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

eps e-payment standard

Signaturprofil E-Government

Version: **1.0**

Datum: **19.03.2004**

Autor: **Gregor Karlinger / Stabstelle IKT-Strategie des Bundes**
Roman Kobylka / SPARDAT
Joachim Geisler / STUZZA

Inhaltsverzeichnis

1. EINLEITUNG 3

1.1. REFERENZEN 3

1.2. VERWENDETE XML NAMENRAUM-PRÄFIXE 4

2. ANFORDERUNGEN AN EINE TRUSTED-CA SEITENS EPS BANKEN 4

3. SIGNATURPROFIL FÜR DIE ZAHLUNGSAUFFORDERUNG 5

3.1. BEISPIEL 5

4. SIGNATURPROFIL FÜR DIE ZAHLUNGSBESTÄTIGUNG 7

4.1. BEISPIEL 7

1. EINLEITUNG

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

Einerseits ist das die Zahlungsaufforderung des Händlers, die an die Bank übermittelt wird, und mit welcher der eigentliche Protokollablauf beginnt (vergleiche [eps], Kapitel 7.2). Diese Zahlungsaufforderung trägt die elektronische Signatur des Händlers.
Andererseits muss in weiterer Folge die Zahlungsbestätigung der Bank, die an den Händler zurückgesendet wird, die elektronische Signatur der Bank enthalten (vergleiche [eps], Kapitel 7.8).
Beide elektronische Signaturen sind nach [XMLDSIG] zu kodieren, und an die in [eps] spezifizierten Positionen in die Zahlungsaufforderung bzw. Zahlungsbestätigung einzufügen. Die nachfolgenden Abschnitte beschreiben detailliert die Vorgaben für beide Signaturen.

1.1. Referenzen

[C14N]
John Boyer: Canonical XML Version 1.0. W3C Recommendation, März 2001.
http://www.w3.org/TR/2001/REC-xml-c14n-20010315.

[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/

[eps]
Joachim Geisler: eps e-payment standard – Technische Beschreibung, Version 2.0. Erarbeitet von Stuzza und Stabstelle IKT-Strategie des Bundes, 1. Oktober 2003.
http://www.stuzza.at
http://www.cio.gv.at/onlineservices/payment/eps-v20-20031001.pdf

[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-Signature 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
epsp	http://www.stuzza.at/namespaces/eps/protocol/20031001
eps	http://www.stuzza.at/namespaces/eps/payment/20031001
ds	http://www.w3.org/2000/09/xmldsig#

2. ANFORDERUNGEN AN EINE TRUSTED-CA SEITENS EPS BANKEN

Folgende Anforderungen müssen an eine trusted CA erfüllt werden:

- Einsatz von X.509 v3 Zertifikaten
- Das Händlerzertifikat 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 Händlerzertifikat 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 der Bank bekannt gegeben werden.
    - Beispiel: ldap://ldap-test.a-trust.at:389/ou=TrustTest-VSC-01,o=A-Trust,c=AT?certificaterevocationlist?
- Händlerzertifikate 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 der Bank 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 Händlerzertifikat muss entsprechend dem Gültigkeitsmodell nach [ISIS-MTT], Teil 5 durchgeführt werden können.

- Zu jeder elektronischen Signatur einer EPS2-Nachricht muss der Händler zumindest das Signatorzertifikat mitsenden, um die Zertifikatskettenbildung zu erleichtern. Des weiteren 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 Händler verwendeten CA müssen den eps Banken zugänglich gemacht werden; auf Grund dieser Informationen wird eine CA von den eps Banken akzeptiert oder abgelehnt.

3. SIGNATURPROFIL FÜR DIE ZAHLUNGSAUFFORDERUNG

Für eine sorgfältige und im Nachhinein belegbare Authentisierung des Händlers muss die Zahlungsaufforderung, mit welcher der Protokollablauf beginnt, eine elektronische Unterschrift des Händlers enthalten.

Um den Händler das Erzeugen der elektronischen Unterschrift möglichst einfach zu machen, muss der gesamte Transportcontainer epsp:EpsProtocolDetails signiert werden, der die eigentliche Protokollnachricht epsp:TransferInitiatorDetails beinhaltet. Als Kanonisierungsalgorithmus muss Canonical XML Version 1.0 [C14N] 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 Zahlungsaufforderung epsp:TransferInitiatorDetails, eingebettet in den (mitunterzeichneten) Transportcontainer epsp:EpsProtocolDetails.

