# TMF – Handleiding Koppelen Afnemers en Registratiehouders (TMF 1.0 - concept)

OVERHEIDSDIENSTEN PLATFORM
e•OVERHEID: BOUW MEE AAN BETERE DIENSTVERLENING

OVERHEIDSDIENSTEN
PLATFORM
e•OVERHEID: BOUW MEE AAN BETERE DIENSTVERLENING

| Versie | Datum | Bewerking |
|---|---|---|
| 0.1 | 20-04-09 | Initieel concept |
| 0.2 | 20-05-09 | Commentaar Olaf van Gorp |
| 0.3 | 22-06-09 | Ervaringen nav koppeling met GBA/BPR in de PoC omgeving. |
| 0.4 | 24-06-09 | Toevoegen OSR |
| 0.5 | 10-07-09 | OSR-referenties geactualiseerd;<br>Algele redactie. |

Auteur Theo de Wit
Versie 0.5
Den Haag, 7-07-09

# Inhoud

# 1. Inleiding

## 1.1 Over de TerugMeldFaciliteit (TMF)

*Basistaken TerugMeldFaciliteit*
De TerugMeldFaciliteit biedt services voor het uitvoeren van de basistaken rond terugmelden(zie voor een grafisch overzicht van de TMF-services Afbeelding 1:[1]

1. **aanmelden:** doorgeven van ‘waarschijnlijke waarde’ en toelichting hierop bij ‘gerede twijfel’ door een afnemer aan TMF. Het gebruikte protocol voor de berichten is ebMS. Deze service wordt tevens gebruikt voor het intrekken van een terugmelding;
2. **afleveren:** ontvangen door een registratiehouder van terugmeldingen door de TMF. Het gebruikte protocol is ebMS;
3. **registreren:** ontvangen van mededelingen vanuit een basisregistratie (status van afhandeling van een terugmelding). Het gebruikte protocol is ebMS;
4. **ophalen:** opvragen door een afnemer van overzichten en (status)informatie van terugmeldingen. Het gebruikte protocol is WUS;
5. **bevragen**: ophalen van (de actuele waarde van) een authentiek gegeven. Het gebruikte protocol voor de berichten is WUS. Dit is een tijdelijke functie die niet meer wordt ondersteund in versie 1.1 van TMF.

In dit document wordt uitsluitend het tot stand komen van het berichtenverkeer voor de *ebMS-services* beschreven (de services onder de hierboven genoemde punten 1, 2 en 3).

Dit document gaat daarbij uit van TMF versie 1.1.

## 1.2 Doelgroep van dit document

Deze technische handleiding is bedoeld voor organisaties die willen koppelen aan TMF. In dit document wordt stap voor stap uitgelegd wat er nodig is voor een koppeling door registratiehouder of afnemer met de centrale TMF-voorziening, ook wel 'TMF Core' genoemd.

[1] Zie voor details het document "TMF Koppelvlakspecificatie"

### 1.3 Registratiehouders en afnemers

In de context van TMF zijn er twee soorten gebruikers (organisaties):

- *Registratiehouder*: voor TMF is de registratiehouder de partij die de terugmeldingen ontvangt uit naam van de betreffende basisregistratie. [2]
- *Afnemer*: dit zijn overheden die de gegevens van de basisregstraties kunnen raadplegen en op deze gegevens kunnen terugmelden.

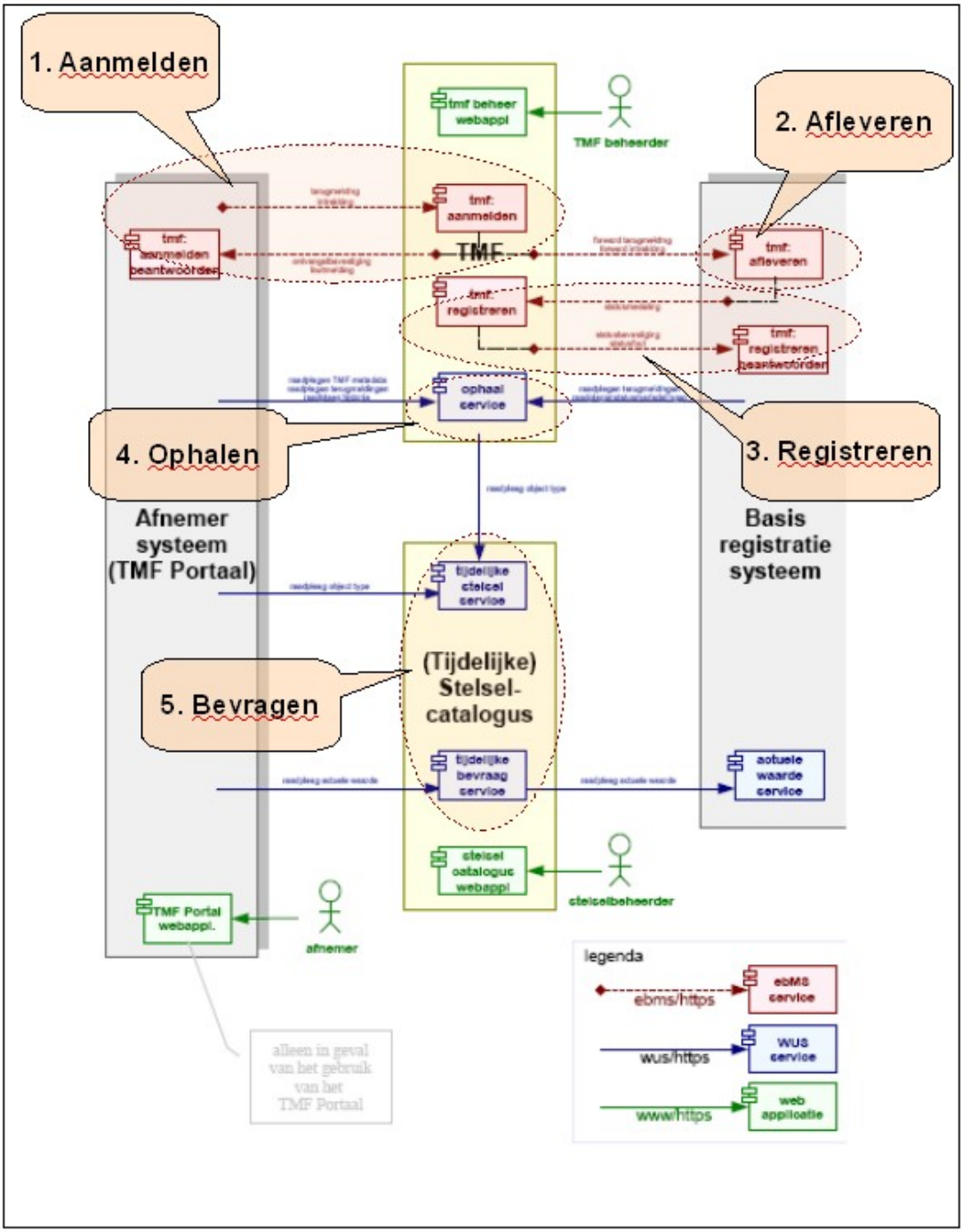
Dit document behandelt de werkwijze voor afnemers en registratiehouders. Het beschrijft de benodigde randvoorwaarden en de stappen die door afnemers/registratiehouders moeten worden genomen om tot een succesvol gebruik van de ebMS-services van TMF te komen. Voor deze services geldt TMF als service provider (TMF is de partij die de services aanbiedt).

---

Opmerking: de beschrijving voor de Productie-omgeving (services!) is nog niet compleet; de definities voor services in de Productie-omgeving zijn nog niet vastgesteld.
Naar verwachting zullen de Productie-services worden aangeboden door GBO.overheid als service provider.

---

[2] Formeelis de registratiehoude de overheidsorganisatie die verantwoordelijk is voor de kwaliteit van de gegevens in een bepaalde basisregistratie. Een aantal basisregistraties maakt gebruik van een landelijke voorziening waarnaar ' generieke' verantwoordelijkheden, zoals het ontvangen van terugmeldingen, worden gedelegeerd.




*Afbeelding 1: Overzicht van TMF-services*

## 1.4 Omgevingen

TMF 1.1 komt beschikbaar op een drietal omgevingen ten behoeve van afnemers en registratiehouders te weten:

- TMF 1.1 - PoC-omgeving
- TMF 1.1 - Ketentestomgeving
- TMF 1.1 - Productie-omgeving

### 1.4.1 TMF 1.1 - PoC-omgeving

De PoC-omgeving wordt door afnemers en registratiehouders gebruikt om te testen of berichtenverkeer tussen afnemer/registratiehouder en TMF correct verloopt. Afnemers en registratiehouders testen met behulp van deze omgeving dus *onafhankelijk van elkaar* hun connectiviteit met TMF.

Naast een 'TMF Core' is binnen de PoC-omgeving ook een 'TMF Portaal' ingericht. Deze Portaal-installatie kan door afnemers worden gebruikt om terugmeldingen naar de 'TMF Core' te sturen[3]. Registratiehouders kunnen het Portaal gebruiken om ten behoeve van hun eigen test de rol van afnemer te simuleren; middels het Portaal kunnen zij een terugmelding in hun eigen systeem inschieten.

