CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Handleiding configuratie smartcard logon UZI-pas

Versie 2.0

Datum 5 november 2010
Status definitief (UZ63.01)

Inhoud

1 Inleiding—4
1.1 Doelstelling—4
1.2 Inleiding smartcard logon Microsoft Windows—4
1.3 Inleiding smartcard logon met UZI-pas—4
1.3.1 Toelichting wijziging certificaatprofiel—4
1.3.2 Invulling UPN door UZI-register—4
1.3.3 Koppeling UPN aan user account—5
1.4 Randvoorwaarden voor werking smartcard logon—5
1.5 CRL distributiepunt voor UZI-passen—5
1.5.1 CRL's UZI-testpassen tweede generatie test—6
1.5.2 CRL's UZI-passen tweede generatie productie—6
1.5.3 CRL's UZI-passen SHA-2 generatie test—6
1.5.4 CRL's UZI-passen SHA-2 generatie productie—7
1.6 Opbouw van het document—7
1.6.1 UZI-passen—7
1.6.2 UZI-testpassen en productiepassen—7
1.6.3 Leeswijzer—7
1.7 Disclaimer—8
1.8 Referenties—8
1.8.1 Documentatie microsoft—8
1.8.2 Documentatie AET Europe BV—9

2 Trusten CA certificaten UZI-register op Domain Controller—10
2.1 CA certificaten downloaden—10
2.1.1 Acceptatieomgeving—10
2.1.2 Productieomgeving—10
2.1.3 Acceptatieomgeving SHA-2—11
2.1.4 Productieomgeving SHA-2—11
2.2 Installeren CA certificaten op Domain Controllers—11
2.2.1 Controle aanwezige certificaten op Domain Controller—12

3 Configuratie Smartcard Logon UZI-pas specifiek—14
3.1 Toevoegen additionele UPN suffix (UPN suffix = abonneenummer)—14
3.2 Toevoegen nieuwe gebruiker (User logon name=UZI-nummer)—15
3.3 Aanpassen bestaande gebruiker—17
3.4 Aanpassen Group Policy m.b.t. "Smartcard Removal Behaviour"—17

4 Probleemoplossing—18
4.1 Mogelijke foutmeldingen bij aanmaken eigen smartcards—18
4.2 Foutmeldingen bij gebruik UZI-pas voor smartcard logon—18
4.2.1 CA's not trusted—18
4.2.2 CRL's onbeschikbaar—18
4.2.3 Certificaat is ingetrokken—18
4.2.4 Verkeerde UPN ingevoerd—19
4.2.5 Pas geblokkeerd—19
4.2.6 Verkeerde pincode—19

BIJLAGE 1: Microsoft Smart card logon architecture and process—20

BIJLAGE 2: Aandachtspunten Registry settings m.b.t. CRL—22

BIJLAGE 3: Third party certificaten op Domain Controller(s)—23

BIJLAGE 4: SHA-2 i.c.m. Windows 2003—26

Versiehistorie

Versie	Datum	Status	Toevoegingen en wijzigingen	Hst/§
1.0	30-06-2008	Definitief	Eerste oplevering voor externe publicatie	
2.0	05-11-2010	Review	Windows 2008 en SHA-2 opgenomen in de documentatie	

Copyright CIBG © te Den Haag
Niets uit deze uitgave mag verveelvoudigd en/of openbaar worden gemaakt (voor willekeurig welke doeleinden) door middel van druk, fotokopie, microfilm, geluidsband, elektronisch of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van CIBG.

1 Inleiding

1.1 Doelstelling

UZI-passen die uitgegeven zijn na 1 mei 2008 kunnen binnen een Microsoft Windows 2003 & 2008 (r2) netwerk gebruikt worden voor smartcard logon. Het doel van dit document is tweeledig:

1 Een algemene handleiding te geven voor de inrichting van smartcard logon in Windows Server omgevingen;
2 Specifieke configuraties te beschrijven om de UZI-pas te kunnen gebruiken voor smartcard logon.

De doelgroep van dit document zijn systeembeheerders en IT specialisten met kennis van gebruikersbeheer in Windows Server omgevingen en met het beheer van Active Directory.

1.2 Inleiding smartcard logon Microsoft Windows

Als de UZI-pas gebruikt wordt voor smartcard logon in Microsoft Windows omgevingen wordt gebruikt gemaakt van een standaard authenticatie mechanisme. Vandaar dat deze handleiding voor uitleg van dat mechanisme zoveel mogelijk verwijst naar reeds beschikbare support documentatie van Microsoft.

Het authenticatie mechanisme is kort samengevat in BIJLAGE 1: Microsoft Smart card logon architecture and process. Verder wordt verwezen naar de referenties die genoemd zijn in paragraaf 1.8.

