Érvényes: 2013.07.01- jétől
Verzió: 1.0

EBT KKK2 kriptográfiai interfész specifikáció

Készítette: NAV Informatikai Intézet

Dokumentum kontroll

Kiosztási jegyzék:

NÉV	BEOSZTÁS	SZERVEZET	TEENDŐ

Tartalomjegyzék

1. Cél és hatókör

Az interfész pontos meghatározása az Ügyfelek kapcsolódó programjainak illeszkedése érdekében. Jelen dokumentum az eBanktitok KKK2 Interfész specifikáció titkosítási és elektronikus aláírási funkciókkal való kiegészítését, valamint a webszolgáltatás hívásakor használt autentikáció X509 tanúsítvánnyal történő bővítését írja le.

2. A titkosítás és elektronikus aláírás célja

A beküldendő üzenet két részre bontható: fejléc (metaadat) és üzenettörzs. A fejlécben levő adatok az üzenet továbbításához és könnyebb feldolgozásához szükségesek, a törzsben pedig maga a szakmai üzenet van.

Az üzenetek küldőjének azonosítása, az üzenetek eredetének igazolása (letagadhatatlanság) és az üzenetek változatlansága (integritás) biztosítása érdekében az üzenettörzs elektronikus aláírására, az üzenetek bizalmasságának biztosítása érdekében pedig az üzenettörzs titkosítására van szükség.

3. KKK üzenetek

A fejezet az eBanktitok KKK2 Interfész specifikáció változásait tartalmazza.

3.1 Boríték

3.1.1 Borítékban alkalmazott címzések és jelölések

3.1.1.1.1 Üzenet típusa (MessageType)

Az üzenettípust nem a borítékba beágyazott elektronikusan aláírt és titkosított üzenettel, hanem még az aláírás előtti szakmai üzenettel kell képezni.

Példa: Ha a beágyazott üzenetnek van névtere

Beágyazott üzenet az elektronikus aláírás és titkosítás előtt:

```
<PENZINTMEGK xmlns="http://schemas.nav.gov.hu/EBT/SZAKR1/1.0">
…
</PENZINTMEGK>
```

Példa MessageType érték:

```
http://schemas.nav.gov.hu/EBT/SZAKR1/1.0#PENZINTMEGK
```

4. KKK-Web alkalmazás üzenetcsere felületei

A fejezet az eBanktitok KKK2 Interfész specifikáció változásait tartalmazza.

Az eBanktitok KKK2 kriptográfiai interfész specifikáció alapján történő üzenetcserére speciális szabályok vonatkoznak a KKK-Web üzenetcsere felületével kapcsolatban.

Az üzenetcserére nem használható:

- KKK Web webalkalmazás
- KKK-Web webszolgáltatás felület BASIC autentikációval

Az üzenetcserére használható:

- KKK-Web webszolgáltatás felület X509 (tanúsítvány alapú) autentikációval

4.1 KKK-Web webszolgáltatás felület X509 (tanúsítvány alapú) autentikációval

A felhasználóhoz a KKK2-n belül X509 tanúsítványt lehet rendelni (csak a publikus kulcsra van szükség). A tanúsítvány azonosítja a KKK-Web webszolgáltatás felületen a felhasználót.

4.1.1.1 X509 (tanúsítvány alapú) autentikáció

A kölcsönönös azonosítás a HTTP rétegben a X509 tanúsítványok segítségével történik (transport security, client certificates). A kliens ellenőrzi a szerver tanúsítványát, illetve a szerver is csak a meghatározott tanúsítvánnyal rendelkező felhasználóknak engedélyezi a hozzáférést.

Technikailag egy-egy felhasználó tanúsítvány egy-egy KKK felhasználóhoz van rendelve szerver oldalon. A felhasználó tanúsítványának privát kulcsát kell, hogy használja kliens az SSL csatorna felépítéséhez, különben a szerver nem tudja azonosítani a klienst.

5. Üzenetcsere elemei

A fent említett titkosítás és elektronikus aláírás a publikus kulcs technológiára épül (Public Key Infrastructure, PKI). A PKI technológia aszimmetrikus kulcspárt használ, a tulajdonos birtokában és védelmében lévő privát kulcsot (private key) és a mindenki által megismerhető publikus kulcsot (public key).

Az üzenet elektronikus aláírása a küldő privát kulcsával történik, a címzett oldalán a feldolgozás pedig a beküldő publikus kulcsával ellenőrzi az üzenetet.

Az üzenet titkosítása a küldő oldalán a címzett által meghatározott publikus kulccsal történik, a fogadás után a titkosított üzenet kibontása csak a címzett privát kulcsával lehetséges, így garantálható a bizalmasság.

