Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

Aansluitvoorwaarden JUBES

Versie 2.1

Datum	Juni 2023
Status	Definitief

Colofon

Afzendgegevens	**Justitiële Informatiedienst**
	Burg. Raveslootsingel 2 7607 GK Almelo Postbus 337 7600 AH Almelo www.justid.nl
Contactpersoon	Afdeling Verbindingen en Veiligheid (Venv)
	T 088 99 89000 info@justid.nl
Projectnaam	Justitie Berichten Service
Auteurs	VenV expertiseteam Gegevensuitwisseling – JUBES beheer

Inhoud

Wijzigingsblad

In onderstaande tabel is een overzicht opgenomen van de voorgaande versies van dit document. De gedane aanpassing(en) worden daarbij vermeld.

Doorgevoerde wijzigingen			
Versie	**Datum**	**Gewijzigd door**	**Aanpassing**
1.6	03-06-2015	Tactisch beheer EBV	
1.8	01-12-2018	Tactisch beheer EBV	Review + aanpassingen André Schluter
1.90	01-03-2022	Ellen van Aalst	Oude versie in nieuwe layout
1.91	01-03-2022	Jack Hanser	Nieuwe versie up-to-date gemaakt en opgeschoond
1.92	29-03-2022	Tjeerd van der Lijn Leon Voshaar	Review + aanpassingen
1.93	07-04-2022	Antoon Bijen	Review + aanpassingen
1.94	13-04-2022	Tolga Ün	Aanpassing lay-out en opmaak
2.0	14-04-2022	Tjeerd van der Lijn	Definitieve versie 2.0
2.1	16-6-2023	Tjeerd van der Lijn	Enkele correcties en toevoeging TLS 1.3

Tabel 1 Versies Document

Inleiding

Binnen het ministerie van Justitie en Veiligheid (JenV) vindt er veel digitale gegevensuitwisseling plaats. Om een veelvoud aan bilaterale oplossingen op technisch gebied, maar ook op de bovenliggende lagen (semantiek, proces) te voorkomen is de Justitie Berichten Service (JUBES) dienstverlening ontwikkeld.
JUBES faciliteert als broker alle digitale gegevensuitwisseling tussen de verschillende JenV-onderdelen, evenals het verkeer tussen JenV en haar (keten)partners buiten JenV. JUBES zorgt ervoor dat de berichten veilig en snel op de juiste plek komen.

JUBES wordt beheerd door de dienst Gegevensuitwisseling van de afdeling Verbindingen en Veiligheid (VenV) van de Justitiële Informatiedienst (Justid).

Verzeker u ervan dat u de meeste actuele versie van dit document "Aansluitvoorwaarden JUBES" voor u hebt. Een nieuwere versie vervangt altijd een oudere.

1. Algemene Aansluitvoorwaarden

Bij het aansluiten op JUBES gelden de volgende voorwaarden:

- Voor het beheer en onderhoud van JUBES zijn de afspraken van toepassing zoals tussen Justid en DI&I zijn vastgelegd in de DNO "JUBES";
- Voordat een koppeling in productie wordt genomen, wordt er eerst een succesvolle technische en functionele test uitgevoerd op de acceptatieomgeving;
- Bij significante uitbreiding van het aantal bevragingen op een bestaande verbinding moet het Jubes beheer door betreffende afnemer tijdig worden geïnformeerd;
- De MSH endpoints (Message Service Handler) dienen bij voorkeur een vast IP-adres te hebben. Indien beschikbaar heeft een FQDN ook de voorkeur. Houd het aantal IP adressen zo beperkt mogelijk. Subnets worden niet toegestaan;
- Om elkaar als vertrouwde partners te beschouwen dient iedere aangesloten partner haar omgeving optimaal beveiligd en 'schoon' te houden (denk aan malware of virus scanners);
- Het gebruik van PKI-O(verheids) certificaten of certificaten met gelijkwaardige hoge vertrouwelijkheidsniveau zijn verplicht (zie ook Bijlage 1 Certificaten);
- Voor transportbeveiliging hanteren we de TLS richtlijnen van het NCSC(1) en Digikoppeling. Jubes ondersteunt TLS 1.2 en 1.3
- Stresstesten zijn niet toegestaan. Andere testen (b.v. capaciteitstesten) dienen vooraf te worden aangemeld;
- Voor reguliere uitwisselingen is de maximale grootte van berichten (payloads) in principe beperkt tot 2 GB (zie ook paragraaf 3.2). Uitwisselen van grotere berichten is eventueel mogelijk. Situaties waarbij payloads structureel groter zijn dan 100MB dienen vooraf gemeld te worden;
- Eventuele verstoringen of vragen worden gemeld via Klant Contact en Service (info@justid.nl).

