NEMZETI ADÓ- ÉS VÁMHIVATAL

KKK2 kriptográfiai interfész specifikáció

Készült: 2007.11.26.
Állapot: végleges
Verzió: 1.12

DOKUMENTUM TÖRTÉNET

Kiadás	Dátum	Leírás	A megváltozott részek
1.0	2007.08.17	Az alprojekt által elfogadásra javasolt verzió.	Teljes dokumentum
1.1	2007.10.12	X509 tanúsítvány alapú autentikációval bővítve. A kriptográfiai feldolgozás során lehetséges hibakódokkal bővítve.	1, 3, 4, 5.5
1.11	2007.10.29	Belső hibakódok részletezve. Példa xml-ek pontosítva.	5
1.12	2007.11.26	Hibakezelés fejezet	6

Tartalomjegyzék

1. Cél és hatókör

Az interfész pontos meghatározása az Ügyfelek kapcsolódó programjainak illeszkedése érdekében. Jelen dokumentum a 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 az üzleti üzenet van.

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

3. KKK üzenetek

A fejezet a 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 titkosított és aláírt üzenettel, hanem még a titkosítás előtti szakmai üzenettel kell képezni.

Példa: Ha a beágyazott üzenetnek van névtere

Beágyazott üzenet a titkosítás és aláírás előtt:

```
<BEFIZETESEK xmlns="http://schemas.vam.gov.hu/EBUK/1.0">
 …
</BEFIZETESEK>
```

