Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr
Tel. +43/1/505 32 80-0 • Fax: +43/1/505 32 80-77
Internet: www.stuzza.at • E-Mail: office@stuzza.at
A-1070 Wien, Stiftgasse 15-17



e-Mandat Signaturprofil

Version: 1.1
Datum: 31.10.2013
Autor: Markus Brejla, MSc / ARZ Allgemeines Rechenzentrum GmbH

Inhaltsverzeichnis

1. EINLEITUNG 3

1.1. REFERENZEN 3

1.2. VERWENDETE XML NAMENRAUM-PRÄFIXE 4

2. ANFORDERUNGEN AN EINE TRUSTED-CA 4

3. INITIIERUNG DER E-MANDAT SERVICE TRANSAKTION 5

3.1. BEISPIEL 5

4. STATUSMELDUNG ZUR E-MANDAT SERVICE TRANSAKTION 7

4.1. BEISPIEL 7

5. STATUSMELDUNG ZUR E-MANDAT SERVICE TRANSAKTION 9

5.1. BEISPIEL 9

1. EINLEITUNG

Das vorliegende Dokument ist eine Ergänzung zur technischen Beschreibung des e-Mandat Service [eMandate]. Es spezifiziert das Signaturprofil für jene Protokollnachrichten, die beim Einsatz des e-Mandat Service im Bereich des E-Government eine elektronische Unterschrift enthalten müssen.

Darunter fällt die *Initiierung der e-Mandat Service Transaktion* durch den Creditor, welche an die Debtorbank übermittelt wird. Diese Initiierung trägt die elektronische Signatur des Creditors. In weiterer Folge muss die *Statusmeldung zur e-Mandat Service Transaktion* die elektronische Signatur der Debtorbank enthalten. Die Statusabfrage zur e-Mandat Service Transaktion enthält wiederum die elektronische Signatur des Creditors.

Die elektronischen Signaturen sind nach [XMLDSIG] zu kodieren, und an die in [eMandate] spezifizierten Positionen einzufügen. Die nachfolgenden Abschnitte beschreiben detailliert die Vorgaben für alle Signaturen.

1.1. Referenzen

[EC14N] John Boyer, Donald Eastlake und Joseph Reagle: Exclusive XML Canonicalization Version 1.0. W3C Recommendation, Juli 2002. http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/

[eMandate] Martin Gruschi: e-Mandat Pflichtenheft, Version 1.1. Erarbeitet von Stuzza, August 2013. http://www.stuzza.at

[XMLDSIG] Donald Eastlake, Joseph Reagle und David Solo: XML-Signature Syntax and Processing. W3C Recommendation, Februar 2002. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212

[XPF2] John Boyer, Merlin Hughes und Joseph Reagle: XML-Signatur XPath Filter 2.0. W3C Recommendation, November 2002. http://www.w3.org/TR/2002/REC-xmldsig-filter2-20021108/

[ISIS-MTT] Brauckmann, Jürgen et. al: ISIS-MTT-Specification. Version 1.0.2, July 19th, 2002. http://www.teletrust.de/Dokumente%5Cag8_isis-mtt-corespec-v1.0.2.pdf

1.2. Verwendete XML Namenraum-Präfixe

In den nachfolgenden Kapiteln werden zur Beschreibung der Protokollelemente folgende Namenraum-Präfixe verwendet:

Präfix	Namenraum
eMandate	http://www.stuzza.at/namespaces/eMandate/2013
eMandateInit	urn:iso:std:iso:20022:tech:xsd:pain.009.001.02
eMandateAcceptance	urn:iso:std:iso:20022:tech:xsd:pain.012.001.02
dsig	http://www.w3.org/2000/09/xmldsig#

2. ANFORDERUNGEN AN EINE TRUSTED-CA

Folgende Anforderungen müssen an eine trusted CA erfüllt werden:

- Einsatz von X.509 v3 Zertifikaten
- Das Zertifikat muss die Zertifikatserweiterung CRL Distribution Points aufweisen. In dieser Zertifikatserweiterung muss zumindest ein LDAP Distribution Point enthalten sein. Weitere Distribution Points (z.B. http oder https) sind zulässig.
- Die Revozierungsliste (CRL) für das Zertifikat sowie für die CA-Zertifikate muss per LDAP von einem Server des Zertifizierungsdienstanbieters geladen werden können. Alle dazu notwendigen Informationen (LDAP-Host, LDAP-Port, LDAP-DN, ggf. LDAP-User und LDAP Passwort, ggf. weitere LDAP-Attribute) müssen dem Scheme Operator bekannt gegeben werden.
    - Beispiel: ldap://ldap-test.a-trust.at:389/ou=TrustTest-VSC-01,o=A-Trust,c=AT?certificaterevocationlist?
- Zertifikate und CA-Zertifikate müssen per LDAP von einem Server des Zertifizierungsdienstanbieters durch Identifikation des Zertifikats mittels IssuerDN und SerialNumber geladen werden können. Alle dazu notwendigen Informationen (LDAP-Host, LDAP-Port, LDAP-DN, ggf. LDAP-User und LDAP Passwort, ggf. weitere LDAP-Attribute) müssen dem Scheme Operator bekannt gegeben werden.
    - Beispiel: ldap://ldap-test.a-trust.at:389/eidCertificateSerialNumber=1234, ou=a-sign-Premium-Sig-01,o=A-Trust,c=AT?userCertificate;binary?
- Die Zertifikatskettenprüfung für das Zertifikat muss entsprechend dem Gültigkeitsmodell nach [ISIS-MTT], Teil 5 durchgeführt werden können.
- Zu jeder elektronischen Signatur einer e-Mandat Nachricht muss der Creditor bzw. die Debtorbank zumindest das Signatorzertifikat mitsenden, um die Zertifikatskettenbildung zu erleichtern. Desweiteren wird empfohlen, auch die zur Bildung einer vollständigen Zertifikatskette benötigten Zertifikate bis hin zu einem Wurzelzertifikat mit der Signatur mitzusenden.
- Certification Practice Statement und Certificate Policy der vom Creditor verwendeten CA müssen dem Scheme Operator zugänglich gemacht werden; auf Grund dieser Informationen wird eine CA vom Scheme Operator akzeptiert oder abgelehnt.

3. INITIIERUNG DER E-MANDAT SERVICE TRANSAKTION

Für eine sorgfältige und im Nachhinein belegbare Authentisierung des Creditors muss die Initiierung der e-Mandat Service Transaktion wahlweise einen SHA256Fingerprint nach [eMandate] oder eine elektronische Unterschrift des Creditors enthalten.

Um dem Creditor das Erzeugen der elektronischen Unterschrift möglichst einfach zu machen, muss der gesamte Transportcontainer eMandate:MandateServiceInitiationRequest signiert werden, der die eigentlichen Initiierungsdaten laut ISO Standard pain.009 beinhaltet. Als Kanonisierungsalgorithmus muss Exclusive Canonical XML Version 1.0 [EC14N] verwendet werden, und zwar sowohl für die Kanonisierung von dsig:SignedInfo, als auch zur Kanonisierung der zu unterschreibenden Protokollnachricht.

Damit wird es möglich, eine Enveloped Signature zu erzeugen, welche nur eine einzige Transformation benötigt, und zwar eine Enveloped Signature Transformation (vergleiche das nachfolgende Beispiel).

An Informationen zum verwendeten Signaturschlüssel muss in dsig:KeyInfo zumindest das Signatorzertifikat selbst (als dsig:X509Certificate) enthalten sein. Es wird empfohlen, darüber hinaus auch die zur Bildung einer vollständigen Zertifikatskette notwendigen Zertifikate anzugeben (als zusätzliche Elemente vom Typ dsig:X509Certificate).

3.1. Beispiel

Das folgende Beispiel zeigt eine signierte e-Mandat Initiierung eMandate:MandateInitiationRequest, eingebettet in den (mitunterzeichneten) Transportcontainer eMandate:MandateServiceInitiationRequest.

