

# Koppelvlakbeschrijving aanleverservice Bancaire Infrastructurele Voorzieningen

Het aanleveren van kredietrapportages bij de BIV

## Inhoudsopgave

1.	Inleiding.....	3
1.1.	Doel en Doelgroep.....	3
1.2.	Leeswijzer .....	3
1.3.	Status.....	3
1.4.	Relatie met koppelvlakbeschrijving overheid (Logius) .....	3
2.	Aanleveren van berichten .....	4
2.1.	Inleiding.....	4
2.2.	Beveiliging .....	4
2.2.1	Transportniveau.....	4
2.2.2	Berichtniveau.....	5
2.2.3	Berichtinhoud niveau .....	5
2.3.	Sessieverloop .....	6
2.3.1	Ontvangen aanleververzoek .....	6
2.3.2	Controleer structuur aanleververzoek .....	6
2.3.3	Bepaal verantwoordingsproces.....	6
2.3.4	Uitvoeren proces .....	7
2.3.5	Verstuur aanleverantwoord .....	7
2.3.6	PI_Kenmerk .....	7
2.3.7	PI_Kenmerk bij aanleveren.....	7
2.3.8	PI_Kenmerk bij ophalen .....	8
2.4.	Berichtopbouw .....	8
2.4.1	Structuur .....	8
	<i>Tabel 3: Toelichting elementen aanleververzoek .....</i>	<i>10</i>
2.4.2	Ondertekening bericht .....	10
3.	Algemene afspraken .....	14
3.1.	Communicatiestandaarden .....	14
3.2.	Namespaces .....	14
3.3.	Karaktercodering en karakterset .....	14
3.4.	Datum en tijd .....	14
4.	Details aanleverservice .....	15
4.1.	Inleiding.....	15
4.2.	SOAP request .....	15
4.3.	SOAP response .....	18
4.4.	SOAP fault.....	19

## **1. Inleiding**

### **1.1. Doel en Doelgroep**

Dit document beschrijft het aanleveren van berichten bij (deelnemende) banken via de Bancaire Infrastructurele Voorzieningen (BIV). De maximale omvang van deze berichten is 3MB.

Dit document is bestemd voor ontwikkelaars van programmatuur voor het aanleveren van berichten bij (deelnemende) banken. Het beschrijft hoe gebruik moet worden gemaakt van de betreffende webservice: de aanleverservice van de BIV. De specificatie van de bij de BIV aan te leveren berichtinhoud (de zogenaamde payload) vormt geen onderdeel van dit document.

### **1.2. Leeswijzer**

Deze koppelvlakbeschrijving is als volgt opgebouwd. Het eerste hoofdstuk bevat algemene informatie. Het tweede hoofdstuk bevat een globale beschrijving van de werking van het aanleveren en de betrokken webservices. Het derde hoofdstuk geeft een overzicht van alle algemeen van toepassing zijnde standaarden en afspraken. Het vierde hoofdstuk beschrijft de betrokken webservices in meer detail.

### **1.3. Status**

Dit document beschrijft geen definitieve eindsituatie voor wat betreft het koppelvlak. De verwachting is dat de gebruikte open standaarden zich de komende jaren verder zullen ontwikkelen en dat de communicatiebehoefte ook aan verandering onderhevig zal zijn. Het gevolg hiervan is dat de eventuele wijzigingen binnen de BIV in gebruik zullen worden genomen. Dit kan gevolgen hebben voor de koppelvlakken van de voorzieningen.

### **1.4. Relatie met koppelvlakbeschrijving overheid (Logius)**

Om het voor marktpartijen snel en eenvoudig mogelijk te maken om gebruik te maken van de BIV, hebben de banken er voor gekozen aan te sluiten op de door de Nederlandse overheid gehanteerde koppelvlakbeschrijving.<sup>1</sup>

Dit betekent dat het koppelvlak identiek is aan dat voor de Digipoort, ook wel procesinfrastructuur genoemd. De koppelvlakbeschrijving van de BIV is derhalve een kopie van de koppelvlakbeschrijving van de overheid, waarin de bankspecifieke benamingen zijn doorgevoerd.<sup>2</sup> Daar waar om moverende redenen wordt afgeweken van de koppelvlakbeschrijving van de overheid is dit herkenbaar aan een uitroepteken in de linkerkantlijn, zie onderstaand voorbeeld:



Deze functionaliteit is binnen de BIV op een andere wijze geïmplementeerd.

De verschillen worden onder andere veroorzaakt omdat bij de BIV is gekozen voor een zuivere toepassing van het modelleren. Daarnaast is voor de naamgeving van nieuwe termen gekozen voor een internationale aanpak en zijn Engelse benamingen toegekend.

---

<sup>1</sup> Koppelvlakbeschrijving aanleverservice OTP SOAP 2008, versie 1.1 d.d. 10 december 2007.

<sup>2</sup> Alleen daar waar gebruik wordt gemaakt van afbeeldingen, schema's en voorbeelden van de overheid kan het zijn dat de overheidsbenamingen nog worden gebruikt.

