

WORKAROUND SSL AUTHENTICATIE CLIENTS  
LANDELIJKE VOORZIENING WKPB

AUTEUR(S) : Adé Mochtar  
DOCUMENTNUMMER :  
VERSIE : 1.1  
BRON : Atos Origin  
STATUS :  
DOCUMENTDATUM : 13 september 2006  
AANTAL PAGINA'S : 8

EIGENAAR :

PARAAF:

## Inhoud

1	Inleiding.....	4
2	Oplossing.....	5
2.1	Stunnel .....	5
2.2	Desproxy.....	5
3	Installatie .....	6
3.1	Stunnel .....	6
3.2	Desproxy.....	6
	Appendix A Stunnel configuratie .....	7
	Appendix B Voorbeeld client-certificaat voor Stunnel.....	8

## Wijzigingsbladen

VERSIE	DATUM	OMSCHRIJVING	AUTEUR
1.0	13-09-2006	Initiële versie	Adé Mochtar
1.1	13-09-2006	Toevoeging beschrijving Stunnel certificaat	Adé Mochtar

## 1 Inleiding

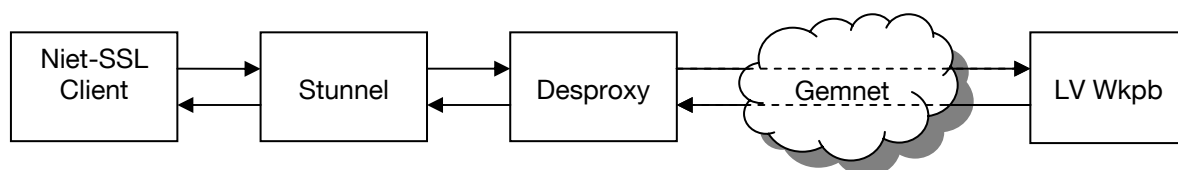
De Landelijke Voorziening Wkpb maakt gebruik van 2-zijdige SSL authenticatie (server- en client-side) de informatie stroom te beveiligen. Daarnaast wordt deze authenticatie gebruikt om de client te kunnen identificeren en vervolgens te autoriseren. Het is dus essentieel dat clients die requests sturen naar de LV Wkpb in staat zijn zichzelf te authenticeren door middel van een client-certificaat.

Wanneer een client niet in staat is een beveiligde verbinding op te zetten met een client-certificaat, kan de identiteit van de client niet achterhaald worden en zal de toegang tot de LV Wkpb geweigerd worden. Om toch de client te kunnen gebruiken, wordt in dit document een workaround beschreven waarmee de authenticatie alsnog toegevoegd wordt.

## 2 Oplossing

Wanneer een client geen ondersteuning heeft voor het opzetten van een SSL verbinding met client-certificaten moet deze functionaliteit door middel van een extern programma toegevoegd worden. Om dit te realiseren wordt gebruik gemaakt van de open-source programma's Stunnel en eventueel Desproxy.

De client communiceert dan via Stunnel en Desproxy over Gemnet met de LV Wkpb. Dit is schematisch samengevat in Figuur 1.



**Figuur 1 Communicatie via Stunnel/Desproxy met LV Wkpb**

### 2.1 Stunnel

Stunnel (<http://www.stunnel.org>) is een programma wat het mogelijk maakt om willekeurige TCP verbindingen te voorzien van een SSL laag. Hiermee is het dus mogelijk om een standaard SOAP-over-HTTP request om te zetten naar een SOAP-over-HTTPS request.

Stunnel beschikt ook over de mogelijkheid om 2-zijdige SSL verbindingen te creëren en biedt dus hiermee ook de mogelijkheid om de benodigde client-certificaten op te nemen in het request.

### 2.2 Desproxy

Desproxy (<http://desproxy.sourceforge.net>) is een programma wat het mogelijk maakt om TCP verbindingen te maken door een HTTP(S) proxy. Wanneer de client draait op een machine die deel uit maakt van een netwerk wat alleen verbindingen toestaat via een proxy, dan is het noodzakelijk om het HTTPS request vanuit Stunnel ook via diezelfde proxy te laten gaan. Aangezien Stunnel hier zelf geen voorziening voor heeft, wordt er gebruik gemaakt van Desproxy.

