



WADI - Installatieprocedure CA Beheerstool

1.07 / RI-4344

Dirk-Willem van Gulik, Michael Angelo Meyer
augustus 2005

Document No. WADI-WebAPI-CA-STD-1.07 (1.31/7996)
URI: [https://intranet.aseantics.net/closed/offers/webfolder/WADI-WebAPI-CA-STD-1.07 .pdf](https://intranet.aseantics.net/closed/offers/webfolder/WADI-WebAPI-CA-STD-1.07.pdf)
RI-4344

Asemantics SRL
via Teulada, 71, I-00195 Rome, VAT.No: I-07052291007
Janvossensteeg 37, 2312 WC Leiden
www.aseantics.com - leiden@aseantics.com

--

Samenvatting

Gebuikers en ontwikkelaars hebben een digitaal X509-certificaat nodig ten-einde toegang tot WADI te krijgen. Hiervoor is een webbased certificaatbeheer-systeem nodig.

Dit document bevat de installatieprocedure voor dit systeem.

Document Change Log

Version	Date	Changes
1.0 (Revision: 1.3)	August 2005	First Issue
2.0 (Revision: 1.41)	August 2005	Changes for XP-SP1 and XP-SP2
3.0 (Revision: 1.5)	August 2005	Spelling & grammar check

Inhoudsopgave

1	Systeemeisen	5
1.1	Systeemeisen	5
1.2	Roottoegang	5
1.3	Datum en Tijd	6
1.3.1	NTP	6
2	Vorbereiding	7
2.1	Aanvragen FQDN	7
2.2	Aanvragen E-mail role account	7
2.3	IP-adres en Firewall rules	7
2.4	Gebruiker	7
2.5	Webserver UID toestaan e-mail te sturen	7
3	Installatie	9
3.1	Uitpakken	9
3.2	Verificatie Perl	9
3.3	Verificatie OpenSSL	10
3.4	Verificatie sendmail	10
3.5	Setup.conf	10
3.5.1	Testmemmonic	10
3.5.2	Controle	10
3.6	Genereren van configuratiebestanden	11
3.7	Genereren van certificaten	12
3.8	Apache-instellingen	12
3.9	CRL-bestand automatisch laten bijhouden	13
3.10	Installatieverificatie	13
3.10.1	Reboot	13
4	Troubleshooting	15
5	Ingebruikname	17
5.1	Beveiligen van het systeem	17
5.2	Web accounts	17
5.3	Definitief certificaat aanmaken	17
5.4	Veiligstellen van de geheime sleutel	17
5.5	Herstart de webserver	18

6	Beheer	19
6.1	Dagelijks beheer	19
6.2	Jaarlijks beheer	19
A	make-certs output	21
B	Secure RM	27

Hoofdstuk 1

Systemeisen

Uitgangspunt is een modern Linux- of Unixstelsysteem. De applicatie is een gewone webapplicatie die in Perl geschreven is en die na installatie normaal gesproken geen verder onderhoud behoeft. Noch gebruikers noch beheerders dienen op een andere wijze dan via de website toegang tot het systeem te hebben.

1.1 Systemeisen

1. RedHat Linux, Enterprise-editie of vergelijkbaar.
Specifiek zijn de volgende systeemcomponenten vereist die alle standaard in RH Linux geïnstalleerd worden:
 - (a) Apache 1.3 of nieuwer
 - (b) SSL support voor Apache
 - (c) OpenSSL 0.9.1 of nieuwer
 - (d) Perl 5 of nieuwerRHES voldoet aan deze eisen.
2. 15 Megabyte hardeschijfruimte
3. Pentium 300Mhz of sneller
4. Publiek IP-adres met inbound TCP-routing op poort 80 en poort 443
5. IP-adres waarvan poort 443 nog niet in gebruik is
6. Mogelijkheid om e-mail te versturen (eventueel via een smartHost).
7. Mogelijkheid om een Fully Qualified Host Name aan DNS toe te voegen.