Az üzenet-előállítás folyamata:

1. Szakmai üzenet összeállítása
2. Szakmai üzenet és opcionális csatolmányok elektronikus aláírása a beküldő privát kulcsával
3. Az elektronikusan aláírt üzenet titkosítása a címzett publikus kulcsával
4. Az elektronikusan aláírt, titkosított üzenet elhelyezése a NAV borítékba, a vp:Body részen belül.

5.1 Támogatott kulcstípusok

Az 5.2 és 5.3 fejezetekben leírt általános elektronikus aláírás és titkosítás formátumokhoz a következő megszorításokat tesszük az eBanktitok rendszer esetén:

- RSA kulcspárok 2048 bit kulcshosszal, a publikus kulcs X509 formátumú tanúsítványként megadva.
- Mind az authentikációnál, elektronikus aláírásnál és a titkosításnál az NMHH által felügyelt, magyarországi tanúsítványkiadótól származó fokozott biztonságú aláíró illetve titkosító tanúsítványt kell használni.
- Az elektronikus aláírás XAdES-T típusú legyen, az NMHH által felügyelt, magyarországi tanúsítványkiadótól származó minősített tanúsítványú időbélyeggel ellátva.
- Az 5.2.1 pontban meghatározott formátumú elektronikus aláírást és az aláírt objektumokat az 5.2.2 pontban meghatározott formátumú aláírás tárolóban kell elhelyezni. Az aláírt objektumok a szakmai üzenetet és az opcionális egyéb csatolmányokat jelentik.
- Az 5.3 pontban meghatározott titkosító formátumnál a titkosítandó tartalom az 5.2.2 pontban leírt formátumú aláírás tároló kell, hogy legyen.

5.2 XML aláírás

5.2.1 Elektronikus aláírás

Vonatkozó ajánlás:

XML Advanced Electronic Signatures: http://www.w3.org/TR/XAdES/,

Formátum:

Leválasztott (Detached): Az elektronikus aláírás hivatkozik a tárolóban levő aláírt tartalomra. Lásd következő 5.2.2 fejezet.

Példa:

```
<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   Id="sigId-id151bf07f2e61576358d486d10c78e413">
  <ds:SignedInfo Id="sig-info-id151bf07f2e61576358d486d10c78e413">
    <ds:CanonicalizationMethod
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    <ds:SignatureMethod
        Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference Id="detached-ref-id" URI="detached-file.dat">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>
        1/SLIHlk/5PwMCU/4gxNkc5qVRJRU+s4I73c+5CyZK8=
      </ds:DigestValue>
    </ds:Reference>
    <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
```

```
        URI="#xades-id151bf07f2e61576358d486d10c78e413">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>
        m6kMmNbKJcOfnBB9WRBkfzZINQCKKGC5JEeilo+vPtc=
      </ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue Id="value-id151bf07f2e61576358d486d10c78e413">
     I53QTbZi3q8qXxNDmtHkmd7xixHcWhwQRqlz/X8=
  </ds:SignatureValue>
  <ds:KeyInfo Id="keyInfoid151bf07f2e61576358d486d10c78e413">
    <ds:X509Data>
      <ds:X509Certificate>
        2LEriYYaY5xWgBn2cTjdhQlA0MNAeCwrvBd1Ew==
      </ds:X509Certificate>
      <ds:X509Certificate>
        MvbGnU6BHeoHKWk2zQ==
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
  <ds:Object Encoding="o1id151bf07f2e61576358d486d10c78e413">
    <QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.3.2#"
        Id="qp-id151bf07f2e61576358d486d10c78e413" Target="#sigId-
id151bf07f2e61576358d486d10c78e413"
        xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
      <SignedProperties Id="xades-id151bf07f2e61576358d486d10c78e413">
        <SignedSignatureProperties>
          <SigningTime>2012-12-14T14:08:39Z</SigningTime>
          <SigningCertificate>
            <Cert>
              <CertDigest>
                <ns2:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ns2:DigestValue>
                  SNNhCL44DMBwLppI//Flrwsv8JPk1F5WaOkLN60wpQY=
                </ns2:DigestValue>
              </CertDigest>
              <IssuerSerial>
                <ns2:X509IssuerName>
                  EMAILADDRESS=testroot@ca.hu, CN=test root
                  ca, OU=INIT, O=NAV, L=Budapest, ST=Pest, C=HU
                </ns2:X509IssuerName>
                <ns2:X509SerialNumber>1</ns2:X509SerialNumber>
              </IssuerSerial>
            </Cert>
          </SigningCertificate>
          <SignaturePolicyIdentifier>
            <SignaturePolicyImplied xmlns:xs="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string" />
          </SignaturePolicyIdentifier>
        </SignedSignatureProperties>
        <SignedDataObjectProperties>
          <DataObjectFormat ObjectReference="#detached-ref-id">
```

```
            <MimeType>text/plain</MimeType>
          </DataObjectFormat>
        </SignedDataObjectProperties>
      </SignedProperties>
      <UnsignedProperties xmlns:ns4="http://uri.etsi.org/01903/v1.4.1#">
        <UnsignedSignatureProperties>
          <SignatureTimeStamp
                Id="time-stamp-8c0dc02b-2dce-453e-829f-a1ff4d333636">
            <ds:CanonicalizationMethod
                  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
            <EncapsulatedTimeStamp
                  Id="time-stamp-token-ac0bddfb-ae98-4f9d-93ba-4003c4009657">
[Ide kerül az időbélyeg]
MIAGCSqGSIb3DQEHAqCAMIACAQMxDzANBglghkAAA==
            </EncapsulatedTimeStamp>
          </SignatureTimeStamp>
        </UnsignedSignatureProperties>
      </UnsignedProperties>
    </QualifyingProperties>
  </ds:Object>
</ds:Signature>
```

