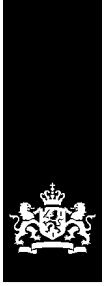


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakstandaard Grote Berichten Digikoppeling 2.0

Versie 1.2

Datum 10/06/2014
Status Definitief

Colofon

Logius Servicecentrum:
Postbus 96810
2509 JE Den Haag

t. 0900 555 4555 (10 ct p/m)
e. servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
25/04/2014	1.1	Logius	-
10/06/2014	1.2	Logius	Redactioneel bijwerken

Inhoud

1 Inleiding

1.1 Doel en doelgroep

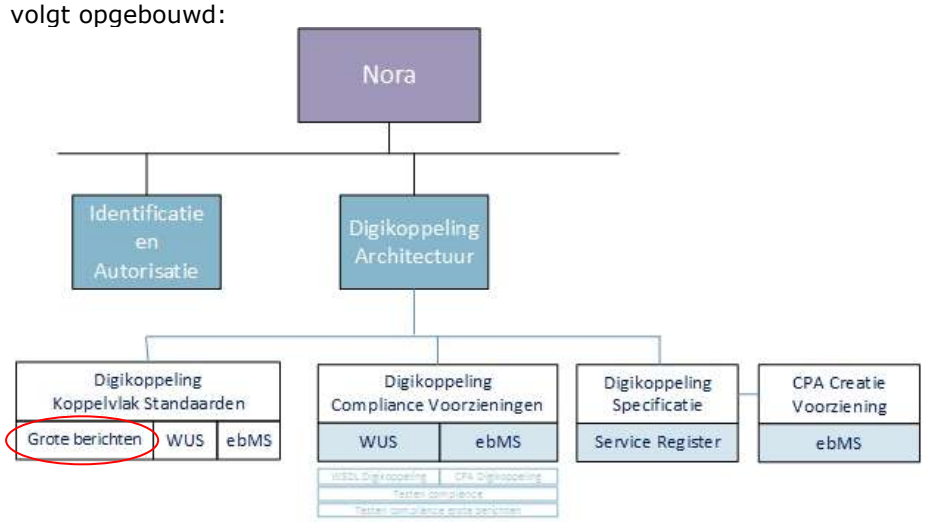
Dit document beschrijft de functionele specificaties voor de DigiKoppeling Grote Berichten, onderdeel van DigiKoppeling.

Het document is bestemd voor architecten en ontwikkelaars die op basis van DigiKoppeling Grote Berichten gegevens willen uitwisselen. Zie onderstaande tabel bij welke taken dit document ondersteunt. Alle webservices die op Grote Berichten gebaseerd zijn, moeten conformeren aan de koppelvlakstandaard Grote Berichten. Deze wordt tot in detail in dit document gespecificeerd. Het doel van dit document is ontwikkelaars te informeren wat deze koppelvlakstandaard nu precies inhoudt en waar zij zich aan moeten conformeren. Het document is bestemd voor architecten en ontwikkelaars die op basis van DigiKoppeling Grote Berichten gegevens willen uitwisselen. Het gaat hierbij om zowel (service) aanbieders als (service) afnemers.

Afkorting	Rol	Taak	Doelgroep?
[MT]	Management	Bevoegdheid om namens organisatie (strategische) besluiten te nemen.	**Nee**
[PL]	Projectleiding	Verzorgen van de aansturing van projecten.	**Nee**
[A&D]	Analyseren & ontwerpen (design)	Analyseren en ontwerpen van oplossings-richtingen. Het verbinden van Business aan de IT.	**Ja**
[OT&B]	Ontwikkelen, testen en beheer	Ontwikkelt, bouwt en configureert de techniek conform specificaties. Zorgen voor beheer na ingebruikname.	**Ja**

1.2 Opbouw Digikoppeling documentatie

Digikoppeling is beschreven in een set van documenten. Deze set is als volgt opgebouwd:



Figuur 1: Opbouw documentatie Digikoppeling

1.3 Doel en scope van Digikoppeling

Digikoppeling biedt de mogelijkheid om op een sterk gestandaardiseerde wijze berichten uit te wisselen tussen partijen. De uitwisseling tussen partijen wordt in drie lagen opgedeeld:

- Inhoud: Op deze laag worden de afspraken gemaakt de inhoud van het uit te wisselen bericht, dus de structuur, semantiek en waardebereiken. DigiKoppeling houdt zich **niet** met de inhoud bezig, 'heeft geen boodschap aan de boodschap'.
- Logistiek: Op deze laag bevinden zich de afspraken betreffende transportprotocollen (HTTP), messaging (SOAP), beveiliging (authenticatie en encryptie)en betrouwbaarheid. **Dit is de DigiKoppeling-laag.**
- Transport: deze laag verzorgt het daadwerkelijke transport van het bericht.