Példa MessageType érték:

```
http://schemas.vam.gov.hu/EBUK/1.0#BEFIZETESEK
```

Példa: Ha a beágyazott üzenetnek nincs névtere

Beágyazott üzenet a titkosítás és aláírás előtt:

```
<CD225A>
  …
</CD225A>
```

Példa MessageType érték:

```
CD225A
```

Példa a HIBÁS üzenettípusra

Beágyazott üzenet a titkosítás és aláírás után:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
   …
 </Signature>
```

Példa a HIBÁS MessageType értékre:

http://www.w3.org/2000/09/xmldsig##Signature

4. KKK-Web alkalmazás üzenetcsere felületei

A fejezet a KKK2 Interfész specifikáció változásait tartalmazza.

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

Az üzenet-előállítás folyamata:

1. Üzleti üzenet összeállítása
2. Üzleti üzenet titkosítása a címzett publikus kulcsával
3. A titkosított üzenet aláírása a beküldő privát kulcsával
4. A titkosított, aláírt üzenet elhelyezése a NAV borítékba, a vp:Body részen belül.

5.1 Támogatott kulcstípusok

RSA kulcspárok 2048 bit kulcshosszal, a publikus kulcs X509 formátumú (self-signed) tanúsítványként megadva.

5.2 XML aláírás

Vonatkozó W3C ajánlás:
XML-Signature Syntax and Processing: http://www.w3.org/TR/xmldsig-core/

Formátum:
Borítékoló (Enveloping): Az aláírás magában foglalja az aláírt tartalmat egy Object elemen belül kódolva.

Példa:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
     20010315" />
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
  <Reference URI="#object-1">
   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
   <DigestValue>L+R9DBDr6CDKPztJiuYdkaOx7GQ=</DigestValue>
  </Reference>
 </SignedInfo>

    <SignatureValue>KX7ecBt7e0l61Md1XmF/ArajyzaFBhEvRmZdyYfyi93EFtZdGQbETrGp1Ajo2k
    6Iw59t4gbOlOd8Nwfc3evVJNhOOXhR2s6c76c3rb+x1fMCqzNjzwo3OzS/1O/cZgKaKWtDvy9aSGLm
    CkEahVjuLTEDqwXNiV8tOTi+mWxXqRk=</SignatureValue>
 <KeyInfo>
  <KeyValue>
   <RSAKeyValue>

    <Modulus>z+YqO3ZYZkeSCqJKUIdiP9p3xupqyBQEEc11YI7R+CZYFrd7+yrGQeNLtATgPvXBZOgnR
    iGwMTPohvg+qZggCLTib0AGqtlyYzW77+opM9pa2SVJSaw8Lkh2Bhb1P/HTK4DIeaHJN67bQMyJUPW
    JKM2YE7NeNKebX66M3lKNSBE=</Modulus>
    <Exponent>AQAB</Exponent>
   </RSAKeyValue>
  </KeyValue>
 <X509Data>

    <X509Certificate>MIIDpzCCAxCgAwIBAgIGQE32jRRtMA0GCSqGSIb3DQEBBQUAMIGaMQswCQYDV
    QQGEwJIVTERMA8GA1UEBxMIQnVkYXBlc3QxFTATBgNVBAoTDE5ldExvY2sgS2Z0LjEaMBgGA1UECxM
    RVGFudXNpdHZhbnlraWFkb2sxJDAiBgNVBAMTG05ldExvY2sgVGVzenQgKENsYXNzIFQyKSBDQTEfM
    B0GCSqGSIb3DQEJARYQaW5mb0BuZXRsb2NrLm5ldDAeFw0wNzEwMjQwOTU0MzJaFw0wNzExMjMwOTU
    0MzJaMIGRMQswCQYDVQQGEwItLTELMAkGA1UECAwCLS0xCzAJBgNVBAcMAi0tMQswCQYDVQQKDAItL
    TELMAkGA1UECwwCLS0xKTAnBgNVBAMMIE5ldExvY2sgVGVzenQgQWxhaXJvIHRhbnVzaXR2YW55MSM
    wIQYJKoZIhvcNAQkBFhRtYXJhaS5wYWxAdmFtLmdvdi5odTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwg
    YkCgYEAz+YqO3ZYZkeSCqJKUIdiP9p3xupqyBQEEc11YI7R+CZYFrd7+yrGQeNLtATgPvXBZOgnRiG
    wMTPohvg+qZggCLTib0AGqtlyYzW77+opM9pa2SVJSaw8Lkh2Bhb1P/HTK4DIeaHJN67bQMyJUPWJK
    M2YE7NeNKebX66M3lKNSBECAwEAAaOB/jCB+zCBhAYJYIZIAYb4QgENBHcWdUZJR1lFTEVNISBFemV
    uIHRhbnVzaXR2YW55IGNzYWsgdGVzenRlbGVzaSBjZWxva3JhIHN6b2xnYWwuIElNUE9SVEFOVCEgV
    GhpcyBjZXJ0aWZpY2F0ZSBpcyBvbmx5IGZvciB0ZXN0aW5nIHB1cnBvc2VzLjARBglghkgBhvhCAQE
    EBAMCBaAwDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBsAwQQYDVR0fBDowODA2oDSgMoYwaHR0c
    DovL2NybDEubmV0bG9jay5uZXQvaW5kZXguY2dpP3JhdyZjcmw9dGVzenQyMA0GCSqGSIb3DQEBBQU
    AA4GBAA56ctPKhcjOPxkYZtoKekf0N6G0+BSJey6vidJTCKf76sD+T3DuI25pYpspDmwYoW1veC1sb
    17zADfQiJJJCXwYbWumeGqYiP+8glkERupQj6WumCAz0b3Vj2dfnYNv96TC1XPnHF65JWM3CkHZT+c
    sIntucp/I+4hLaLs792PJ</X509Certificate>
   </X509Data>
  </KeyInfo>
```

```
            <Object Id="object-1">[… az aláírt xml rész…, jelen specifikáció szerint ide jön a már
titkosított üzenet, ez van aláírva]
        </Object>
        </Signature>
```

5.3 XML titkosítás

Vonatkozó W3C ajánlás:
XML Encryption Syntax and Processing: http://www.w3.org/TR/xmlenc-core/