1.3 Inleiding smartcard logon met UZI-pas

1.3.1 Toelichting wijziging certificaatprofiel

De UZI-pas bevat 3 eindgebruikercertificaten: 1 voor authenticatie, 1 voor elektronische handtekening en 1 voor vertrouwelijkheid. Ten behoeve van smartcard logon is het certificaatprofiel van het authenticatiecertificaat aangepast zodat deze bruikbaar is voor smartcard logon in Windows omgevingen. De wijzigingen die doorgevoerd zijn bij invoering van de tweede generatie van de CA hiërarchie zijn:

1 Toevoegen van Entended Key Usage attribuut
  Dit is een standaard attribuut dat voor ieder authenticatiecertificaat identiek zal zijn.
2 Uitbreiding van subject.AltName attribuut
  Hierin dient in een extra otherName de Microsoft UPN (User Principal Name) toegevoegd te worden in het formaat 'gebruiker@domein'. Het UZI-register ondersteunt dit door het vullen van de UPN met de volgende waarde:
  <UZI-nummer>@<abonneenummer>

1.3.2 Invulling UPN door UZI-register

Deze invulling van de UPN is mogelijk omdat bij de Microsoft implementatie noch het gebruikerdeel, noch het abonneedeel een directe relatie hoeft te hebben met een daadwerkelijke gebruikersnaam, respectievelijk domeinnaam in het Windows domein. Beide delen zijn vrij in te vullen karakterreeksen. Microsoft's enige

voorwaarde is dat elke UPN uniek is binnen een Domain Forest. Aan deze voorwaarde wordt voldaan:

- het UZI-nummer is altijd uniek voor een persoon (of per functie voor een Medewerkerpas niet op naam).
- het abonneenummer is altijd uniek voor de abonnee.

Voordelen van deze invulling van de UPN zijn:

- De nummers zijn nu al opgenomen in het certificaat en dus beschikbaar zonder wijziging in de interfaces tussen de systemen;
- De nummers zijn onveranderlijk bij vernieuwing van een pas (m.u.v. Medewerkerpas niet op naam);
- Er ontstaat geen directe relatie met de lokale infrastructuur van zorginstellingen. Dat zou namelijk kunnen leiden tot vernieuwing van alle UZI-passen bij wijziging van de lokale infrastructuur (fusie, migratie domeinstructuur);
- De wijziging heeft geen invloed op de gegevens die het UZI-register in het registratieproces vast moeten leggen. De aanvrager zou anders UPN's van toekomstige pashouders moeten opgeven.

1.3.3 Koppeling UPN aan user account

Uiteraard moet in de lokale Active Directory infrastructuur de relatie gelegd worden van de nummers naar een specifiek gebruikersaccount. In een Proof of Concept is aangetoond dat het beschikbaar maken van een abonneenummer als domain een standaard actie is binnen Active Directory: het toevoegen van een user principal name suffix. In de handleiding is dit toegelicht in paragraaf 3.1. Zie verder Microsoft technet artikel:
Add user principal name suffixes:
http://technet2.microsoft.com/windowsserver/en/library/c61f2430-fcc3-41fd-b722-20cb11e1bf021033.mspx?mfr=true

Ook het aanpassen van de "User logon name" in <UZI-nummer> is standaard user account beheer in Active Directory. In de handleiding is dit toegelicht in paragraaf 3.2.

1.4 Randvoorwaarden voor werking smartcard logon

Deze handleiding gaat er vanuit dat de volgende middelen beschikbaar zijn:

- 1 Windows 2003 of Windows 2008 (r2) server ingericht als domain controller
- 1 werkstation + kaartlezer + SafeSign middleware. Zie voor actuele versie en installatie instructie:
  http://www.uziregister.nl/technischesupport/installerenuzipasenkaartlezer/windows/
- UZI-testpassen met productiedatum na 1 mei 2008
- Windows support tools (t.b.v. ADSI Edit Tool) geïnstalleerd op de Domain Controllers
- Domain Controllers en werkstations dienen toegang te hebben tot de volgende URLs waarop de CRL's van de UZI-passen worden gepubliceerd.

1.5 CRL distributiepunt voor UZI-passen

Zoals aangegeven is het een randvoorwaarde dat de CRL's benaderbaar zijn. Hieronder zijn de CRL distributiepunten opgenomen voor tweede generatie UZI-passen.