DigiKoppeling richt zich dus uitsluitend op de logistieke laag. Deze afspraken komen in de koppelvlakstandaards en andere voorzieningen. In het geval van WUS en ebMS komt de logistieke laag overeen met de 'header' van het bericht en gaat de 'body' uitsluitend over de inhoud. In het geval van Digikoppeling grote berichten is een deel van de logistieke informatie opgenomen in de 'body' van het bericht in de vorm van gestandaardiseerde meta-data.

1.3.1 Leidend principe

De koppelvlakstandaarden dienen te leiden tot een maximum aan interoperabiliteit met een minimum aan benodigde ontwikkelinspanning. Daarom wordt gekozen voor bewezen interoperabele internationale standaarden.

Digikoppeling maakt berichtenuitwisseling mogelijk op basis van de ebXML/ebMS en WUS families van standaarden inclusief de daarbij behorende verwante standaarden.

Aan te sluiten overheidsorganisaties hebben aangegeven op een uniforme manier (één stekker) te willen aansluiten aan Digikoppeling. Organisaties die beschikken over eigen middleware (ESB, broker) kunnen de aansluiting aan Digikoppeling, de adapters, in het algemeen realiseren via voorzieningen in die middleware.

De architectuur voor toepassing van Digikoppeling versie 2.0 is beschreven in het document "Digikoppeling_2.0_Architectuur_vx.x"[1] en voor Digikoppeling versie 3.0 "Digikoppeling_3.0_Architectuur_vx.x".

1.4 Koppelvlak & koppelvlakstandaard

Een koppelvlak is een interface die volgens vergaande standaards de gegevensuitwisseling verzorgt. Het werken met vaste standaards is essentieel voor een koppelvlak. Hierdoor wordt implementatie vergemakkelijkt. Ook wordt het mogelijk diverse soorten berichten door te sturen met een grote mate van interoperabiliteit, omdat via de standaard afspraken over hun inhoud gemaakt is.

Een van de belangrijkste eisen die door de overheid gesteld wordt bij de inrichting van generieke voorzieningen is dat er niet veel maatwerk ontwikkeld hoeft te worden, maar dat er van "off the shelf" commercieel of OPEN geleverde software gebruik gemaakt kan worden. Voor DigiKoppeling, dus voor de logistieke laag, betreft dat het niet willen ontwikkelen van software voor de adapters. Dit doel kan bereikt (benaderd) worden doordat gekozen wordt voor internationale (de jure of

[1] Met "vx.x" wordt de laatst gepubliceerde versie op de Logius website bedoeld.

de facto) vastgelegde standaards, die door "alle" leveranciers interoperabel zijn geïmplementeerd.

Een andere eis is dat met name afnemers gebruik kunnen maken van één "stekker" (één logistiek koppelpunt).

1.4.1 Specificatie van de koppelvlakstandaard

De koppelvlakspecificatie beschrijft de eisen waar de adapters aan moeten voldoen om interoperabel met elkaar te kunnen communiceren. DigiKoppeling gaat over logistiek, dus over de envelop en niet over de inhoud. De hele set info die tezamen nodig is voor een complete generieke DigiKoppeling koppelvlakdefinitie (Raamwerk Specificatie genoemd) bestaat uit:

- interfacedefinitie "on the wire", (voorbeeld)listing van SOAP headers, en informatie over velden en hun specifieke inhoud.

1.5 Opbouw van dit document

Hoofdstuk 1 bevat een aantal algemene inleidende onderwerpen.
Hoofdstuk 2 bevat de kern van de standaard met de algemene gebruiksvoorwaarden.
Hoofdstuk 3 gaat in op het gebruik van de metadata.
Hoofdstuk 4 gaat in op de wijze waarop grote bestanden uitgewisseld worden.