[1] https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

2. Beschrijving dienst JUBES

De inzet en het gebruik van JUBES verbetert en vereenvoudigt de beheersbaarheid van digitale gegevensuitwisseling en het verbinden van (JenV) partners aanzienlijk. De dienst maakt het mogelijk om op een veilige, snelle en eenduidige manier digitale informatie met elkaar uit te wisselen.
Er is maar één betrouwbare en veilige verbinding naar de JUBES-infrastructuur nodig in plaats van meerdere één-op-één verbindingen naar de verschillende partners.
De belangrijkste functionaliteit van deze gemeenschappelijke dienst is het veilig en snel routeren van inkomende informatie naar de juiste bestemming, waarbij de inhoud van de informatie ongewijzigd blijft. JUBES is derhalve een transparante broker. Routering vindt plaatst op basis van adresseringsinformatie wat meegeven is aan het bericht en niet op basis van de inhoud van het bericht (content-based-routing).

Als er sprake is van informatie-uitwisseling met JenV sectoren dan dient dit via JUBES te lopen. JUBES wordt vanuit een JenV-gemeenschappelijk budget gefinancierd en er gelden daardoor geen aansluitkosten.

2.1. Standaarden

Om binnen en buiten JenV interoperabiliteit te bereiken tussen meerdere actoren en te voorkomen dat er binnen het ministerie verschillende oplossingen gaan leven gebruiken we standaarden om informatie uit te wisselen.

De standaard voor informatie-uitwisseling binnen het Rijk is de Digikoppeling-standaard. Digikoppeling heeft als functioneel toepassingsgebied het intersectorale verkeer. Naast de Digikoppeling standaard kennen we binnen JenV ook de JAB (Justitie Asynchroon Berichtenverkeer) standaard, die op hoofdlijnen overeenkomt met de Digikoppeling ebMS standaard. Tenslotte wordt voor grensoverschrijdend verkeer (verkeer tussen Europese lidstaten) het AS4 profiel van ebMS 3.0 gehanteerd.

Dit resulteert in de volgende opties:

Tussen JenV onderdelen:
- JAB
- Digikoppeling (ebMS, WUS en RESTful API)

Tussen JenV onderdelen en andere overheidsorganisaties:
- Digikoppeling (ebMS, WUS en RESTful API)

Tussen JenV onderdelen en Europese lidstaten:
- AS4 profiel van ebMS3.0

Tussen JenV onderdelen en private partijen:
- Digikoppeling (ebMS, WUS en RESTful API)
- AS4 profiel van ebMS3.0
- RESTful API’s

2.1.1. JAB

De Justitiestandaard Asynchrone Berichtenuitwisseling (JAB-standaard) vormt de basis waarop de dienstverlening oorspronkelijk is gebaseerd. De JAB standaard beschrijft een manier van berichten transport (protocol) en een standaard envelop voor de berichten. Doordat de JAB standaard gebaseerd is op de open standaard ebusiness XML messaging standaard (ebMS) zijn er diverse producten in de markt die dit ondersteunen en is een grote mate van interoperabiliteit gegarandeerd.

De JAB standaard komt vrijwel volledig overeen met de Digikoppeling ebMS standaard.