5.2.2 Aláírás tároló

Vonatkozó ETSI ajánlás: Associated Signature Containers
http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=38258

Formátum:

Az aláírási formák közül az „Associated Signature Extended form” (ASiC-E) támogatott a következő megszorításokkal:

- Az aláírások XAdES formátumot követik.
- Az aláírás csak a <ds:Reference> elemmel hivatkozik az aláírt állományokra.
- Az aláírás a „META-INF/signatures.xml" állományban helyezkedik el.
- Az aláírás gyökér eleme a <asic:XAdESSignatures> tag.
- Alkalmazásfüggő információkat a „META-INF/manifest.xml” állomány tartalmazhat.

Példa:

Aláírás tároló ZIP állomány tartalma:

- „mimetype” tartalma „application/vnd.etsi.asic-e+zip”
- „file1.xml” tartalmazza az első aláírt állományt
- „file2.xml” tartalmazza a második aláírt állományt
- „/META-INF/signatures.xml” tartalmazza az aláírást, lásd lentebb.

META-INF/signatures.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<asic: XAdESSignatures=""
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:asic="http://uri.etsi.org/02918/v1.1.1#">
```

```
        <ds:Signature>
          <!-- ... -->
          <ds:Reference URI="file1.xml">
            <!-- ... -->
          </ds:Reference>
          <!-- ... -->
          <ds:Reference URI="file2.xml">
            <!-- ... -->
          </ds:Reference>
          <!-- ... -->
        </ds:Signature>
      </asic:XAdESSignatures>
```

5.3 XML titkosítás

A titkosítandó tartalom az RFC5652 (Cryptographic Message Syntax, CMS) ajánlás titkosításra vonatkozó részének megfelelően kerül titkosításra, EncryptedData struktúrában, majd az alább bemutatott formátum szerint kerül az xml üzenetben beágyazásra.

A KeyInfo rész azokat a publikus kulcsokat sorolja fel, amelyekhez tartozó privát kulccsal dekódolható az üzenet.

```
<?xml version="1.0" encoding="utf-8" ?>
<EncryptedData MimeType="application/vnd.etsi.asic-e+zip"
xmlns="http://schemas.nav.gov.hu/xmlenc/1.0">
  <KeyInfo>
    <X509Data>
      <X509IssuerSerial>
        <X509IssuerName>CN= Teszt tanúsítvány kiadó, OU=INIT, O=NAV, L=Budapest,
C=HU</X509IssuerName>
        <X509SerialNumber>12345678</X509SerialNumber>
      </X509IssuerSerial>
      <X509SKI>31d97bff</X509SKI>
      <X509SubjectName>NAV teszt titkosító tanúsítvány</X509SubjectName>

<X509Certificate>MIICKzCCAZigAwIBAgIQVw7hBxT5zZxMfvOtfBR50zAJBgUrDgMCHQUAMCIxIDAeBgNVBA
MTF0tLSzIgV0VCIFRlc3QgQXV0aG9yaXR5MB4XDTA3MTAwNDEwNTE0NloXDTM5MTIzMTIzNTk1OVowHjEcMBoGA
1UEAxMTVGVzdCBWUCBDcnlwdGVyIEtleTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtcSQvQfy5i2WGf9w
qLqN/+xAwJw+kj/LqzccMbW2Dn3Wi7zCv6I+wfXbihk+z8Cn/vpBW9TtKdiHiMHXEAkiihp2QJae+5S1WCi3y4Z
jehJ7HDbkFq+vNX73ud+psa2TunOke/mBIwtFR7TBInVefAH/DTSDxEwQ5HW1ELkyEPECAwEAAaNuMGwwFQYDVR
0lBA4wDAYKKwYBBAGCNwoDDDBTBgNVHQEETDBKgBDLCV0X1F6i7wnGQ4effz04oSQwIjEgMB4GA1UEAxMXS0tLM
iBXRUIgVGVzdCBBdXRob3JpdHmCEAFToJVZJlmGToZZtvh2avcwCQYFKw4DAh0FAAOBgQBVibiwXhhgAfHXFGk9
9K6aTg75TfbcLbUL7jK1e9asIUCSahdTRw+oT4/t025OcZ2jzW8p1J1ixiUxScs39uencImnOI9gYNXkk/d6uCf
1gvDGdxkOk1KC0UT17iGGQorCuc0ffuEiD7pGAiddTRKaLecNW7onJOje7tdkoC2Sow==</X509Certificate>
    </X509Data>
  </KeyInfo>
  <CipherData>
    <!--Ez a rész az elektronikusan aláírt, zip tárolóban lévő üzleti üzenet
titkosított formában -->