### 1.4.2 TMF 1.1 - Ketentestomgeving

De Ketentestomgeving is de omgeving waarin registratiehouders en afnemers in een onderlinge keten (afnemer - TMF - registratiehouder) tests kunnen uitvoeren met terugmelden. De omgeving is gelijk aan de productie-omgeving met twee belangrijke verschillen:

- de Ketentestomgeving werkt op basis van testcertificaten in plaats van werkelijke PKI.Overheid-productiecertificaten;
- in de Ketentestomgeving mogen alleen testgegevens gebruikt worden. Dit wordt ook zo afgesproken in de bewerkersovereenkomt met een registratiehouder.

### 1.4.3 TMF 1.1 - Productie-omgeving

De productie-omgeving is de omgeving waarin daadwerkelijk productie wordt gedraaid. In deze omgeving gaan dan ook ' echte' gegevens over en weer tussen afnemer en TMF en registratiehouder en TMF. Deze omgeving accepteert alleen PKI.Overheid-productiecertificaten.

---

[3] In een niet-testsituatie zal het TMF Portaal door een afnemer worden geïmplementeerd binnen diens eigen infrasctructuur.

### 1.5 Vooraf: wat heeft u nodig?

Om afnemers of registratiehouders te laten koppelen met TMF is het volgende nodig:

- Aansluiting op de OSB is randvoorwaardelijk voor aansluiting op TMF. Voor meer informatie:

  http://www.overheidsservicebus.nl/aanmeldenbijdeosb/

- Netwerkverbinding

  Er zijn twee mogelijkheden om verbindingen te leggen:

- *Publiek Internet:* hiermee wordt getest in de PoC-omgeving van ICTU;

- *Koppelnetwerk Publieke Sector (KPS): d*eze verbinding is in ontwikkeling. Zolang KPS nog niet volledig is gerealiseerd, wordt de ketentest over KPS mogelijk gemaakt met maatwerk. De productie-omgeving maakt ook gebruik van KPS.

- Netwerkconnectiviteit (geen OSB-standaard, maar een randvoorwaarde).
  - IP adressen van servers en routering devices;
  - Vaststellen parameters bij gebruik van Network Address Translation;
  - Vaststellen DNS indien beschikbaar;
  - Configuratie firewall aanpassen bij firewall gebruik;
  - Secure Sockets Layer inregelen (PKI.overheid (test) certificaat).

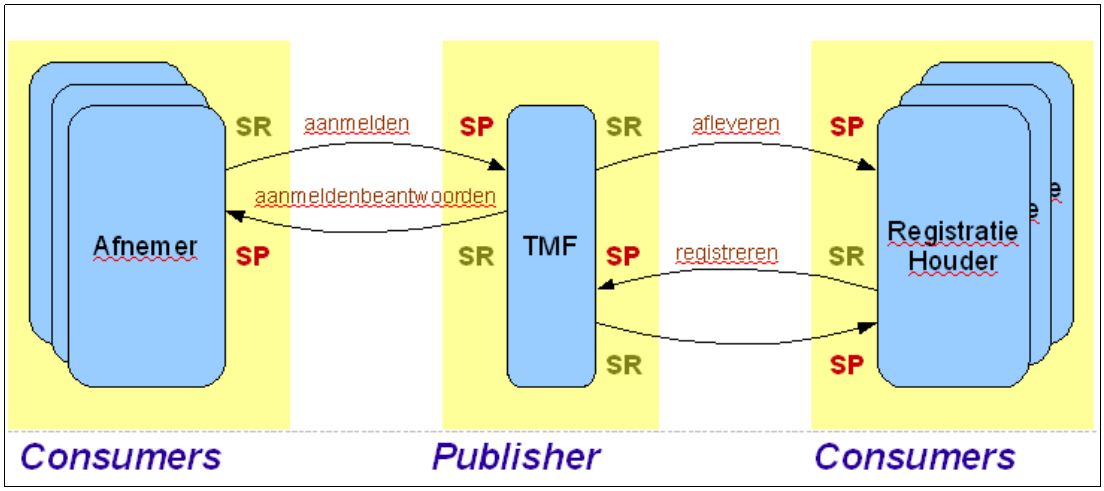
- Servicegegevens
  TMF is ingericht op basis van een servicegerichte architectuur. TMF-functies worden aangeboden middels web-services (reeds genoemd in §1.1). Partijen die willen aansluiten op TMF zullen hun infrastructuur moeten inrichten op basis van deze services. Hiertoe dienen zij te beschikken over de benodigde servicegegevens (o.a. technische documenten als Service Specificaties). In dit document richten we ons expliciet op de ebMS-services omdat daar een aantal specifieke zaken bij komen kijken. Het is hierbij van belang om een goed overzicht te hebben van de *rol* die een partij op een bepaald moment in de berichtuitwisseling inneemt, en het effect hiervan op het creëren van bijvoorbeeld de benodigde CPA's.

  Het gaat om de volgende drie ebMS-services:

  - Aanmelden / Aanmelden beantwoorden

- Registreren / Registreren beantwoorden
- Afleveren

Afbeelding 2 geeft een overzicht van de drie partijen die bij TMF zijn betrokken, en de functionele rollen (SP of SR) die deze partijen respectievelijk spelen bij de berichtuitwisseling zoals die op basis van deze services wordt gerealiseerd.




*Afbeelding 2: ebMS-services van TMF en bijbehorende rollen*

***Voorbeeld:*** in het geval van 'Aanmelden' stuurt de Afnemer een bericht (de terugmelding) naar 'TMF Core'. 'TMF Core' acteert in dit geval als *service provider* (SP). De Afnemer acteert dan als *service requester*. In deze context zeggen deze twee rollen, SP en SR, dus vooral iets over de richting van het ' Aanmelden'-bericht.

Voor alle TMF-services worden de servicedefinities gepubliceerd door TMF (en zijn als zodanig terug te vinden in het OSB Service Register - zie §1.7.Toegang tot servicegegevens). Het is echter aan de implementerende partij (Afnemer of Registratiehouder) om de bijbehorende CPA's te maken. Hierbij is het essentieel om de juiste roldefinities te hanteren (zie verder §1.9, §2.9).

Het is handig om van te voren een plaatje te tekenen ("inkleuren" van het relevante deel van Afbeelding 2), zodat helder wordt welke rol een partij binnen het totaalplaatje inneemt.
Merk op dat een registratiehouder ook afnemer kan zijn en andersom.

### 1.5.1 Toegang tot servicegegevens: OSB Service Register

Het OSB Service Register is een centrale faciliteit waarin service providers de gegevens van de services, die zij via de OSB aanbieden, kunnen publiceren ten behoeve van afnemers van deze services. Het gaat hierbij om bijvoorbeeld functionele documenten (FO, procesbeschrijving, etc.) en gegevens die nodig zijn bij de technische implementatie van de service-aanroep (door de service requester), zoals servicespecificaties en certificaatgegevens.

Het OSB Service Register is uitsluitend toegankelijk voor geregistreerde gebruikers. Toegang is aan te vragen via GBO.Overheid (als onderdeel van de 'Aansluit-procedure OSB')[4] . Op aanvraag kan GBO.Overheid tevens de Gebruikers-handleiding voor het OSB Service Register verstrekken

Gegevens van de TMF-services zijn in het OSB Service Register te vinden door hierin een zoekopdracht te geven (zoektermen: "TMF", functie - bijv. "Afleveren", "Registreren" - en eventueel een 'omgevings-identifier' – bijv. "PoC").

Merk op dat services in het OSB Service Register primair worden gepubliceerd als *business service.* De technische-implementatiegegevens (ebMS Service Specificatie, etc.) zijn terug te vinden in de *implementatie*-sectie onder de Business Service.

Zie voor meer details de *OSB Service Register Gebruikershandleiding*.

Het OSB Service Register biedt de mogelijkheid om servicespecificaties (in het Register vastgelegd als .zip-bestand) en certificaatgegevens te downloaden. Deze bestanden zijn terug te vinden onder de *Implementatie* van de business service. De bestanden kunnen het beste lokaal worden opgeslagen om er verder binnen de organisatie mee aan de slag te kunnen gaan.

[4] zie http://www.overheidsservicebus.nl/aanmeldenbijdeosb/

### 1.5.2 Identificerende namen

Alle TMF-services worden voor elke omgeving (PoC, Ketentest en Productie) apart gepubliceerd. Hiervoor is een naamgevingsconventie afgesproken waardoor de services makkelijk in OSB Service Register en CPA-Creatievoorziening zijn terug te vinden.

Services worden in het OSB Service Register primair gepubliceerd als *business service*: een beschrijving van de service waarbij technische details achterwege blijven. De TMF-services die een ebMS-implementatie hebben, zijn in het OSB Service Register gepubliceerd onder drie business services:

- **ICTU_TMF_Aanmelden_v1.0_PoC**
- **ICTU_TMF_Registreren_v1.0_PoC**
- **ICTU_TMF_Afleveren_v1.0_PoC**

Onder deze business services zijn de volgende ebMS-services terug te vinden:

- **ICTU_TMF_Aanmelden_PoC**
- **ICTU_TMF_AanmeldenBeantwoorden_PoC**
- **ICTU_TMF_Registreren_PoC**
- **ICTU_TMF_RegistrerenBeantwoorden_PoC**
- **ICTU_TMF_Afleveren_PoC**

In hoofdstuk 2 en 3 wordt beschreven welke gegevens precies benodigd zijn.

### 1.5.3 CPA-creatie

Een CPA is een formele beschrijving (in XML) voor het vastleggen van de gegevensuitwisseling op basis van de ebMS Koppelvlakstaard.