Begrippen en afkortingen worden toegelicht in het document "Digikoppeling_3.0_Architectuur_vx.x.pdf". Deze zit in de Digikoppeling aansluitkit.

Dit document en andere documentatie is beschikbaar op www.logius.nl/digikoppeling

2 Koppelvlakstandaard Grote Berichten

2.1 Inleiding

De situatie kan zich voordoen dat een WUS en/of ebMS bericht een grootte krijgt die niet meer efficiënt door de WUS / ebMS adapters verwerkt kan worden. Ook kan het zich voordoen dat er behoefte bestaat aan het buiten de normale procesgang ('out-of-band') sturen van aanvullende informatie naar systemen. In die gevallen zal dit "grote bericht" op een andere wijze verstuurd moeten worden: middels de DigiKoppeling Koppelvlakstandaard Grote Berichten. De volgende aanpak wordt dan gehanteerd:

- De verzender stelt een bestand samen uit (een deel van) de gegevens die normaliter in het "grote bericht" verzonden zou worden. Het resultaat wordt aangeduid met de term "groot bestand". Merk op dat dit ook een "groot" xml bestand kan zijn, een CAD bestand, een PDF document, een ZIP bestand, et cetera.
- De verzender stelt metadata samen over het grote bestand en verstuurt deze metadata in een WUS- of ebMS-bericht [in een zgn. stuurbericht].
- De ontvanger haalt het grote bestand op via het gespecificeerde HTTP 1.1 protocol (zoals in dit document gespecificeerd).
  De bestandsoverdracht is niet "betrouwbaar"; hiervoor dient de ontvanger aanvullende maatregelen te implementeren (retry-mechnisme, foutafhandeling). De Koppelvlakstandaard bevat hiervoor handvatten. Toepassing van deze handvatten in concrete implementaties vallen buiten de scope van het koppelvlak.

Merk op dat het stuurbericht naast metadata ook voorzien kan zijn van inhoudelijke informatie die al nodig is bij ontvangst van het bericht voorafgaand aan het nog op te halen grote bestand.

Dit document beschrijft welke gegevens er in de metadata opgenomen moeten worden en hoe het HTTP 1.1 protocol gebruikt moet worden voor de overdracht van het grote bestand.

2.2 Gebruiksvoorwaarden

Voor het gebruik van het DigiKoppeling Koppelvlakstandaard Grote Berichten gelden een aantal algemene eisen, zoals hieronder gespecificeerd.

Referentie	Specificatie
VW000	Partijen MOGEN bilateraal overeen komen of èn bij hoeveel MB berichtomvang de standaard Grote Berichten van toepassing is of volstaan kan worden met Digikoppeling WUS (bevragingen) danwel Digikoppeling ebMS (meldingen) sec.
	Een harde grens voor de berichtomvang is lastig te bepalen en in praktische zin is er sprake van overlap. Daarom is er voor gekozen dat partijen bilaterale afspraken kunnen maken waarin afgeweken wordt van de genoemde grens onder VW001, met dien verstande dat door het bilateraal karakter het nooit als argument gebruikt kan worden om andere organisaties te verplichten hieraan te voldoen.
VW001	Als partijen niet tot overeenstemming komen MOETEN zij berichten groter dan 20 MB via het Koppelvlak Grote Berichten afhandelen.
	Niet elke ontvanger is in staat om grote berichten te ontvangen (en te verwerken). Daarnaast dient te worden voorkomen dat grote berichten het transactionele berichtenverkeer eventueel zouden kunnen verstoren. Daarom dient ten aanzien van de omvang een harde grens te worden afgesproken.
VW002	Voor de overdracht van metadata MOET gebruik gemaakt worden van Digikoppeling, zoals aangeven in het hoofdstuk Metadata in dit document.
VW003	Voor de overdracht van grote bestanden MOET gebruik gemaakt worden van het mechanisme zoals aangeven in het hoofdstuk Bestandsoverdracht in dit document.