## 2. Aanleveren van berichten

### 2.1. Inleiding

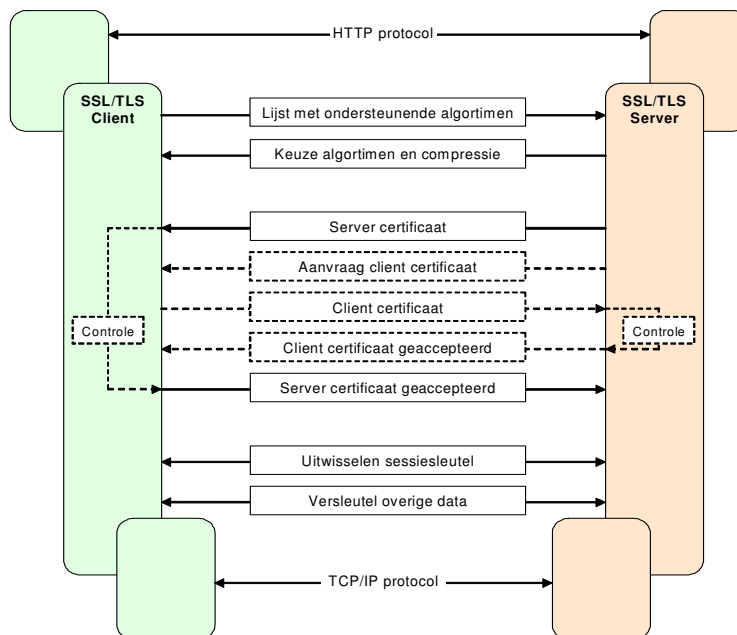
Alle verzoekberichten met betrekking tot het aanleveren van berichten worden door de BIV afgehandeld. De aanleverservice is de eerste service binnen de BIV en wordt uitgevoerd nadat de controles op de netwerklaag succesvol zijn afgerond. De aanleverservice stelt vast of een aanleververzoek van een direct belanghebbende of intermediair voldoet aan de vastgestelde koppelvlaakspecificaties. Vervolgens worden de andere services doorlopen en vindt de aflevering bij de betreffende bank plaats.

### 2.2. Beveiliging

#### 2.2.1 Transportniveau

De authenticiteit van de BIV en van gebruikers van de aanleverservice moet door alle deelnemende partijen vastgesteld kunnen worden voordat een datacommunicatiesessie wordt gestart. De authenticiteit van systemen wordt door X.509 (PKI-Overheid) certificaten gecontroleerd.

Feitelijk wordt de authenticiteit van aanleverservice bepaald aan de hand van het X.509 PKI-Overheid (client) certificaat dat zich op het clientsysteem bevindt. Met behulp van dit certificaat opent de client een verbinding volgens het SSL/TLS protocol. Dit protocol biedt naast authenticatie ook encryptie op transportniveau.



*Figuur 1: SSL/TLS sessie verloop*

In bovenstaand figuur zijn de fases van een SSL/TLS-sessie aangegeven met toelichting wanneer het certificaat voor controle gebruikt wordt.

De BIV dwingt het gebruik van client-authenticated SSL/TLS af om:

1. De vertrouwelijkheid en betrouwbaarheid van data tijdens transport te kunnen garanderen;
2. Gebruikers de mogelijkheid te bieden om de authenticiteit van de BIV te controleren voordat zij data inzenden of ophalen;

3. De BIV te beschermen tegen ongeautoriseerde gebruikers en alleen gebruikers met de juiste authenticatiemiddelen, in dit geval een geldig X.509 certificaat van een vertrouwde uitgever, toegang te verlenen tot de BIV.

Toegang tot de BIV kan pas plaatsvinden, nadat gecontroleerd is of het SSL/TLS X.509 clientcertificaat geldig is en of het certificaat vertrouwd (trusted) wordt.

De controle bestaat uit een correcte challenge/response tijdens het opzetten van de SSL/TLS-sessie. Daarin wordt onder andere gecontroleerd of het clientcertificaat uitgegeven is onder een door de BIV vertrouwde Certificate Authority (trusted CA). Alleen met een dergelijk certificaat kan toegang verkregen worden.

De geldigheid van het clientcertificaat wordt aan de hand van de gegevens in het certificaat gecontroleerd.

### **2.2.2 Berichtniveau**

Op berichtniveau wordt beveiliging toegepast door middel van WS-Security. Het bericht dient ondertekend te zijn met een handtekening over de SOAP body. Het certificaat dat hiervoor gebruikt wordt, moet aan dezelfde eisen voldoen als het certificaat dat gebruikt wordt op transportniveau. Het hoeft echter niet hetzelfde certificaat te zijn.

Deze beveiliging verzekert de integriteit en de herkomst van het bericht zelf.

Controle van de WS-Security handtekening houdt in het controleren dat de handtekening is gezet met een geldig certificaat. Deze relatie kan er uit bestaan dat het certificaat van het bedrijf zelf is, of dat het certificaat hoort bij een partij die door het bedrijf is gemachtigd om namens het bedrijf informatie uit te wisselen met overheidspartijen.

De controle of een relatie bestaat tussen het certificaat en het bedrijf waarop het bericht betrekking heeft vindt plaats door een externe Autorisatie Service Provider (AuSP). De AuSP houdt een register bij waarin staat vermeld welke vertegenwoordigingsrelaties er bestaan tussen bedrijven en intermediairs. Dit register vermeldt voor welke bedrijven de inzender, dus degene die de handtekening heeft gezet, verantwoordingsinformatie mag inzenden en de status/retour informatie mag inzien. Dit is niet alleen nodig voor intermediairs, maar ook voor bedrijven die meerdere Kamer van Koophandel- of andere identificerende nummers hebben.