CPA's worden binnen de OSB gebruikt vanwege de volgende redenen:

- het is een formeel contract tussen twee partijen die op basis van ebMS gegevens willen uitwisselen;
- het automatiseert de configuratie van de ebMS-adapter (het inlezen van de CPA volstaat);
- het biedt de zekerheid dat beide partijen dezelfde instellingen gebruiken.

De CPA-Creatievoorziening is een OSB-voorziening die kan worden gebruikt om de benodigde CPA's te genereren. De CPA-Creatievoorziening beschikt reeds over 'CPA-halffabrikaten' die zijn gemaakt op basis van de ebMS Service Specificaties van de respectievelijke TMF-services. Een service requester kan deze

'halffabrikaten' opzoeken in de CPA-Creatievoorziening en op basis hiervan een CPA creëren.

De service requester voert hiertoe, in de rol van 'Consumer', diens 'Consumer Specificatie'-gegevens in in de CPA-Creatievoorziening. De ID waaronder de service in de CPA-Creatievoorziening wordt gevonden is de naam waaronder deze service(-implementatie!) is gepubliceerd in het OSB Service Register
(meer details: 2.2 Voorbereiden CPA creatie (afnemers)
en 3.2.Voorbereiden CPA creatie (registratiehouders).

Meer info: "OSB CPA Creatie Handleiding", te vinden op
http://www.overheidsservicebus.nl/documentatie/algemeen/.

## 1.6 Checklist: wat dient te zijn ingeregeld aan de kant van de TMF?

*De hieronder opgenomen informatie is van belang voor TMF als betrokken partij en kan worden gebruikt als checklist.*

**TMF**
Voor TMF is *per omgeving* (PoC, Ketentest, Productie) het volgende benodigd in elk geval waarbij een koppeling met TMF wordt gerealiseerd:

- OSB-testcertificaat (alleen voor PoC en Ketentest) aanleveren ten behoeve van Afnemer/Registratiehouder
  *Let erop dat na het aanmaken van de certificaten de 3 root-certificaten in het PKCS bestand worden geïmporteerd. Daarnaast moet de alias van de gegenereerde server certificaten 'osb_test_cert` genoemd zijn;*
- OSB-PKI.Overheid-certificaat (voor Productie): deze certificaten dienen door Afnemer/Registratiehouder bij een Certificate Service Provider te worden aangevraagd;

- Parameters van de omgevingen (infrastructuur) van TMF (PoC, Ketentest, Productie) voor de koppeling met afnemers en/of registratiehouders. Deze parameters zullen normaliter zijn opgenomen in de ebMS Service Specificatie;

- ebMS Service Specificaties van de volgende ebMS-services, gepubliceerd in het OSB Service Register:
  - Aanmelden
  - AanmeldenBeantwoorden
  - Afleveren

- Registreren
- RegisterenBeantwoorden

De services worden per omgeving apart gepubliceerd (PoC, Ketentest, Productie);

- De ebMS Consumer Specificaties worden door Afnemer/Registratiehouder zelf gemaakt. Mogelijk moet een voorbeeld ('template') worden aangeboden;

- De hierboven genoemde ebMS Service Specificaties moeten zijn opgenomen in de CPA-Creatievoorziening onder de juiste identifiers;

- Iedere afnemer of registratiehouder die koppelt aan TMF moet worden geregistreerdals gebruiker in TMF-Core;

- Van iedere registratiehouder waarop via TMF terugmelden mogelijk is, moet het datamodel van de basisregistratie worden geïmporteerd in TMF-Core.

# 2. Stappen voor Afnemers

**Zoals in hoofdstuk 1 is beschreven, biedt TMF drie omgevingen (PoC, Ketentest en Productie) die door Afnemers en Registratiehouders kunnen worden gebruikt om hun aansluiting met TMF gefaseerd te realiseren.**
**Om met elke afzonderlijke omgeving een aansluiting te realiseren, moet een Afnemer/Registratiehouder een aantal stappen doorlopen, zoals het inrichten van de beveiliging middels certificaten en het creëren van Consumer Specificaties en CPA's.**
**Hieronder worden deze stappen beschreven voor de Afnemer. Elke omeving kent in beginsel dezelfde stappen, maar de bij een stap behorende artefacten kunnen per omgeving afwijken (de PoC- en Ketentest-omgeving werken bijvoorbeeld met testcertificaten, terwijl in de Productie-omgeving PKI.Overheid-certificaten worden gebruikt). Waar dit het geval is, worden deze artefacten expliciet per omgeving genoemd.**

Afnemers implementeren de TMF-service '**Aanmelden**' (waarmee een terugmelding aan TMF wordt doorgegeven).

**Benodigde servicegegevens:**
De bijbehorende ebMS-services zijn in OSB Service Register en CPA-Creatievoorziening onder de volgende namen gepubliceerd:

`ICTU_TMF_Aanmelden_< omgevingsID >` *

Voor deze service acteren TMF en Afnemer in de volgende rollen:
Rol Afnemer ('Consumer') : **SR**
Rol TMF ('Publisher') : SP

`ICTU_TMF_AanmeldenBeantwoorden_< omgevingsID >` *

Voor deze service acteren TMF en Afnemer in de volgende rollen:
Rol Afnemer ('Consumer') : **SP**
Rol TMF ('Publisher') : SR

(zie ook **Afbeelding 2** voor een overzicht van deze rollen**)**

* *Opmerking:* < omgevingsID > kan de waarde "PoC", "Keten" of "Prod" hebben.

**Benodigde certificaten:**
**- PoC en Ketentestomgeving:**

- OSB-testcertificaten (client en server[5]) voor de Afnemer
  (aan te vragen bij de TMF-beheerder).
  *Let op:* ook het root-(test)certificaat (CA) dient te worden meegeleverd!;
- Publieke sleutel van TMF-OSB-testcertificaten (client en server)
  (gepubliceerd in OSB Service Register onder de ebMS-services voor PoC- of Ketentest-omgeving);

- **Productie-omgeving:**

- OSB-PKI.Overheidcertificaten (client en server) voor de Afnemer
  (aan te vragen bij een Certificate Service Provider);
- Publieke sleutel van TMF-OSB-PKI.Overheidscertificaten[6]
  (gepubliceerd in OSB Service Register onder de ebMS-services voor de Productie-omgeving).

## 2.1 Installeren van benodigde certificaten

**Certificaten voor de Afnemer: configuratie van SSL aan de Afnemer-zijde**
*PoC/Ketentest*
De Afnemer heeft van de TMF-beheerder de testcertificaten ontvangen (inclusief private sleutel en certificaathiërarchie (root-certificaat)).

*Productie*
De Afnemer heeft van de CSP de benodigde OSB-PKI.Overheidcertificaten ontvangen.

De Afnemer installeert het *servercertificaat* op de juiste server (PoC, Ketentest, Productie) (let erop dat ook de certificaathiërarchie op deze server beschikbaar moet zijn!). Het servercertificaat kan vervolgens worden geconfigureerd in de ebMS-adapter.

Certificaat en bijbehorende hiërarchie zijn daarmee opgenomen in de 'truststore' van de ebMS-adapter.

De Afnemer slaat het clientcertificaat op op dezelfde server. Ook dit certificaat kan vervolgens worden geconfigureerd in de ebMS-adapter.

---

[5] PoC en Ketentestomgeving zullen veelal een eigen server-certificaat nodig hebben (verschillende servers). Voor beide omgevingen kan wel worden volstaan met hetzelfde client-certificaat.

[6] PoC- en Ketentestomgeving gebruiken hetzelfde (test)certificaat als client- en server-certificaat.

**Publieke sleutels van TMF-(test)certificaten**
De Afnemer heeft de publieke sleutel(s) (client en server) voor die TMF-omgeving waarmee de Afnemer wil communiceren, opgezocht in het OSB Service Register en de certificaatbestanden gedownload.

Voor de *testomgevingen* is de bijbehorende certificaathiërarchie beschikbaar doordat deze is meegeleverd met de TMF-testcertificaten (ervan uitgaande dat de testcertificaten op de server zijn geïnstalleerd). Er wordt in dit document van uitgegaan dat ook voor PKI.Overheid-certificaten, gebruikt in een Productie-omgeving, de hiërarchie beschikbaar is.

Mogelijk moet het TMF client-certificaat handmatig worden opgenomen in de truststore van de adapter; in andere gevallen kan worden volstaan met het importeren van de CPA in de adapter (de publieke sleutels van client- en servercertificaten zijn hierin opgenomen). Dit is afhankelijk van de gebruikte ebMS-infrastructuur (en mogelijk van het beveiligingsbeleid van de Afnemer-organisatie).

## 2.2 Voorbereiden CPA-creatie

De OSB maakt gebruik van CPA-bestanden waarmee ebMS-adapters kunnen worden geconfigureerd. Een CPA kan worden gegenereerd met behulp van de CPA-Creatievoorziening. De ebMS Service Specificaties zijn reeds door de TMF-beheerder geïmporteerd in deze voorziening. De Afnemer kan een CPA voor de betreffende service genereren door de bijbehorende *ebMS Consumer Specificatie (ECS)* te maken en in te voeren in de CPA-Creatievoorziening.