1.5.1 CRL's UZI-testpassen tweede generatie test

Type	CRL Distribution Point
Zorgverlenertestpas	http://www.uzi-register-test.nl/cdp/test_uzi-register_zorgverlener_ca_g2.crl
Medewerkertestpas op naam	http://www.uzi-register-test.nl/cdp/test_uzi-register_medewerker_op_naam_ca_g2.crl
Medewerkertestpas niet op naam	http://www.uzi-register-test.nl/cdp/test_uzi-register_medewerker_niet_op_naam_ca_g2.crl
Test Zorg CSP CA	http://www.uzi-register-test.nl/cdp/test_zorg_csp_ca.crl
Test UZI level 2 CA	http://www.uzi-register-test.nl/cdp/test_uzi-register_level_2_ca.crl
Test UZI Root CA	http://www.uzi-register-test.nl/cdp/test_uzi-register_root_ca.crl

Tabel 1: Overzicht van CRL's voor tweede generatie UZI-testpassen

Dit overzicht is ook beschikbaar via
http://www.uziregister.nl/technischesupport/testomgeving/geldigheidtestpassen/

1.5.2 CRL's UZI-passen tweede generatie productie

Type	CRL Distribution Point
Zorgverlenerpas	http://www.csp.uzi-register.nl/cdp/uzi-register_zorgverlener_ca_g2.crl
Medewerkerpas op naam	http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_op_naam_ca_g2.crl
Medewerkerpas niet op naam	http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_niet_op_naam_ca_g2.crl
Zorg CSP CA	http://www.csp.uzi-register.nl/cdp/zorg_csp_ca.crl
Domein CA	Zie www.pkioverheid.nl
Root CA	Zie www.pkioverheid.nl

Tabel 2: Overzicht van CRL's voor tweede generatie UZI-passen

1.5.3 CRL's UZI-passen SHA-2 generatie test

Naam UZI-pastype	CRL Distribution Point
Zorgverlenertestpas	http://www.uzi-register-test.nl/cdp/test_uzi-register_zorgverlener_ca_g21.crl
Medewerkertestpas op naam	http://www.uzi-register-test.nl/cdp/test_uzi-register_medewerker_op_naam_ca_g21.crl
Medewerkertestpas niet op naam	http://www.uzi-register-test.nl/cdp/test_uzi-register_medewerker_niet_op_naam_ca_g21.crl
TEST Zorg CSP CA G21	http://www.uzi-register-test.nl/cdp/test_zorg_csp_ca_g21.crl
TEST UZI-register Level 2 CA G21	http://www.uzi-register-test.nl/cdp/test_uzi-register_level_2_ca_g21.crl
TEST UZI-register Root CA G21	http://www.uzi-register-test.nl/cdp/test_uzi-register_root_ca_g21.crl

Tabel 3: Overzicht van CRL's voor SHA-2 generatie UZI-testpassen

1.5.4 CRL's UZI-passen SHA-2 generatie productie

Type	CRL Distribution Point
Zorgverlenerpas	http://www.csp.uzi-register.nl/cdp/uzi-register_zorgverlener_ca_g21.crl
Medewerkerpas op naam	http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_op_naam_ca_g21.crl
Medewerkerpas niet op naam	http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_niet_op_naam_ca_g21.crl
Zorg CSP CA	http://www.csp.uzi-register.nl/cdp/zorg_csp_ca_g21.crl
Domein CA	Zie www.pkioverheid.nl
Root CA	Zie www.pkioverheid.nl

Tabel 4: Overzicht van CRL's voor SHA-2 generatie UZI-passen

Dit overzicht is ook beschikbaar via
http://www.uziregister.nl/ikhebeenuzipas/geldigheiduzipassen/

1.6 Opbouw van het document

1.6.1 UZI-passen

Deze handleiding beschrijft smartcard logon op basis van UZI-testpassen.

1.6.2 UZI-testpassen en productiepassen

Voor productiepassen en testpassen zijn de handelingen identiek. Alleen dienen op de relevante plaatsten productie CA certificaten geïnstalleerd te worden.

1.6.3 Leeswijzer

Het document is als volgt opgebouwd:

- Hoofdstuk 1 bevat de algemene inleiding
- Hoofdstuk 2 Trusten CA certificaten UZI-register op Domain Controller beschrijft hoe de CA certificaten van UZI-passen vertrouwd moeten worden binnen de Windows Server omgeving. Dit is een stap die specifiek nodig is bij het gebruik van UZI-passen.
- Hoofdstuk 3 beschrijft de Werkplek configuratie. Op alle werkplekken die gebruik willen maken van smartcard logon dient de actuele versie van SafeSign plus een kaartlezer te worden geïnstalleerd. Dit hoofdstuk beschrijft met name de configuratie van een beheerwerkplek die geschikt is om zelf smartcard aan te maken en van certificaten te voorzien.
- Hoofdstuk 4 Configuratie Smartcard Logon UZI-pas specifiek bevat de stappen die specifiek nodig zijn om een UZI-pas t.b.v. van smartcard logon te koppelen een bepaald Active Directory user account.
- Hoofdstuk 5 gaat in op veel voorkomende problemen en foutmeldingen.