2.1.2. Digikoppeling

De standaard voor informatie-uitwisseling binnen het Rijk is de Digikoppeling-standaard. Digikoppeling heeft als toepassingsgebied het intersectorale verkeer. Binnen de standaard is er de keuze voor 3 verschillende mogelijkheden van informatie-uitwisseling:

- Digikoppeling ebMS[2]
- Digikoppeling WUS[3]
- Digikoppeling API[4]

Bij het opzetten van een nieuw koppelvlak zal er een keuze gemaakt moeten worden voor de toe te passen standaard. Om dit gefundeerd te kunnen doen is het van belang te kijken naar de interactiepatronen binnen het koppelvlak:

Digikoppeling onderscheidt deze patronen: *bevragingen* en *meldingen*.

Kenmerkend voor bevragingen is dat deze niet-transactioneel zijn, er vindt geen wijziging plaats bij de bevraagde partij. Hierdoor is het voor de serviceprovider niet relevant hoe vaak een bevraging gebeurt. Bij het falen van een bevraging kan deze zonder consequenties opnieuw worden gedaan. Als er geen betrouwbaarheid in de uitwisseling nodig (en gewenst) is, kan er binnen Digikoppeling voor bevragingen **Digikoppeling WUS** ingezet worden.

Kenmerkend voor meldingen is dat deze transactioneel zijn, met andere woorden: er vindt een wijziging plaats bij de ontvangende ketenpartner. Hierdoor is de betrouwbaarheid belangrijk; er mag geen twijfel zijn omtrent de ontvangst van de berichten.
Als betrouwbaarheid in de uitwisseling vereist is, wordt **Digikoppeling ebMS** ingezet.
Opmerking: de Digikoppeling Architectuur uit 2021 schijft voor dat er geen onderscheid meer is in 'WUS voor bevragingen' en 'ebMS voor meldingen'
(https://publicatie.centrumvoorstandaarden.nl/dk/architectuur/2.0vv/).

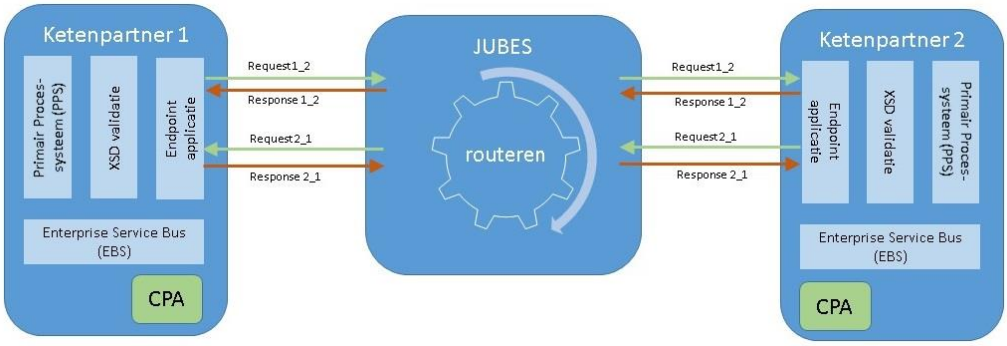
[2] https://publicatie.centrumvoorstandaarden.nl/dk/ebms/

[3] https://publicatie.centrumvoorstandaarden.nl/dk/wus/

[4] https://publicatie.centrumvoorstandaarden.nl/dk/restapi/

2.1.2.1. Digikoppeling ebMS

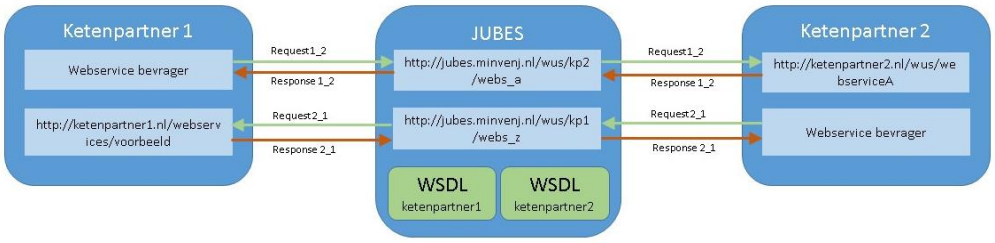
Bij het uitwisselen van informatie via ebMS wordt betrouwbaarheid belangrijker gevonden dan de snelheid (wat in onze omgeving vrijwel niet merkbaar is). Het gaat hierbij in de regel om 'once-and-only-once-delivery', waarbij dus zowel de gegarandeerde aflevering als ook het voorkomen van duplicaatberichten van belang is. Dit wordt mogelijk gemaakt door ontvangstbevestigingen (waarmee de verzendende partij weet dat zijn bericht door de ontvangende partij is ontvangen) en duplicate elimination (waarmee de ontvangende partij herzendingen op reeds ontvangen berichten zal negeren). EbMS heeft een retry mechanisme; mocht het verzendende endpoint geen bevestiging ontvangen van het ontvangende endpoint dan wordt het bericht opnieuw verstuurd vanaf het verzendende endpoint.