Um die Lesbarkeit zu verbessern, wurden der Signaturwert sowie das Signatorzertifikat ausgeblendet.

```
<?xml version="1.0" encoding="UTF-8"?>
<eMandate:MandateServiceInitiationRequest
xmlns:eMandate="http://www.stuzza.at/namespaces/eMandate/2013"
xmlns:eMandateInit="urn:iso:std:iso:20022:tech:xsd:pain.009.001.02"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eMandate/2013 eMandateService_v1.0.xsd">
  <eMandate:MsgHeader>
    <eMandate:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eMandate:MsgId>
    <eMandate:CreDtTm>2014-06-12T12:06:40Z</eMandate:CreDtTm>
  </eMandate:MsgHeader>
  <eMandate:MandateInitiationRequest>
    <eMandateInit:MndtInitnReq>
      <eMandateInit:GrpHdr>
        <eMandateInit:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eMandateInit:MsgId>
        <eMandateInit:CreDtTm>2014-06-12T12:06:40Z</eMandateInit:CreDtTm>
      </eMandateInit:GrpHdr>
      <eMandateInit:Mndt>
        <eMandateInit:MndtReqId>NOTPROVIDED</eMandateInit:MndtReqId>
        <eMandateInit:Tp>
          <eMandateInit:SvcLvl>
            <eMandateInit:Cd>SEPA</eMandateInit:Cd>
          </eMandateInit:SvcLvl>
          <eMandateInit:LclInstrm>
            <eMandateInit:Cd>CORE</eMandateInit:Cd>
          </eMandateInit:LclInstrm>
        </eMandateInit:Tp>
```

```
        <eMandateInit:Ocrncs>
          <eMandateInit:SeqTp>RCUR</eMandateInit:SeqTp>
        </eMandateInit:Ocrncs>
        <eMandateInit:CdtrSchmeId>
          <eMandateInit:Id>
            <eMandateInit:PrvtId>
              <eMandateInit:Othr>
                <eMandateInit:Id>AT12ZZZ00000000001</eMandateInit:Id>
                <eMandateInit:SchmeNm>
                  <eMandateInit:Cd>SEPA</eMandateInit:Cd>
                </eMandateInit:SchmeNm>
              </eMandateInit:Othr>
            </eMandateInit:PrvtId>
          </eMandateInit:Id>
        </eMandateInit:CdtrSchmeId>
        <eMandateInit:Cdtr>
          <eMandateInit:Nm>Mustershop</eMandateInit:Nm>
          <eMandateInit:PstlAdr>
            <eMandateInit:Ctry>DE</eMandateInit:Ctry>
            <eMandateInit:AdrLine>Skyline-Center</eMandateInit:AdrLine>
            <eMandateInit:AdrLine>Kohlestraße 1-5</eMandateInit:AdrLine>
          </eMandateInit:PstlAdr>
        </eMandateInit:Cdtr>
        <eMandateInit:UltmtCdtr>
          <eMandateInit:Nm>Mustershop Filiale Headquarter</eMandateInit:Nm>
        </eMandateInit:UltmtCdtr>
        <eMandateInit:Dbtr/>
        <eMandateInit:DbtrAgt>
          <eMandateInit:FinInstnId/>
        </eMandateInit:DbtrAgt>
        <eMandateInit:UltmtDbtr>
          <eMandateInit:Nm>Max Mustermann</eMandateInit:Nm>
        </eMandateInit:UltmtDbtr>
        <eMandateInit:RfrdDoc>
          <eMandateInit:Nb>Pol.Nr. 08/15</eMandateInit:Nb>
        </eMandateInit:RfrdDoc>
      </eMandateInit:Mndt>
    </eMandateInit:MndtInitnReq>
  </eMandate:MandateInitiationRequest>
  <eMandate:MerchantData>
    <eMandate:ReturnUrl>https://shop.example.net/emandate-
landing/x25fec002133</eMandate:ReturnUrl>
    <eMandate:Lang>NL</eMandate:Lang>
    <eMandate:ExpirationTime>2014-06-12T12:16:00Z</eMandate:ExpirationTime>
  </eMandate:MerchantData>
  <eMandate:AuthenticationDetails>
    <eMandate:UserId>ARZTAT22XXX_120674</eMandate:UserId>
    <dsig:Signature Id="signature-1-1" 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/2001/04/xmldsig-more#rsa-sha256"/>
        <dsig:Reference Id="reference-1-1" URI="">
          <dsig:Transforms>
            <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
          </dsig:Transforms>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <dsig:DigestValue>pgUupKi2xPFK+dvASNE+0y1tw8ivKh5B3iWAAH1iBEs=</dsig:DigestValue>
        </dsig:Reference>
      </dsig:SignedInfo>
      <dsig:SignatureValue><!-- Signaturwert --></dsig:SignatureValue>
      <dsig:KeyInfo>
        <dsig:X509Data>
          <dsig:X509Certificate><!-- Zertifikat --></dsig:X509Certificate>
        </dsig:X509Data>
      </dsig:KeyInfo>
    </dsig:Signature>
  </eMandate:AuthenticationDetails>
</eMandate:MandateServiceInitiationRequest>
```