Degene die een aanleververzoek doet, kan zelf aangeven bij welke AuSP-service hij geregistreerd staat middels het "cspEndpoint" element in het aanleververzoek.<sup>3</sup>

Om een bericht bij de BIV aan te kunnen leveren, dient de gebruiker zich te kunnen autoriseren middels een X.509 certificaat, een berichtsoort en een bedrijfsnummer. De combinatie van deze drie gegevens dient bekend te zijn in het betreffende autorisatieregister van de AuSP.

### **2.2.3 Berichtinhoud niveau**

Afhankelijk van de berichtsoort kan het verplicht zijn de berichtinhoud (payload) ook te ondertekenen met behulp van een X.509 certificaat.



Deze functionaliteit is binnen de BIV (op dit moment) niet vereist.

---

<sup>3</sup> Het gegeven "cspEndpoint" moet binnen de BIV geregistreerd zijn.

De handtekening is bestemd voor de bank waar het bericht afgeleverd wordt.

### 2.3. Sessieverloop

Het aanleverproces wordt getriggerd door het aanleververzoek (SOAP request). Als het verantwoordingsproces is doorlopen, ontvangt de aanleverservice een procesantwoord (SOAP response). Naar aanleiding hiervan wordt door de aanleverservice een antwoord (SOAP response) opgesteld en aan de gebruiker verstuurd.

Als het verantwoordingsproces om een bepaalde reden niet volledig kan worden doorlopen, ontvangt de aanleverservice een foutmelding. Naar aanleiding hiervan wordt door de aanleverservice een aanleverfoutmelding opgesteld en aan de gebruiker verstuurd.

#### 2.3.1 Ontvangen aanleververzoek

Elk verzoek aan de aanleverservice wordt vastgelegd in de audittrail. De berichtinhoud, het XBRL instance document, wordt niet opgeslagen.

#### 2.3.2 Controleer structuur aanleververzoek

Om verantwoordingsinformatie aan de BIV aan te kunnen bieden wordt gebruik gemaakt van een aanleververzoek met een voorgedefinieerde structuur. Deze structuur is vastgelegd met de Web Service Definition Language (WSDL).



De WSDL is bij de BIV op te vragen: <https://www.btp-frcportaal.nl/ode/processes/Kredietrapportageproces/FilingProcess/Process/Client?wsdl>.

Nadat een aanleververzoek door de BIV is ontvangen, worden de volgende zaken gecontroleerd:

Controle	Toelichting
Is een element aanwezig?	Hierbij wordt gecontroleerd of alle verplichte elementen zoals beschreven in de WSDL voorkomen in het aanleververzoek.
Bevat het element een waarde?	Hierbij wordt gecontroleerd of alle verplichte elementen ook daadwerkelijk een waarde bevatten.
Betreft het een toegestane waarde?	Hierbij wordt gecontroleerd of alle elementen toegestane waarden bevatten. Bijvoorbeeld het element "tijdstempelAangemaakt". Hierbij wordt gecontroleerd of het element een bestaande datum en tijdstip bevat. Ook wordt gecontroleerd of de lengte van elke waarde niet langer is dan de toegestane lengte.

Tabel 1: Controles aanleververzoek



Andere in het aanleververzoek voorkomende elementen die niet in de WSDL zijn gespecificeerd, worden genegeerd.

#### 2.3.3 Bepaal verantwoordingsproces



In de Digipoort wordt op dit punt aan de hand van het berichtsoort bepaald welk verantwoordingsproces moet worden doorlopen. Binnen de implementatie van de BIV geschiedt dit reeds bij het ontvangen van het aanleververzoek.

### 2.3.4 Uitvoeren proces

Door de BIV wordt het proces uitgevoerd zoals in de procesdefinities bepaald. Als het proces niet met succes kan worden doorlopen, wordt een foutmelding aan de gebruiker verstuurd.

### 2.3.5 Verstuur aanleverantwoord

Als het proces met succes is doorlopen, wordt een aanleverantwoord verstuurd. Het aanleverantwoord bestaat uit de volgende elementen:

Element	Toelichting
PI_kenmerk	Het door de BIV toegekende unieke kenmerk aan het verantwoordingsproces.
aanleverKenmerk	Het kenmerk dat door een gebruiker aan een verantwoordingsproces is meegegeven.
berichtsoort	Het soort verantwoordingsproces waarop de verantwoordingsinformatie betrekking heeft.
tijdstempelAangemaakt	De datum en het tijdstip waarop het verzoek door een gebruiker is verzonden aan de BIV.
bedrijfsnummer	Het nummer waarmee het bedrijf kan worden geïdentificeerd.
cspEndpoint	Het endpoint van de AuSP-webservice die gebruikt wordt voor het autoriseren van de ondernemer of intermediair.
tijdstempelOntvangst	De datum en het tijdstip waarop de aanlevering is ontvangen door de BIV.

*Tabel 2: Elementen aanleverantwoord*

Een aantal elementen in het aanleverantwoord is rechtstreeks overgenomen uit het aanleververzoek. Dit vergroot de traceerbaarheid van verzoek- en antwoordberichten die bij elkaar horen, bijvoorbeeld in archieven.

Het aanleverantwoord bevat tevens een handtekening van de BIV volgens de WS-Security standaard. Deze handtekening is gezet over de body van het aanleverantwoord.