Belangrijk bij het gebruik van ebMS is de zgn. CPA (Collaboration Protocol Agreement). In dit formele XML-document staan alle technische en functionele eigenschappen over de gegevensuitwisseling. Dit document wordt bij beide partner op het endpoint geïmporteerd.
Naast betrouwbaarheid biedt ebMS ook uitgebreide mogelijkheden voor MLS (message-level security). Met MLS is het mogelijk om het bericht end-2-end te versleutelen (encryption) en/of te ondertekenen (signing). Met ondertekenen kan de afzender worden gegarandeerd en kan het bericht onderweg niet worden aangepast, het bericht blijft dus integer.
Welk profiel van toepassing is wordt gedaan vanuit de analyse. Bij extreem gevoelige data kan er gekozen worden voor een combinatie.

2.1.2.2. Digikoppeling WUS

WUS wordt vooral gebruikt voor het bevragen van informatiesystemen. Uitgangspunt hierbij is dat op de vraag die men stelt direct reactie wordt verwacht, waarbij de snelheid van afleveren en ontvangst van de respons het belangrijkste kenmerk is. Als een service niet beschikbaar is of er geen antwoord ontvangen wordt, kan de bevrager ervoor kiezen de vraag opnieuw aan te bieden (of juist niet). Een vraag kan zonder gevolgen opnieuw aangeboden worden.
Net zoals ebMS kunnen de berichten digitaal worden ondertekend (signing). Hiervoor wordt gebruik gemaakt van de 'WS-Security'-standaard. Ondertekenen geldt voor zowel request- als responsberichten. Met ondertekenen kan de integriteit van het bericht worden aangetoond, de identiteit kan worden vastgesteld en door de opname van een tijdstempel wordt aangegeven wanneer het bericht is gecreëerd.
De WUS-standaard is niet geschikt voor uitwisselingen waarbij betrouwbaarheid van aflevering van belang is, omdat de standaard hier geen functionaliteit voor biedt.



De tegenhanger van de CPA zoals die bij ebMS gebruikt wordt is de WSD. In tegenstelling tot een CPA die bilateraal wordt vastgelegd, bepaalt bij WSDL de serviceprovider zelf hoe de WSDL wordt opgebouwd. Deze WSDL wordt door de serviceprovider bij Jubes beheer aangeleverd en vervolgens op JUBES gepubliceerd.

2.1.2.3. Digikoppeling REST API

Een opkomende manier van gegevensuitwisseling zijn RESTful API's. Waar bij SOAP als dataformaat XML gebruikt, wordt REST meestal in combinatie gebruikt met JSON.

Het Digikoppeling REST API profiel [Digikoppeling Koppelvlakstandaard REST API] is gebaseerd op de REST API Design rules die in 2020 door het Kennisplatform API's zijn ontwikkeld.

Een application programming interface (API) is een gestructureerd en gedocumenteerd koppelvlak voor communicatie tussen applicaties. In de laatste 10 jaar heeft REpresentational State Transfer (REST) zich ontwikkeld tot een bepalend principe voor het realiseren van API's.

De standaard REST API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST API's aanbiedt. Dit maakt het voor ontwikkelaars gemakkelijker om betrouwbare applicaties met te ontwikkelen met API's van de overheid.

2.1.3. AS4 (profiel op ebMS3.0)

AS4 is de voorkeursstandaard vanuit de Europese Commissie[5]. We gebruiken deze standaard bij grensoverschrijdende uitwisseling met andere Europese Lidstaten.