3 Metadata

De metadata beschrijft de informatie over het bestand dat verstuurd wordt met HTTP 1.1. De metadata zelf wordt verzonden via het WUS/ebMS Koppelvlak.

3.1 Functionele beschrijving

De onderstaande regels zijn van toepassing.

Referentie	Specificatie
MD000	Metadata MOET verstuurd worden middels een WUS en/of ebMS bericht.
MD001	De metadata XML structuur MOET voldoen aan het XML schema in hoofdstuk Metadata XML Schema Definitie.
	De metadata kan een op zich zelf stand bericht zijn, maar ook een deel van een groter bericht. Het is daarbij ook toegestaan om meerdere grote bestanden in een bericht op te nemen; voor iedere afzonderlijke bestand dient dan afzonderlijke metadata in het bericht te worden opgenomen.
MD002	Voor ieder groot bestand MOET een unieke URL gegenereerd te worden; deze URL dient gebruikt te worden om het betreffende bestand op te halen. De URL is dus uniek voor het gehele DigiKoppeling domein en wordt in het meta-bericht via het element <senderUrl> verstrekt aan de ontvanger.
	Door aan ieder bestand een unieke URL toe te kennen kan gegarandeerd worden dat het meta-bericht altijd aan het juiste bestand refereert. Het is wel toegestaan om hetzelfde bestand meerdere keren te verzenden (meerdere ontvangers); iedere ontvanger ontvangt dan wel een eigen meta-bericht, maar de URL verwijst dan telkens naar hetzelfde bestand. Ook is het toegestaan om meerdere unieke URL's naar hetzelfde bestand te laten verwijzen.
MD003	De metadata MAG het moment aangeven (datum/tijd) waarop het grote bestand beschikbaar zal zijn (element <creationTime>). Het datum/tijd formaat is een DateTime W3C formaat [W3C-DateTime] met de 'Z' (UTC) aanduiding. ALS dit veld ontbreekt of het moment ligt in het verleden MOET het bestand, uiterlijk op het moment dat de metadata verzonden wordt, beschikbaar zijn.
MD004	De metadata MAG het moment aangeven tot wanneer het grote bestand beschikbaar zal zijn.Het grote bestand MOET dan tenminste beschikbaar zijn tot het moment dat in de metadata aangegeven wordt (element <expirationTime>).; na dat moment is de beschikbaarheid van het bestand niet meer gegarandeerd. Het datum/tijd formaat is een DateTime W3C formaat [W3C-DateTime] met de 'Z' (UTC) aanduiding.
	Door een beperking op te leggen aan de beschikbaarheid wordt voorkomen dat het niet duidelijk is wanneer de betreffende bestanden weer mogen worden verwijderd.
MD005	De metadata MOET aangeven hoe groot het bestand is, uitgedrukt in het aantal bytes (element <size>).
	Door de omvang van een bestand vooraf ter beschikking te stellen kunnen de benodigde resources al vooraf gepland worden.

Referentie	Specificatie
MD006	De metadata MOET een checksum geven van het bestand (element <checksum>). Voorlopig dient alleen het MD5 algoritme ondersteund te worden; andere algoritmes kunnen in de toekomst eventueel worden toegevoegd. Deze checksum dient te worden weergegeven als een string van 32 hexadecimale digits (i.e. a t/m f en 0 t/m 9, case-insensitive) [RFC1321].
	Door een checksum toe te voegen kan de inhoud van een bestand na de overdracht geverifieerd worden. Voorlopig dient alleen het MD5 algoritme te worden ondersteund; andere algoritmes kunnen in de toekomst eventueel worden toegevoegd.
MD007	De metadata MOET de naam van het bestand opgeven, als string, met een lengte van maximaal 200 karakters (element <filename>). De toegestane karakters zijn letters, cijfers, punt, underscore, en hyphen. De naam van het bestand moet uniek zijn in de context van de uitwisseling tussen twee partijen (OIN verzender – OIN ontvanger).
	De eisen ten aanzien van bestandnamen kunnen voor ieder platform verschillend zijn; daarom kan de opgegeven bestandsnaam niet altijd als bestandsnaam aan de zijde van de ontvanger gebruikt worden.
MD008	De metadata MAG aangeven wat de context is van het WUS/ebMS bericht waar het onderdeel vanuit maakt (attribuut <contextId>).
	Met behulp van de contextID is het mogelijjk om de context van de applicatie op te nemen. Ook is het mogelijk een correlatie aan te brengen tussen het bestand en de metadata. Daarvoor moet het bestand dezelfde contextID bevatten.
MD009	De metadata MOET het Internet media type (MIME type of Content-type) specificeren van het bestand (element <contentType>) [RFC2046].
MD010	De metadata MOET de URL van de verzender (element <senderUrl>) of ontvanger (element <receiverUrl>) bevatten. De URL van de ontvanger MOET NIET gebruikt worden.
	De URL van de ontvanger dient vooralsnog niet gebruikt te worden. Daarom is momenteel alleen het ophalen (http-get) van grote bestanden mogelijk.