### 2.3.6 PI\_Kenmerk

Bij de aanleverservice en de mededelingen- en statusinformatieservice is er sprake van een PI\_Kenmerk. Op basis van het PI\_Kenmerk kan men mededelingen en of statusinformatie ophalen. Het PI\_Kenmerk biedt de gebruiker de mogelijkheid om informatie van een specifiek verantwoordingsproces op te halen. Bijvoorbeeld: "de nog niet opgehaalde mededelingen behorende bij de verantwoordingsinformatie met PI\_Kenmerk ABC-100401-0000001".

### 2.3.7 PI\_Kenmerk bij aanleveren

Bij het aanleveren van verantwoordingsinformatie kent de BIV een uniek PI\_Kenmerk toe, het PI\_kenmerk wordt in de SOAP response aan de gebruiker teruggegeven. De verantwoordingsinformatie wordt met PI\_Kenmerk afgeleverd bij de betreffende bank.

Ook kan men een relatie met een bestaand PI\_Kenmerk leggen door in het aanleververzoek het "betreftPI\_Kenmerk" te vullen. Hiermee kan de aangeleverde verantwoording gerelateerd worden aan een eerdere uitnodiging. Bijvoorbeeld: Bank

XYZ verstuurde eerder een uitnodiging tot het aanleveren van financiële rapportages. De ondernemer refereert aan deze uitnodiging door het PI\_Kenmerk in het "betreftPI\_Kenmerk" in te vullen.



Deze functionaliteit is binnen de BIV (op dit moment) niet geactiveerd; het gebruik van het veld "betreftPI\_Kenmerk" resulteert in een foutmelding.

### 2.3.8 PI\_Kenmerk bij ophalen

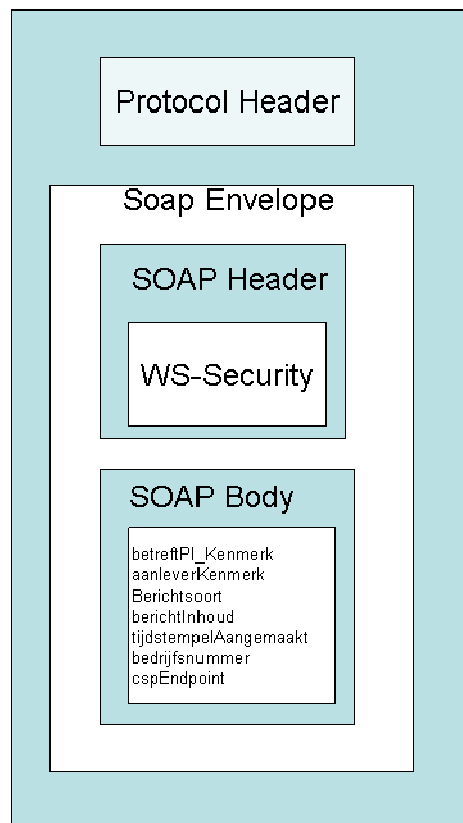
Banken kunnen een mededeling bezorgen bij de BIV, zodat de gebruiker deze mededeling kan ophalen. Bij het bezorgen van een mededeling bij de BIV dient de bank te vermelden: het bedrijfsnummer van de gebruiker waarvoor het bericht bestemd is, het berichtsoort en eventueel het PI\_Kenmerk van de aanlevering waarop het bericht betrekking heeft. Indien het bericht geen relatie heeft met een specifieke aanlevering, dan hoeft de bank geen PI\_Kenmerk mee te geven. De BIV zal dan zelf een nieuw kenmerk aanmaken.

Bij het ophalen van de mededelingen is het PI\_Kenmerk optioneel. Indien geen PI\_Kenmerk meegegeven wordt, dan zal op basis van het berichtsoort en het bedrijfsnummer de niet eerder opgehaalde mededelingen teruggegeven worden.

## 2.4. Berichtopbouw

### 2.4.1 Structuur

In onderstaand figuur wordt de opbouw van een SOAP bericht getoond:





Figuur 2: Samenstelling SOAP bericht

Het SOAP bericht bestaat uit:

1. De transportprotocol header
2. De SOAP envelope met daarin:
  - De SOAP header
  - De SOAP body

De SOAP header bevat de WS-Security elementen. De SOAP body bevat de inhoudelijke gegevens. Daarin kunnen de volgende elementen worden meegegeven:

Element	Formaat / Lengte	Verplicht	Beschrijving
betreftPI_Kenmerk	Tekst	Nee	Een optioneel element waarmee een relatie met een eerdere uitnodiging gelegd kan worden. Een dergelijke uitnodiging dient een bank in de vorm van een mededeling aan te leveren.  Deze functionaliteit is momenteel niet in gebruik.
aanleverKenmerk	Tekst / 40	Ja	Het element "aanleverKenmerk" beschrijft het kenmerk dat door een gebruiker aan het verantwoordingsproces is meegegeven.  De volgende eisen worden aan dit element gesteld: Het element is verplicht; De waarde van het element mag niet meer dan 40 karakters bevatten.
berichtsoort	Tekst	Ja	Het element "berichtsoort" beschrijft het soort verantwoordingsproces waarop de verantwoordingsinformatie betrekking heeft.  De volgende eisen worden aan dit element gesteld: Het element is verplicht; Het element dient een bekende waarde te hebben.  Een lijst met geldige berichtsoorten is apart beschikbaar.
berichtInhoud	Tekst	Ja	Het element "berichtInhoud" bevat de verantwoordingsinformatie in de vorm van een XBRL instance document.  De volgende eisen worden aan