Ten slotte zijn er nog 3 bijlagen:

- BIJLAGE 1: Microsoft Smart card logon architecture and process
- BIJLAGE 2: Aandachtspunten SmartCard Logon (Registry settings CRL)
- BIJLAGE 2: Beschrijft de aanvraag en installatie van Domain Controller certificaten indien deze door een externe Certificate Service Provider worden uitgegeven.

1.7 Disclaimer

Het UZI-register biedt de garantie dat het UPN veld en de andere specifieke aanpassingen voor smartcard logon conform de beschrijving in par. 1.3 opgenomen zal blijven in toekomstige generatie UZI-passen, tenzij dit mechanisme bij Microsoft volledig uitfaseert.

Het UZI-register kan echter geen garanties naar de toekomst bieden over de toepasbaarheid in toekomstige versies van Microsoft omgevingen. De beschreven configuratie is getest in een Windows 2003 / 2008 omgeving met Xp, Vista en Windows 7 client.

Door deze handleiding wil het UZI-register zo goed mogelijk informeren over de toepassing van smartcard logon met de UZI-pas. Een zorgaanbieder c.q. ICT dienstverlener dient zelf een impact analyse te maken voor het al dan niet gebruiken van de UZI-pas voor smartcard logon. Aandachtspunten zijn hierbij:

- Consequenties van specifieke vulling UPN attribuut. Dit is relevant als men kiest voor het werken met 1 UZI-pas per persoon. In die gevallen kunnen er binnen 1 Windows omgeving veel verschillende abonneenummers voorkomen. Dit resulteert in veel verschillende UPN suffixen. Het is niet duidelijk wat het effect hiervan is op performance;
- Koppelen van UZI-passen van gebruikers aan (bestaande) AD accounts;
- Toenemende impact van verlies c.q. vergeten van UZI-pas. Dit onderwerp staat onder de titel 'Reservepas' al langer op de agenda, maar smartcard logon zal de noodzaak van een alternatief bij onbeschikbaar van de UZI-pas alleen maar vergroten.
- Afhankelijkheid van de bereikbaarheid van CRL's. Het UZI-register doet alles wat redelijkerwijs mogelijk is om de CRL's online beschikbaar te hebben op het Internet. Dit betreft onder andere redundante configuratie netwerken en systemen plus een fysiek gescheiden uitwijkomgeving. Of de CRL's dan ook beschikbaar zijn op locatie van de zorgaanbieder hangt ook af van de infrastructuur bij de zorgaanbieder en de internet provider(s).
- Support. Het UZI-register kan geen support bieden bij specifieke configuratieproblemen binnen de Active Directory omgeving van een bepaalde zorgaanbieder.

Het UZI-register accepteert geen aansprakelijkheid voor gevolgschade bij het niet beschikbaar zijn van CRL's of het niet functioneren van smartcard logon binnen de Windows omgeving van een zorgaanbieder.

1.8 Referenties

1.8.1 Documentatie microsoft

[1] "Smart cards" TechNet article
http://www.microsoft.com/technet/security/topics/identitymanagement/scard.mspx

[2] "Troubleshooting Windows 2000 PKI Deployment and Smart Card Logon" white paper:
http://www.microsoft.com/technet/prodtechnol/windows2000serv/support/smrtcrdtrbl.mspx

[3] "Guidelines for enabling smart card logon with third-party certification authorities"

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q281245

[4] "Requirements for Domain Controller Certificates from a Third-Party CA, support Q291010"
http://support.microsoft.com/kb/291010

[5] "Enterprise Smart Card Deployment in the Microsoft Windows Smart Card Framework", June 2006, Derek Adam, Microsoft Corporation.
http://www.microsoft.com/downloads/details.aspx?FamilyID=fa7ec97c-11be-4e53-a0c4-04719b6a7ab6&DisplayLang=en

[6] "Planning a Smart Card Deployment"
http://technet2.microsoft.com/WindowsServer/f/?en/Library/5229033e-232b-4f91-9f86-0cbbd7cfc5a81033.mspx

[7] "Checklist: Deploying smart cards for logging on to Windows"
http://technet2.microsoft.com/WindowsServer/en/Library/b989f4fd-febd-42e1-a130-9e0f338007341033.mspx

[8] "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure"
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx

[9] "Smart Card Deployment at Microsoft"
http://www.microsoft.com/technet/itsolutions/msit/security/smartcrd.mspx

[10] "How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store"
http://support.microsoft.com/kb/295663/en-us