4. STATUSMELDUNG ZUR E-MANDAT SERVICE TRANSAKTION

Damit die Statusmeldung (Mandat) der Debtorbank vom Creditor dauerhaft im Sinne eines elektronischen Belegs verwendet werden kann, muss sie eine elektronische Signatur der Debtorbank aufweisen.

Signiert werden muss das gesamte Element eMandate:MandateAcceptanceReport, welches das eigentliche Mandat laut ISO Standard pain.012 beinhaltet. Der Rest der Protokollnachricht eMandate:ProcessStatus sowie der Transportcontainer eMandate:MandateServiceStatusResponse dürfen nicht mit signiert werden.

Die Auswahl der zu unterschreibenden Daten ist so vorzunehmen, dass die Signatur auch dann noch überprüfbar ist, wenn sie in einem anderen Kontext aufbewahrt wird (beispielsweise, wenn die Protokollnachricht aus dem Transportcontainer herausgelöst wird). Es wird daher empfohlen, für die Auswahl eine Transformation nach XPath Filter 2 [XPF2] zu verwenden.

Als Kanonisierungsalgorithmus muss Exclusive XML Canonicalisation [EC14N] verwendet werden, und zwar sowohl für die Kanonisierung von dsig:SignedInfo, als auch zur Kanonisierung der zu unterschreibenden Protokollnachricht.

An Informationen zum verwendeten Signaturschlüssel muss in dsig:KeyInfo zumindest das Signatorzertifikat selbst (als dsig:X509Certificate) enthalten sein. Es wird empfohlen, darüber hinaus auch die zur Bildung einer vollständigen Zertifikatskette notwendigen Zertifikate anzugeben (als zusätzliche Elemente vom Typ dsig:X509Certificate).

4.1. Beispiel

Das nachfolgende Beispiel zeigt eine signierte Statusmeldung eMandate:MandateAcceptanceReport, eingebettet in den Transportcontainer eMandate:MandateServiceStatusResponse.