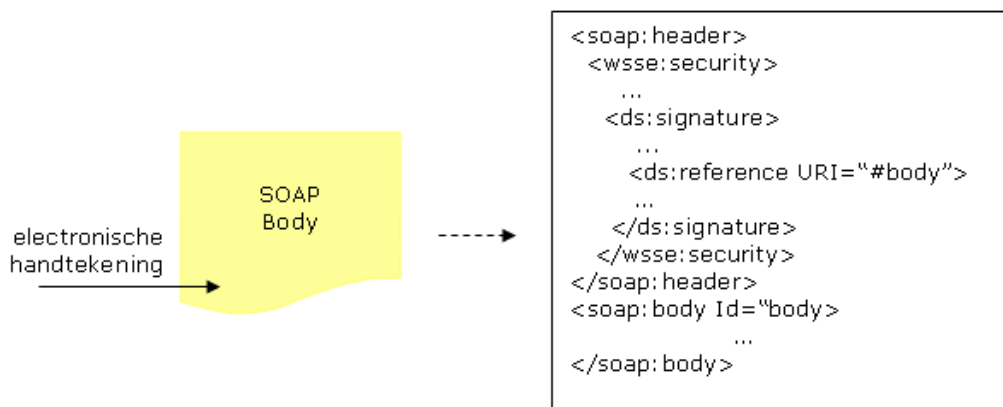
Element	Formaat / Lengte	Verplicht	Beschrijving
			<p>dit element gesteld:</p> <ul style="list-style-type: none"> <li>• Het element is verplicht;</li> <li>• De inhoud is gecodeerd met base64. De XML die gecodeerd wordt dient van het UTF-8 formaat te zijn.</li> <li>• De inhoud mag niet groter dan 3 MB zijn.</li> </ul> <p> De maximale omvang is beperkt tot 3MB (in plaats van 20MB voor Digipoort).</p>
tijdstempelAangemaakt	datetime	Ja	<p>Het element "tijdstempelAangemaakt" beschrijft de datum en het tijdstip waarop het verzoek door een gebruiker is gemaakt.</p> <p>De volgende eisen worden aan dit element gesteld:</p> <ul style="list-style-type: none"> <li>• Het element is verplicht;</li> <li>• Het element dient een geldige datum te bevatten;</li> <li>• De opmaak van deze datum dient te voldoen aan het volgende formaat: "YYYYMMDDTHH:MM:SS".</li> <li>• Het gebruik van milliseconden en tijdzone is optioneel</li> </ul>
bedrijfsnummer	Tekst / 20	Ja	Het bedrijfsnummer is het nummer waarmee het bedrijf kan worden geïdentificeerd waarover de rapportage betrekking heeft.
cspEndpoint	Tekst	Ja	Het element "cspEndpoint" bevat het endpoint van de webservice die gebruikt wordt voor het autoriseren van de ondernemer of intermediair. De endpoint van deze AuSP dient bij de BIV geregistreerd te staan.

Tabel 3: Elementen aanleververzoek

#### 2.4.2 Ondertekening bericht

Een belanghebbende of intermediair dient de body van het aanleververzoek te tekenen. Dit tekenen geschiedt met een X.509 certificaat. Het gebruikte certificaat, de handtekening en de gebruikte algoritmes dienen als WS-Security element in de header opgenomen te worden.

In onderstaande afbeelding is dit schematisch weergegeven:



Figuur 3: Handtekening van de body in de header

Voor het ondertekenen van het aanvraagverzoek kan de gebruiker gebruik maken van een portaal of service van marktpartijen die deze dienst leveren.

Onderstaand een voorbeeld van een WS-Security handtekening.

```

<wsse:security>
  <wsse:BinarySecurityToken ValueType="wsse:X509v3"
    EncodingType="wsse:Base64Binary"
    Id="X509Token">
    MIIIEUTCCAzmGAWIBAgIERX/lkT...
  </wsse:BinarySecurityToken>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:CanonicalizationMethod>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
</ds:SignatureMethod>
      <ds:Reference URI="#body">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
</ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
</ds:DigestMethod>
        <ds:DigestValue>0h4bgn6pB....</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>RHXzu6Z24Dc...</ds:SignatureValue>
    <ds:KeyInfo>
      <wsse:SecurityTokenReference>
        <wsse:Reference URI="#X509Token"/>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
</wsse:security>

```

De volgende eisen gelden voor de WS-Security elementen:

Security element	Waarde
Te hanteren Security Token	Base64-encoded X.509 certificaat
Te gebruiken algoritme voor de ondertekening	rsa-sha1 (RSA encryption Algorithm met een Secure Hash Algorithm)
Te ondertekenen deel	De gehele SOAP body.

Tabel 4: Eisen WS-Security elementen

Voor WS-Security dient versie 1.0 uit 2004 gehanteerd te worden, zoals gespecificeerd in het schema:

<http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>

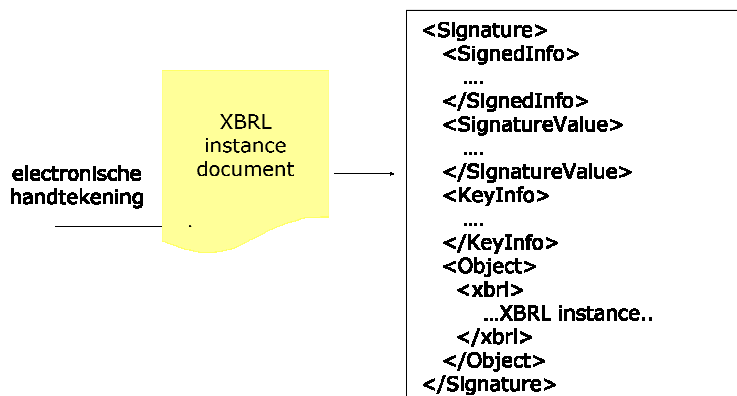
De gehele body van het aanleververzoek dient hierbij ondertekend te worden. Het element "berichtInhoud" dient gecodeerd te zijn volgens base64, alvorens de body ondertekend wordt.

