id="94">
          <terminalType>AT</terminalType>
        </identifier>
</de.persosim.simulator.cardobjects.TrustPointCardObject>
```

Unterhalb des Trust Anchors befindet sich der einzige und derzeitig gültige Trust Point in Form des Elements `currentCertificate`.

```
<currentCertificate id="79">
          <certificateProfileIdentifier>0</certificateProfileIdentifier>
          <certificateAuthorityReference id="80">
            <countryCode>DE</countryCode>
            <holderMnemonic>TESTeID</holderMnemonic>
            <sequenceNumber>00004</sequenceNumber>
          </certificateAuthorityReference>
          <publicKeyOid id="81">
            <oidByteArray id="82">04007F00070202020203</oidByteArray>
            <idString>id-TA-ECDSA-SHA-256</idString>
          </publicKeyOid>
          <publicKey  id="83">
            <algorithm>EC</algorithm>
<value>308201333081EC06072A8648CE3D02013081E0020101302C06072A8648CE3D0101022100A
9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377304404207D5A0975F
C2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9042026DC5C6CE94A4B44F330B
5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B60441048BD2AEB9CB7E57CB2C4B482FFC81B7A
FB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E5
```

```
45C1D54C72F046997022100A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E829
74856A70201010342000474FF63AB838C73C303AC003DFEE95CF8BF55F91E8FEBCB7395D942036E4
7CF1845EC786EC95BB453AAC288AD023B6067913CF9B63F908F49304E5CFC8B3050DD</value>
          </publicKey>
          <certificateHolderReference id="84">
            <countryCode>DE</countryCode>
            <holderMnemonic>TESTeID</holderMnemonic>
            <sequenceNumber>00004</sequenceNumber>
          </certificateHolderReference>
          <certificateHolderAuthorizationTemplate id="85">
            <objectIdentifier id="86">
              <oidByteArray id="87">04007F000703010202</oidByteArray>
              <idString>id-AT</idString>
            </objectIdentifier>
            <relativeAuthorization id="88">
              <role>CVCA</role>
              <authorization id="89">
                <storedBits id="90">
                  ...
                  <boolean>true</boolean>
                  ...
                  <boolean>false</boolean>
                  ...
                </storedBits>
              </authorization>
            </relativeAuthorization>
          </certificateHolderAuthorizationTemplate>
          <certificateEffective id="91">2012-05-10 22:00:00.0
            UTC</certificateEffective>
          <certificateExpiration id="92">2015-05-10 22:00:00.0
            UTC</certificateExpiration>
          <certificateExtensions id="93"/>
        </currentCertificate>
```

Ändern eines bestehehenden Trust Points

Das vorhandene Trust Point Element `currentCertificate` soll nun so abgeändert werden, dass es den Trust Point aus `DECVCAeIDCT00001.bin` enthält passend zu `DECVCAeIDCT00001.cvcert`.
Hierfür muss der Trust Point aus `DECVCAeIDCT00001.bin` zuerst z.B. mit Hilfe eines Hex-Editors in eine hexadezimale Repräsentation überführt werden.

Der hexadezimal kodierte Trust Point sieht aus wie folgt:
"308201333081EC06072A8648CE3D02013081E0020101302C06072A8648CE3D0101022100A9FB57D
BA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377304404207D5A0975FC2C305
7EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9042026DC5C6CE94A4B44F330B5D9BBD
77CBF958416295CF7E1CE6BCCDC18FF8C07B60441048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE2
7E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D5
4C72F046997022100A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A
7020101034200047EC402F29B04079C9D89A8F732AD09BABC6538849128C6539B6C0F17EA4B72F56
DD632376FA8CFD0E08E0DCA0F54802344F3137599121D20F9CADD358E5C3C7E"

Dieser Hex-String ersetzt nun unter dem Element <publicKey> den alten im Sub-Element <value>.

Als nächstes müssen in den Sub-Elementen des Elements **`<certificateHolderReference>`** der countryCode, der holderMnemonic und die sequenceNumber angepasst werden.
Gleiches gilt bei Bedarf auch für das Gültigkeitsdatum

(`<certificateEffective id="91">`
`2012-05-10 22:00:00.0 UTC`
`</certificateEffective>`)
und das Ablaufdatum
(`<certificateExpiration id="92">`
`2015-05-10 22:00:00.0 UTC`
`</certificateExpiration>`).

Nach erfolgreichem Abschluss aller Änderungen sieht die Personalisierung im Wesentlichen aus wie folgt:

```
<de.persosim.simulator.perso.Profile01 id="1">
      ...
  <mf id="12">
    <children id="13">
          ...
      <de.persosim.simulator.cardobjects.TrustPointCardObject id="77">
        <parent class="de.persosim.simulator.cardobjects.MasterFile"
          reference="12"/>
        <children id="78"/>
        <lifeCycleState>CREATION</lifeCycleState>
        <currentCertificate id="79">
          <certificateProfileIdentifier>0</certificateProfileIdentifier>
          <certificateAuthorityReference id="80">
            <countryCode>DE</countryCode>
            <holderMnemonic>TESTeID</holderMnemonic>
            <sequenceNumber>00004</sequenceNumber>
```