[11] "Advanced Certificate Enrollment and Management". This white paper documents and focuses on domain controller certificate enrollment for Windows 2000 and Windows Server™ 2003 domain controllers from a Windows 2000 or Windows Server 2003 stand-alone certificate authority (CA) as well as from a Windows Server 2003 enterprise CA.
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx#E1C

1.8.2 Documentatie AET Europe BV

[12] "SafeSign Identity Client User Guide, Microsoft Windows 2003", v2.1, 03-01-2007, A.E.T. Europe B.V.
http://www.uziregister.nl/Images/Windows2003_SafeSign-IC_v2.1_tcm38-22384.pdf

of via

http://www.uziregister.nl/technischesupport/installeren/overigehandleidingen/

2 Trusten CA certificaten UZI-register op Domain Controller

Dit hoofdstuk beschrijft hoe de CA certificaten van UZI-passen vertrouwd moeten worden binnen de Windows 2003 omgeving. Dit is een stap die specifiek nodig is bij het gebruik van UZI-passen. Zie voor verdere achtergrond informatie Microsoft support[10] *How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store*.

2.1 CA certificaten downloaden

De volledige CA hiërarchie van de acceptatie- of productie omgeving dient geïnstalleerd te worden indien gebruik gemaakt wordt van UZI-(test)passen. De CA's van de tweede generatie zijn op de hieronder vermelde locaties te downloaden. Verderop in dit document staat beschreven hoe de CA's geïnstalleerd dienen te worden:

2.1.1 Acceptatieomgeving

Type	**CA download locatie**
Zorgverlenertestpas	http://www.uzi-register-test.nl/cacerts/test_uzi-register_zorgverlener_ca_g2.cer
Medewerkertestpas op naam	http://www.uzi-register-test.nl/cacerts/test_uzi-register_medewerker_op_naam_ca_g2.cer
Medewerkertestpas niet op naam	http://www.uzi-register-test.nl/cacerts/test_uzi-register_medewerker_op_naam_ca_g2.cer
Test Zorg CSP CA	http://www.uzi-register-test.nl/cacerts/test_zorg_csp_ca.cer
Test UZI level 2 CA	http://www.uzi-register-test.nl/cacerts/test_uzi-register_level_2_ca.cer
Test UZI Root CA	http://www.uzi-register-test.nl/cacerts/test_uzi-register_root_ca.cer

Tabel 5: Overzicht van CA certificaten in acceptatieomgeving (tweede generatie)

Dit overzicht is ook beschikbaar via
http://www.uziregister.nl/technischesupport/testomgeving/hierarchietestomgeving/

2.1.2 Productieomgeving

Type	**CA download locatie**
Zorgverlenerpas	http://www.csp.uzi-register.nl/cacerts/uzi-register_zorgverlener_ca_g2.cer
Medewerkerpas op naam	http://www.csp.uzi-register.nl/cacerts/uzi-register_medewerker_op_naam_ca_g2.cer
Medewerkerpas niet op naam	http://www.csp.uzi-register.nl/cacerts/uzi-register_medewerker_niet_op_naam_ca_g2.cer
Zorg CSP CA	http://www.csp.uzi-register.nl/cacerts/zorg_csp_ca.cer
Staat der Nederlanden	Downloaden vanaf http://www.pki-overheid.nl
UZI Root CAStaat der Nederlanden Overheid	Downloaden vanaf http://www.pki-overheid.nl

Tabel 6: Overzicht van CA certificaten in Productieomgeving (tweede generatie)

2.1.3 Acceptatieomgeving SHA-2

Naam CA	URL van CA certificaat
TEST UZI-register Root CA G21	http://www.uzi-register-test.nl/cacerts/test_uzi-register_root_ca_g21.cer
TEST UZI-register Level 2 CA G21	http://www.uzi-register-test.nl/cacerts/test_uzi-register_level_2_ca_g21.cer
TEST Zorg CSP CA G21	http://www.uzi-register-test.nl/cacerts/test_zorg_csp_ca_g21.cer
TEST UZI-register Zorgverlener CA G21	http://www.uzi-register-test.nl/cacerts/test_uzi-register_zorgverlener_ca_g21.cer
TEST UZI-register Medewerker op naam CA G21	http://www.uzi-register-test.nl/cacerts/test_uzi-register_medewerker_op_naam_ca_g21.cer
TEST UZI-register Medewerker niet op naam CA G21	http://www.uzi-register-test.nl/cacerts/test_uzi-register_medewerker_niet_op_naam_ca_g21.cer

Tabel 7: Overzicht van CA certificaten in Acceptatieomgeving (SHA-2)

