HDN POORTWACHTER

WEBSERVICE KOPPELING

HDN Helpdesk – **T**: 0182 – 750 585 **F**: 0182 – 750 589 **M**: helpdesk@hdn.nl

Inhoudsopgave

1. Inleiding

1.1 – Het doel van dit document

Dit document beschrijft de functies die gebruikt kunnen worden om de HDN Poortwachter applicatie via een webservice koppeling te benaderen en beheren.

1.2 – Doelgroep van dit document

De doelgroep bestaat uit ontwikkelaars van web applicaties die met behulp van de webservice koppeling de HDN Poortwachter willen raadplegen.

1.3 – Reikwijdte

In dit document wordt de HDN Poortwachter/DARTS functionaliteit niet beschreven. Dit document beschrijft voor de via de webservice beschikbare functies hoe deze aangeroepen kunnen worden maar niet waar deze toe dienen.

Verder wordt de webserver configuratie aan de hand van Apache gedemonstreerd. Indien de ontwikkelaar voor een andere webserver kiest wordt verwacht dat deze zelf de vertaalslag kan maken.

2. Algemene beschrijving

2.1 – Inleiding

De HDN poortwachter webservice koppeling is een uitbreiding op de HDN Poortwachter web applicatie. De web applicatie, die via https://poortwachter.hdn.nl/ geraadpleegd kan worden, biedt de gebruiker de mogelijkheid om de eigen groepen en/of diensten te configureren.

Configuratiewijzigingen via de HDN Poortwachter web applicatie vereisen een handmatige actie binnen de browser waar de HDN Poortwachter web applicatie actief is.

Door gebruik te maken van de webservice koppeling kan zonder tussenkomst van een gebruiker scriptmatig een webservice aangeroepen worden die de interactie met de HDN Poortwachter web applicatie realiseert.

In hoofdstuk 3 worden de beschikbare webservice functies beschreven. In hoofdstuk 4 wordt beschreven hoe de webserver ingericht kan worden zodat gebruik gemaakt kan worden van mutual SSL.

3. Webservice aanroep

3.1 – Inleiding

Door de webserver te configureren zoals in hoofdstuk 4 is beschreven kan e.g. een web applicatie het serienummer van het cliënt certificaat lezen. Het serienummer en de dienst waartegen geautoriseerd dient te worden kan via een webservice naar CSNET verzonden worden.

De webservice aanroep verloopt over een vergelijkbare verbinding als die van het cliënt certificaat. De CSNET server accepteert alleen een request indien deze ook een HDN certificaat gebruikt.

De URL van de webservice is:

https://poortwachter.hdn.nl/service/httpreq.php

3.2 – Webservice aanroep

De webservice functies dienen aangeroepen te worden door middel van een http post request. Op basis van name/value pairs in het post request dienen de functie en de parameters opgegeven te worden.

De http header dient in ieder geval te bevatten:

```
Accept: application/json
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

Het post request is in de vorm

```
qtype=web_service&query=[Functie]&[param]=[value]
```

Het antwoord van de webservice is een JSON object.

3.3 – Functies

3.3.1 – Lijst van alle beschikbare groepen

Dit request toont de beschikbare gebruikersgroepen.

```
qtype=web_service&query=getUserGroups&filter=
```


```
{
   "result": true,
   "resultStr": "Ok.",
   "retvalue": [
      {
         "id": "451",
         "p": "59",
         "label": "Mijn Intermediaries",
         "branch": [
            {
               "id": "459",
               "p": "451",
               "label": "Mijn_IM_AE",
               "branch": null
            },
            {
               "id": "453",
               "p": "451",
               "label": "Mijn_IM_BL",
               "branch": null
            }
         ]
      }
   ]
}
```


Het resultaat kan hiërarchisch zijn (zoals hierboven het geval is) . Hier is “Mijn_IM_AE” een child van "Mijn Intermediaries".

Eventueel kan een filter opgegeven worden. Indien bijv.

```
qtype=web_service&query=getUserGroups&filter=BL
```

wordt uitgevoerd zal het resultaat allen de groep “Mijn_IM_BL” bevatten:


```
{
   "result": true,
   "resultStr": "Ok.",
   "retvalue": [
      {
         "id": "453",
         "p": "451",
         "label": "SD_IM_BL",
         "branch": null
      }
   ]
}
```

3.3.2 – NAW gegevens certificaat

Toont de NAW gegevens voor het opgegeven certificaat. Hiertoe moet het serie nummer van het certificaat meegegeven worden. Dit serienummer is beschikbaar als de webserver voor mutual SSL ingericht is en de gebruiker zich met een geldig HDN certificaat aanmeld.