3.2 Metadata XML Schema Definitie

Dit hoofdstuk publiceert de XSD van de metadata.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified"
 xmlns:tns="http://www.logius.nl/digikoppeling/gb/2010/10"
 targetNamespace="http://www.logius.nl/digikoppeling/gb/2010/1
0">
 <xs:element name="digikoppeling-external-data-
references"type="tns:external-data-reference">
 </xs:element>

 <xs:complexType name="external-data-reference">
   <xs:sequence>
     <xs:element name="data-reference" maxOccurs="unbounded"
                          type="tns:data-reference" />
   </xs:sequence>
   <xs:attribute name="profile" type="tns:gb-profile" />
 </xs:complexType>


   <xs:complexType name="data-reference">
     <xs:sequence minOccurs="1">
       <xs:element name="lifetime">
```

```
          <xs:complexType>
            <xs:sequence>
              <xs:element name="creationTime"
type="tns:datetimeType"

minOccurs="0"  />
              <xs:element name="expirationTime"
type="tns:datetimeType"

minOccurs="0" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="content">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="filename" type="xs:NCName" />
              <xs:element name="checksum"
type="tns:checksumType" />
              <xs:element name="size" type="xs:unsignedLong" />
            </xs:sequence>
            <xs:attribute name="contentType" use="required"

   type="xs:string"/>
          </xs:complexType>
        </xs:element>
        <xs:element name="transport">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="location">
                <xs:complexType>
                  <xs:choice>
                    <xs:element name="senderUrl"
type="tns:urlType" />
                    <xs:element name="receiverUrl"
type="tns:urlType" />
                  </xs:choice>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="contextId" use="optional"/>
    </xs:complexType>


 <xs:simpleType name="gb-profile" final="restriction">
   <xs:restriction base="xs:string">
     <xs:enumeration value="digikoppeling-gb-1.0" />
     <!--
       DigiKoppeling GB profiel 1 aanduiding
     -->
   </xs:restriction>
 </xs:simpleType>

 <xs:complexType name="datetimeType">
   <xs:simpleContent>
     <xs:extension base="xs:dateTime">
       <xs:attribute name="type" use="required"
                                  type="xs:string"
fixed="xs:dateTime" />
     </xs:extension>
   </xs:simpleContent>
 </xs:complexType>
```

```
 <xs:complexType name="checksumType">
   <xs:simpleContent>
     <xs:extension base="tns:md5String">
       <xs:attribute name="type" use="required">
         <xs:simpleType>
         <xs:restriction base="xs:string">
           <xs:enumeration value="MD5" />
         </xs:restriction>
         </xs:simpleType>
       </xs:attribute>
     </xs:extension>
   </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="urlType">
   <xs:simpleContent>
     <xs:extension base="tns:anyString">
     <xs:attribute name="type" use="required"
fixed="xs:anyURI" />
   </xs:extension>
   </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="md5String">
   <xs:simpleContent>
     <xs:restriction base="tns:anyString">
     <xs:pattern value="[0-9a-fA-F]*" />

     </xs:restriction>
   </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="anyString">
   <xs:simpleContent>
     <xs:extension base="xs:string" />