[5] https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/eDelivery+AS4+conformant+solutions

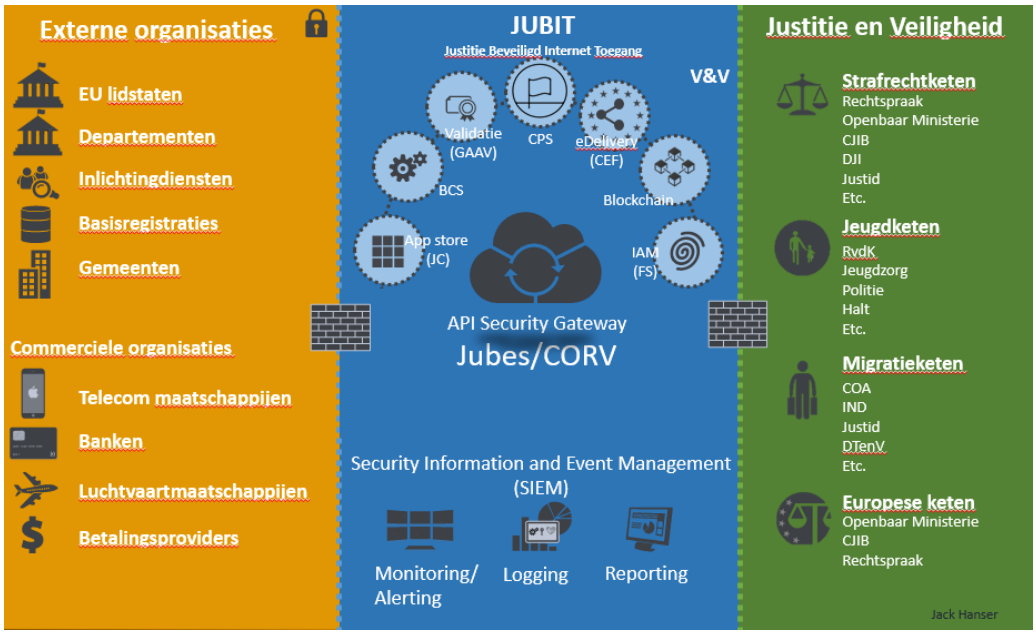
2.2. Jubes-infrastructuur

JUBES is een bilaterale oplossing en functioneert als het ware een "hub", die bereikbaar is via een groot aantal koppelvlakken:

- JustitieNet / PolJus
- Internet
- DIGINetwerk / HaagseRing
- Rijksweb
- OSB VPN
- DOC VPN
- Europese netwerken
- Partnerkoppelingen

Net als veel andere gemeenschappelijke diensten staat JUBES in het Jubit (Justitie Beveiligde Internet Toegang), de DMZ van JenV. Jubit is het beveiligd koppelvlak tussen het interne vertrouwde landelijke datacommunicatie netwerk (Justitienet) dat JenV in gebruik heeft en externe netwerken zoals Internet, partnernetwerken (Publieke partijen en semi-overheidspartijen) en overheidsnetwerken (Haagse Ring, Diginetwerk, Rijksoverheidsnetwerk). Doordat JUBES in het Jubit draait is het voor organisaties eenvoudiger om aan te sluiten en ook voor andere gemeenschappelijke diensten is het eenvoudiger om onderliggend gebruik te maken van JUBES.

JUBES is technisch dubbel uitgevoerd en verdeeld over 2 geografisch gescheiden datacenters. JUBES kent inmiddels zo'n 700 (direct of indirect) aangesloten partners.



2.2.1. Scheiding van ontwikkeling, testen en productie

JUBES ondersteunt naast productie koppelingen, ook acceptatie aansluitingen. Deze zijn, conform de BIO[6] gescheiden. Op basis van adres en URL. Dit om risico op fouten, onbevoegde toegang of wijzigingen in productiesysteem te verminderen.