```
qtype=web_service&query=certInfo&serial=10CF000010BA
```


```
{
   "result": true,
   "resultStr": "Ok.",
   "retvalue":
            {
      "aansluitnummer": "321775",
      "volgnummer": "0",
      "O": "CS Net",
      "emailAddress": "ontwikkeling@corp.csnet.nl",
      "name": "R Vos",
      "street": "adres 1",
      "postalcode": "1234AA",
      "L": ""
            }
}
```


3.3.3 – Groepen waar een aansluitnummer in zit

Toont de gebruikersgroepen waar een aansluitnummer in zit. Het resultaat bevat de naam en het id van een groep. Het id van een groep is nodig om bijv. een aansluitnummer aan een groep toe te voegen.

```
qtype=web_service&query=getUserGroupsForNode&node=321775&filter=
```


```
{
   "result": true,
   "resultStr": "Ok.",
   "retvalue": [
      {
         "id": "453",
         "label": "Mijn _IM_BL",
         "p": "451",
         "branch": null
      }
   ]
}
```

3.3.4 – Aansluitnummer toevoegen aan groep

Hiermee wordt een aansluitnummer aan een groep toegevoegd. Het id van een groep kan verkregen worden door de webservice calls in bijv. 3.3.1 of 3.3.3 aan te roepen.

```
qtype=web_service&query=addNodeToGroup&node=321739&group=459
```

```
{
   "result": true,
   "resultStr": "Aansluitnummer toegevoegd aan groep."
}
```

3.3.5 – Aansluitnummer verwijderen uit groep

Hiermee wordt een aansluitnummer van een groep verwijderd.

```
qtype=web_service&query=removeNodeFromGroup&node=321880&group=453
```

```
{
   "result": true,
   "resultStr": "Aansluitnummer is verwijderd uit groep."
}
```

3.3.6 – Overzicht Aansluitnummers in groep

Geeft een opsomming van alle aansluitnummers in een groep.