Um die Lesbarkeit zu verbessern, wurden der Signaturwert sowie das Signatorzertifikat ausgeblendet.

```
<?xml version="1.0" encoding="UTF-8"?>
<eMandate:MandateServiceStatusResponse xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eMandate="http://www.stuzza.at/namespaces/eMandate/2013"
xmlns:eMandateAcceptance="urn:iso:std:iso:20022:tech:xsd:pain.012.001.02"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eMandate/2013 eMandateService_v1.0.xsd">
  <eMandate:MsgHeader>
    <eMandate:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eMandate:MsgId>
    <eMandate:CreDtTm>2014-06-12T12:06:40Z</eMandate:CreDtTm>
  </eMandate:MsgHeader>
  <eMandate:MandateAcceptanceReport>
    <eMandateAcceptance:MndtAccptncRpt>
      <eMandateAcceptance:GrpHdr>

<eMandateAcceptance:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eMandateAcceptance:MsgId>
        <eMandateAcceptance:CreDtTm>2014-06-12T12:06:40Z</eMandateAcceptance:CreDtTm>
      </eMandateAcceptance:GrpHdr>
      <eMandateAcceptance:UndrlygAccptncDtls>
        <eMandateAcceptance:OrgnlMsgInf>

<eMandateAcceptance:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eMandateAcceptance:MsgId>
```

```
<eMandateAcceptance:MsgNmId>123451406122EMANDAT000000001</eMandateAcceptance:MsgNmId>
          <eMandateAcceptance:CreDtTm>2014-06-12T12:19:14Z</eMandateAcceptance:CreDtTm>
        </eMandateAcceptance:OrgnlMsgInf>
        <eMandateAcceptance:AccptncRslt>
          <eMandateAcceptance:Accptd>true</eMandateAcceptance:Accptd>
        </eMandateAcceptance:AccptncRslt>
        <eMandateAcceptance:OrgnlMndt>
          <eMandateAcceptance:OrgnlMndt>
            <eMandateAcceptance:MndtId>NOTPROVIDED</eMandateAcceptance:MndtId>
            <eMandateAcceptance:Tp>
              <eMandateAcceptance:SvcLvl>
                <eMandateAcceptance:Cd>SEPA</eMandateAcceptance:Cd>
              </eMandateAcceptance:SvcLvl>
              <eMandateAcceptance:LclInstrm>
                <eMandateAcceptance:Cd>CORE</eMandateAcceptance:Cd>
              </eMandateAcceptance:LclInstrm>
            </eMandateAcceptance:Tp>
            <eMandateAcceptance:Ocrncs>
              <eMandateAcceptance:SeqTp>RCUR</eMandateAcceptance:SeqTp>
            </eMandateAcceptance:Ocrncs>
            <eMandateAcceptance:CdtrSchmeId>
              <eMandateAcceptance:Id>
                <eMandateAcceptance:PrvtId>
                  <eMandateAcceptance:Othr>
                    <eMandateAcceptance:Id>AT12ZZZ00000000001</eMandateAcceptance:Id>
                    <eMandateAcceptance:SchmeNm>
                      <eMandateAcceptance:Cd>SEPA</eMandateAcceptance:Cd>
                    </eMandateAcceptance:SchmeNm>
                  </eMandateAcceptance:Othr>
                </eMandateAcceptance:PrvtId>
              </eMandateAcceptance:Id>
            </eMandateAcceptance:CdtrSchmeId>
            <eMandateAcceptance:Cdtr>
              <eMandateAcceptance:Nm>Mustershop</eMandateAcceptance:Nm>
              <eMandateAcceptance:PstlAdr>
                <eMandateAcceptance:Ctry>DE</eMandateAcceptance:Ctry>
                <eMandateAcceptance:AdrLine>Skyline-Center</eMandateAcceptance:AdrLine>
                <eMandateAcceptance:AdrLine>Kohlestraße 1-5</eMandateAcceptance:AdrLine>
              </eMandateAcceptance:PstlAdr>
            </eMandateAcceptance:Cdtr>
            <eMandateAcceptance:UltmtCdtr>
              <eMandateAcceptance:Nm>Mustershop Filiale Headquarter</eMandateAcceptance:Nm>
            </eMandateAcceptance:UltmtCdtr>
            <eMandateAcceptance:Dbtr>
              <eMandateAcceptance:Nm>Franz Mustermann</eMandateAcceptance:Nm>
            </eMandateAcceptance:Dbtr>
            <eMandateAcceptance:DbtrAcct>
              <eMandateAcceptance:Id>
                <eMandateAcceptance:IBAN>AT694321012345678901</eMandateAcceptance:IBAN>
              </eMandateAcceptance:Id>
            </eMandateAcceptance:DbtrAcct>
            <eMandateAcceptance:DbtrAgt>
              <eMandateAcceptance:FinInstnId>
                <eMandateAcceptance:BICFI>ARZWAT24INN</eMandateAcceptance:BICFI>
              </eMandateAcceptance:FinInstnId>
            </eMandateAcceptance:DbtrAgt>
            <eMandateAcceptance:UltmtDbtr>
              <eMandateAcceptance:Nm>Max Mustermann</eMandateAcceptance:Nm>
            </eMandateAcceptance:UltmtDbtr>
            <eMandateAcceptance:RfrdDoc>
              <eMandateAcceptance:Nb>Pol.Nr. 08/15</eMandateAcceptance:Nb>
            </eMandateAcceptance:RfrdDoc>
          </eMandateAcceptance:OrgnlMndt>
        </eMandateAcceptance:OrgnlMndt>
      </eMandateAcceptance:UndrlygAccptncDtls>
    </eMandateAcceptance:MndtAccptncRpt>
  </eMandate:MandateAcceptanceReport>
  <eMandate:ProcessStatus from="BANK">
    <eMandate:Status>OK</eMandate:Status>
  </eMandate:ProcessStatus>
  <dsig:Signature Id="signature-1-1" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
    <dsig:SignedInfo>
      <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
```

```
      <dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <dsig:Reference Id="reference-1-1" URI="">
        <dsig:Transforms>
          <dsig:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
            <xf2:XPath Filter="intersect" xmlns:xf2="http://www.w3.org/2002/06/xmldsig-
filter2">here()/ancestor::eMandate:MandateServiceStatusResponse/eMandate:MandateAcceptanceRep
ort[1]</xf2:XPath>
          </dsig:Transform>
          <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </dsig:Transforms>
        <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <dsig:DigestValue>KkEttmnxyuPG3Jrd7WI0WlFdBWoN0jD3MQC/gp6qO+0=</dsig:DigestValue>
      </dsig:Reference>
    </dsig:SignedInfo>
    <dsig:SignatureValue><!-- Signaturwert --></dsig:SignatureValue>
    <dsig:KeyInfo>
      <dsig:X509Data>
        <dsig:X509Certificate><!-- Zertifikat --></dsig:X509Certificate>
      </dsig:X509Data>
    </dsig:KeyInfo>
  </dsig:Signature>
</eMandate:MandateServiceStatusResponse>
```