2.1.4 Productieomgeving SHA-2

Type	CA download locatie
Zorgverlenerpas	http://www.csp.uzi-register.nl/cacerts/uzi-register_zorgverlener_ca_g21.cer
Medewerkerpas op naam	http://www.csp.uzi-register.nl/cacerts/uzi-register_medewerker_op_naam_ca_g21.cer
Medewerkerpas niet op naam	http://www.csp.uzi-register.nl/cacerts/uzi-register_medewerker_niet_op_naam_ca_g21.cer
Zorg CSP CA	http://www.csp.uzi-register.nl/cacerts/zorg_csp_ca_g21.cer
Staat der Nederlanden	Downloaden vanaf http://www.pki-overheid.nl
UZI Root CAStaat der Nederlanden Overheid	Downloaden vanaf http://www.pki-overheid.nl

Tabel 8: Overzicht van CA certificaten in Productieomgeving (SHA-2)

Dit overzicht is ook beschikbaar via
http://www.uziregister.nl/watisdeuzipas/betrouwbaarheid/hierarchie/

2.2 Installeren CA certificaten op Domain Controllers

Onderstaande dient uitgevoerd te worden op de Domain Controller. De Issuing CA's en de hiërarchie tot en met het root CA certificaat worden gepubliceerd in Active Directory met als doel dat deze CA's door alle servers en werkstations in het domain worden "ge-trust". Dit is noodzakelijk om met een certificaat uitgegeven door één van de CA's in te kunnen loggen. Voer hiervoor de volgende commando's uit:

certutil -dsPublish -f test_uzi-register_root_ca.cer rootca
certutil -dsPublish -f test_uzi-register_root_ca.cer ntauthca
certutil -dsPublish -f test_uzi-register_level_2_ca.cer rootca
certutil -dsPublish -f test_uzi-register_level_2_ca.cer ntauthca
certutil -dsPublish -f test_zorg_csp_ca.cer rootca
certutil -dsPublish -f test_zorg_csp_ca.cer ntauthca
certutil -dsPublish -f test_uzi-register_medewerker_op_naam_ca_g2.cer rootca
certutil -dsPublish -f test_uzi-register_medewerker_op_naam_ca_g2.cer ntauthca

certutil -dsPublish -f test_uzi-register_medewerker_op_naam_ca_g2.cer rootca
certutil -dsPublish -f test_uzi-register_medewerker_op_naam_ca_g2.cer ntauthca
certutil -dsPublish -f test_uzi-register_zorgverlener_ca_g2.cer rootca
certutil -dsPublish -f test_uzi-register_zorgverlener_ca_g2.cer ntauthca

LET OP:
Vervang de testbenamingen voor de productiebenamingen als er met productie UZI-passen wordt gewerkt (of met SHA-2).

Nadat bovenstaande acties zijn uitgevoerd dient de Domain Controller te worden herstart.

2.2.1 *Controle aanwezige certificaten op Domain Controller*

Controleer of de Domain Controller zelf een certificaat heeft en of alle CA's geïnstalleerd zijn middels het commando:

certutil -dcinfo

Hieronder is de output ter illustratie weergegeven. Met gele highlights is de hiërarchie weergegeven die vertrouwd moet worden om UZI-testpassen te kunnen gebruiken voor smartcard logon binnen deze Windows omgeving.

```
0: WINDOWS2003SERV

*** Testing DC[0]: WINDOWS2003SERV
** Enterprise Root Certificates for DC WINDOWS2003SERV
Certificate 0:
Serial Number: 308623941085fd03d2c14e669139be5c
Issuer: CN=TEST Zorg CSP CA, O=agentschap Centraal Informatiepunt Beroepen
Gezondheidszorg, C=NL
Subject: CN=TEST UZI-register Zorgverlener CA G2, O=agentschap Centraal
Informatiepunt Beroepen Gezondheidszorg, C=NL
Non-root Certificate
Cert Hash(sha1): f2 08 52 d8 31 69 fe 81 5e 77 4f eb 16 bb 2f a5 a5 35 22 37

Certificate 1:
Serial Number: 6c14648682bd20f5b7bc8ff31ecf185a
Issuer: CN=TEST UZI-register Root CA, O=agentschap Centraal Informatiepunt
Beroepen Gezondheidszorg, C=NL
Subject: CN=TEST UZI-register Level 2 CA, O=agentschap Centraal Informatiepunt
Beroepen Gezondheidszorg, C=NL
Non-root Certificate
Cert Hash(sha1): c4 0b cb 2f 81 d0 a4 f2 42 57 41 37 23 d0 e2 00 dd 14 92 6b

Certificate 2:
Serial Number: 1d48ba1f366c5fdaf8e5c659c5e36ccb
Issuer: CN=TEST Zorg CSP CA, O=agentschap Centraal Informatiepunt Beroepen
Gezondheidszorg, C=NL
Subject: CN=TEST UZI-register Medewerker niet op naam CA G2, O=agentschap
Centraal Informatiepunt Beroepen Gezondheidszorg, C=NL
Non-root Certificate
Cert Hash(sha1): 5a 40 5f d7 66 5d 44 3f d4 c5 ac 90 d3 c0 43 5b d6 64 a6 a2
```

```
Certificate 3:
Serial Number: 033c8d9c3b100786dbcba7e9e3fbf160
Issuer: CN=TEST UZI-register Level 2 CA, O=agentschap Centraal Informatiepunt
Beroepen Gezondheidszorg, C=NL
Subject: CN=TEST Zorg CSP CA, O=agentschap Centraal Informatiepunt Beroepen
Gezondheidszorg, C=NL
Non-root Certificate
Cert Hash(sha1): 54 ab e5 61 0a af 70 10 3e 2d 13 2f 15 44 3c 47 a0 ae a6 1d

Certificate 4:
Serial Number: 2a584bd1612401e629141189a285669b
Issuer: CN=TEST Zorg CSP CA, O=agentschap Centraal Informatiepunt Beroepen
Gezondheidszorg, C=NL
Subject: CN=TEST UZI-register Medewerker op naam CA G2, O=agentschap Centraal
Informatiepunt Beroepen Gezondheidszorg, C=NL
Non-root Certificate
Cert Hash(sha1): 28 1a 22 c1 d1 bc c4 c3 a3 1a d3 63 aa 22 50 cf 86 3d eb 11

Certificate 5:
Serial Number: aac4bb2a93ea63e191d7556d576e6107
Issuer: CN=TEST UZI-register Root CA, O=agentschap Centraal Informatiepunt
Beroepen Gezondheidszorg, C=NL
Subject: CN=TEST UZI-register Root CA, O=agentschap Centraal Informatiepunt
Beroepen Gezondheidszorg, C=NL
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 13 87 5f 2d ac 9d ce 65 13 7d 6c 3e 53 bc 9d 6e 31 0f 1f 95

CertUtil: -DCInfo command completed successfully.
```

3 Configuratie Smartcard Logon UZI-pas specifiek

Dit hoofdstuk beschrijft de stappen die specifiek nodig zijn om een UZI-pas geschikt te maken voor smartcard logon voor een bepaald Active Directory user account.

Op alle werkplekken die gebruik willen maken van smartcard logon dient de actuele versie van SafeSign plus een kaartlezer te worden geïnstalleerd. Voor SafeSign zijn geen specifieke configuraties noodzakelijk. De standaardinstallatie voldoet. Installatiebeschrijving en de software zijn terug te vinden op de website van het UZI-register:
http://www.uziregister.nl/technischesupport/installeren/kaartlezeruzi-pas/

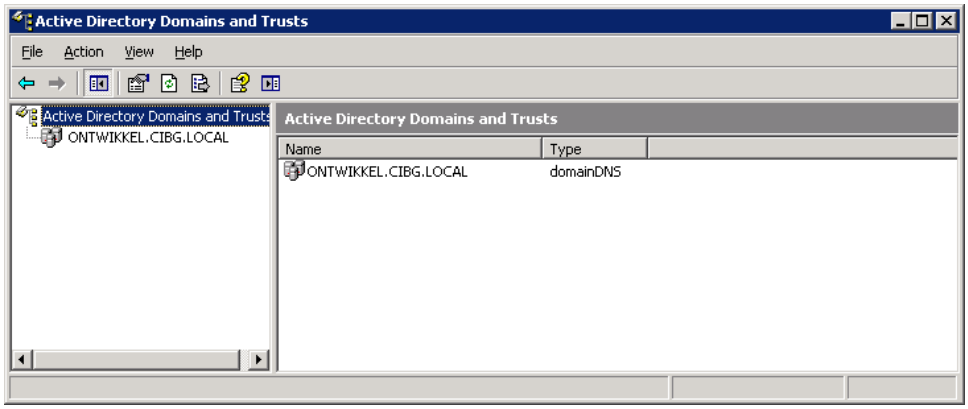
Bij smartcard logon wordt de Microsoft UPN (User Principal Name) uit het authenticatiecertificaat gebruikt om een betreffend gebruikersaccount te vinden. Standaard is de UPN in het formaat 'gebruiker@domein'. Het UZI-register ondersteunt door het opnemen van <UZI-nummer>@<abonneenummer> zoals toegelicht in paragraaf 1.3.

Hierdoor is het noodzakelijk om:
- een relatie tussen abonneenummer en domain. Dit gebeurt d.m.v. een UPN suffix;
- een relatie tussen UZI-nummer en username. Dit gebeurt d.m.v. de User logon name.