```
qtype=web_service&query=getNodesInGroup&group=453
```


```
{
  "result": true,
  "resultStr": "Ok.",
  "retvalue": [
    {
      "aansluitNummer": "321875",
      "O": "Communications Security Net B.V.",
      "name": "Persoon 1",
      "street": "Adres 1",
      "postalcode": "1234AA",
      "L": "Waddinxveen",
      "ST": "Zuid-Holland",
      "kvkNummer": "12345678"
    },
    {
      "aansluitNummer": "321747",
      "O": "RV bv",
      "name": " Persoon 2",
      "street": "Adres 2",
      "postalcode": "1234aa",
      "L": "Waddinxveen",
      "ST": "Zuid-Holland",
      "kvkNummer": "12345678"
    },
    {
      "aansluitNummer": "321875",
      "O": " CS Net",
      "name": " Persoon 3",
      "street": "Adres 3",
      "postalcode": "1234AA",
      "L": " Waddinxveen",
      "ST": " Zuid-Holland",
      "kvkNummer": "12345678"
    }
  ]
}
```

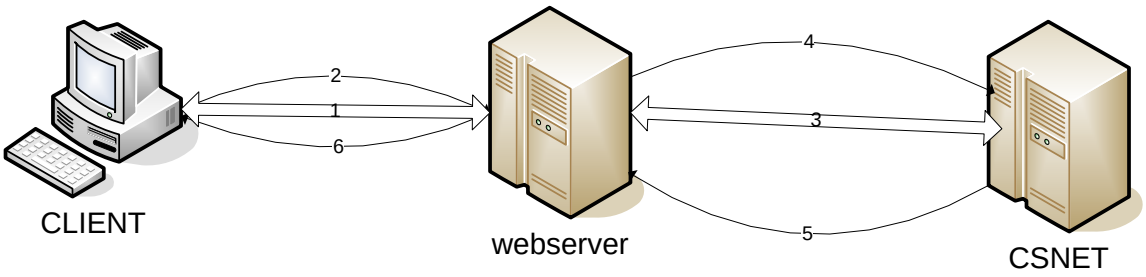
4. De Webserver

4.1 – Inleiding

Alle authenticatie via de HDN Poortwachter geschiedt op basis van certificaten (Mutual SSL authentication). Aan een browser kan door de webserver om een cliënt certificaat gevraagd worden. Hiervoor dient de webserver dan geconfigureerd te worden.

Nadat de webserver het cliënt certificaat ontvangen heeft dient de webserver zichzelf ook met een eigen certificaat bij de CSNET server (HDN Poortwachter server) te authentiseren.

In onderstaand figuur is schematisch weergeven welke stappen doorlopen worden.



De cliënt maakt via een web-browser verbinding met de webserver. Hiervoor wordt een SSL verbinding opgezet (1). De webserver is zo geconfigureerd dat deze om een cliënt certificaat vraagt. Indien de cliënt een certificaat heeft en deze selecteert wordt het certificaat naar de webserver verzonden (2).

Met dit certificaat weet de webserver alleen dat het een geldig HDN certificaat is. Om te autoriseren dient de webserver een webrequest naar de CSNET server te maken (3). Dit verloopt ook over een SSL verbinding.

De CSNET server authentiseert de aanroep ook op basis van een HDN certificaat. De webserver dient dus ook geauthentiseerd te worden. Dit gebeurt ook met behulp van een HDN certificaat (4).

Indien de beheerder toegang heeft zal de CSNET webservice het verzoek afhandelen. In dit verzoek kan een serie nummer van het in (2) verkregen certificaat meegegeven worden om specifiek voor dat aansluitnummer een verzoek in te dienen.

4.2 – Webserver configuratie

Het valt buiten de scope van dit document om voor alle webservers te beschrijven hoe gebruik gemaakt kan worden van cliëntcertificaat authenticatie. Als voorbeeld wordt hier rudimentair uiteen gezet hoe Apache geconfigureerd kan worden.

De communicatie in (3),(4) wordt opgezet door de CSNET server. Hier hoeft dus op de webserver niets voor geconfigureerd te worden. Er wordt wel om een certificaat gevraagd. De webserver applicatie moet deze dus aan kunnen bieden.

(1) en (2) verlopen over een beveiligde verbinding. Dit gebeurt m.b.v. een SSL verbinding. Hiervoor is dus een Server Certificaat benodigd. Dit certificaat is niet perse gerelateerd aan HDN certificaten (mag wel).

Configureer een SSL verbinding op de webserver

De server is op de volgende manier geconfigureerd voor port# 443

SSLEngine ON

SSLCertificateFile [path]/server.pem

SSLCertificateKeyFile [path]/server.key

Server.pem/server.key zijn hier dus het server certificaat (en hoeft dus geen HDN certificaat te zijn). Nadat de SSL verbinding geconfigureerd is kan de webserver de cliënt om cliënt-certificaten vragen. Hiervoor dienen additionele instellingen toegevoegd te worden.

Op webserver wordt optioneel om een cliënt certificaat gevraagd d.m.v. e.g.:

SSLCACertificateFile [path]/ hdnca.pem

SSLVerifyClient optional

SSLOptions +ExportCertData +StdEnvVars

SSLVerifyDepth 1

Indien de cliënt een certificaat heeft die dezelfde CN als het root CA certificaat hdnca.pem heeft zal de browser de cliënt vragen het certificaat te selecteren. Als de cliënt deze selecteert wordt deze naar de server verzonden. Indien dit certificaat ook daadwerkelijk door het root certificaat ondertekend is wordt de verbinding door de server geaccepteerd.

Door de optie +ExportCertData kan in e.g. PHP het serienummer via `$_SERVER['SSL_CLIENT_M_SERIAL']` uitgelezen worden.

4.2.1 – Certificaten formaten

HDN certificaten zijn standaard van binair (cer of p12) formaat. Apache vereist een BASE64 encoded DER certificaat. Op de volgende manier kan een p12 omgezet worden naar een .pem formaat:

openssl pkcs12 -in cert.p12 -out cert.pem

4.2.2 – HDN Root certificaat

Het HDN root certificaat kan via http://www.hdn.nl/downloads/basic-software gedownload worden. Dit is het certificaat die de webserver gebruikt om de HDN cliënt certificaten te valideren. Met

openssl verify -CAfile hdnca.pem -verbose xxx.pem

kan gecontroleerd worden of een cliënt HDN certificaat (xxx.pem) ook daadwerkelijk door dit CA certificaat ondertekend is.