Példa:

```
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
    xmlns="http://www.w3.org/2001/04/xmlenc#">
 <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
   <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <KeyName>rsaKey</KeyName>
   </KeyInfo>
   <CipherData>

    <CipherValue>gTCmIpX4ng+o8X4qUR2mJqT8wNJs6trhfklDJKVP+efxY8hFe/4nt2N1iK5LkNqCe
    r0xLWxx8ZXxNGDOLd0ij7QH1hobXGQ0QfzpsdvwoXraWYF0ZwLejzSQnVy0rDqmd6zSHvv5fL6eryZ
    g+mQpnyWqNJP9UzIRnz32uTlZmDM=</CipherValue>
   </CipherData>
  </EncryptedKey>
 <KeyValue>
 <RSAKeyValue>

    <Modulus>tcSQvQfy5i2WGf9wqLqN/+xAwJw+kj/LqzccMbW2Dn3Wi7zCv6I+wfXbihk+z8Cn/vpBW
    9TtKdiHiMHXEAkiihp2QJae+5S1WCi3y4ZjehJ7HDbkFq+vNX73ud+psa2TunOke/mBIwtFR7TBInV
    efAH/DTSDxEwQ5HW1ELkyEPE=</Modulus>
 <Exponent>AQAB</Exponent>
   </RSAKeyValue>
  </KeyValue>
 <X509Data>

    <X509Certificate>MIICKzCCAZigAwIBAgIQVw7hBxT5zZxMfvOtfBR50zAJBgUrDgMCHQUAMCIxI
    DAeBgNVBAMTF0tLSzIgV0VCIFRlc3QgQXV0aG9yaXR5MB4XDTA3MTAwNDEwNTE0NloXDTM5MTIzMTI
    zNTk1OVowHjEcMBoGA1UEAxMTVGVzdCBWUCBDcnlwdGVyIEtleTCBnzANBgkqhkiG9w0BAQEFAAOBj
    QAwgYkCgYEAtcSQvQfy5i2WGf9wqLqN/+xAwJw+kj/LqzccMbW2Dn3Wi7zCv6I+wfXbihk+z8Cn/vp
    BW9TtKdiHiMHXEAkiihp2QJae+5S1WCi3y4ZjehJ7HDbkFq+vNX73ud+psa2TunOke/mBIwtFR7TBI
    nVefAH/DTSDxEwQ5HW1ELkyEPECAwEAAaNuMGwwFQYDVR0lBA4wDAYKKwYBBAGCNwoDDDBTBgNVHQE
    ETDBKgBDLCV0X1F6i7wnGQ4effz04oSQwIjEgMB4GA1UEAxMXS0tLMiBXRUIgVGVzdCBBdXRob3Jpd
    HmCEAFToJVZJlmGToZZtvh2avcwCQYFKw4DAh0FAAOBgQBVibiwXhhgAfHXFGk99K6aTg75TfbcLbU
    L7jK1e9asIUCSahdTRw+oT4/t025OcZ2jzW8p1J1ixiUxScs39uencImnOI9gYNXkk/d6uCf1gvDGd
    xkOk1KC0UT17iGGQorCuc0ffuEiD7pGAiddTRKaLecNW7onJOje7tdkoC2Sow==</X509Certifica
    te>
   </X509Data>
  </KeyInfo>
 <CipherData>
 <CipherValue>[ez a rész az üzleti üzenet titkosított formában]

    sA7zcZKI/syc/wLGSRRSbAEf7ywroNp/iD0TXLY1uVe7No34vS68vD1Lo4IT/6o8xxemgW3T1FOydQ
    A1GEor738HY6CWhmkUQEfcIuONd/e3MSV+iwOqtzZXCCZvY8Vm/JKkodA+4MdyavVtjFAO4+48zdAY
    /Heql6qjzagwvBNnwm1zs0IqKQ6vUaAXrNYEd66B4WxDEunBcYbmYCI9rlrEPM/5b0nLYfqS2LCCz7
    Crix7pu2syLsx4pmMprw06k6TbPChKP6cH2scMJ5VV8LCwlA7l3RZ8t5VcvztUpz9Nr/fiu+X6f/2M
    UVgglJRJ/R+88tTVI5bxss3HAQyHZnKJux30pOee+IHgdhivxbUGxp5zcj9QNBXDHVSngutiIIO+pm
    eOZMkKhd5OLhjbCH1Q4938BiDNLzXlyS4k8tAV0seLkvNtNdSrUIe1gEX2wEwJ3G2MoMc8I6+H59zS
    NSb3EXkNHuVx6ZBkRQ+yjm03LaA0hxaOTDzGlgswx1Z5GsWS9ncay7nDjkUVQRRjsZ7VryuaO4QOa0
    mBjBYpWVFoEvdnRUAD2x/OUFq/0O1vpcyk5ojp///3faELasumpecIKnoAouJx43LsKnJ2BDKuVylC