JUBES Productie FQDN:
jubes.nl (internet en Justitienet)
jubes.minjenv.nl (Diginetwerk)
jubes.eu

JUBES Acceptatie FQDN:
acc.jubes.nl (internet en Justitienet)
acc.jubes.minjenv.nl (Diginetwerk)
acc.jubes.eu

2.3. JUBES support en ondersteuning

Het team Gegevensuitwisseling – JUBES beheer ondersteunt bij:

- Functionele en technische vragen;
- Advies m.b.t. tot te koppelen/integreren toepassing(en);
- Advies m.b.t. de meest effectieve manier om te integreren;
- Het definiëren van partner agreements (afspraken tussen zendende en ontvangende partij). Dit gebeurt bij voorkeur o.b.v. van de daarvoor bedoelde CPA;
- De technische routeringen (openstellen van firewalls etc.). T.b.v. digitale gegevensuitwisseling dient er veelal in de infrastructuur van betrokken partner(s) e.e.a. geconfigureerd/aangepast te worden;
- Ondersteuning bij de acceptatietests aansluiting JUBES. Om van JUBES gebruik te kunnen en mogen maken, moet via acceptatietests bewezen worden dat de standaards op de juiste wijze zijn gebruikt.

[6] https://bio-overheid.nl

3. Gebruik van de dienst JUBES

JUBES is hét technische knooppunt voor informatie-uitwisseling binnen JenV en met aanpalende domeinen. Als JenV-partners informatie willen uitwisselen buiten de eigen organisatie (ongeacht binnen of buiten het JenV domein) dan dient dit via Jubes gerouteerd te worden waarbij te conformeren aan de standaarden voor informatie-uitwisseling.

3.1. Hoe kunt u gebruik maken van deze dienst

Indien u als organisatie aanvullende informatie wilt of u wilt gebruik maken van de dienst JUBES, dan kunt u contact opnemen met het team Gegevensuitwisseling – JUBES beheer.
Dit kan via Klant Contact en Service van de Justitiële Informatiedienst (info@justid.nl of 088 998 90 00).

De hele doorlooptijd van een aansluittraject (van aanmelden tot daadwerkelijk in productie) kan variëren van enkele dagen tot enkele maanden en hangt sterk af van de fase waarin de te koppelen partner zich bevindt (zijn berichtenstromen al gedefinieerd, applicaties al ontwikkeld, technische voorbereidingen getroffen m.b.t. de nieuwe aansluiting, etc.) en de integratiewijze die gekozen wordt.

3.2. Grootte en hoeveelheid berichten

JUBES is zo geconfigureerd dat deze gestructureerde XML bestanden tot 35 MB doorlaat en overige payloads tot een maximale grootte van in principe 2 GB.

Per aansluiting wordt een maximale doorvoer gehanteerd van in principe 20 documenten per seconde. Dit om te voorkomen dat het achterliggende endpoint overbelast kan raken.

Is er sprake van een payload groter dan 2GB of bij meer dan 20 documenten per seconden dan dient dit vooraf gemeld te worden.

3.3. Reliable messaging

JUBES ondersteunt het gebruik van ebMS reliable messaging, d.w.z. het ontvangen van een ontvangstbevestiging (Acknowledgment) op het afleveren van een bericht. Afhankelijk van de afgesproken CPA, uitgaande van standaard 8 (retries) x 3 (uur) zal het endpoint van de verzendende party het bericht gedurende 24 uur opnieuw aanbieden.
Bij het uitblijven van een ontvangstbevestiging zal het verzonden bericht bij de verzendende party op de status “Falen” komen te staan. De zendende partij kan dan actie ondernemen (opnieuw zenden, ontvangende partij raadplegen, etc.).

Bijlage 1: CERTIFICATEN

Certificaateisen

Certificaten moet aan een aantal eisen voldoen:

- Het certificaat is uitgegeven door een gerenommeerde Certificaat Autoriteit;
- Geen self signed certificaten
- Het certificaat is minimaal Organization Validated;
  → zie 'Uitleg type certificaten'
- Het certificaat is minimaal een jaar geldig;
- Een PKI-O certificaat dient in het onderwerpveld(subject) het OIN of HRN nummer van de betreffende organisatie te bevatten
- De FQDN/Common name:
  - mag niet leeg zijn
  - De domeinnamen zijn compleet (alleen hostname is niet voldoende)
  - Is geen IP-adres
  - Is geen Internationalized Domain Names (IDN)
  - Gebruikt geen wildcards en spaties (bijvoorbeeld: *.bing.com)
    Dit is ook van toepassing op de extensie Alternative Name (SAN)
  - Bevat geen interne domeinnamen