1.2 Roottoegang

Een normale installatie behoeft roottoegang om de volgende redenen:

1. Er moet een gebruiker aangemaakt worden

2. Er moeten groepen aangemaakt worden
3. Permissies en ‘user/group ownership’ moeten over meerdere UID’s ingesteld worden
4. Apache bind() moet ingesteld worden voor poorten onder de 1024

Indien dit niet mogelijk is, kan een en ander onder één UID geïnstalleerd worden in een minder veilige modus waarbij het userID van de admin, `wadiadmin`, gelijk is aan het effectieve UID van de webserver. Eventueel kan men in dit geval de ‘suexec’-faciliteit van Apache gebruiken.

Na installatie is roottoegang niet meer nodig.

1.3 Datum en Tijd

Het is *cruciaal* dat de tijd, tijdzone en datum op de server correct zijn ingesteld, omdat het certificaat door de gebruiker verworpen wordt als dit niet het geval is. Er verschijnt dan een melding dat het certificaat uit de ‘toekomst’ komt c.q. reeds verlopen is

1.3.1 NTP

Om bovengenoemde reden adviseren wij om ‘ntpd’ of ‘xntpd’ te activeren. Deze faciliteit wordt standaard met RedHat Linux meegeleverd. Een adequaat configuratiebestand is hieronder te zien:

```
# /etc/ntp.conf
restrict ntp0.nl.net mask 255.255.255.255 nomodify notrap noquery
restrict ntp1.nl.net mask 255.255.255.255 nomodify notrap noquery
restrict ntp.xs4all.nl mask 255.255.255.255 nomodify notrap noquery
server ntp0.nl.net
server ntp1.nl.net
server ntp.xs4all.nl
```

Voordat u ‘ntpd’ start dient u de juiste tijd in te stellen met het volgende commando:

```
ntpdate -u ntp1.nl.net
```

Met het volgende commando zorgt u dat ‘ntpd’ voortaan gestart wordt bij het opstarten van de server:

```
/sbin/chkconfig ntpd on
```

5. Start de ‘ntpd’ onmiddellijk met:

```
/sbin/service ntpd start
```

Hoofdstuk 2

Vorbereiding

2.1 Aanvragen FQDN

Er dient een Fully Qualified Domain Name (bijv. 'ca.wadi.nl') aangevraagd te worden.

2.2 Aanvragen E-mail role account

Er dient een e-mail role account/alias aangemaakt te worden. E-mail die naar dit adres gestuurd wordt, wordt doorgestuurd naar alle beheerders.

2.3 IP-adres en Firewall rules

De server moet inbound TCP verkeer op poort 80 en poort 443 toelaten. Verkeer op poort 80 kan gedeeld worden met andere websites op de server. Poort 443 dient echter geheel toegekend te worden aan dit systeem.

2.4 Gebruiker

Er dient een extra gebruiker, bijv. `wadiadmin`, gecreëerd te worden. Deze gebruiker heeft geen rechten, login of shell nodig. Hij dient in dezelfde groep te zitten als de effectieve gebruiker van de webserver¹.

2.5 Webserver UID toestaan e-mail te sturen

De webservergebruiker (`www`) is normaal gesproken niet 'trusted' en mag tijdens het versturen van e-mail niet de 'From header' specificeren. Het is echter wenselijk om deze instelling te veranderen, omdat de gebruiker in het bovenstaande geval de gewone beantwoordfunctie van zijn of haar e-mailprogramma niet kan gebruiken.

¹Zie het directive `Group` in het `httpd.conf`-bestand

Om deze reden dient de `www`-gebruiker toegevoegd te worden aan de ‘trusted list’ in `/etc/mail/sendmail.ct`. Daarna dient ‘sendmail’ opnieuw te worden gestart.

Hoofdstuk 3

Installatie

De installatie kan het best als root uitgevoerd worden via een normale terminalverbinding.