```
          </certificateAuthorityReference>
          <publicKeyOid id="81">
            <oidByteArray id="82">04007F00070202020203</oidByteArray>
            <idString>id-TA-ECDSA-SHA-256</idString>
          </publicKeyOid>
          <publicKey  id="83">
            <algorithm>EC</algorithm>
<value>308201333081EC06072A8648CE3D02013081E0020101302C06072A8648CE3D0101022100A
9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377304404207D5A0975F
C2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9042026DC5C6CE94A4B44F330B
5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B60441048BD2AEB9CB7E57CB2C4B482FFC81B7A
FB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E5
45C1D54C72F046997022100A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E829
74856A7020101034200047EC402F29B04079C9D89A8F732AD09BABC6538849128C6539B6C0F17EA4
B72F56DD632376FA8CFD0E08E0DCA0F54802344F3137599121D20F9CADD358E5C3C7E</value>
          </publicKey>
          <certificateHolderReference id="84">
            <countryCode>DE</countryCode>
            <holderMnemonic>TESTeID</holderMnemonic>
            <sequenceNumber>00004</sequenceNumber>
          </certificateHolderReference>
          <certificateHolderAuthorizationTemplate id="85">
            <objectIdentifier id="86">
              <oidByteArray id="87">04007F000703010202</oidByteArray>
              <idString>id-AT</idString>
            </objectIdentifier>
            <relativeAuthorization id="88">
              <role>CVCA</role>
              <authorization id="89">
                <storedBits id="90">
                  ...
                  <boolean>true</boolean>
                  ...
                  <boolean>false</boolean>
                  ...
                </storedBits>
              </authorization>
            </relativeAuthorization>
          </certificateHolderAuthorizationTemplate>
          <certificateEffective id="91">2012-05-10 22:00:00.0
            UTC</certificateEffective>
          <certificateExpiration id="92">2015-05-10 22:00:00.0
            UTC</certificateExpiration>
          <certificateExtensions id="93"/>
        </currentCertificate>
        <identifier id="94">
          <terminalType>AT</terminalType>
        </identifier>
      </de.persosim.simulator.cardobjects.TrustPointCardObject>
          ...
    </children>
          ...
  </mf>
</de.persosim.simulator.perso.Profile01>
```

Hinzufügen eines weiteren Trust Points zu einem bestehenden Trust Anchor

Für den Fall, dass ein Trust Point nicht geändert sondern neu bzw. zusätzlich hinzugefügt werden soll, kann man einen bestehenden Trust Point

```
<currentCertificate id="continuousId">
          ...
</currentCertificate>
```

bzw.

```
<previousCertificate id="continuousId">
          ...
</previousCertificate>
```

einfach in dieselbe Hierarchieebene kopieren und entsprechend der obigen Anleitung ändern.

Die Reihenfolge, in der die Trust Points auf die Karte aufgebracht wurden, wird über den Namen des Elements festgelegt, in dem der TrustPoint abgelegt wird. Als Namen stehen hierbei `currentCertificate` sowie `previousCertificate` zur Verfügung. Der zuletzt hinzugefügte Trust Point wird als Element `currentCertificate` abgelegt während ein vorausgehender Trust Point als Element `previousCertificate` abgelegt wird. Dabei gilt zu beachten, dass innerhalb eines Trust Anchors lediglich zwei Trust Points, d.h. jeweils genau ein `currentCertificate` sowie ein `previousCertificate` abgelegt werden können.

```
<de.persosim.simulator.cardobjects.TrustPointCardObject id="77">
        <parent class="de.persosim.simulator.cardobjects.MasterFile"
            reference="12"/>
        <children id="78"/>
        <lifeCycleState>CREATION</lifeCycleState>
          ...
        <currentCertificate id="continuousId">
          ...
        </currentCertificate>
          ...
        <previousCertificate id="continuousId">
          ...
        </previousCertificate>
          ...
        <identifier id="94">
          <terminalType>AT</terminalType>
        </identifier>
</de.persosim.simulator.cardobjects.TrustPointCardObject>
```

Um unbeabsichtigten Konflikten beim Unmarshalling zu entgehen wird strengstens empfohlen rekursiv die `id="continuousId"` jedes einzelnen kopierten Tags und seiner Subtags auf laufende Werte zu setzen, die noch von keinem anderen Tag reserviert wurden. Es gilt dabei zu beachten gültige Verweise (`reference="continuousId"`) auf externe Objekte unverändert zu belassen oder bei internen Objekten entsprechend der neuen Ids anzupassen.