    pF1VXRyVb4+eegkBqdDfnDk0SWD5YEDqukVSnkKHjYr+2zED7nRNiHkAButOb7JV1jditYX1a2ACaC
    NHxROoez+ocY1HQ3ewJgX8qSxT4XSJ6QNANZEdJBlIInV56Xx/SJiAuzO8hG9jA57zrOKmlg/pd+V7
    bSu1UOwjvrr7YOfk+I0LIdWkrT6GXqY9cSP/jh1xJuUomfgWxb4txrui+NnPgzZRNG0m6DcYqiKbgX
```

```
5itXkpT2zY2x0nExTvlfPKLgWIHWnbsFfE5+wS6o6EQZCnohqoyMl+jFRKnena9BlYUrMeNozbaslF
2EkY6pQ/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>2007-03-01T13:52:40.3825253+01:00</vp:Created>
    <vp:Properties>[adott rendszer specifikációjában meghatározott tulajdonságok]
        <vp:Property name="AAAAA">BBBBBB</vp:Property>
    </vp:Properties>

  </vp:Header>
  <vp:Body>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
     <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
        20010315" />
     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
     <Reference URI="#object-1">
     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
     <DigestValue>L+R9DBDr6CDKPztJiuYdkaOx7GQ=</DigestValue>
       </Reference>
       </SignedInfo>

       <SignatureValue>KX7ecBt7e0l61Md1XmF/ArajyzaFBhEvRmZdyYfyi93EFtZdGQbETrGp1Ajo2k
       6Iw59t4gbOlOd8Nwfc3evVJNhOOXhR2s6c76c3rb+x1fMCqzNjzwo3OzS/1O/cZgKaKWtDvy9aSGLm
       CkEahVjuLTEDqwXNiV8tOTi+mWxXqRk=</SignatureValue>
     <KeyInfo>
     <KeyValue>
     <RSAKeyValue>

       <Modulus>z+YqO3ZYZkeSCqJKUIdiP9p3xupqyBQEEc11YI7R+CZYFrd7+yrGQeNLtATgPvXBZOgnR
       iGwMTPohvg+qZggCLTib0AGqtlyYzW77+opM9pa2SVJSaw8Lkh2Bhb1P/HTK4DIeaHJN67bQMyJUPW
       JKM2YE7NeNKebX66M3lKNSBE=</Modulus>
     <Exponent>AQAB</Exponent>
       </RSAKeyValue>
       </KeyValue>
     <X509Data>

       <X509Certificate>MIIDpzCCAxCgAwIBAgIGQE32jRRtMA0GCSqGSIb3DQEBBQUAMIGaMQswCQYDV
       QQGEwJIVTERMA8GA1UEBxMIQnVkYXBlc3QxFTATBgNVBAoTDE5ldExvY2sgS2Z0LjEaMBgGA1UECxM
       RVGFudXNpdHZhbnlraWFkb2sxJDAiBgNVBAMTG05ldExvY2sgVGVzenQgKENsYXNzIFQyKSBDQTEfM
       B0GCSqGSIb3DQEJARYQaW5mb0BuZXRsb2NrLm5ldDAeFw0wNzEwMjQwOTU0MzJaFw0wNzExMjMwOTU
       0MzJaMIGRMQswCQYDVQQGEwItLTELMAkGA1UECAwCLS0xCzAJBgNVBAcMAi0tMQswCQYDVQQKDAItL
       TELMAkGA1UECwwCLS0xKTAnBgNVBAMMIE5ldExvY2sgVGVzenQgQWxhaXJvIHRhbnVzaXR2YW55MSM
       wIQYJKoZIhvcNAQkBFhRtYXJhaS5wYWxAdmFtLmdvdi5odTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwg
       YkCgYEAz+YqO3ZYZkeSCqJKUIdiP9p3xupqyBQEEc11YI7R+CZYFrd7+yrGQeNLtATgPvXBZOgnRiG
       wMTPohvg+qZggCLTib0AGqtlyYzW77+opM9pa2SVJSaw8Lkh2Bhb1P/HTK4DIeaHJN67bQMyJUPWJK
       M2YE7NeNKebX66M3lKNSBECAwEAAaOB/jCB+zCBhAYJYIZIAYb4QgENBHcWdUZJR1lFTEVNISBFemV