Optioneel mag ook het "berichtInhoud" element getekend te zijn. Ook dit geschiedt met behulp van een elektronische handtekening met een X.509 certificaat. Dit mag hetzelfde certificaat zijn als waarmee de gehele body is ondertekend.



Deze functionaliteit is binnen de BIV (op dit moment) niet vereist.

De handtekening zit om de berichtinhoud. In onderstaande afbeelding is schematisch weergegeven hoe de elektronische handtekening om een XBRL instance document wordt geplaatst:



Figuur 4: Het XBRL instance document en de elektronische handtekening

De handtekening wordt geplaatst zoals omschreven in de XML-DSig standaard (<http://www.w3.org/TR/xmlsig-core/>). De handtekening wordt om het XBRL instance document gezet als een zogenaamde "Enveloping signature".

Onderstaand een voorbeeld van een elektronische handtekening.

```

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmlsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
      Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
    </ds:CanonicalizationMethod>
    <ds:SignatureMethod
      Algorithm="http://www.w3.org/2000/09/xmlsig#rsa-sha1">
    </ds:SignatureMethod>
  
```

```

<ds:Reference URI="">
  <ds:Transforms>
    <ds:Transform
      Algorithm="http://www.w3.org/TR/2001/
        REC-xml-c14n-20010315#WithComments">
    </ds:Transform>
  </ds:Transforms>
  <ds:DigestMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
  </ds:DigestMethod>
  <ds:DigestValue>0h4bgn6pBcWygTUNw8aTPUpkYKM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
RHXwoeuouoo4w3ufo534nv55ouvtowuetoevtowueotuwvoeuvton
6+i/98/ZNhwZmZ5weoiruoiuerouqorniowrnrvnourWERHWERRC
wrruwruwrowurweQWRY
</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>
MIwIBAgIERX/IG9w0BAQUFADBfMQswCQYDVQQGEwJOTDEwSMBA
5dGFyMRowGAYDVQQDEExFEaWdpbdCBDQTEgMB4GCSqGSIb3DQE
pbm90YXludmwwHjsjdfsljdjfsjdfMDcwNjE0MTAzNTQ1WjCB4TEL
xIjAgBgNVBAoTGUlub2xAoMDAyNzE5MTEyMykxIjAgBgwwNVBAcTG
zZXdlZyA2NCAoMDANVBAsTHEVudshfkhshfhskWwwZpY2FhdCatI
TBgNVBAMTDElubLjEnMCjkjkdwehrhskfhkshfhkshfhkGV0cm8uc3Rh
5Lm5sMSMwIQYDVQQJExpHghdfhshfhshfhshfhHb3VkYTCBnzANB
FAAOBjQAwwY4RHJYsdhfruioweoriuhkshfwroweiffh1CvDdjTnLdIR8Pt
    </ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>

```

Het volgende geldt voor de signature elementen:

Security element	Waarde
Gehanteerd Certificaat	Base64-encoded X509 certificaat
Gebruikt algoritme voor de ondertekening	rsa-sha1 (RSA encryption Algorithm met een Secure Hash Algorithm)
Ondertekende deel	Het XBRL instance document

Tabel 5: Eisen signature elementen

### 3. Algemene afspraken

#### 3.1. Communicatiestandaarden

De communicatie tussen persoon en de aanleverservice verloopt over een aantal lagen. Per laag gelden standaarden. Samengevat gaat het om de volgende standaarden:

Laag	Standaard
Applicatielaag	XML
	SOAP
Sessiel laag	HTTP
Transportlaag	TCP
Netwerklaag	IP

Tabel 6: De gebruikte communicatiestandaarden per laag

#### 3.2. Namespaces

Door de aanleverservice worden de onderstaande prefixen gehanteerd:

Prefix	Namespace URI
soap-env	<a href="http://schemas.xmlsoap.org/soap/envelope/">http://schemas.xmlsoap.org/soap/envelope/</a>
wSDL	<a href="http://schemas.xmlsoap.org/wSDL">http://schemas.xmlsoap.org/wSDL</a>
ds	<a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a>
wsse	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd</a>

Tabel 7: Gehanteerde prefixen aanleverservice

#### 3.3. Karaktercodering en karakterset

Door de aanleverservice wordt de Extensible Markup Language (XML) 1.0 (Third Edition) W3C Recommendation 04 February 2004 gehanteerd. Hierbij worden zowel het UTF-8 als het UTF-16 karaktercoderingsmechanisme ondersteund.

#### 3.4. Datum en tijd

Voor alle datum/tijd velden wordt gebruik gemaakt van het type xs:date en xs:dateTime, ingevuld naar de UTC (Z) variant op de ISO 8601 (NEN28601) standaard. Het gebruik van fracties van seconden en een tijdzone is optioneel.