3.1 Uitpakken

Pak het installatiebestand uit en hernoem de uitgekakte map ‘cawadi’. Dit doet u met de volgende commando’s:

```
# tar xzf /cdrom/cawadi-1.01.tgz -C /usr/local
# mv /usr/local/cawadi-1.01 /usr/local/cawadi
```

3.2 Verificatie Perl

Controleer vervolgens of alle Perlmodules aanwezig zijn. Dit is normaal gesproken het geval bij elke distributie van Linux RedHat. Dit doet u door de volgende commando’s uit te voeren:

```
# which perl
/usr/bin/perl
# /usr/bin/perl bin/check-perl.pl
Ok - all modules present
#
```

Indien u een afwijkend resultaat te zien krijgt, kunt u de benodigde pakketten installeren met:

```
# cpan HTTP::Date
...
```

Dit kan ook gedaan worden met de RedHat Package Manager (RPM).

3.3 Verificatie OpenSSL

Verifieer op de volgende wijze of OpenSSL aanwezig is:

```
# which openssl
/usr/bin/openssl
# /usr/bin/openssl version
OpenSSL 0.9.7g 11 Apr 2005
#
```

3.4 Verificatie sendmail

Verifieer op de volgende wijze of sendmail functioneert:

```
# which sendmail
/usr/sbin/sendmail
# sh test-email.sh eigen@email.address.nl
...
```

Als het goed is, ontvangt u een e-mail met als afzender `test@wadi.nl` op het adres dat u zojuist heeft opgegeven. Indien de afzender met `www@` begint, is de `www`-gebruiker niet opgenomen in de ‘trusted list’ van sendmail.

3.5 Setup.conf

Alle configuratie-instellingen zijn opgenomen in het `setup.conf`-bestand. Met behulp van dit bestand worden configuratiebestanden gegenereerd voor de webserver (`etc/httpd-ca-wadi.conf`) en de webapplicatie (`lib/local.conf.pl`). Daarvoor moet u eerst het bestand `setup.conf.sample` kopiëren naar `setup.conf`:

```
# cp setup.conf.sample setup.conf
# vi setup.conf
```

Pas vervolgens in ieder geval de cruciale variabelen aan uit tabel 3.1. De meeste andere variabelen worden direct afgeleid van deze 5 basiswaarden.

3.5.1 Testmemmonic

We raden u aan om gedurende de installatie als naam ‘Wadi-Test’ als systeemnaam te gebruiken om later duidelijk onderscheid te kunnen maken tussen de testcertificaten en het definitieve certificaat (zie volgende hoofdstuk).

3.5.2 Controle

Controleer vervolgens de syntax van `setup.conf` met het volgende commando:

Tabel 3.1: Belangrijkste configuratie variabelen

<i>Variable</i>	<i>Functie</i>
WADI_DIR	De map waarin dit systeem staat bijv. <code>/usr/local/cawadi</code> .
NAME	Naam van het systeem bijv. 'WADI-Test'
E-MAIL	Role e-mailadres van de beheerders en toezichhouders. Een e-mail die naar dit adres gaat, wordt doorgestuurd naar alle beheerders.
SECRET	Een willekeurige 'secret'-tekenreeks. Deze wordt gebruikt als 'seed' voor diverse random generators. De waarde die u invoert is niet van belang.
FQDN	De Fully Qualified Domain Name waarop de webserver te bereiken is en deze moet ingevoerd worden zonder 'http://' ervoor.
O, L, ST en C	De basisdetails van de organisatie.
ADMIN_UID	UserID van het Beheerderaccount, bijv. <code>wadiadmin</code> .
SENDMAIL	Locatie van de sendmailbestanden (uit sectie 3.4).
OPENSLL	Locatie van de OpenSSL-bestanden (uit sectie 3.3).

```
# ./bin/conf2perl.pl setup.conf
# Generated on Wed Aug 17 18:24:48 2005
# from setup.conf
...
#
```

3.6 Genereren van configuratiebestanden

Genereer de configuratiebestanden als volgt:

```
# ./install.sh
Ok - all modules present
Installing...

Done.
#
```

Verifieer eventueel handmatig of de gegenereerde bestanden `etc/httpd-ca-wadi.conf` en `lib/local.conf.pl` correct zijn.