<CipherValue>sA7zcZKI/syc/wLGSRRSbAEf7ywroNp/iD0TXLY1uVe7No34vS68vD1Lo4IT/6o8xxemgW3T1F
```

```
OydQA1GEor738HY6CWhmkUQEfcIuONd/e3MSV+iwOqtzZXCCZvY8Vm/JKkodA+4MdyavVtjFAO4+48zdAY/Heql
6qjzagwvBNnwm1zs0IqKQ6vUaAXrNYEd66B4WxDEunBcYbmYCI9rlrEPM/5b0nLYfqS2LCCz7Crix7pu2syLsx4
pmMprw06k6TbPChKP6cH2scMJ5VV8LCwlA7l3RZ8t5VcvztUpz9Nr/fiu+X6f/2MUVgglJRJ/R+88tTVI5bxss3
HAQyHZnKJux30pOee+IHgdhivxbUGxp5zcj9QNBXDHVSngutiIIO+pmeOZMkKhd5OLhjbCH1Q4938BiDNLzXlyS
4k8tAV0seLkvNtNdSrUIe1gEX2wEwJ3G2MoMc8I6+H59zSNSb3EXkNHuVx6ZBkRQ+yjm03LaA0hxaOTDzGlgswx
1Z5GsWS9ncay7nDjkUVQRRjsZ7VryuaO4QOa0mBjBYpWVFoEvdnRUAD2x/OUFq/0O1vpcyk5ojp///3faELasum
pecIKnoAouJx43LsKnJ2BDKuVylCpF1VXRyVb4+eegkBqdDfnDk0SWD5YEDqukVSnkKHjYr+2zED7nRNiHkABut
Ob7JV1jditYX1a2ACaCNHxROoez+ocY1HQ3ewJgX8qSxT4XSJ6QNANZEdJBlIInV56Xx/SJiAuzO8hG9jA57zrO
Kmlg/pd+V7bSu1UOwjvrr7YOfk+I0LIdWkrT6GXqY9cSP/jh1xJuUomfgWxb4txrui+NnPgzZRNG0m6DcYqiKbg
X5itXkpT2zY2x0nExTvlfPKLgWIHWnbsFfE5+wS6o6EQZCnohqoyMl+jFRKnena9BlYUrMeNozbaslF2EkY6pQ/
a5PerNxt9OxzueO1</CipherValue>
  </CipherData>
</EncryptedData>
```

5.4 Teljes üzenet formátuma

A teljes beküldhető üzenet a két fenti transzformáció és az utána következő borítékolás végrehajtásával áll össze.

Példa:

```
<vp:VPEnvelope xmlns:vp="http://schemas.vam.gov.hu/VPEnvelope/1.0">
  <vp:Header>
    <vp:MessageID>uuid:d0b24e0e-f454-4656-9fdf-054a241ab81e</vp:MessageID>
    <vp:MessageType>[adott üzenet típusa]</vp:MessageType>
    <vp:From>userid:10000045</vp:From>
    <vp:To>[adott rendszer azonosítója]</vp:To>
    <vp:OnBehalfOf>[adott rendszer specifikációjában meghatározott formátumú
ügyfélazonosító]</vp:OnBehalfOf>
    <vp:Created>2012-12-14T13:52:40.3825253+01:00</vp:Created>
    <vp:Properties>[adott rendszer specifikációjában meghatározott tulajdonságok]
        <vp:Property name="AAAAA">BBBBBB</vp:Property>
    </vp:Properties>

  </vp:Header>
  <vp:Body>
<EncryptedData Mimetype="application/vnd.etsi.asic-e+zip"
    xmlns="http://schemas.nav.gov.hu/xmlenc/1.0">
  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <X509Data>
      <X509IssuerSerial>
        <X509IssuerName>CN= Teszt tanúsítvány kiadó, OU=INIT, O=NAV, L=Budapest,
C=HU</X509IssuerName>
        <X509SerialNumber>12345678</X509SerialNumber>
    </X509IssuerSerial>
      <X509SKI>31d97bff</X509SKI>
      <X509SubjectName>NAV teszt titkosító tanúsítvány</X509SubjectName>
    <X509Certificate>MIICKzCCAZigAwIBAgIQVw7hBxT5zZxMfvOtfBR50zAJBgUrDgMCHQUAMCIxIDAe
BgNVBAMTF0tLSzIgV0VCIFRlc3QgQXV0aG9yaXR5MB4XDTA3MTAwNDEwNTE0NloXDTM5MTIzMTIzNTk
1OVowHjEcMBoGA1UEAxMTVGVzdCBWUCBDcnlwdGVyIEtleTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgY
kCgYEAtcSQvQfy5i2WGf9wqLqN/+xAwJw+kj/LqzccMbW2Dn3Wi7zCv6I+wfXbihk+z8Cn/vpBW9TtK
```