       uIHRhbnVzaXR2YW55IGNzYWsgdGVzenRlbGVzaSBjZWxva3JhIHN6b2xnYWwuIElNUE9SVEFOVCEgV
       GhpcyBjZXJ0aWZpY2F0ZSBpcyBvbmx5IGZvciB0ZXN0aW5nIHB1cnBvc2VzLjARBglghkgBhvhCAQE
       EBAMCBaAwDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBsAwQQYDVR0fBDowODA2oDSgMoYwaHR0c
       DovL2NybDEubmV0bG9jay5uZXQvaW5kZXguY2dpP3JhdyZjcmw9dGVzenQyMA0GCSqGSIb3DQEBBQU
```

```
            AA4GBAA56ctPKhcjOPxkYZtoKekf0N6G0+BSJey6vidJTCKf76sD+T3DuI25pYpspDmwYoW1veC1sb
            17zADfQiJJJCXwYbWumeGqYiP+8glkERupQj6WumCAz0b3Vj2dfnYNv96TC1XPnHF65JWM3CkHZT+c
            sIntucp/I+4hLaLs792PJ</X509Certificate>
           </X509Data>
           </KeyInfo>
         <Object Id="object-1">
         <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
            xmlns="http://www.w3.org/2001/04/xmlenc#">
         <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
         <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
         <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
         <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
         <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
         <KeyName>rsaKey</KeyName>
           </KeyInfo>
         <CipherData>

            <CipherValue>gTCmIpX4ng+o8X4qUR2mJqT8wNJs6trhfklDJKVP+efxY8hFe/4nt2N1iK5LkNqCe
            r0xLWxx8ZXxNGDOLd0ij7QH1hobXGQ0QfzpsdvwoXraWYF0ZwLejzSQnVy0rDqmd6zSHvv5fL6eryZ
            g+mQpnyWqNJP9UzIRnz32uTlZmDM=</CipherValue>
           </CipherData>
           </EncryptedKey>
         <KeyValue>
         <RSAKeyValue>

            <Modulus>tcSQvQfy5i2WGf9wqLqN/+xAwJw+kj/LqzccMbW2Dn3Wi7zCv6I+wfXbihk+z8Cn/vpBW
            9TtKdiHiMHXEAkiihp2QJae+5S1WCi3y4ZjehJ7HDbkFq+vNX73ud+psa2TunOke/mBIwtFR7TBInV
            efAH/DTSDxEwQ5HW1ELkyEPE=</Modulus>
         <Exponent>AQAB</Exponent>
           </RSAKeyValue>
           </KeyValue>
         <X509Data>

            <X509Certificate>MIICKzCCAZigAwIBAgIQVw7hBxT5zZxMfvOtfBR50zAJBgUrDgMCHQUAMCIxI
            DAeBgNVBAMTF0tLSzIgV0VCIFRlc3QgQXV0aG9yaXR5MB4XDTA3MTAwNDEwNTE0NloXDTM5MTIzMTI
            zNTk1OVowHjEcMBoGA1UEAxMTVGVzdCBWUCBDcnlwdGVyIEtleTCBnzANBgkqhkiG9w0BAQEFAAOBj
            QAwgYkCgYEAtcSQvQfy5i2WGf9wqLqN/+xAwJw+kj/LqzccMbW2Dn3Wi7zCv6I+wfXbihk+z8Cn/vp
            BW9TtKdiHiMHXEAkiihp2QJae+5S1WCi3y4ZjehJ7HDbkFq+vNX73ud+psa2TunOke/mBIwtFR7TBI
            nVefAH/DTSDxEwQ5HW1ELkyEPECAwEAAaNuMGwwFQYDVR0lBA4wDAYKKwYBBAGCNwoDDDBTBgNVHQE
            ETDBKgBDLCV0X1F6i7wnGQ4effz04oSQwIjEgMB4GA1UEAxMXS0tLMiBXRUIgVGVzdCBBdXRob3Jpd