3.7 Genereren van certificaten

Genereer vervolgens de certificaten zoals wordt aangegeven:

```
# ./make-certs.sh
.. kies optie 1
..
Ok.
#
```

Zie appendix A voor de volledige uitvoer. Er worden *twee* server certificaten aangemaakt: `server.pem` en `server.jks`. Het eerste certificaat is ten behoeve van de Server; het tweede certificaat is voor de soap/java omgeving.

3.8 Apache-instellingen

Voeg vervolgens een ‘include’ toe aan het Apacheconfiguratiebestand `httpd.conf`:

```
# vi /usr/local/httpd/conf/httpd.conf
    # httpd.conf
    ...
    # Include the WADI configuration.
    include "/usr/local/cawadi/etc/httpd-ca-wadi.conf"
# apachectl configtest
...
Processing config file: /usr/local/cawadi/etc/httpd-ca-wadi.conf
Syntax OK
#
# apachectl stop
# apachectl start
```

Het is noodzakelijk om de eerste keer Apache te stoppen, omdat de SSL engine anders niet gestart kan worden, een ‘gracefull’ is niet genoeg.

Kies tot slot beheerwachtwoorden voor de beheerders die toegang krijgen tot de website. Dit doet u als volgt:

```
# htpasswd etc/htpasswd fred
# htpasswd etc/htpasswd mary
```

Indien nodig dient u er ook voor te zorgen dat Apache opstart tijdens het opstarten van de server (via de optie ‘Apache’ in de RedHat bootmanager).

3.9 CRL-bestand automatisch laten bijhouden

De WebAPI maakt gebruik van een zogenaamde CRL-bestand (CertificateRevocationList). Hierin wordt een lijst bijgehouden van alle certificaten/gebruikers die niet langer toegang tot het systeem hebben. Dit bestand wordt gekoppeld naar de WebAPI om zo gebruikers die in de lijst staan de toegang aan het systeem te wijgeren.

Om het systeem dit bestand automatisch te laten bijhouden dient u de volgende stappen uit te voeren:

```
# ./bin/conf2crontab setup.conf
...
#
```

Hiermee wordt een zogenaamde 'crontab' op de server opgeslagen waarmee het systeem elke dag van het jaar om de 6 uur het CRL-bestand verversst. Het programma dat het CRL-bestand bijhoudt wordt aangeroepen als de www-gebruiker die ingesteld is in het bestand `setup.conf` zodat ook de web interface dit bestand tussendoor kan verversen.

3.10 Installatieverificatie

Open vervolgens met een browser de URL (uit tabel 3.1) en verifieer of men een webpagina te zien krijgt. Vraag vervolgens een certificaat aan.

3.10.1 Reboot

We raden u aan om het systeem indien mogelijk ten minste een maal opnieuw op te starten om te verifiëren of de Apacheserver naar behoren werkt en of eventuele IP-aliases en firewall-regels correct zijn vastgelegd.

Hoofdstuk 4

Troubleshooting

Eventuele fouten zullen opgenomen worden in het bestand `error_log` van de Apache webserver (meestal opgeslagen in `/var/log/httpd/error_log`). Indien men het bestand `setup.conf` verandert, dient men ervoor te zorgen dat de instellingen van de map waarin dit bestand is opgeslagen correct zijn.

Een typische volgorde van stappen is als volgt:

```
# tail -f /var/log/httpd/error_log
... fout...
ctrl-C
# vi setup.conf
# ./install.sh
# ./make-certs.sh
# apachectl restart
```

Hierna raadpleegt men wederom de website.

Hoofdstuk 5

Ingebruikname

Indien alles naar behoren werkt en getest is, kan men het systeem in gebruik nemen.

5.1 Beveiligen van het systeem

Allereerst worden eventuele Unixwachtwoorden voor de `www` en `wwwadmin` opgehaald en wordt gecontroleerd of de `WADI_DIR` alleen toegankelijk is voor deze twee gebruikers.

5.2 Web accounts

Verifieer of het `etc/htpasswd`-bestand geen testaccounts meer bevat.

5.3 Definitief certificaat aanmaken

Kies de definitieve naam in `setup.conf` en voer `install.sh` nogmaals uit.