5. STATUSMELDUNG ZUR E-MANDAT SERVICE TRANSAKTION

Damit nur ein autorisierter Creditor für ihn gültige Statusmeldungen (Mandate) abfragen kann, muss die Statusabfrage wahlweise einen SHA256Fingerprint nach [eMandate] oder eine elektronische Signatur des Creditors aufweisen.

Um dem Creditor das Erzeugen der elektronischen Unterschrift möglichst einfach zu machen, muss der gesamte Transportcontainer eMandate:MandateServiceStatusRequest signiert werden. Als Kanonisierungsalgorithmus muss Exclusive XML Canonicalisation [EC14N] verwendet werden.

An Informationen zum verwendeten Signaturschlüssel muss in dsig:KeyInfo zumindest das Signatorzertifikat selbst (als dsig:X509Certificate) enthalten sein. Es wird empfohlen, darüber hinaus auch die zur Bildung einer vollständigen Zertifikatskette notwendigen Zertifikate anzugeben (als zusätzliche Elemente vom Typ dsig:X509Certificate).

5.1. Beispiel

Das nachfolgende Beispiel zeigt eine signierte Statusabfrage eMandate:MandateServiceStatusRequest.

Um die Lesbarkeit zu verbessern, wurden der Signaturwert sowie das Signatorzertifikat ausgeblendet.

```
<?xml version="1.0" encoding="UTF-8"?>
<eMandate:MandateServiceStatusRequest
xmlns:eMandate="http://www.stuzza.at/namespaces/eMandate/2013"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eMandate/2013 eMandateService_v1.0.xsd">
  <eMandate:MsgHeader>
    <eMandate:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eMandate:MsgId>
    <eMandate:CreDtTm>2014-06-12T12:06:40Z</eMandate:CreDtTm>
  </eMandate:MsgHeader>
```

```
<eMandate:StatusReference>OTVjNWY0OTgtNTkzYy00MDUzLTliNjgtYjhlNjMyODFiYWI0</eMandate:StatusRe
ference>
<eMandate:AuthenticationDetails>
    <eMandate:UserId>ARZTAT22XXX_120674</eMandate:UserId>
    <dsig:Signature Id="signature-1-1" 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/2001/04/xmldsig-more#rsa-sha256"/>
        <dsig:Reference Id="reference-1-1" URI="">
          <dsig:Transforms>
            <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
          </dsig:Transforms>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <dsig:DigestValue>pgUupKi2xPFK+dvASNE+0y1tw8ivKh5B3iWAAH1iBEs=</dsig:DigestValue>
        </dsig:Reference>
      </dsig:SignedInfo>
      <dsig:SignatureValue><!-- Signaturwert --></dsig:SignatureValue>
      <dsig:KeyInfo>
        <dsig:X509Data>
          <dsig:X509Certificate><!-- Zertifikat --></dsig:X509Certificate>
        </dsig:X509Data>
      </dsig:KeyInfo>
    </dsig:Signature>
  </eMandate:AuthenticationDetails>
</eMandate:MandateServiceStatusRequest>
```