De 'Aanmelden'-service kent twee aparte ebMS-implementaties (per omgeving!): Aanmelden en AanmeldenBeantwoorden. Voor beide services moet per omgeving een aparte CPA worden gemaakt (met name de 'rolverdeling' tussen Afnemer en TMF – SP en SR – verschilt!).[7]

*Opmerking:* per omgeving (PoC, Ketentest, Productie) moeten apart de hieronder beschreven ECS'en en CPA's worden gecreëerd!

Om een ECS te maken:

[7] Dit is het geval voor TMF1.0. Vanaf TMF1.1 en verder is het mogelijk om Aanmelden en AanmeldenBeantwoorden in 1 CPA op te nemen.

- Haal de ebMS Service Specificatie van de betreffende ebMS-service en de bijbehorende certificaatgegevens op uit het OSB Service Register (zie beschrijving onder 1.5.1) .Sla de bestanden op in een lokale map;
- Zet met behulp van de CPA-Creatievoorziening de certificaten van de Afnemer om in 'keyinfo'-formaat (een XML-formaat waarin de certificaatgegevens komen te staan zoals ze moeten worden opgenomen in de ebMS Consumer Specificatie);

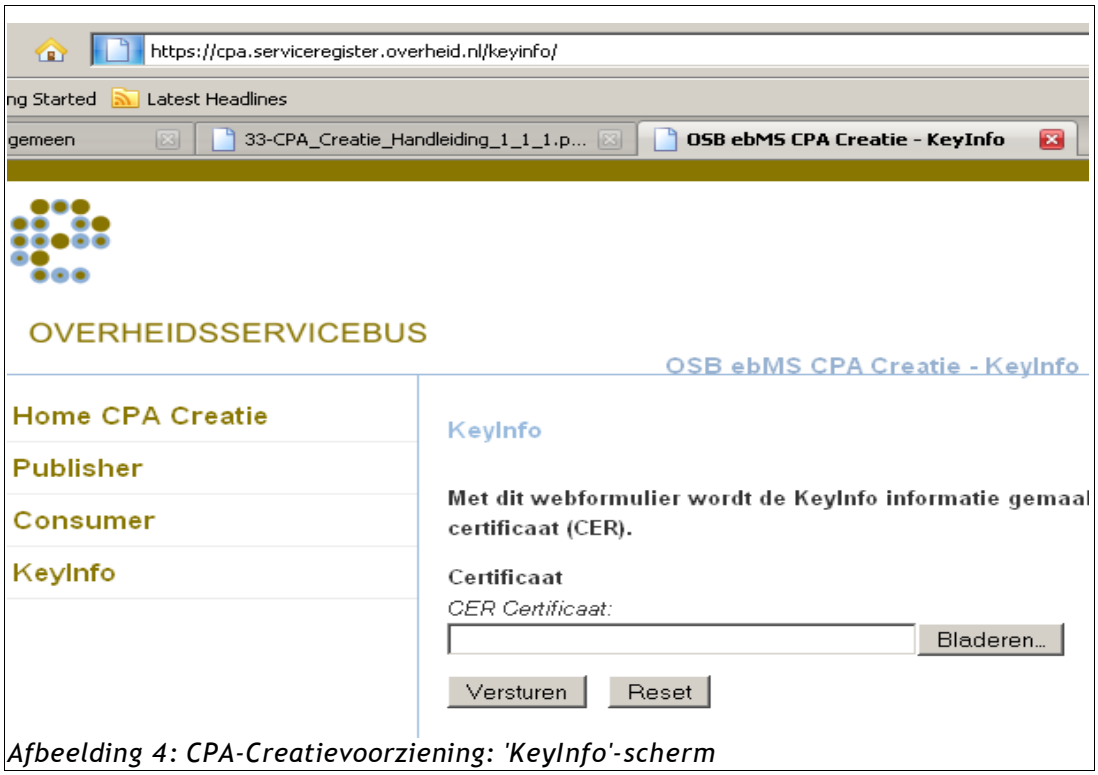
  Dit gaat als volgt:

- Ga naar de CPA-Creatievoorziening op onderstaande link:
  http://cpa.serviceregister.overheid.nl

  Meld je aan met de username/password-combinatie die door de TMF-beheerder is verstrekt. Het onderstaande scherm verschijnt (Afb. 3):

*Afbeelding 3: CPA-Creatievoorziening: 'Home'*

- Klik op 'KeyInfo'. Het volgende scherm verschijnt (Afb. 4):




*Afbeelding 4: CPA-Creatievoorziening: 'KeyInfo'-scherm*

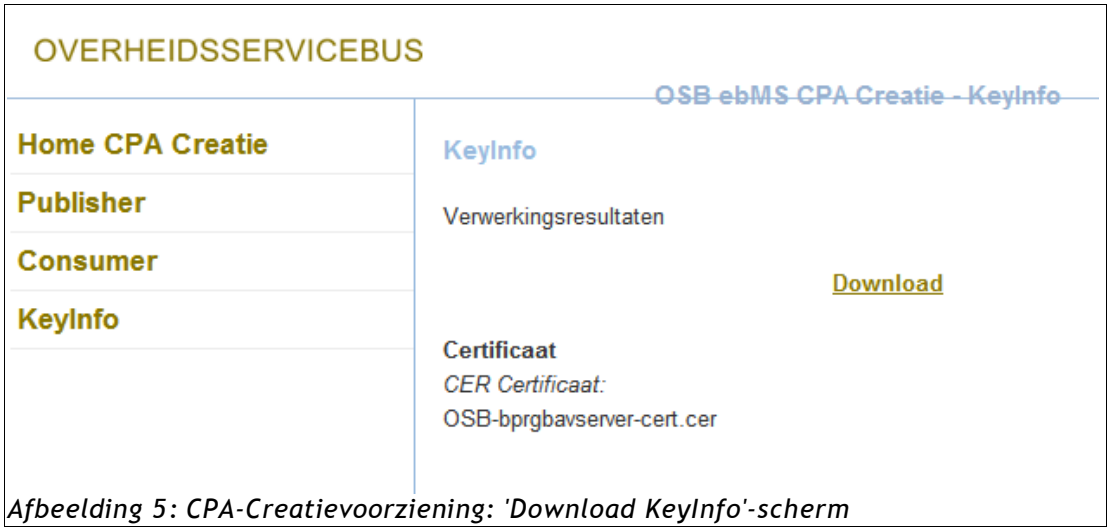
- Blader naar het opgeslagen *servercertificaat* (.cer-file) van de Afnemer (let op de de juist server- (of 'TMF-omgeving'-)context!);
- Druk op 'Versturen'. Een ogenblik later verschijnt het volgende scherm (Afb. 5):

- Download de keyInfo-file (XML-bestand) en sla deze op. U heeft dit bestand later nog nodig!

- Herhaal deze stappen voor het *clientcertificaat* van de Afnemer;

- Sla ook deze resulterende keyinfo-file op (naast de keyinfo-file van het servercertificaat van de de Afnemer);

- Maak vervolgens de ebMS Consumer Specificatie voor de beoogde omgeving. (Zie de *OSB CPA-creatie Handleiding* voor meer informatie over het aanmaken van een Consumer Specificatie).




*Afbeelding 5: CPA-Creatievoorziening: 'Download KeyInfo'-scherm*

De ebMS Consumer Specification bevat de gegevens van de Afnemer en kent de volgende (op de Service Specificatie lijkende) XML-structuur:

```
<?xml version="1.0" encoding="UTF-8"?>
<osb-ebms-service-specificatie>
 <parameters>
  <parameter name="PartyName"> </parameter>
  <parameter name="PartyId"> </parameter>
  <parameter name="EndpointUri"> </parameter>
  <parameter name="ClientCert"> </parameter>
  <parameter name="ServerCert"> </parameter>
 </parameters>
</osb-ebms-service-specificatie>
```

*Opmerking:* bovenstaand overzicht bevat alleen de *verplichte* parameters. Zie voor een volledig overzicht van op te nemen parameters Bijlage 1 van de OSB CPA-creatie Handleiding.

De parameters moeten van de juiste 'consumer'-waarden worden voorzien:

| Parameter | Omschrijving waarde | Opmerking |
|---|---|---|
| PartyName | De organisatienaam zoals die is opgenomen in het clientcertificaat van de (consumer) organisatie. | |

| | | |
|---|---|---|
| PartyID | Het OIN zoals opgenomen in het clientcertificaat van de (consumer) organisatie. | |
| EndpointUri | De HTTPS (dus met TLS/SSL) transport-url van de ebMS -adapter van de organisatie. | **Voor testdoeleinden zonder HTTP:** gebruik de parameter **HTTPEndpointUri** |
| ClientCert | Het publieke deel van het client-certificaat van de organisatie. | Opnemen in de vorm van een 'KeyInfo'-structuur. |
| ServerCert | Het publieke deel van het server-certificaat van de organisatie. | Opnemen in de vorm van een 'KeyInfo'-structuur. |