```
diHiMHXEAkiihp2QJae+5S1WCi3y4ZjehJ7HDbkFq+vNX73ud+psa2TunOke/mBIwtFR7TBInVefAH/
DTSDxEwQ5HW1ELkyEPECAwEAAaNuMGwwFQYDVR0lBA4wDAYKKwYBBAGCNwoDDDBTBgNVHQEETDBKgBD
LCV0X1F6i7wnGQ4effz04oSQwIjEgMB4GA1UEAxMXS0tLMiBXRUIgVGVzdCBBdXRob3JpdHmCEAFToJ
VZJlmGToZZtvh2avcwCQYFKw4DAh0FAAOBgQBVibiwXhhgAfHXFGk99K6aTg75TfbcLbUL7jK1e9asI
UCSahdTRw+oT4/t025OcZ2jzW8p1J1ixiUxScs39uencImnOI9gYNXkk/d6uCf1gvDGdxkOk1KC0UT1
7iGGQorCuc0ffuEiD7pGAiddTRKaLecNW7onJOje7tdkoC2Sow==</X509Certificate>
</X509Data>
</KeyInfo>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">További titkosító
kulcsok…</KeyInfo>
<CipherData>
<CipherValue>[ez a rész az elektronikusan aláírt, zip tárolóban lévő szakmai
üzenet titkosított formában]
sA7zcZKI/syc/wLGSRRSbAEf7ywroNp/iD0TXLY1uVe7No34vS68vD1Lo4IT/6o8xxemgW3T1FOydQA
1GEor738HY6CWhmkUQEfcIuONd/e3MSV+iwOqtzZXCCZvY8Vm/JKkodA+4MdyavVtjFAO4+48zdAY/H
eql6qjzagwvBNnwm1zs0IqKQ6vUaAXrNYEd66B4WxDEunBcYbmYCI9rlrEPM/5b0nLYfqS2LCCz7Cri
x7pu2syLsx4pmMprw06k6TbPChKP6cH2scMJ5VV8LCwlA7l3RZ8t5VcvztUpz9Nr/fiu+X6f/2MUVgg
lJRJ/R+88tTVI5bxss3HAQyHZnKJux30pOee+IHgdhivxbUGxp5zcj9QNBXDHVSngutiIIO+pmeOZMk
Khd5OLhjbCH1Q4938BiDNLzXlyS4k8tAV0seLkvNtNdSrUIe1gEX2wEwJ3G2MoMc8I6+H59zSNSb3EX
kNHuVx6ZBkRQ+yjm03LaA0hxaOTDzGlgswx1Z5GsWS9ncay7nDjkUVQRRjsZ7VryuaO4QOa0mBjBYpW
VFoEvdnRUAD2x/OUFq/0O1vpcyk5ojp///3faELasumpecIKnoAouJx43LsKnJ2BDKuVylCpF1VXRyV
b4+eegkBqdDfnDk0SWD5YEDqukVSnkKHjYr+2zED7nRNiHkAButOb7JV1jditYX1a2ACaCNHxROoez+
ocY1HQ3ewJgX8qSxT4XSJ6QNANZEdJBlIInV56Xx/SJiAuzO8hG9jA57zrOKmlg/pd+V7bSu1UOwjvr
r7YOfk+I0LIdWkrT6GXqY9cSP/jh1xJuUomfgWxb4txrui+NnPgzZRNG0m6DcYqiKbgX5itXkpT2zY2
x0nExTvlfPKLgWIHWnbsFfE5+wS6o6EQZCnohqoyMl+jFRKnena9BlYUrMeNozbaslF2EkY6pQ/a5Pe
rNxt9OxzueO1</CipherValue>
</CipherData>
</EncryptedData>