Vervolgens maakt men met `make-certs.sh` de definitieve certificaten aan.

5.4 Veiligstellen van de geheime sleutel

De map `offline` bevat de geheime sleutel van het rootcertificaat. Deze dient op een draagbaar medium opgeslagen te worden, bijvoorbeeld op een floppy. Vervolgens wordt de geheime sleutel van de hardeschijf gewist.

Normaal gesproken dient dit met het `srm`-commando (zie appendix B en figuur B.1) ‘secure remove’ gedaan worden. Echter niet alle versies van Linux ondersteunen ‘secure remove’ ten gevolge van US-export beperkingen. Een kant-en-klare RPM kan vanaf het adres uit appendix B op pagina 27 gehaald worden.

```
# cp offline/ca.key /mount/floppy/  
# srm offline/ca.key
```

Eventueel kan men hierna een ‘snapshot’ maken van de `ca-` en `cawww-` mappen en ook deze op een draagbaar medium, zoals een floppy, bewaren.

5.5 Herstart de webserver

Ten slotte dient de webserver opnieuw te worden opgestart.

Hoofdstuk 6

Beheer

6.1 Dagelijks beheer

De `error_log` en de `access_log` groeien gestaag, namelijk zo'n 3-5kbyte per verstrekt certificaat. Ze zullen dus op gezette tijden geroteerd moeten worden. Dit kan tezamen met de met de 'newsyslogrotatie' of de 'weekly periodic functie' van Linux uitgevoerd worden.

Indien nodig dient men de `error_log` van de webserver te controleren op fouten.

6.2 Jaarlijks beheer

Eén maal per jaar dienen de certificaten vernieuwd te worden. Dit doet men met optie '3' van de `make-certs.sh`-tool. Hiervoor is de CA-sleutel, die u in paragraaf 5.4 heeft veiliggesteld, weer nodig:

```
# cd /usr/local/cawadi
# cp /mount/floppy/ offline/ca.key
# ./make-certs.sh 3
# srm offline/ca.key
# apachectl restart
```

Normaal gesproken doet men er goed aan deze vernieuwing 2 tot 6 weken voor het certificaat daadwerkelijk verloopt uit te voeren. Na tien jaar verloopt ook het rootcertificaat. Deze kan met optie '2' vernieuwd worden.