## 4. Details aanleverservice

### 4.1. Inleiding

De aanleverservice kent drie typen berichten:

Onderdeel	Toelichting
SOAP request	Het bericht aan de aanleverservice waarmee verantwoordingsinformatie aan de BIV kan worden aangeleverd.
SOAP response	Een antwoordbericht dat wordt verstuurd wanneer de verantwoordingsinformatie door de aanleverservice correct is verwerkt.
SOAP fault	Een foutbericht dat wordt verstuurd wanneer een fout is geconstateerd.

Tabel 8: Typen berichten aanleverservice

In dit hoofdstuk zijn deze berichten nader uitgewerkt.

### 4.2. SOAP request

Er wordt geen gebruik gemaakt van UDDI voor het ontdekken van services.

Het adres van de aanleverservice is:

[https://www.btp-frcportaal.nl/ode/processes/Kredietrapportageproces/FilingProcess/Process/Client<sup>4</sup>](https://www.btp-frcportaal.nl/ode/processes/Kredietrapportageproces/FilingProcess/Process/Client<sup>4</sup)

Het SOAP request dat aan de aanleverservice kan worden verstuurd, dient er als volgt uit te zien (let op: voor de in te vullen elementen zijn fictieve waarden gebruikt):

```
<soapenv:Envelope xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Header>
    <wsse:Security soapenv:mustUnderstand="1"
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <wsse:BinarySecurityToken
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
        wsu:Id="x509bst_43"
        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">MII...kLIM</wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
```

<sup>4</sup> In de URL van de BIV is een nadere aanduiding opgenomen van de betreffende BIV middels een kenmerk (in dit voorbeeld btp), het van toepassing zijnde kenmerk is opgenomen in het factsheet (www.rapportageportaal.nl).

```

    <ec:InclusiveNamespaces PrefixList="wsse ds xsi soapenc xsd soapenv"
      xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
  </ds:CanonicalizationMethod>
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
  <ds:Reference URI="#wssecurity_signature_id_42">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <ec:InclusiveNamespaces
          PrefixList="p178 xsi soapenc xsd wsu soapenv "
          xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>yxo2e2qdJUdUk2IEz69/WWQodK0=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>Sd8...OP2GY=</ds:SignatureValue>
  <ds:KeyInfo>
    <wsse:SecurityTokenReference>
      <wsse:Reference URI="#x509bst_43" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
    </wsse:SecurityTokenReference>
  </ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="wssecurity_signature_id_42"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd">
  <mes:leverAan xmlns:mes="http://servicelibrary.sbr-nl.nl/messagecheckservice"
    <mes:betreftPI_Kenmerk/>
    <mes:aanleverKenmerk>test aanlevering</mes:aanleverKenmerk>
    <mes:berichtsoort>ABNAMRO_kred</mes:berichtsoort>
    <mes:berichtInhoud>MIIEE ... QW=</mes:berichtInhoud>
    <mes:tijdstempelAangemaakt>2010-04-
01T10:00:00.000</mes:tijdstempelAangemaakt>
    <mes:bedrijfsnummer>12345678</mes:bedrijfsnummer>
    <mes:cspEndpoint>http://autorisatieregister/AuSPService</mes:cspEndpoint>
  </mes:leverAan>
</soapenv:Body>
</soapenv:Envelope>

```

Als de base64-gecodeerde berichtinhoud een XBRL instance document bevat, dan zal deze er gedecodeerd als volgt uit zien:

```

<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315">
    </CanonicalizationMethod>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
    </SignatureMethod>
    <Reference URI="#xbrl">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments">
        </Transform>
      </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">

```

```

</DigestMethod>
  <DigestValue>0...KM= </DigestValue>
</Reference>
</SignedInfo>
<SignatureValue> CH...4qTo= </SignatureValue>
<KeyInfo>
  <X509Data>
    <X509Certificate> MIIETCCAzmGAW ... jg34J5dS8= </X509Certificate>
  </X509Data>
</KeyInfo>
<Object id="xbrl">
  <xbrli:xbrl xmlns:xbrli="http://www.xbrl.org/2003/instance"
    xmlns:iso4217="http://www.xbrl.org/2003/iso4217"
    xmlns:bank="http://www.rapportagedomein.nl/BT2010/bank/domein/bank/bankj"
    xmlns:link="http://www.xbrl.org/2003/linkbase"
    xmlns:xlink="http://www.w3.org/1999/xlink">
    <link:schemaRef xlink:arcrole="http://www.w3.org/1999/xlink/properties/linkbase"
      xlink:href="http://www.rapportagedomein.nl/BT2010/bank/report/rpt-bank-kred-
klein-2009.xsd"
      xlink:type="simple"/>
    <xbrli:context id="Y0INST">
      <xbrli:entity>
        <xbrli:identifier scheme="http://www.bank.nl/bank-id">12345678</xbrli:identifier>
      </xbrli:entity>
      <xbrli:period>
        <xbrli:instant>2009-12-31</xbrli:instant>
      </xbrli:period>
    </xbrli:context>
    <xbrli:context id="Y1INST">
      <xbrli:entity>
        <xbrli:identifier scheme="http://www.bank.nl/bank-id">12345678</xbrli:identifier>
      </xbrli:entity>
      <xbrli:period>
        <xbrli:instant>2009-12-31</xbrli:instant>
      </xbrli:period>
    </xbrli:context>
    <xbrli:context id="Y0DUR">
      <xbrli:entity>
        <xbrli:identifier scheme="http://www.bank.nl/bank-id">12345678</xbrli:identifier>
      </xbrli:entity>
      <xbrli:period>
        <xbrli:startDate>2009-01-01</xbrli:startDate>
        <xbrli:endDate>2009-12-31</xbrli:endDate>
      </xbrli:period>
    </xbrli:context>
    <xbrli:context id="Y1DUR">
      <xbrli:entity>
        <xbrli:identifier scheme="http://www.bank.nl/bank-id">12345678</xbrli:identifier>
      </xbrli:entity>
      <xbrli:period>
        <xbrli:startDate>2009-01-01</xbrli:startDate>
        <xbrli:endDate>2009-12-31</xbrli:endDate>
      </xbrli:period>
    </xbrli:context>
    <xbrli:unit id="CUR">
      <xbrli:measure>iso4217:EUR</xbrli:measure>
    </xbrli:unit>
    <xbrli:unit id="U0">
      <xbrli:measure>xbrli:pure</xbrli:measure>
    </xbrli:unit>

    <!-- Verantwoordingsinformatie -->