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

```
<?xml version="1.0" encoding="UTF-8"?>
<epsp:EpsProtocolDetails SessionLanguage="DE" Version="V1.0"
  xmlns:atrule="http://www.stuzza.at/namespaces/eps/austrianrules/20031001"
  xmlns:epi="http://www.ecbs.org/epi/15092003"
  xmlns:eps="http://www.stuzza.at/namespaces/eps/payment/20031001"
  xmlns:epsp="http://www.stuzza.at/namespaces/eps/protocol/20031001">
  xsi:schemaLocation="http://www.stuzza.at/namespaces/eps/protocol/20031001
  EPSProtocol-V21.xsd" SessionLanguage="DE">
  <epsp:TransferInitiatorDetails>
    <eps:PaymentInitiatorDetails Version="V1.0">
      <epi:EpiDetails Version="V1.0">
        <epi:IdentificationDetails>
          <epi:Date>2004-03-19</epi:Date>
```

```
          <epi:ReferenceIdentifier>1234567890ABCDEFG</epi:ReferenceIdentifier>
        </epi:IdentificationDetails>
        <epi:PartyDetails>
          <epi:BfiPartyDetails>
            <epi:BfiBicIdentifier>GAWIATW1XXX</epi:BfiBicIdentifier>
          </epi:BfiPartyDetails>
          <epi:BeneficiaryPartyDetails>
            <epi:BeneficiaryNameAddressText>Max Mustermann</epi:BeneficiaryNameAddressText>
            <epi:BeneficiaryAccountIdentifier>
              AT611904300234573201
            </epi:BeneficiaryAccountIdentifier>
          </epi:BeneficiaryPartyDetails>
        </epi:PartyDetails>
        <epi:PaymentInstructionDetails>
          <epi:RemittanceIdentifier>AT1234567890XYZ</epi:RemittanceIdentifier>
          <epi:InstructedAmount AmountCurrencyIdentifier="EUR">150.00</epi:InstructedAmount>
          <epi:ChargeCode>SHA</epi:ChargeCode>
          <epi:DateOptionDetails DateSpecificationCode="CRD">
            <epi:OptionDate>2004-03-19</epi:OptionDate>
            <epi:OptionTime>14:20:00-05:00</epi:OptionTime>
          </epi:DateOptionDetails>
        </epi:PaymentInstructionDetails>
      </epi:EpiDetails>
      <atrule:AustrianRulesDetails>
        <atrule:Realization>GAR</atrule:Realization>
        <atrule:DigSig>SIG</atrule:DigSig>
      </atrule:AustrianRulesDetails>
    </eps:PaymentInitiatorDetails>
    <epsp:TransferMsgDetails>
      <epsp:ConfirmationUrl>
        http://10.18.70.8:7001/vendorconfirmation
      </epsp:ConfirmationUrl>
      <epsp:TransactionOkUrl>
        http://10.18.70.8:7001/transactionok?danke.asp
      </epsp:TransactionOkUrl>
      <epsp:TransactionNokUrl>
        http://10.18.70.8:7001/transactionnok?fehler.asp
      </epsp:TransactionNokUrl>
      <epsp:BasketUrl> http://10.18.70.8:7001/vendoreinkaufswagen?shop.asp</epsp:BasketUrl>
      <epsp:PaymentModeUrl>
        http://10.18.70.8:7001/anderezahlung?zvalternative.asp
      </epsp:PaymentModeUrl>
    </epsp:TransferMsgDetails>
    <epsp:WebshopDetails>
      <epsp:WebshopArticle ArticleCount="1" ArticleName="Toaster" ArticlePrice="150.00"/>
    </epsp:WebshopDetails>
    <epsp:AuthenticationDetails>
      <epsp:UserId>AKLJS231534</epsp:UserId>
      <ds:Signature Id="signature-1-1" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod
            Algorithm=" http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference Id="reference-1-1" URI="">
            <ds:Transforms>
              <ds:Transform
                Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>s94P3gHP2G/cv/0ERJT+bz6cOWc=</dsig:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue><!-- Signaturwert --></dsig:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate><!-- Zertifikat --></dsig:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </epsp:AuthenticationDetails>
  </epsp:TransferInitiatorDetails>
</epsp:EpsProtocolDetails>
```

4. SIGNATURPROFIL FÜR DIE ZAHLUNGSBESTÄTIGUNG

Damit die Zahlungsbestätigung der Bank vom Händler dauerhaft im Sinne eines elektronischen Belegs verwendet werden kann, muss sie eine elektronische Signatur der Bank aufweisen.