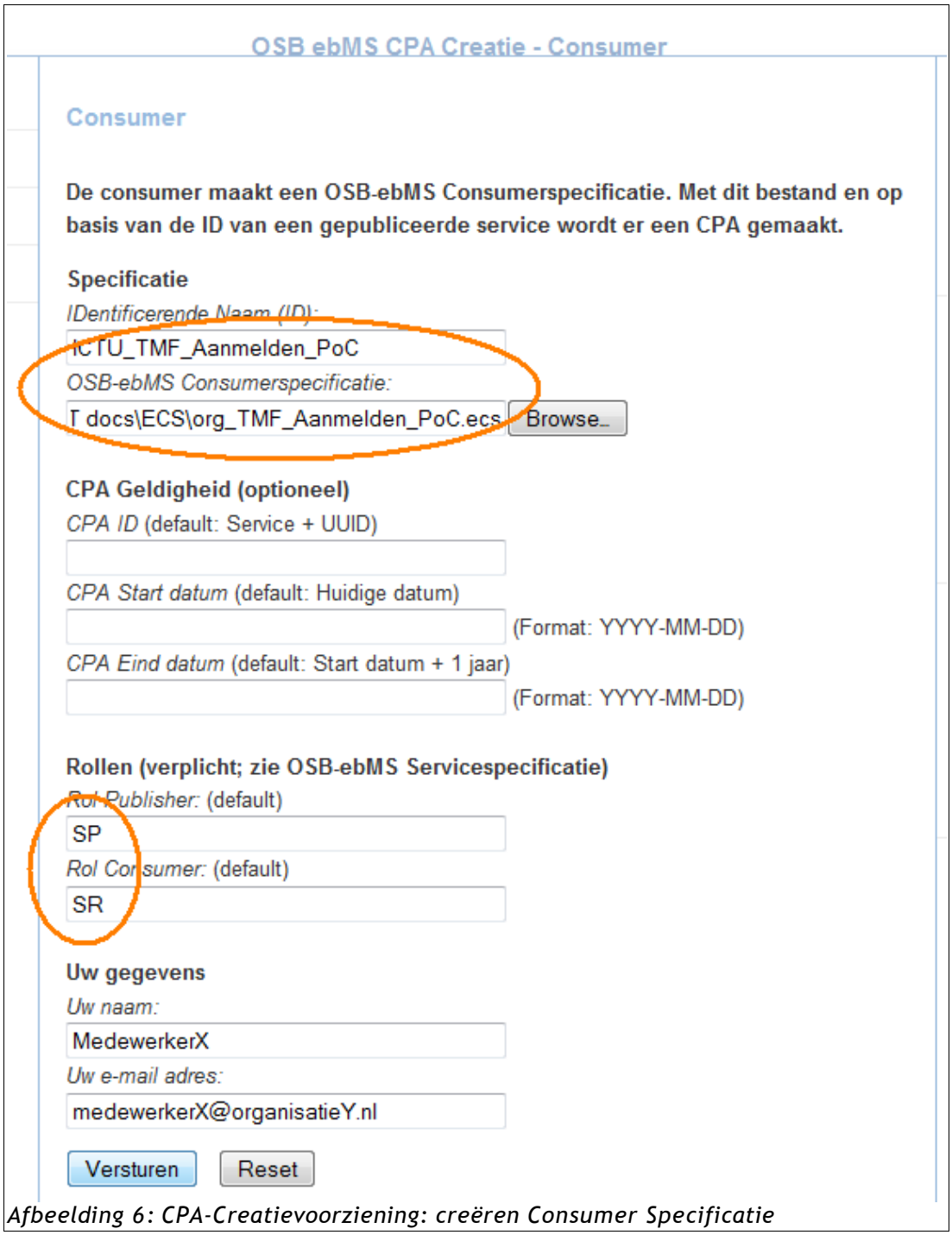
Zie voor een uitgewerkt voorbeeld Bijlage 1.

### 2.3 CPA-creatie voor de Afnemer

Zoals eerder is aangegeven, moeten er voor de services 'Aanmelden' en 'Aanmelden-Beantwoorden' twee aparte CPA's worden gemaakt[8]. De CPA's kunnen met behulp van de CPA-Creatievoorziening worden gegenereerd door de juiste ECS onder de juiste service-identifier te importeren.

- Ga naar de CPA-Creatievoorziening op onderstaande link: http://cpa.serviceregister.overheid.nl
- Meld je aan met de username/password-combinatie die door de TMF-beheerder is verstrekt;
- Klik op Consumer. (de Afnemer wordt gezien als *consumer* van de TMF-service). Het scherm (Afbeelding 6) verschijnt;

[8] Onder TMF 1.0 moeten er twee aparte CPA's worden gemaakt. Vanaf TMF1.1 kan worden volstaan met 1 CPA om een dergelijke 'berichten-roundtrip' in te configureren.




*Afbeelding 6: CPA-Creatievoorziening: creëren Consumer Specificatie*

- Om een CPA voor de 'Aanmeldenservice' (PoC-omgeving) aan te maken:
- Blader naar de juiste ECS (bijv. < org >_TMF_PoC.ecs);
- Vul de benodigde velden in.
  Let hierbij op de volgende waarden:

| Veld | Waarde | Opmerking |
|---|---|---|
| ServiceID | **ICTU_TMF_Aanmelden_PoC** | |
| Rol publisher | **SP** | TMF acteert als service *provider* |
| Rol consumer | **SR** | Afnemer acteert als service *requester* |
| Uw naam | Uw eigen naam | |
| Uw e-mail adres | Uw (valide!) e-mailadres | Een bevestiging van het aanmaken van de CPA wordt naar dit adres verstuurd. |

- Druk op versturen.
  Het resultaat is het volgende (Afb. 7):


*Afbeelding 7: CPA-Creatievoorziening: bevestiging CPA*

- Download de geproduceerde CPA (sla het CPA-bestand op onder een duidelijk identificeerbare naam, bijv.
  “< organisatie >_TMF_Aanmelden_PoC_cpa< datum >.xml";

- Herhaal de generatiestappen voor AanmeldenBeantwoorden.
  Let daarbij op het volgende:
  - gebruik de juiste serviceID
  - de Afnemer ('Consumer') acteert in dit geval als *provider,* de TMF acteert nu als *requester*. Vul het scherm ditmaal dus als volgt in:

| Veld | Waarde | Opmerking |
|---|---|---|
| ServiceID | **ICTU_TMF_AanmeldenBeantwoorden_PoC** | |
| Rol publisher | **SR** | TMF acteert als service *requester* |
| Rol consumer | **SP** | Afnemer acteert als service *provider* |
| Uw naam | Uw eigen naam | |
| Uw e-mail adres | Uw (valide!) e-mailadres | Een bevestiging van het aanmaken van de CPA wordt naar dit adres verstuurd. |

### 2.3.1 'Verwerken' van de CPA

Het CPA-bestand wordt door beide partijen gebruikt om hun ebMS-adapter te configureren. Het is de taak van de Afnemer om het bestand aan de TMF-beheerder te zenden.

**Consumption Request**

De Afnemer doet dit door de TMF-beheerder formeel in kennis te stellen van afname van de ebMS-service: via het OSB Service Register stuurt de Afnemer een *Consumption Request* naar de TMF-beheerder.

Zie voor meer informatie over het indienen van Consumption Request de *OSB Service Register Gebruikershandleiding*.

In het geval van een Consumption Request op een ebMS-service wordt de door de Afnemer gecreëerde CPA als bijlage met het Consumption Request

meegestuurd. De TMF-beheerder kan de CPA controleren en, indien het Request wordt geaccepteerd, deze CPA direct gebruiken om de ebMS-adapter te configureren.

Nadat de Afnemer van acceptatie op de hoogte is gebracht, kan ook die zijn ebMS-adapter op basis van het CPA-bestand configureren.

Daarmee wordt berichtenverkeer op basis van de OSB Koppelvlakstandaard ebMS mogelijk.

# 3. Stappen voor Registratiehouders

**Zoals in hoofdstuk 1 is beschreven, biedt TMF drie omgevingen (PoC, Ketentest en Productie) die door Afnemers en Registratiehouders kunnen worden gebruikt om hun aansluiting met TMF gefaseerd te realiseren.**
**Om met elke afzonderlijke omgeving een aansluiting te realiseren, moet een Afnemer/Registratiehouder een aantal stappen doorlopen, zoals het inrichten van de beveiliging middels certificaten en het creëren van Consumer Specificaties en CPA's.**
**Hieronder worden deze stappen beschreven voor de Registratiehouder. Elke omeving kent in beginsel dezelfde stappen, maar de bij een stap behorende artefacten kunnen per omgeving afwijken (de PoC- en Ketentest-omgeving werken bijvoorbeeld met testcertificaten, terwijl in de Productie-omgeving PKI.Overheid-certificaten worden gebruikt). Waar dit het geval is, worden deze artefacten expliciet per omgeving genoemd.**

Registratiehouders implementeren de TMF-services '**Registreren**' (sturen van status meldingen naar ' TMF Core' ) en '**Afleveren**' (ontvangen van terugmeldingen en intrekkingen).

**Benodigde servicegegevens:**
De bijbehorende ebMS-services zijn in OSB Service Register en CPA-Creatievoorziening onder de volgende namen gepubliceerd:

`ICTU_TMF_Registreren_< omgevingsID >` *

Voor deze service acteren TMF en Afnemer in de volgende rollen:
Rol Afnemer ('Consumer') : **SR**
Rol TMF ('Publisher') : SP

`ICTU_TMF_RegistrerenBeantwoorden_< omgevingsID >` *

Voor deze service acteren TMF en Afnemer in de volgende rollen:
Rol Afnemer ('Consumer') : **SP**
Rol TMF ('Publisher') : SR

`ICTU_TMF_Afleveren_< omgevingsID >` *

Voor deze service acteren TMF en Afnemer in de volgende rollen:
Rol Afnemer ('Consumer') : **SP**
Rol TMF ('Publisher') : SR

(zie ook **Afbeelding 2** voor een overzicht van deze rollen**)**

* *Opmerking:* < omgevingsID > kan de waarde "PoC", "Keten" of "Prod" hebben.