```

```
</xbri:xbri>
</Object>
</Signature>
```

### 4.3. SOAP response

Het antwoordbericht van de aanleverservice ziet er als volgt uit:

```
<soapenv:Envelope
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Header>
    <wsse:Security
      soapenv:mustUnderstand="1"
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd">
      <wsse:BinarySecurityToken
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"
        wsu:Id="x509bst_62"
        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd">MIIEUDCC...QnWDuCWzvSQ==</wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces
              PrefixList="wsse ds xsi soapenc xsd soapenv "
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
          <ds:Reference URI="#wssecurity_signature_id_61">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces
                  PrefixList="p178 xsi soapenc xsd wsu soapenv "
                  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <ds:DigestValue>6H25/wr1Kff+eQ9LGKkWS2F3yO0=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>VMXcOyq1K7...G2Qt0o=</ds:SignatureValue>
        <ds:KeyInfo>
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#x509bst_62"
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-
token-profile-1.0#X509v3" />
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="wssecurity_signature_id_61"
    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
    <mes:leverAanResponse xmlns:mes="http://servicelibrary.sbr-
```

```

nl.nl/messagecheckservice">
  <mes:leverAanReturn>
    <mes:PI_Kenmerk>BTP-100401-0000001</mes:PI_Kenmerk>
    <mes:aanleverKenmerk>test</mes:aanleverKenmerk>
    <mes:berichtsoort>ABNAMRO_kred</mes:berichtsoort>
    <mes:tijdstempelAangemaakt>2010-04-
01T10:00:00.000</mes:tijdstempelAangemaakt>
    <mes:bedrijfsnummer>12345678</mes:bedrijfsnummer>
    <mes:cspEndpoint>http://autorisatieregister/AuSPService</mes:cspEndpoint>
    <mes:tijdstempelOntvangst>2010-04-01T10:00:12.345</mes:tijdstempelOntvangst>
  </mes:leverAanReturn>
</mes:leverAanResponse>
</soapenv:Body>
</soapenv:Envelope>

```

#### 4.4. SOAP fault

Als er tijdens de aanlevering van verantwoordingsinformatie een fout optreedt, wordt deze als SOAP fault geretourneerd. Deze SOAP fault ziet er als volgt uit:


```

<soapenv:Envelope
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Header/>
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Server</faultcode>
      <faultstring xmlns:axis2ns29="http://servicelibrary.sbr-
nl.nl/FilingProcess/Process">axis2ns29:FilingFault</faultstring>
      <detail>
        <Receive__requestFilingFault xmlns="http://servicelibrary.sbr-
nl.nl/FilingProcess/Process">
          <ErrorMessage:foutOmschrijving xmlns:ErrorMessage="http://servicelibrary.sbr-
nl.nl/errormessage">Het verzoek voldoet niet aan de koppelvlakspecificaties en kan hierdoor
niet door de infrastructurele voorzieningen worden verwerkt. De volgende fout is opgetreden:
MCS106: bedrijfsnummer niet aanwezig.</ErrorMessage:foutOmschrijving>
          <ErrorMessage:foutCode xmlns:ErrorMessage="http://servicelibrary.sbr-
nl.nl/errormessage">ALS100</ErrorMessage:foutCode>
          <ErrorMessage:PI_Kenmerk xmlns:ErrorMessage="http://servicelibrary.sbr-
nl.nl/errormessage" />
        </Receive__requestFilingFault>
      </detail>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

```

De volgende elementen zijn in dit SOAP fault opgenomen:

Element	Toelichting
faultcode	Veld dat het type fout aangeeft. Voor de BIV zijn er twee mogelijkheden, namelijk: <ul style="list-style-type: none"> <li>Client: de fout is opgetreden door toedoen van de aanleverende partij.</li> <li>Server: de fout is opgetreden door toedoen van de BIV.</li> </ul>
faultstring	Geeft de aard van de fout weer in voor

	mensen begrijpelijke taal.
detail/foutCode	Een unieke code waarmee een fout kan worden geïdentificeerd.
detail/foutOmschrijving	Een omschrijving van de fout.
detail/PI_Kenmerk	Het door de BIV toegekende unieke kenmerk.   Indien de fout optreedt nadat een PI-Kenmerk is toegekend (na het doorlopen van de berichtcontrole) wordt het PI-Kenmerk hier gegeven.

Tabel 9: Elementen SOAP fault