</vp:Body>
</vp:VPEnvelope>
```

5.5 Hibaüzenetek

A KKK2 rendszerben előforduló hibaüzeneteket az eBanktitok KKK2 Interfész Specifikáció definiálja. Jelen dokumentum a kriptográfiai műveletek hibaüzeneteivel bővíti az eBanktitok KKK2 Interfész Specifikációban leírtakat. Hibaüzenet esetén továbbra is a „http://schemas.vam.gov.hu/VPFault/1.0” névtérben definiált Fault típus kerül borítékoltan visszaküldésre a következő módon:

A Fault tag-ben levő Code tag értéke „OtherFault”, a SubCode elem Value tag-je „XMLSignatureError” vagy „XMLDecryptionError”, a Text tag üres. A SubCode elem tartalmazhat egy újabb SubCode elemet, ahol a Value tag a belső hibakód, mely az adott típusú hibát pontosíthatja és a Text tag pedig a hibaszöveget tartalmazhatja.

XMLSignatureError hiba fordul elő várhatóan azokban az esetekben, amikor a várt elem nem elektronikus aláírással ellátott üzenet, nem regisztrált, visszavont vagy lejárt kulccsal történt az aláírás vagy maga az aláírás érvénytelen. XMLSignatureError hiba esetén a belső hibakód lehetséges értékei:

Érték neve	Jelentés

crypto_sign_check.missing_signature	A várt elem nem elektronikus aláírással ellátott üzenet
crypto_sign_check.invalid_certificate	Az aláírásnál használt kulcs hibás, a kulcs tanúsítványa nem került regisztrálásra vagy letiltották a KKK rendszerben, még nem érvényes, lejárt vagy visszavonták
crypto_sign_check.invalid_signature	Az aláírás érvénytelen vagy nem pontosan egy xml elem van aláírva

XMLDecriptionError hiba fordul elő várhatóan azokban az esetekben, amikor a várt elem nem titkosított üzenet, nem a NAV által kiadott titkosító kulcs publikus részével történt a titkosítás vagy a titkosított üzenet sérült. XMLDecryptionError hiba esetén a belső hibakód lehetséges értékei:

Érték neve	**Jelentés**
crypto_decrypt.missing_encrypted_data	A várt elem nem titkosított üzenet
crypto_decrypt.unknown_key	A titkosításhoz használt kulcs tanúsítványa (EncryptedData/KeyInfo/X509Data/X509Certificate) nem található az xml-ben, illetve nem a NAV publikus kulcsával történt a titkosítás
crypto_decrypt.unable_to_decrypt	Nem sikerült a titkosítás feloldása, feltehetőleg sérült a titkosított üzenet
crypto_decrypt.keystore_error	Hiba történt a NAV privát kulcsa kezelése miatt. Ez nem ügyfél, hanem NAV oldali hibát jelent, várhatóan ügyfelek nem kapnak ilyen üzenetet.

Példa hibaüzenet részlet:

```
<vpf:Fault xmlns:vpf="http://schemas.vam.gov.hu/VPFault/1.0">
  <vpf:Code>OtherFault</vpf:Code>
  <vpf:Subcode>
    <vpf:Value>XMLSignatureError</vpf:Value>
    <vpf:Text></vpf:Text>
    <vpf:Subcode>
      <vpf:Value>crypto_sign_check.invalid_certificate</vpf:Value>
      <vpf:Text>Az üzenetben található tanusítvány nem egyezik meg a felhasználó
egyetlen regisztrált tanusítványával sem.</vpf:Text>
    </vpf:Subcode>
  </vpf:Subcode>
</vpf:Fault>
```

6. Hibakezelés

6.1 KKK-Web webszolgáltatás felület

6.1.1 Kapcsolati hibák

6.1.1.1 HTTP hibaválasz kiolvasása

Ha a webszerver, vagy a közben található proxy vagy tűzfal HTTP hibát ad vissza, akkor fontos, hogy a teljes hibaüzenet megismerje a felhasználó. A gyakorlati tapasztalatok alapján nemcsak a HTTP státuszkód fontos, hanem a válaszoló által a response-ba írt teljes leíró szöveges tartalom, ami általában egy HTML lap. Innen lehet megérteni a tűzfal üzenetét, vagy megtudni a webszerver által küldött részletes státuszkódot. Az SSL kapcsolat miatt arra sincs lehetőség, hogy hálózatmonitorozó eszközzel megnézzük a választ, ezért mindenképpen a programba be kell építeni diagnosztikát segítő funkciót.

Java alatt a keletkezett RemoteException-ben benne van a HTTP response.

.NET alatt bizonyos esetekben a keletkezett WebException-ben benne van a válasz, ha nincs, akkor a System.Net trace-ből lehet kinyerni az információt.

6.1.1.2 HTTP kapcsolati teszt böngésző alól

Ügyfél oldalon először célszerű böngészőből elpróbálni a kliens gépen a webszolgáltatás elérését, majd ha az megy, akkor lehet a kliens programból próbálkozni.

Az Internet Explorter akkor tud autentikálni, ha:

- ha a tanúsítványtárban a kliens tanúsítvány privát kulccsal együtt benne van (Personal nevű tároló).
- ha kliens tanúsítvány tanúsítványláncában található közbenső CA(k) tanúsítványa bent van az Intermediate Certification Authorities tárolóban,
- ha nincs közbenső CA a kliens tanúsítványának tanúsítványláncában, akkor a legfelső szintű CA benne van a Trusted Root Certification Authorities tárolóban,
- ha a szerver SSL tanúsítványát kiadó CA tanúsítványa megbízható.

Működés Internet Explorer alatt:

- A kapcsolat felépítésénél az Internet Explorer a szerverrel egyezteti, hogy a szerver mely CA-któl származó tanúsítványt fogadja el. Ezek alapján a böngésző eldönti, hogy kliens oldalon rendelkezésre álló tanúsítványok közül melyek használhatóak fel. Ha 1 vagy 0 az előállt lista elemszáma, akkor az IE automatikusan kiválasztja a tanúsítványt, vagy tanúsítvány nélkül folytatja a folyamatot, ha több tanúsítvány van, akkor megjelenik a lista, melyből választani kell egy elemet.

- Az automatikus kiválasztás tiltása:

- IE / Internet Options / Security / Megfelelő zóna kiválasztása / Custom Level / Miscellaneous / Don't prompt for client certificate selection when no certificates, or only one certificate exists – Disable

6.1.1.3 Lehetséges HTTP hibák a kapcsolat felépítés során

HTTP Error 403.7 - Forbidden: SSL client certificate is required

- Egyáltalán nem adott meg a kliens tanúsítványt,
- felhasználónál levő tanúsítvány beállításai nem teljesek a kliens oldalon (nincs meg a tanúsítvány privát kulcsa, vagy a CA nem megbízható), és ezért nem jelenik meg a kiválasztható tanúsítványok listájában a kliens oldalon a kliens tanúsítvány.
- felhasználónál levő tanúsítvány CA-ja nem megbízható a szerver számára, és ezért nem jelenik meg a kiválasztható tanúsítványok listájában a kliens oldalon a kliens tanúsítvány. (tanúsítványláncban a közbenső CA fel van véve a szerveren, de a root CA nem.)
- tanúsítvány nem autentikációra való (Certification Purpose: Client Authentication, OID: 1.3.6.1.5.5.7.3.2)
- tűzfal nem engedi át a kliens tanúsítványt (ha a tűzfal újraépíti az SSL kapcsolatot, akkor lehet ilyen, lásd SSL bridging, SSL tunneling fogalmak a tűzfalaknál)

HTTP Error 403.13 - Forbidden: Client certificate has been revoked on the Web server.

- a visszavonási lista ellenőrzése nem sikerült a szerveren, vagy visszavonták a tanúsítványt

HTTP Error 403.16 - Forbidden: Client certificate is ill-formed or is not trusted by the Web server.

- kliens tanúsítványláncban a root CA fel van véve a szerveren, de közbenső CA viszont nem. Ekkor még meg is jelenik a böngésző listájában a tanúsítvány, és el is küldi a szervernek, de a webszerver már nem tekinti érvényesnek a tanúsítványt.
- CA tanúsítványok binárisan különböznek: a kliens oldalon egy "AA" self signed nevű CA-val generáltak egy tanúsítványt, de szerver oldalon egy másik "AA" nevű self signed CA-t van a megbízható CA-k közé felvéve.
- Egyéb probléma

HTTP Error 403.17 - Forbidden: Client certificate has expired or is not yet valid

- a tanúsítvány lejárt

7. Felhasznált és hivatkozott dokumentációk

A termék készítése során az alábbi dokumentumok kerültek felhasználásra:

Kód	Hivatkozási szám	Cím	Verzió
1.	PQP	Minőségbiztosítási Terv	2.0
2.		eBanktitok KKK2 interfész	1.0

		specifikáció	
3.		eBanktitok Működési modell	1.0

8. Betűszavak és rövidítések

Jelen dokumentáció a következő betűszavakat és rövidítéseket használja:

Betűszó	Leírás
KKK	NAV Külső Kommunikációs Központ
PKI	Public Key Infrastructure - nyilvános kulcsú titkosítás
PQP	Project Quality Plan - Projekt Minőségterv
SSL	Secure Sockets Layer - "RSA" eljárással titkosított biztonságos adatátviteli protokoll webszerverek és klienseik közötti kommunikációra