**Benodigde certificaten:**
**- PoC en Ketentestomgeving:**

- OSB-testcertificaten (client en server[9]) voor de Registratiehouder (aan te vragen bij de TMF-beheerder).
  *Let op:* ook het root-(test)certificaat (CA) dient te worden meegeleverd!;
- Publieke sleutel van TMF-OSB-testcertificaten (client en server) (gepubliceerd in OSB Service Register onder de ebMS-services voor PoC- of Ketentest-omgeving);

- **Productie-omgeving:**

- OSB-PKI.Overheidcertificaten (client en server) voor de Registratiehouder (aan te vragen bij een Certificate Service Provider);
- Publieke sleutel van TMF-OSB-PKI.Overheidscertificaten[10] (gepubliceerd in OSB Service Register onder de ebMS-services voor de Productie-omgeving).

## 3.1 Installeren van benodigde certificaten

**Certificaten voor de Registratiehouder: configuratie van SSL aan de Registratiehouder-zijde**
*PoC/Ketentest*
De Registratiehouder heeft van de TMF-beheerder de testcertificaten ontvangen (inclusief private sleutel en certificaathiërarchie (root-certificaat)).

*Productie*
De Registratiehouder heeft van de CSP de benodigde OSB-PKI.Overheidcertificaten ontvangen.

[9] PoC en Ketentestomgeving zullen veelal een eigen server-certificaat nodig hebben (verschillende servers). Voor beide omgevingen kan wel worden volstaan met hetzelfde client-certificaat.
[10] PoC- en Ketentestomgeving gebruiken hetzelfde (test)certificaat als client- en server-certificaat.

De Registratiehouder installeert het *servercertificaat* op de juiste server (PoC, Ketentest, Productie) (let erop dat ook de certificaathiërarchie op deze server beschikbaar moet zijn!). Het servercertificaat kan vervolgens worden geconfigureerd in de ebMS-adapter.

Certificaat en bijbehorende hiërarchie zijn daarmee opgenomen in de 'truststore' van de ebMS-adapter.

De Registratiehouder slaat het clientcertificaat op op dezelfde server. Ook dit certificaat kan vervolgens worden geconfigureerd in de ebMS-adapter.

**Publieke sleutels van TMF-(test)certificaten**
De Registratiehouder heeft de publieke sleutel(s) (client en server) voor die TMF-omgeving waarmee de Registratiehouder wil communiceren, opgezocht in het OSB Service Register en de certificaatbestanden gedownload.

Voor de *testomgevingen* is de bijbehorende certificaathiërarchie beschikbaar doordat deze is meegeleverd met de TMF-testcertificaten (ervan uitgaande dat de testcertificaten op de server zijn geïnstalleerd). Er wordt in dit document van uitgegaan dat ook voor PKI.Overheid-certificaten, gebruikt in een Productie-omgeving, de hiërarchie beschikbaar is.

Mogelijk moet het TMF client-certificaat handmatig worden opgenomen in de truststore van de adapter; in andere gevallen kan worden volstaan met het importeren van de CPA in de adapter (de publieke sleutels van client- en servercertificaten zijn hierin opgenomen). Dit is afhankelijk van de gebruikte ebMS-infrastructuur (en mogelijk van het beveiligingsbeleid van de Registratiehouder-organisatie).

## 3.2 Voorbereiden CPA-creatie

De OSB maakt gebruik van CPA-bestanden waarmee ebMS-adapters kunnen worden geconfigureerd. Een CPA kan worden gegenereerd met behulp van de CPA-Creatievoorziening. De ebMS Service Specificaties zijn reeds door de TMF-beheerder geïmporteerd in deze voorziening. De Registratiehouder kan een CPA voor de betreffende service genereren door de bijbehorende *ebMS Consumer Specificatie (ECS)* te maken en in te voeren in de CPA-Creatievoorziening.

De 'Registreren'-service kent twee aparte ebMS-implementaties (per omgeving!): Registreren en RegistrerenBeantwoorden. Voor beide services moet per omgeving een aparte CPA worden gemaakt (met name de 'rolverdeling' tussen Registratiehouder

en TMF – SP en SR – verschilt!).[11]

De 'Afleveren'-service kent één ebMS-implementatie (per omgeving!). Hiervoor hoeft dus slechts één CPA te worden gemaakt.

*Opmerking:* per omgeving (PoC, Ketentest, Productie) moeten apart de hieronder beschreven ECS'en en CPA's worden gecreëerd!

Om een ECS te maken:

- Haal de ebMS Service Specificatie van de betreffende ebMS-service en de bijbehorende certificaatgegevens op uit het OSB Service Register (zie beschrijving onder 1.5.1) .Sla de bestanden op in een lokale map;
- Zet met behulp van de CPA-Creatievoorziening de certificaten van de Registratiehouder om in 'keyinfo'-formaat (een XML-formaat waarin de certificaatgegevens komen te staan zoals ze moeten worden opgenomen in de ebMS Consumer Specificatie);

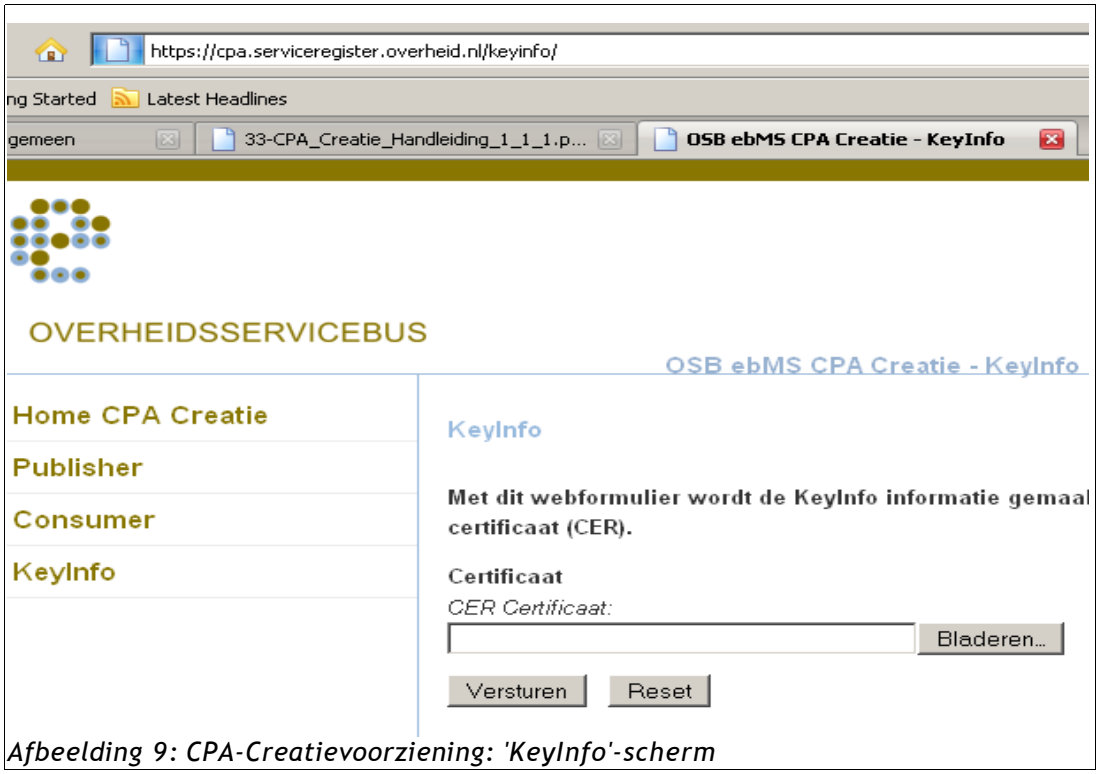
Dit gaat als volgt:

- Ga naar de CPA-Creatievoorziening op onderstaande link:
  http://cpa.serviceregister.overheid.nl

Meld je aan met de username/password-combinatie die door de TMF-beheerder is verstrekt. Het onderstaande scherm verschijnt (Afb. 8):


*Afbeelding 8: CPA-Creatievoorziening: 'Home'*

- Klik op 'KeyInfo'. Het volgende scherm verschijnt (Afb. 9):



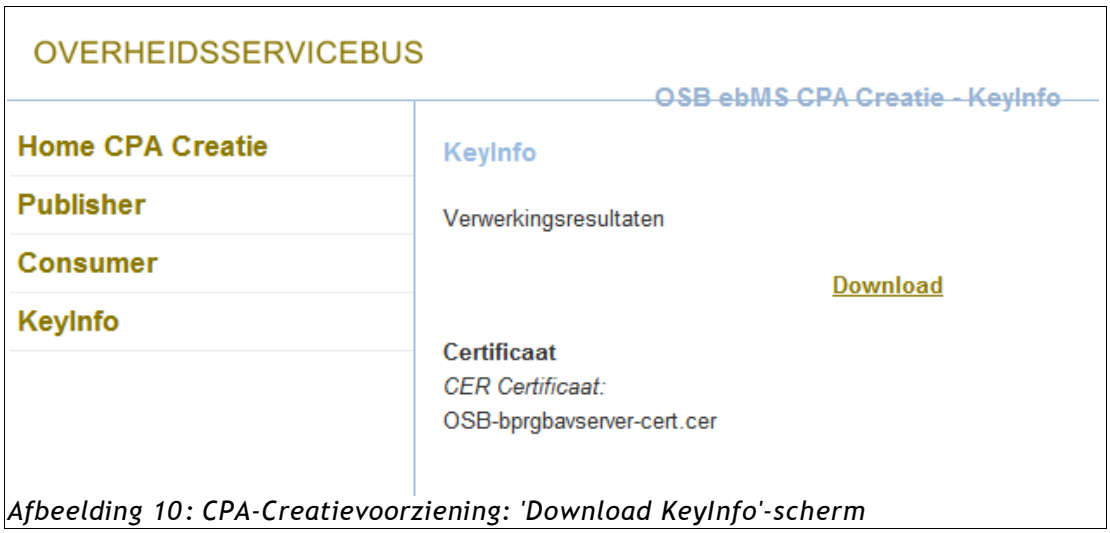

*Afbeelding 9: CPA-Creatievoorziening: 'KeyInfo'-scherm*

- Blader naar het opgeslagen *servercertificaat* (.cer-file) van de Registratiehouder
  (let op de de juist server- (of 'TMF-omgeving'-)context!);

- Druk op 'Versturen'. Een ogenblik later verschijnt het volgende scherm (Afb. 10):

- Downlad de keyInfo-file (XML-bestand) en sla deze op. U heeft dit bestand later nog nodig!