Bijlage A

make-certs output

```
# ./make-certs.sh
Certificate maintenance tool

    1)      Reset the entire CA infrastructure (only
           used during testing).

    2)      Generate a new long term root certificate.

    3)      Update and resign the worker certificate
           for another year.

           This requires the offline 'root key' to
           be present in:
           /usr/local/ca-wadi/offline/ca.key

    4)      Print current validity of the worker
           certificate.

Choise [ 1, 2 or 3]:1
This will wipe all certificates, root keys
and so on. This should never be done on an
operational system.

Are you sure yes/no:yes
Generating a 1024 bit RSA private key
...+++++
.....+++++
writing new private key to '/usr/local/ca-wadi/offline/ca.key'
-----
Root certificate:
Certificate:
  Data:
    Version: 3 (0x2)
```

```
Serial Number:
  85:c9:a3:43:36:e6:88:ca
Signature Algorithm: md5WithRSAEncryption
Issuer: CN=WADI Certificate Authority, C=NL, L=Den Haag, ST=Zuid Holland, O=
Validity
  Not Before: Aug 17 18:31:38 2005 GMT
  Not After : Aug 15 18:31:38 2015 GMT
Subject: CN=WADI Certificate Authority, C=NL, L=Den Haag, ST=Zuid Holland, O=
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:ac:16:d7:fe:f5:be:27:d2:a6:8d:03:6e:05:7d:
      58:36:2c:50:30:66:9f:1c:65:fc:d8:0f:ca:97:0e:
      77:78:28:d9:93:aa:88:6c:a9:05:46:0b:0b:db:e4:
      fb:08:f5:9c:65:c4:66:5e:d3:38:90:a8:3e:99:2a:
      94:9f:39:5e:27:16:77:32:a4:a5:81:7c:aa:75:c5:
      05:5b:90:90:f8:a6:10:9e:dd:e1:13:b3:97:4f:b7:
      9b:74:ab:dc:ad:eb:ba:fc:41:7a:87:5f:ec:68:31:
      63:16:22:7d:f5:cb:c9:8a:91:31:a0:a0:5e:a2:6e:
      7a:5e:c1:03:42:85:bd:f6:d5
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Key Identifier:
    84:24:F0:CC:4F:C7:D3:FB:D7:D8:58:CB:E2:2B:16:60:72:36:4C:BC
  X509v3 Authority Key Identifier:
    keyid:84:24:F0:CC:4F:C7:D3:FB:D7:D8:58:CB:E2:2B:16:60:72:36:4C:BC
    DirName:/CN=WADI Certificate Authority/C=NL/L=Den Haag/ST=Zuid Holla
    serial:85:C9:A3:43:36:E6:88:CA

  X509v3 Basic Constraints:
    CA:TRUE
  X509v3 Key Usage:
    Certificate Sign, CRL Sign
  X509v3 Subject Alternative Name:
    email:ca@asemantics.com, URI:http://10.11.0.217/
  X509v3 Issuer Alternative Name:
    URI:http://10.11.0.217//issuer.html#longtermRootCertificate
Signature Algorithm: md5WithRSAEncryption
  20:a2:17:0b:df:4e:53:72:79:62:f2:75:26:f6:12:c1:d6:eb:
  ac:54:b4:c7:a2:b1:12:19:08:0a:66:cf:48:81:af:52:e2:2e:
  33:f1:c5:cf:1f:2b:ee:96:80:28:71:4c:3e:f1:8c:40:9a:a1:
  8f:78:02:70:a3:2e:40:c9:6a:cb:50:11:dc:ec:75:f4:f1:fa:
  3c:db:4a:87:f2:4d:02:ca:1e:29:82:27:2a:3f:25:4c:3e:4a:
  1a:03:6f:4d:ac:8d:d4:80:00:7d:e0:ff:21:de:c7:0f:db:35:
  a8:89:6d:df:c8:93:9a:46:e0:d6:f4:66:40:7c:85:82:18:e4:
  74:35
```

```

Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to '/usr/local/ca-wadi/ca/ca-xs.key'
-----
Using configuration from /usr/local/ca-wadi/etc/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 0 (0x0)
  Validity
    Not Before: Aug 17 18:31:39 2005 GMT
    Not After : Aug 17 18:31:39 2006 GMT
  Subject:
    countryName           = NL
    stateOrProvinceName  = Zuid Holland
    organizationName      = WADI
    organizationalUnitName = Access Management
    commonName            = WADI Certificaat beheer
    localityName          = Den Haag
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:TRUE
    X509v3 Subject Key Identifier:
      OC:5C:B6:88:29:2C:E5:81:72:AD:9D:75:88:C1:A7:C9:4F:73:83:C2
    X509v3 Authority Key Identifier:
      keyid:84:24:F0:CC:4F:C7:D3:FB:D7:D8:58:CB:E2:2B:16:60:72:36:4C:BC
      DirName:/CN=WADI Certificate Authority/C=NL/L=Den Haag/ST=Zuid Holland
      serial:85:C9:A3:43:36:E6:88:CA

    X509v3 Subject Alternative Name:
      URI:http://10.11.0.217//issuer.html#annualXsCertificate
    X509v3 Issuer Alternative Name:
      email:ca@asemantics.com, URI:http://10.11.0.217/
    X509v3 Key Usage:
      Certificate Sign, CRL Sign
Certificate is to be certified until Aug 17 18:31:39 2006 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to '/usr/local/ca-wadi/ca/server.key'
-----
Using configuration from /usr/local/ca-wadi/etc/openssl.cnf
DEBUG[load_index]: unique_subject = "yes"

```

Check that the request matches the signature

Signature ok

Certificate Details:

Serial Number: 1 (0x1)