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
X509	PKI szabvány
XML	Kiterjesztett Jelölő Nyelv (Extensible Markup Language)

9. Minőségi kritériumok

Az eBanktitok KKK2 kriptográfiai interfész specifikáció dokumentum az alábbi minőségi kritériumok figyelembevételével készült:

- Érthető, egyértelmű és pontos.
- Összhangban van az elkészítése során felhasznált termékekkel.

10. Minőségellenőrzés

Az eBanktitok KKK2 kriptográfiai interfész specifikáció termékére irányuló minőségbiztosítási tevékenység végrehajtása személyes minőségellenőrzés és minőségi szemle keretében történik.

11. Mellékletek

11.1 EncryptedData üzenet sémája

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="EncryptedData"
    targetNamespace="http://schemas.nav.gov.hu/xmlenc/1.0"
    elementFormDefault="qualified"
    xmlns:tns="http://schemas.nav.gov.hu/xmlenc/1.0"
    xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name='EncryptedData' type='tns:EncryptedDataType'/>
  <xs:complexType  name='EncryptedDataType' >
    <xs:annotation>
      <xs:documentation>Titkosított adatok tárolója</xs:documentation>
    </xs:annotation>
```

```
    <xs:sequence>
      <xs:element ref='tns:KeyInfo' minOccurs='0'>
        <xs:annotation>
          <xs:documentation>A titkosításkor használt kulcs(ok)</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element ref='tns:CipherData'>
        <xs:annotation>
          <xs:documentation>A titkosított adat</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element ref='tns:EncryptionProperties' minOccurs='0'>
        <xs:annotation>
          <xs:documentation>Egyéb adatok</xs:documentation>
        </xs:annotation>
      </xs:element>
    </xs:sequence>
    <xs:attribute name='Id' type='xs:ID' use='optional'/>
    <xs:attribute name='MimeType' type='xs:string' use='optional'>
      <xs:annotation>
        <xs:documentation>A titkosított adat formátuma</xs:documentation>
      </xs:annotation>
    </xs:attribute>
    <xs:attribute name='Encoding' type='xs:anyURI' use='optional'>
      <xs:annotation>
        <xs:documentation>A titkosított adat kódolása</xs:documentation>
      </xs:annotation>
    </xs:attribute>
  </xs:complexType>


  <xs:element name="KeyInfo" type="tns:KeyInfoType"/>
  <xs:complexType name="KeyInfoType" mixed="true">
    <xs:annotation>
      <xs:documentation>A titkosító kulcsokról szolgál információval</xs:documentation>
    </xs:annotation>
    <xs:choice maxOccurs="unbounded">
      <xs:element ref="tns:X509Data"/>
      <xs:element ref="tns:PGPData"/>
    </xs:choice>
    <xs:attribute name="Id" type="xs:ID" use="optional"/>
  </xs:complexType>

  <xs:element name="X509Data" type="tns:X509DataType"/>
  <xs:complexType name="X509DataType">
    <xs:annotation>
      <xs:documentation>X509 tanúsítvány adatok</xs:documentation>
    </xs:annotation>
    <xs:sequence maxOccurs="unbounded">
      <xs:choice>
        <xs:element name="X509IssuerSerial" type="tns:X509IssuerSerialType"/>
        <xs:element name="X509SKI" type="xs:base64Binary"/>
        <xs:element name="X509SubjectName" type="xs:string"/>
        <xs:element name="X509Certificate" type="xs:base64Binary"/>
        <xs:element name="X509CRL" type="xs:base64Binary"/>
        <xs:any namespace="##other" processContents="lax"/>
```

```
      </xs:choice>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="X509IssuerSerialType">
    <xs:annotation>
      <xs:documentation>A tanúsítványt kiadó CA tanúsítvány adatai</xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="X509IssuerName" type="xs:string"/>
      <xs:element name="X509SerialNumber" type="xs:integer"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="PGPData" type="tns:PGPDataType"/>
  <xs:complexType name="PGPDataType">
    <xs:annotation>
      <xs:documentation>PGP kulcs adatok</xs:documentation>
    </xs:annotation>
    <xs:choice>
      <xs:sequence>
        <xs:element name="PGPKeyID" type="xs:base64Binary"/>
        <xs:element name="PGPKeyPacket" type="xs:base64Binary" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:sequence>
        <xs:element name="PGPKeyPacket" type="xs:base64Binary"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:choice>
  </xs:complexType>

  <xs:element name='CipherData' type='tns:CipherDataType'/>
  <xs:complexType name='CipherDataType'>
    <xs:sequence>
      <xs:element name='CipherValue' type='xs:base64Binary'/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name='EncryptionProperties' type='tns:EncryptionPropertiesType'/>
  <xs:complexType name='EncryptionPropertiesType'>
    <xs:sequence>
      <xs:element ref='tns:EncryptionProperty' maxOccurs='unbounded'/>
    </xs:sequence>
    <xs:attribute name='Id' type='xs:ID' use='optional'/>
  </xs:complexType>

  <xs:element name='EncryptionProperty' type='tns:EncryptionPropertyType'/>
  <xs:complexType name='EncryptionPropertyType' mixed='true'>
    <xs:choice maxOccurs='unbounded'>
      <xs:any namespace='##other' processContents='lax'/>
    </xs:choice>
    <xs:attribute name='Target' type='xs:anyURI' use='optional'/>
    <xs:attribute name='Id' type='xs:ID' use='optional'/>
```

```
    <xs:anyAttribute namespace="http://www.w3.org/XML/1998/namespace"/>
  </xs:complexType>

</xs:schema>
```