- Herhaal deze stappen voor het *clientcertificaat* van de Registratiehouder;




*Afbeelding 10: CPA-Creatievoorziening: 'Download KeyInfo'-scherm*

- Sla ook deze resulterende keyinfo-file op (naast de keyinfo-file van het servercertificaat van de de Registratiehouder);

- Maak vervolgens de ebMS Consumer Specificatie voor de beoogde omgeving. (Zie de *OSB CPA-creatie Handleiding* voor meer informatie over het aanmaken van een Consumer Specificatie).

  De ebMS Consumer Specification bevat de gegevens van de Registratiehouder en kent de volgende (op de Service Specificatie lijkende) XML-structuur:

```
<?xml version="1.0" encoding="UTF-8"?>
<osb-ebms-service-specificatie>
 <parameters>
  <parameter name="PartyName"> </parameter>
  <parameter name="PartyId"> </parameter>
  <parameter name="EndpointUri"> </parameter>
  <parameter name="ClientCert"> </parameter>
  <parameter name="ServerCert"> </parameter>
 </parameters>
</osb-ebms-service-specificatie>
```

  *Opmerking:* bovenstaand overzicht bevat alleen de *verplichte* parameters. Zie

voor een volledig overzicht van op te nemen parameters Bijlage 1 van de OSB CPA-creatie Handleiding.

De parameters moeten van de juiste 'consumer'-waarden worden voorzien:

| Parameter | Omschrijving waarde | Opmerking |
|---|---|---|
| PartyName | De organisatienaam zoals die is opgenomen in het clientcertificaat van de (consumer) organisatie. | |
| PartyID | Het OIN zoals opgenomen in het clientcertificaat van de (consumer) organisatie. | |
| EndpointUri | De HTTPS (dus met TLS/SSL) transport-url van de ebMS -adapter van de organisatie. | **Voor testdoeleinden zonder HTTP:** gebruik de parameter **HTTPEndpointUri** |
| ClientCert | Het publieke deel van het client-certificaat van de organisatie. | Opnemen in de vorm van een 'KeyInfo'-structuur. |
| ServerCert | Het publieke deel van het server-certificaat van de organisatie. | Opnemen in de vorm van een 'KeyInfo'-structuur. |

Zie voor een uitgewerkt voorbeeld Bijlage 1.

### 3.3 CPA-creatie voor de Registratiehouder

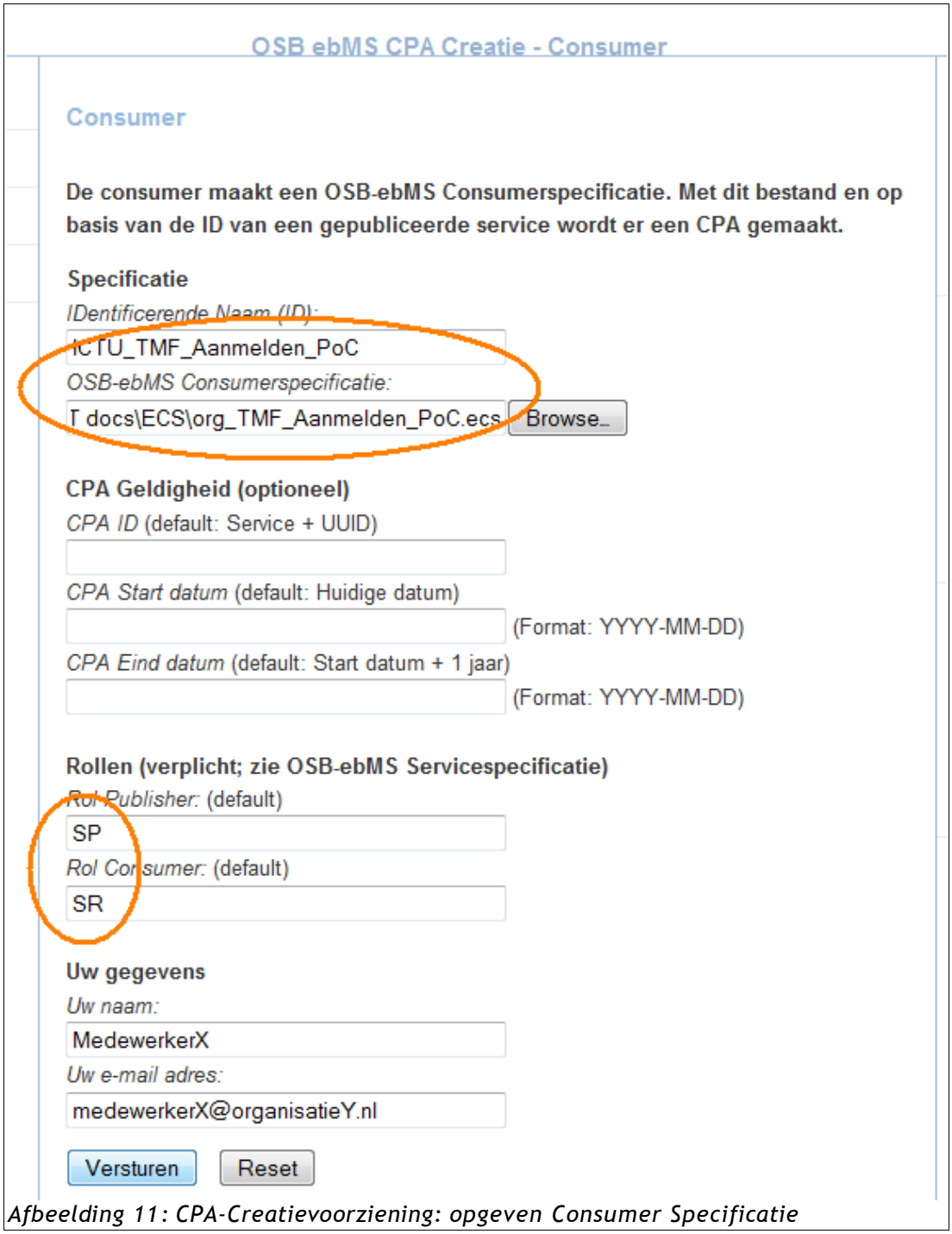
Zoals eerder is aangegeven, moeten er voor de services 'Registreren' en 'RegistrerenBeantwoorden' twee aparte CPA's worden gemaakt[12]. Voor de 'Afleveren'-service moet één CPA worden gemaakt. De CPA's kunnen met behulp van de CPA-Creatievoorziening worden gegenereerd door de juiste ECS onder de juiste service-identifier te importeren.

- Ga naar de CPA-Creatievoorziening op onderstaande link: http://cpa.serviceregister.overheid.nl
- Meld je aan met de username/password-combinatie die door de TMF-beheerder is verstrekt;
- Klik op Consumer. (de Registratiehouder wordt gezien als *consumer* van de TMF-service). Het scherm (afb. 11) verschijnt;

- Om een CPA voor de 'Registreren-service' (PoC-omgeving) aan te maken:
- Blader naar de juiste ECS (bijv. < org >_TMF_PoC.ecs);
- Vul de benodigde velden in.
  Let hierbij op de volgende waarden:

| Veld | Waarde | Opmerking |
|---|---|---|
| ServiceID | **ICTU_TMF_Registreren_PoC** | |
| Rol publisher | **SP** | TMF acteert als service *provider* |
| Rol consumer | **SR** | Registratiehouder acteert als service *requester* |
| Uw naam | Uw eigen naam | |
| Uw e-mail adres | Uw (valide!) e-mailadres | Een bevestiging van het aanmaken van de CPA wordt naar dit adres verstuurd. |

[12] Onder TMF 1.0 moeten er twee aparte CPA's worden gemaakt. Vanaf TMF1.1 kan worden volstaan met 1 CPA om een dergelijke 'berichten-roundtrip' in te configureren.