Als het lokale netwerk dus geen gebruik maakt van een proxy, kan de installatie van Desproxy achterwege gelaten worden.

### 3 Installatie

#### 3.1 Stunnel

1. Download Stunnel 4.16 van <http://www.stunnel.org/download/>;
2. Installeer deze op de computer waar ook de client op geïnstalleerd staat;
3. Kopieer de stunnel configuratie uit Appendix A naar de stunnel.conf die meegeleverd is met de installatie van Stunnel.  
NB: Wanneer er op het lokale netwerk geen gebruik gemaakt wordt van een proxy, kan het connect commando van regel 17 vervangen worden door die van regel 21. Bovendien kan dan de installatie van Desproxy (zie 3.2) achterwege gelaten worden;
4. Maak een wkp\_client.pem bestand aan in de installatiemap van Stunnel en plaats daarin de private key (<naam>-certificate-key.pem) en het x509 certificaat (<naam>-certificate-x509.pem). Zie Appendix B voor een voorbeeld;
5. Start Stunnel;
6. Stunnel is nu gestart en luistert op poort 8008. Alle requests voor de LV Wkpb kunnen nu gestuurd worden naar <http://localhost:8008> (in plaats van naar <https://145.7.218.141>).

#### 3.2 Desproxy

1. Download Desproxy 0.1.0-pre3 van <http://sourceforge.net/projects/desproxy/>;
2. Installeer deze op de computer waar ook de client op geïnstalleerd staat  
NB: Voor Windows hoeft slechts het zip-bestand (desproxy-0.1.0-pre3-windows.zip) uitgepakt te worden naar een map op de computer;
3. Start Desproxy met het volgende commando:  

```
desproxy 145.7.218.141 443 <proxy-host> <proxy-port> 8443
```

  
Hierbij moet <proxy-host> vervangen worden door de hostnaam van de proxy; en <proxy-port> moet vervangen worden door de poort van de proxy.
4. Desproxy is nu gestart en luistert op poort 8443.

## Appendix A Stunnel configuratie

### stunnel.conf:

```
1. ; Client-certificate
2. cert = wkpb_client.pem
3.
4. ; Some performance tunings
5. socket = l:TCP_NODELAY=1
6. socket = r:TCP_NODELAY=1
7.
8. ; Use it for client mode
9. client = yes
10.
11. ; Service-level configuration
12. [wkpb]
13. accept = localhost:8008
14.
15. ; Gebruik deze connect wanneer er gebruik gemaakt wordt van Desproxy
16. ; Adres van Desproxy is localhost:8443
17. connect = localhost:8443
18.
19. ; Gebruik deze connect wanneer er geen gebruikt gemaakt wordt van Desproxy
20. ; Adres van de externe testomgeving van de LV WKPB is 145.7.218.141:443
21. ;connect = 145.7.218.141:443
22.
23. TIMEOUTclose = 0
```

## Appendix B Voorbeeld client-certificaat voor Stunnel

wkpb\_client.pem

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCzcGQw6ph9L3KpXLIohDZXsYp7zJaMEMwwt2Ny8I/7JMMVcn3P
q6qeupPJ39i88QVygnYAAJS2ITN/AyJFHjiX2GCyVdUw9BCn2cDBAjthkzYOZyj1
...
...
...
NUzPiIbj3ePo965y1bqRAkEAoH85XjEXXDmTapqoGmmhtAT1j9tQxnoS89MeXGXH
jcWfyVE+vbBxV/namINoDAS5WucM3yCu+4OwHwuHCu1EKQ==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICCzCCAQQCCQDbCvBiYi/vvDANBgkqhkiG9w0BAQUFADBFMQswCQYDVQQGEwJO
TDERMA8GA1UEBxMIUmlqc3dpamsxDTALBgNVBAoTBFNETUMxFDASBgNVBAMTC0F0
...
...
...
SqdI+7+10wI1RqTCfbuhmnNJWZO1a5+rIbKLh8AR4U4PoIn341xVuLpl1M7PACOp
XW0FOPVCM533d9wyYBVi0BTPlOeEH2KHtHjNaLXsb1DMo7D1RxxCqPxxq7RTAK/U=
-----END CERTIFICATE-----
```