Certificaatvoorkeuren

- Uitgegeven door PKI-O Private root;
- Sleutelsterkte/keylength van 4096 bits
- Bij ebMS/CPA een geldigheid van 3 jaar (geldigheid van een CPA is gelijk aan het eerstverlopende certificaat in een CPA)

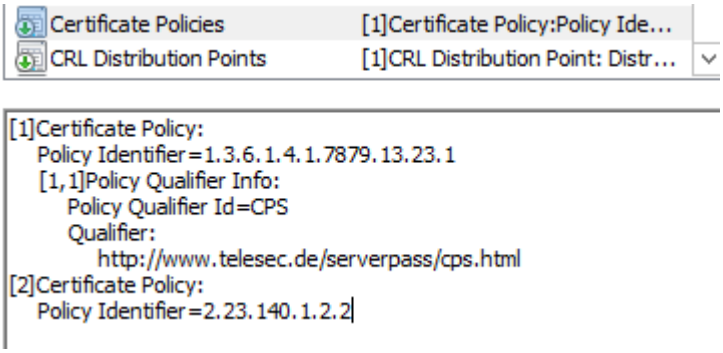
Uitleg type certificaten

Domain validated (DV)
De eigenaar van het domein is gevalideerd als de aanvrager van het certificaat en het WHOIS record wordt gecontroleerd.

Organization Validated (OV)
De aanvrager is gevalideerd als eigenaar van het domein en de organisatie is gecontroleerd in het (KVK) register). Er vindt een telefonische validatie plaats met het bedrijf en de WHOIS registratie wordt gecontroleerd.
Let op: Quovadis hanteert andere benamingen voor OV

Extended Validated (EV).
Dezelfde eisen als DV + OV, alleen wordt de aanvrager ook gevalideerd door het ondertekenen van een formulier.
Let op: Quovadis hanteert andere benamingen voor EV

Door de eigenschappen van het certificaat te bekijken kan er vastgesteld worden welk certificaat type het betreft:



DV, OV en EV hebben de volgende object ID's (OID):

Type	Policy Identifier
Domain Validated	2.23.140.1.2.1
Organization Validated	2.23.140.1.2.2
Extended Validated	2.23.140.1.1

Niet alle Certificate authorities (CA's) hebben het gebruik van Certificate Policy geïmplementeerd. Een andere manier om het type certificaat te herkennen is om de organization data in het subject te bekijken. Deze extensie zal informatie weergeven over de domein naam en de geregistreerde wettelijke naam. Optioneel kan het ook de geografische locatie van de stad, state (provincie) en land bevatten van waar het bedrijf geregistreerd is om zaken te doen.

Bijlage 2: STUURGEGEVENS

Adressering
Organisaties bij de Nederlandse overheid die digitaal zaken doen, zijn verplicht om een "Organisatie Identificatie Number" of OIN te hebben (Identificatienummer van de overheid). Voor de communicatie tussen overheid en bedrijfsleven wordt gebruik gemaakt van het "handelsregisternummer" of HRN. De OIN of HRN is opgenomen in de client- en server PKI Public certificaten die worden gebruikt voor authenticatie van de zender en ontvanger.

Centrale OIN raadpleegvoorziening
Elke organisatie in de Nederlandse overheid kan een OIN aanvragen (https://www.logius.nl/diensten/oin/aanvragen). Het OIN wordt samen met informatie van de organisatie geregistreerd in het "Digikoppeling Service Register" https://portaal.digikoppeling.nl/registers/

PartyIdType
De PartyId wordt geidentificeerd door het PartyIdType "urn:osb:oin".