*Afbeelding 11: CPA-Creatievoorziening: opgeven Consumer Specificatie*

- Druk op versturen.
  Het resultaat is her volgende (Afb. 12):


*Afbeelding 12: CPA-Creatievoorziening: bevestiging CPA-creatie*

- Download de geproduceerde CPA (sla het CPA-bestand op onder een duidelijk identificeerbare naam, bijv.
  "< organisatie >_TMF_Registreren_PoC_cpa< datum >.xml";

- Herhaal de generatiestappen voor RegistrerenBeantwoorden.
  Let daarbij op het volgende:
  - gebruik de juiste serviceID
  - de Registratiehouder ('Consumer') acteert in dit geval als *provider,* de TMF acteert nu als *requester*. Vul het scherm ditmaal dus als volgt in:

| Veld | Waarde | Opmerking |
|---|---|---|
| ServiceID | **ICTU_TMF_RegistrerenBeantwoorden_PoC** | |
| Rol publisher | **SR** | TMF acteert als service *requester* |
| Rol consumer | **SP** | Registratiehouder acteert als service *provider* |
| Uw naam | Uw eigen naam | |
| Uw e-mail adres | Uw (valide!) e-mailadres | Een bevestiging van het aanmaken van de CPA wordt naar dit adres verstuurd. |

- Herhaal de generatiestappen voor Afleveren.
  Let daarbij op het volgende:
  - gebruik de juiste serviceID
  - de Registratiehouder ('Consumer') acteert in dit geval als *provider,* de TMF acteert als *requester*. Vul het scherm ditmaal dus als volgt in:

| Veld | Waarde | Opmerking |
|---|---|---|
| ServiceID | **ICTU_TMF_Afleveren_PoC** | |
| Rol publisher | **SR** | TMF acteert als service *requester* |
| Rol consumer | **SP** | Registratiehouder acteert als service *provider* |
| Uw naam | Uw eigen naam | |
| Uw e-mail adres | Uw (valide!) e-mailadres | Een bevestiging van het aanmaken van de CPA wordt naar dit adres verstuurd. |

### 3.3.1 'Verwerken' van de CPA

Het CPA-bestand wordt door beide partijen gebruikt om hun ebMS-adapter te configureren. Het is de taak van de Registratiehouder om het bestand aan de TMF-beheerder te zenden.

**Consumption Request**

De Registratiehouder doet dit door de TMF-beheerder formeel in kennis te stellen van afname van de ebMS-service: via het OSB Service Register stuurt de Registratiehouder een *Consumption Request* naar de TMF-beheerder.

Zie voor meer informatie over het indienen van Consumption Request de *OSB Service Register Gebruikershandleiding*.

In het geval van een Consumption Request op een ebMS-service wordt de door de Registratiehouder gecreëerde CPA als bijlage met het Consumption Request meegestuurd. De TMF-beheerder kan de CPA controleren en, indien het Request wordt geaccepteerd, deze CPA direct gebruiken om de ebMS-adapter te configureren.

Nadat de Registratiehouder van acceptatie op de hoogte is gebracht, kan ook die zijn ebMS-adapter op basis van het CPA-bestand configureren.

Daarmee wordt berichtenverkeer op basis van de OSB Koppelvlakstandaard ebMS mogelijk.

## Bijlage 1: voorbeeld ebMS Consumer Specification

Hieronder is een voorbeeld van een ebMS Consumer Specificatie (ECS) te zien.
De in grijs gemarkeerde delen moeten worden vervangen door feitelijke 'consumer-waarden'.

Onder de ECS is een voorbeeld van de inhoud van het 'KeyInfo'-element te vinden.

```
<?xml version="1.0" encoding="UTF-8"?>
 <osb-ebms-service-specificatie>
  <parameters>
   <parameter name="PartyName">
     De_Organisatienaam_zoals_opgenomen_in_het_client_certificaat
   </parameter>
   <parameter name="PartyId">
     Het_OIN_zoals_opgeneomen_in_het_client_certificaat
   </parameter>
   <parameter name="EndpointUri">
     https://Uw_FullyQualifiedDomainName_of_IP_adres
   </parameter>
   <parameter name="ClientCert">
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      Het_KeyInfo_deel_van_het_client_certificaat_van_de_organisatie
    </KeyInfo>
   </parameter>
   <parameter name="ServerCert">
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      Het_KeyInfo_deel_van_het_server_certificaat_van_de_organisatie
    </KeyInfo>
   </parameter>
  </parameters>
 </osb-ebms-service-specificatie>
```

Voorbeeld van een 'KeyInfo'-structuur (als uit een *test*certificaat geëxtraheerd met behulp van de CPA-Creatievoorziening):

```
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
 <KeyValue>
  <RSAKeyValue>
   <Modulus>
       bOzkZUnkEzAZMs1whnIw5C1DNjjKZms3S5hOGPvc/6tPrv7AHUIXQrTxBEG2wVrGKf
       IDIVkBndYdPd1NCCiOdJowHfP2vOPBEEo03ydcDRS4sp6W1kpCjpUQXrWXTxJdBO2u
       rDGgTssqqsJ30/c2YMtUGpm4Pc19tGf09ciuXN2=
   </Modulus>
   <Exponent>AQAB</Exponent>
  </RSAKeyValue>
 </KeyValue>
 <X509Data>
  <X509IssuerSerial>
   <X509IssuerName>CN=TEST OSB CSP CA,O=OSB,C=NL</X509IssuerName>
   <X509SerialNumber>19791228183506</X509SerialNumber></X509IssuerSerial>
   <X509SKI>ahFeg06B+hMpk/5jVXXaI9nG</X509SKI>
   <X509SubjectName>
       CN=S794.nxs.nl,serialNumber=00000003271987420000,O=ICTU,C=NL
   </X509SubjectName>
   <X509Certificate>
       giiEakCCA1GgAJiBAgiGEgABiCPSgA0GCSqGSib3DQEBBQUAgDUxCzAJBgNVBAYkAk5ggQ
       JcgYDVQQKEJNPU0ixGDAWBgNVBAgkD1RFU1Qgk1NCiENkUCBDQkAeFJ0JOkAygDQJNzgJN
       NDNaFJ0xgjAygDkJNzgJNDNagFExCzAJBgNVBAYkAk5ggQ0JCJYDVQQKEJRJQQ1RVgR0JG
       R0JGJYDVQQFExQJgDAJgDAJgzi3gkk4NzQygDAJgDEUgBiGA1UEAxgLUzcSN5swfcwESSd
       5NC5ueHgubmJJgZ8JDQYJKoZihvcNAQEBBQADgY0AgiGJAoGBAgD...
       ...s5D1DZBgJGkLNciZygOQtQzY4ymZrPEuYkhj73P+rk67+JB1CF0K08QRBtsFaxinyAy
       AyFZAZ3WHkJ9kQgojnSagB3z+7zjJRBKNN8nXA0UurKelu56Qo6VEF61l08SXQktrqs8A=
   </X509Certificate>
  </X509Data>
</KeyInfo>
```

# Bijlage 2: aandachtspunten (TMF-beheer

In dit hoofdstuk worden een aantal aandachtspunten (met name voor de TMF-beheerder, of voor terugkoppeling naar de TMF-beheerder) genoemd.

***URL ebMS adapter van de Afnemer en Registratiehouder:***
Controleer of de domeinnaam in de URL van de Afnemer en Registratiehouder overeenkomt met de CN uit zijn server certificaat. Indien de CN uit het server cert niet matcht met de domeinnaam van de server dan faalt de SSL verbinding met de melding:

*“Hostname verification failed”.*

***TMF, Afnemer of Registratiehouder geregistreerd in TMF***
Controleer of TMF, Afnemer of Registratiehouder in TMF is geregistreerd onder het juiste OIN. Dit doe je door het OIN uit de CPA´s te vergelijken met het OIN van TMF, Afnemer of Registratiehouder in de volgende tabellen:

| **Database** | **Tabel** |
|---|---|
| tmf | users |
| stelselcatalogus | users |

Beide tabellen kennen dezelfde structuur:

| **id** | **OIN** | **organisation_name** | **organisation_unit_name** | **Role** |
|---|---|---|---|---|
| <AUTOMATISCH> | <OIN_AFN> | <NAAM_AFN> | <NAAM_AFN> | AFNEMER |
| <AUTOMATISCH> | <OIN_RH> | <NAAM_RH> | <NAAM_RH> | REGISTRATIE_HOUDER |
| <AUTOMATISCH> | <OIN_TMF_EIGENAAR> | <NAAM_TMF_EIGENAAR> | <NAAM_TMF_EIGENAAR> | TMF |

Controleer goed of er geen spaties aan het eind van de ingevoerde waarden staan!

***Gebruik juiste client certificaat***

Controleer of het client-certificaat uit de CPA´s ook daadwerkelijk door TMF, Afnemer of Registratiehouder gebruikt worden om de SSL-verbinding op te zetten. Daarnaast moet het OIN dat in het certificaat vermeld staat, overeenkomen met het OIN waaronder de organisatie is geregistreerd bij TMF.

***Importeer de root certificaten in de PKCS12 keystore waarin het server-certificaat is aangemaakt***

Na het aanmaken van een server-certificaat in een PKCS12 keystore moeten de root certificaten (Root, Domein en CSP) worden toegevoegd aan deze PKCS12 keystore. Indien dit niet gedaan wordt dan krijgt TMF, Afnemer of Registratiehouder de volgende SSL fout:

*“Certificate chain not trusted”*

.

Wilhelmina van Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag

T +31 (070) 888 77 22
F +31 (070) 888 78 88
www.overheidsdienstenplatform.nl