   </xs:simpleContent>
 </xs:complexType>

</xs:schema>
```

3.3 Metadata XML Voorbeeld

Dit hoofdstuk presenteert een voorbeeld van de metadata van een bestand.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:digikoppeling-external-data-references
 profile="digikoppeling-gb-1.0"
 xmlns:tns="http://www.logius.nl/digikoppeling/gb/2010/10"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.logius.nl/digikoppeling/gb/2010/10/gb
-meta.xsd">
 <tns:data-reference contextId="12345">
  <tns:lifetime>
   <tns:creationTime type="xs:dateTime">2001-12-
31T12:00:00Z</tns:creationTime>
   <tns:expirationTime type="xs:dateTime">2001-12-
31T12:00:00Z</tns:expirationTime>
  </tns:lifetime>
  <tns:content contentType="application/xml">
```

```
      <tns:filename>NCName</tns:filename>
      <tns:checksum
type="MD5">0123456789abcdef0123456789abcdef</tns:checksum>
      <tns:size>0</tns:size>
    </tns:content>
    <tns:transport>
      <tns:location>
        <tns:senderUrl
type="xs:anyURI">https://any.url/any.name</tns:senderUrl>
      </tns:location>
    </tns:transport>
  </tns:data-reference>
</tns:digikoppeling-external-data-references>
```

4 Bestandsoverdracht

4.1 Functionaliteit

Bestandsoverdracht vindt plaats van de server naar de client op verzoek van de client. Voorafgaand aan iedere bestandsoverdracht dient eerst een bijbehorend meta-bericht via Digikoppeling te worden verzonden.

Referentie	Specificatie
GB000	De bestandsoverdracht MOET gerealiseerd worden op basis van het HTTP protocol, versie 1.1, conform [RFC2616].
GB001	Zowel de client als de server MOET de BYTE-RANGE optie ondersteunen conform [RFC2616] (i.e. Range, If-match, If-range, ETag en Content-range).
	De BYTE-RANGE optie wordt gebruikt om in geval van een resume onnodige hertransmissie van data te voorkomen. Hierdoor kan de voortgang van de bestandsoverdracht gegarandeerd worden. De ondersteuning van de byte ranges is niet verplicht conform de RFC maar in de Digikoppeling-context wel.
GB002	De client MOET de bestandsoverdracht ïnitieren door middel van een HTTP GET request conform [RFC2616].
GB003	Indien de client een OK response ontvangt (200), dan kan de client het grote bestand op basis van deze response reconstrueren; eventuele eerder ontvangen bytes MOET de client daarbij negeren (of overschrijven).
GB004	Indien de client een Partial Content response ontvangt (206), dan MOET de client het grote bestand op basis van deze en alle eerdere (partiële) responses reconstrueren; eventuele overlappende byte ranges MOET de client daarbij overschrijven met de laatst ontvangen data.
GB005	Indien de HTTP verbinding verbroken wordt voordat het volledige grote bestand ontvangen is,en de client wil de overdracht hervatten dan MOET dit plaatsvinden door middel van een "Range Retrieval" request conform [RFC2616].
	De "Range Retrieval" request maakt deel uit van de BYTE-RANGE optie. Indien the server byte ranges ondersteunt, dan zal deze een Partial Content response (206) naar de client sturen; indien de server geen byte ranges ondersteunt, dan zal deze een OK response sturen. De exacte response van de server is afhankelijke van eventueel aanwezige condities (if-range, if-match en if-unmodified-since) [RFC2616].

4.2 Beveiliging

Alleen de beoogde ontvanger moet in staat zijn om een groot bestand op te halen. Autorisatie van de client moet daarom plaatsvinden aan de hand van het OIN uit het certificaatvan deze client[2].

Referentie	Specificatie
GB006	Het HTTP transport MOET beveiligd zijn met TLS [RFC2246, RFC2818] op basis van een valide PKIoverheid certificaat [PKI-Cert].