Het eb:PartyIdType element in de message header van bv het ministerie van Justitie en Veiligheid is:
<tns:PartyId tns:type="urn:osb:oin">00000004000000002000</tns:PartyId>

Handelsregisternummer
Het HRN is afgeleid van het Kamer van Koophandel nummer. Bedrijven en particuliere instellingen zonder publieke taak of autoriteit moeten door overheden worden geïdentificeerd. Hier gebruiken we het HRN. Alle ondernemers en rechtspersonen in Nederland zijn geregistreerd. Zelfs groepen die voorheen geen registratieplicht hadden, zoals eenmanszaken in de landbouw en de vrije beroepen. http://www.kvk.nl/

PartyIdType
De PartyId wordt geïdentificeerd door het PartyIdType "urn:epv:kvk".

Het eb:PartyIdType element in de message header van bv "De Nederlandsche Bank" is:
<tns:PartyId tns:type="urn:epv:kvk">33003396</tns:PartyId>

SYSDA tabel code
Voor de digitalisering van papieren documentstromen werd een adresseringsmechanisme gebruikt op basis van de codetabel van het agentschap, SYSDA. Bij de ontwikkeling van onze elektronische berichtendiensten hebben we hetzelfde model gebruikt als de traditionele papieren post. Dit register wordt veel gebruikt op het Ministerie maar langzaam vervangen door het OIN.

PartyIdType
De PartyId wordt geïdentificeerd door het PartyIdType "urn:epv:sysda".

Het eb:PartyIdType element in de message header van bv de "Justitiele Informatiedienst" is:
<tns:PartyId tns:type="urn:epv:sysda">JD0001</tns:PartyId>

IATA
De International Air Transport Association (IATA[7]) ondersteunt de luchtvaart met wereldwijde normen voor luchtvaartveiligheid, beveiliging, efficiëntie en duurzaamheid. IATA codes worden gebruikt bij de aanlevering van gegevens door luchtvaartmaatschappijen.

PartyIdType
De PartyId wordt geïdentificeerd door het "urn:oasis:names:tc:ebcore:partyid-type:unregistered:iata:airline".

Het eb:PartyIdType element in de message header van de KLM is b.v.:
<eb:PartyIdtype="urn:oasis:names:tc:ebcore:partyid-type:iso3166-1">KL</eb:PartyId>

ISO land code
Voor gegevensuitwisseling tussen Europese Lidstaten gebruiken we unieke tweeletterige landcodes codes volgens de ISO 3166-1 alpha-2[8] standaard

PartyIdType
De PartyId wordt geïdentificeerd door het "urn:oasis:names:tc:ebcore:partyid-type:iso3166-1".

Het eb:PartyIdType element in de message header van The Netherlands is b.v.:
<eb:PartyIdtype="urn:oasis:names:tc:ebcore:partyid-type:iso3166-1">NL</eb:PartyId>

PartyId Postfix
Om onderscheid te maken tussen omgevingen maken we gebruik van een postfix. De gebruikte naamgevingsconventie is:

- Ontwikkelomgeving met postfix "_O"
- Test environment met postfix "_T"
- Acceptatie omgeving met postfix "_A"
- Productieomgeving. Geen postfix.

Bij ebMS/CPA gebruik wordt veelal postfix _OTA gebruikt

Role based routing
Sommige organisaties hebben meerdere MSH's. Dan kan er voor worden gekozen om te routeren op basis van basis van To:PartyId en de To:Role

End entities
In het 4-corner model routeren we berichten van punt 3 naar punt 4 op PartyId, wat in het geval van e-codex is gebaseerd op landcode. Deze PartyId's zijn niet de eind-entiteiten (punt 1 en punt 4). Hier gebruiken we het element:
"eb: MessageProperties" met "eb:Property name=finalRecipient"
De finalRecipient definieert de uiteindelijke ontvanger van het bericht. In het geval van MLA bevat het de nationale ID van een rechtbank of autoriteit. In Nederland zijn deze ID's afgeleid van onze SYSDA tabel.

De finalRecipient in de message header van Internationale Rechtshulp Centrum, IRC (International Legal Assistance Center) is:

```
<MessageProperties>
    <Property name="finalRecipient">IRC003</Property>
    <Property name="originalSender">the original senders name</Property>
</MessageProperties>
```

[7] https://www.iata.org/en/publications/directories/code-search/

[8] https://www.forumstandaardisatie.nl/open-standaarden/iso-3166-1