Validity

Not Before: Aug 17 18:31:40 2005 GMT

Not After : Aug 17 18:31:40 2006 GMT

Subject:

countryName = NL

stateOrProvinceName = Zuid Holland

organizationName = WADI

organizationalUnitName = WADI Certificaat beheer Webserver

commonName = 10.11.0.217

localityName = Den Haag

X509v3 extensions:

X509v3 Basic Constraints:

CA:TRUE

X509v3 Subject Key Identifier:

67:B4:6F:9E:39:57:9A:9B:75:00:30:0C:8E:28:12:60:0B:3E:05:9F

X509v3 Authority Key Identifier:

keyid:84:24:F0:CC:4F:C7:D3:FB:D7:D8:58:CB:E2:2B:16:60:72:36:4C:BC

DirName:/CN=WADI Certificate Authority/C=NL/L=Den Haag/ST=Zuid Holl

serial:85:C9:A3:43:36:E6:88:CA

X509v3 Subject Alternative Name:

URI:http://10.11.0.217//issuer.html#annualXsCertificate

X509v3 Issuer Alternative Name:

email:ca@asemantics.com, URI:http://10.11.0.217/

X509v3 Key Usage:

Certificate Sign, CRL Sign

Certificate is to be certified until Aug 17 18:31:40 2006 GMT (365 days)

Write out database with 1 new entries

Data Base Updated

Please ensure that the offline key at

/usr/local/ca-wadi/offline/ca.key

is moved to offline storage, such a floppy

or a USB stick, and subsequently

is deleted with a secure rm (e.g. srm).

Using configuration from /usr/local/ca-wadi/etc/openssl.cnf

DEBUG[load_index]: unique_subject = "yes"

Using configuration from /usr/local/ca-wadi/etc/openssl.cnf

DEBUG[load_index]: unique_subject = "yes"

Ok.

#

cp /usr/local/ca-wadi/offline/ca.key /mnt/floppy

srm /usr/local/ca-wadi/offline/ca.key

#

Bijlage B

Secure RM

De broncode en de installatiebestanden (Red Hat Packages, RPMs) kunnen gevonden worden op <http://srm.sourceforge.net/>. Secure RM is in alle ‘non-domestic’ versies van Red Hat (versies na 2004) standaard bijgeleverd. Zie figuur B.1 voor een samenvatting van de handleiding.

```
SRM(1)
NAME
  srm - securely remove files or directories
SYNOPSIS
  srm [OPTION]... FILE...
DESCRIPTION
  srm removes each specified file by overwriting, renaming, and truncating it before unlinking. This prevents
  other people from undeleting or recovering any information about the file from the command line.
  srm, like every program that uses the getopt function to parse its arguments, lets you use the -- option to
  indicate that all following arguments are non-options. To remove a file called '-f' in the current directory,
  you could type either "srm -- -f" or "srm ./-f".
OPTIONS
  -d, --directory
      ignored (for compatibility with rm(1))
  -f, --force
      ignore nonexistent files, never prompt
  -i, --interactive
      prompt before any removal
  -r, -R, --recursive
      remove the contents of directories recursively
  -s, --simple
      only overwrite with a single pass of random data
  -m, --medium
      overwrite the file with 7 US DoD compliant passes (0xF6, 0x00, 0xFF, random, 0x00, 0xFF, ran-
      dom)
  -z, --zero
      after overwriting, zero blocks used by file
  -n, --nounlink
      overwrite file, but do not rename or unlink it
  -v, --verbose
      explain what is being done
  --help
      display this help and exit
  --version
      output version information and exit
NOTES
  srm can not remove write protected files owned by another user, regardless of the permissions on the direc-
  tory containing the file.
  The -s option overrides the -m option, if both are present. If neither is specified, the 35-pass Gutmann algo-
  rithm is used.
  Development and discussion of srm is carried out at <http://sourceforge.net/project/?group_id=3297>,
  which is also accessible via <http://srm.sourceforge.net>.
SEE ALSO
  rm(1)
Linux ESD
20 September 2004
1
```

Figuur B.1: “Manual page srm(1)”