Signiert werden muss das gesamte Element eps:PaymentConfirmationDetails, das die eigentliche Zahlungsbestätigung enthält. Der Rest der Protokollnachricht epsp:BankConfirmationDetails sowie der Transportcontainer epsp:EpsProtocolDetails dürfen nicht mitsigniert 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.

Nachdem die Signatur (das Element dsig:Signature) Teil von eps:PaymentConfirmationDetails ist, muss nach der Auswahl der zu unterschreibenden Daten eine Enveloped Signature Transformation angewendet werden.

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 Zahlungsbestätigung epsp:BankConfirmationDetails, eingebettet in den Transportcontainer epsp:EpsProtocolDetails.

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

```
<?xml version="1.0" encoding="UTF-8"?>
<epsp:EpsProtocolDetails SessionLanguage="DE" Version="V1.0"
  xmlns:atrule="http://www.stuzza.at/namespaces/eps/austrianrules/20031001"
  xmlns:epi="http://www.ecbs.org/epi/15092003"
  xmlns:eps="http://www.stuzza.at/namespaces/eps/payment/20031001"
  xmlns:epsp="http://www.stuzza.at/namespaces/eps/protocol/20031001">
  xsi:schemaLocation="http://www.stuzza.at/namespaces/eps/protocol/20031001
  EPSProtocol-V21.xsd" SessionLanguage="DE">
  <epsp:BankConfirmationDetails>
    <epsp:SessionId>13212452dea</epsp:SessionId>
    <eps:PaymentConfirmationDetails Version="V1.0">
      <eps:PaymentInitiatorDetails Version="V1.0">
        <epi:EpiDetails Version="V1.0">
          <epi:IdentificationDetails>
            <epi:Date>2004-03-19</epi:Date>
```

```
            <epi:ReferenceIdentifier>1234567890ABCDEFG</epi:ReferenceIdentifier>
          </epi:IdentificationDetails>
          <epi:PartyDetails>
            <epi:BfiPartyDetails>
              <epi:BicIdentifier>GAWIATW1XXX</epi:BicIdentifier>
            </epi:BfiPartyDetails>
            <epi:BeneficiaryPartyDetails>
              <epi:NameAddressText>Max Mustermann</epi:NameAddressText>
              <epi:AccountIdentifier>AT611904300234573201</epi:AccountIdentifier>
            </epi:BeneficiaryPartyDetails>
          </epi:PartyDetails>
          <epi:PaymentInstructionDetails>
            <epi:RemittanceIdentifier>AT1234567890XYZ</epi:RemittanceIdentifier>
            <epi:InstructedAmount
              AmountCurrencyIdentifier="EUR">150.00</epi:InstructedAmount>
            <epi:ChargeCode>SHA</epi:ChargeCode>
            <epi:DateOptionDetails DateSpecificationCode="CRD">
              <epi:OptionDate>2004-03-19</epi:OptionDate>
              <epi:OptionTime>14:20:00-05:00</epi:OptionTime>
            </epi:DateOptionDetails>
          </epi:PaymentInstructionDetails>
        </epi:EpiDetails>
        <atrule:AustrianRulesDetails>
          <atrule:Realization>GAR</atrule:Realization>
          <atrule:DigSig>SIG</atrule:DigSig>
        </atrule:AustrianRulesDetails>
      </eps:PaymentInitiatorDetails>
      <eps:PayConApprovingUnitDetails>
        <eps:ApprovingUnitBankIdentifier>BKAUATWW</eps:ApprovingUnitBankIdentifier>
      </eps:PayConApprovingUnitDetails>
      <eps:PayConApprovalTime>2003-04-07T09:30:47-05:00</eps:PayConApprovalTime>
      <eps:PaymentReferenceIdentifier>
        120000302122320812201106461
      </eps:PaymentReferenceIdentifier>
      <eps:StatusCode>OK</eps:StatusCode>
      <ds:Signature Id="signature-1-1" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference Id="reference-1-1" URI="">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                <xf2:XPath Filter="intersect"
                  xmlns:eps="http://www.stuzza.at/namespaces/eps/20030201"
                  xmlns:xf2="http://www.w3.org/2002/06/xmldsig-filter2">
                  here()/ancestor::eps:PaymentConfirmationDetails[1]
                </xf2:XPath>
              </ds:Transform>
              <ds:Transform
                Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>9VEhsMCVk2Lb21r5ay3oWp2VzlQ=</dsig:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue><!-- Signaturwert --></dsig:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate><!-- Zertifikat --></dsig:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </eps:PaymentConfirmationDetails>
  </epsp:BankConfirmationDetails>
</epsp:EpsProtocolDetails>
```