2 *Dit moet niet verward worden met een PKI.Overheid client-certificaat. Het betreffende certificaat zal vaak niet alleen geschikt zijn als client maar ook als server; in deze context wordt het echter gebruikt in de client-rol.*

Referentie	Specificatie
GB007	De onderstaande TLS encryptie algoritmen en sleutellengtes MOETEN minimaal worden ondersteund: TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	Langere sleutellengtes zijn ook toegestaan mits deze minimale sleutellengtes ook beschikbaar zijn. Deze set is gebaseerd op bevindingen van NIST.
GB008	Zowel de client als de server organisatie MOET zich authenticeren met een PKIoverheid certificaat [PKI-CA, PKI-Cert].
	De basis voor authenticatie en autorisatie in Digikoppeling is OIN. Achtergronden over dit gebruik zijn opgenomen in de DigiKoppeling richtlijnen [Digikoppeling-Cert] (2-zijdig TLS).
GB009	De server organisatie MOET het transport autoriseren op basis van het OIN van een valide client certificaat [Digikoppeling-Cert].
GB010	Indien de server een HTTP request ontvangt van een niet geautoriseerd OIN (in het client certificaat) dan MOET een HTTP 403 (Forbidden) response naar de client gestuurd worden.
GB011	De server moet certificaat-revocatie-lijsten (CRL) gebruiken [PKI-Policy].
GB012	Het HTTPS transport MOET over poort 443 plaatsvinden.

4.3 Betrouwbaarheid

De noodzaak van betrouwbaarheid is afhankelijk van de context. Indien de bestandsoverdracht een melding (in combinatie met ebMS) betreft, is ook betrouwbaarheid noodzakelijk. Indien de bestandsoverdracht een bevraging (vaak in combinatie met WUS) betreft, is dit niet noodzakelijk maar hoogstwaarschijnlijk we wenselijk.
Voor de context van meldingen dient de client een retry mechanisme te implementeren rekening houdend met eventuele beperkte beschikbaarheid van het netwerk en/of de server (service-window).

Referentie	Specificatie
GB013	Voor meldingen, zoals bedoeld in de Digikoppeling architectuur, MOET een retry mechanisme toegepast worden dat rekening houdt met eventuele beperkte beschikbaarheid van het netwerk en/of de server (service-window)
	De specificatie van het aantal retries en tijdswindow vormt een situationeel af te spreken gegeven. Dit komt overeen met (afspraken over) de configuratie van ebMS implementaties.
GB014	Indien na ontvangst de omvang van het bestand niet overeen komt met de omvang uit het meta-bericht, dan MOET de bestandsoverdracht als niet-succesvol beschouwd worden (size error).
GB015	Indien na ontvangst de checksum van het bestand niet overeen komt met de checksum uit het meta-bericht, dan MOET de bestandsoverdracht als niet-succesvol beschouwd worden (checksum error).

5 References

5.1 Normative

[RFC 2246] IETF RFC 2246: The Transport Layer Security (TLS) Protocol, versie 1.0, januari 1999, IETF, http://www.ietf.org/rfc/rfc2246.txt

[RFC 2818] "HTTP Over TLS", distinguishes secured traffic from insecure traffic by the use of a different 'server port'.

[RFC 2616] "Hypertext Transfer Protocol, HTTP/1.1", Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, , June 1999**.** http://tools.ietf.org/html/rfc2616

[PKI-CA] PKI Overheid toegetreden certificatiehouders. http://www.logius.nl/pkioverheid/

[PKI-Cert] PKI Overheid Programma van Eisen PvE deel 3b, Certificate Policy – Services, Bijlage bij CP Domeinen Overheid/Bedrijven en Organisatie, januari 2009.
Zie www.logius.nl/pkioverheid, zoekterm "deel 3b".

[PKI-Policy] PKI Overheid Programma van Eisen PvE deel 2, Toetreding tot en Toezicht binnen de PKI voor de overheid, januari 2009.
Zie www.logius.nl/pkioverheid, zoekterm "deel 2".

[Digikoppeling-Cert] Document "Gebruik en achtergrond van Digikoppeling certificaten". www.logius.nl/digikoppeling.

[W3C-DateTime] XML Schema Part 2: Datatypes Second Edition, W3C Recommendation 28 Oktober 2004. http://www.w3.org/TR/xmlschema-2/

[RFC 1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992. http://www.ietf.org/rfc/rfc1321.txt

[RFC 2046] IETF RFC 2046: Multipurpose Internet Mail Extensions, (MIME) Part Two: Media Types, november 1996, IETF. http://www.ietf.org/rfc/rfc2046.txt http://www.iana.org/assignments/media-types/

5.2 Non-normative

Geen.