            HmCEAFToJVZJlmGToZZtvh2avcwCQYFKw4DAh0FAAOBgQBVibiwXhhgAfHXFGk99K6aTg75TfbcLbU
            L7jK1e9asIUCSahdTRw+oT4/t025OcZ2jzW8p1J1ixiUxScs39uencImnOI9gYNXkk/d6uCf1gvDGd
            xkOk1KC0UT17iGGQorCuc0ffuEiD7pGAiddTRKaLecNW7onJOje7tdkoC2Sow==</X509Certifica
            te>
           </X509Data>
           </KeyInfo>
         <CipherData>
         <CipherValue>[ez a rész az üzleti üzenet titkosított formában]

            sA7zcZKI/syc/wLGSRRSbAEf7ywroNp/iD0TXLY1uVe7No34vS68vD1Lo4IT/6o8xxemgW3T1FOydQ
            A1GEor738HY6CWhmkUQEfcIuONd/e3MSV+iwOqtzZXCCZvY8Vm/JKkodA+4MdyavVtjFAO4+48zdAY
            /Heql6qjzagwvBNnwm1zs0IqKQ6vUaAXrNYEd66B4WxDEunBcYbmYCI9rlrEPM/5b0nLYfqS2LCCz7
            Crix7pu2syLsx4pmMprw06k6TbPChKP6cH2scMJ5VV8LCwlA7l3RZ8t5VcvztUpz9Nr/fiu+X6f/2M
            UVgglJRJ/R+88tTVI5bxss3HAQyHZnKJux30pOee+IHgdhivxbUGxp5zcj9QNBXDHVSngutiIIO+pm
            eOZMkKhd5OLhjbCH1Q4938BiDNLzXlyS4k8tAV0seLkvNtNdSrUIe1gEX2wEwJ3G2MoMc8I6+H59zS
            NSb3EXkNHuVx6ZBkRQ+yjm03LaA0hxaOTDzGlgswx1Z5GsWS9ncay7nDjkUVQRRjsZ7VryuaO4QOa0
            mBjBYpWVFoEvdnRUAD2x/OUFq/0O1vpcyk5ojp///3faELasumpecIKnoAouJx43LsKnJ2BDKuVylC
            pF1VXRyVb4+eegkBqdDfnDk0SWD5YEDqukVSnkKHjYr+2zED7nRNiHkAButOb7JV1jditYX1a2ACaC
            NHxROoez+ocY1HQ3ewJgX8qSxT4XSJ6QNANZEdJBlIInV56Xx/SJiAuzO8hG9jA57zrOKmlg/pd+V7
            bSu1UOwjvrr7YOfk+I0LIdWkrT6GXqY9cSP/jh1xJuUomfgWxb4txrui+NnPgzZRNG0m6DcYqiKbgX
            5itXkpT2zY2x0nExTvlfPKLgWIHWnbsFfE5+wS6o6EQZCnohqoyMl+jFRKnena9BlYUrMeNozbaslF
            2EkY6pQ/a5PerNxt9OxzueO1</CipherValue>
           </CipherData>
          </EncryptedData>
         </Object>
        </Signature>

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

5.5 Hibaüzenetek

A KKK2 rendszerben előforduló hibaüzeneteket a KKK2 Interfész Specifikáció definiálja. Jelen dokumentum a kriptográfiai műveletek hibaüzeneteivel bővíti az 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.	KKK2/DOC/ISP/V1.14/2007. 10.11.	KKK2 Interfész specifikáció	1.14

8. Betűszavak és rövidítések

Jelen dokumentáció a következő betűszavakat és rövidítéseket használja:

Betűszó	Leírás
KKK	Külső Kommunikációs Központ
PKI	Public Key Infrastructure - nyilvános kulcsú titkosítás
PQP	Project Quality Plan - Projekt Minőségterv
X509	PKI szabvány

9. Minőségi kritériumok

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

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

10. Minőségellenőrzés

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