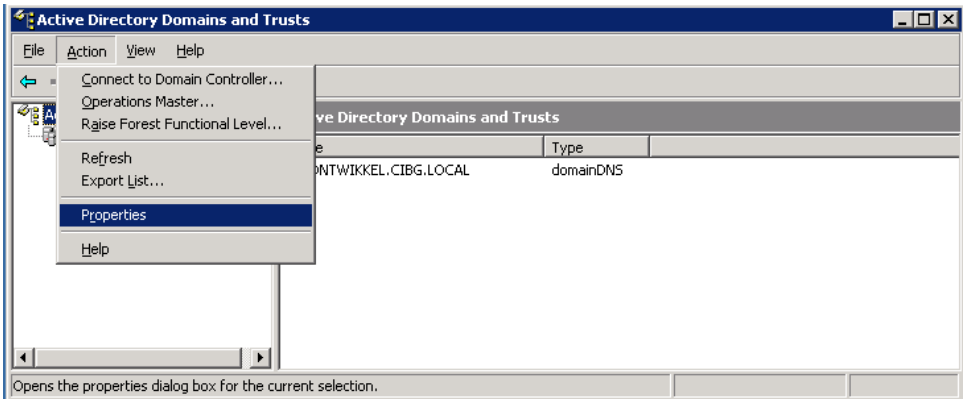
Beide acties zijn in dit hoofdstuk toegelicht.

3.1 Toevoegen additionele UPN suffix (UPN suffix = abonneenummer)

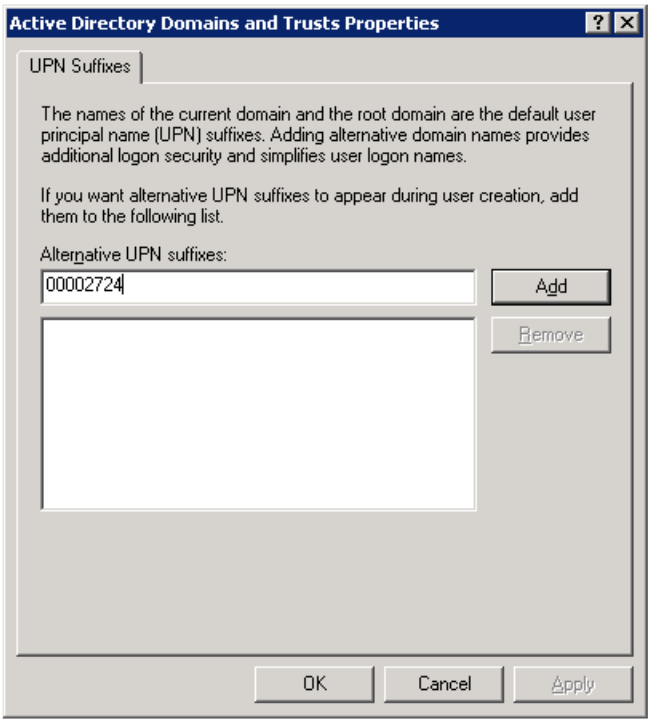
Ga **naar All Programs -> Administrative Tools -> Active Directory Domain and Trusts:**



Rechtermuisklik op **"Active Directory Domains and Trusts"** -> Kies **"Properties"**:



Voeg de UPN suffix toe:

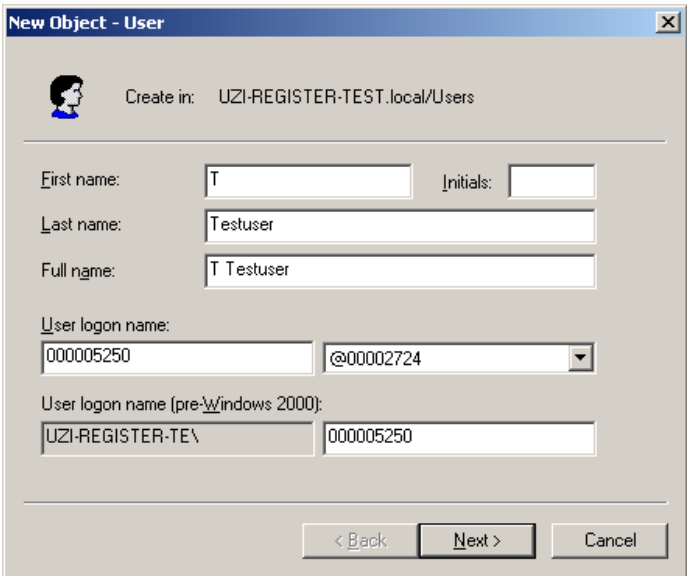


Dit is het abonneenummer van de UZI-pas. Dit gaat binnen de Active Directory omgeving gezien worden als een alias van het domein.

3.2 Toevoegen nieuwe gebruiker (User logon name=UZI-nummer)

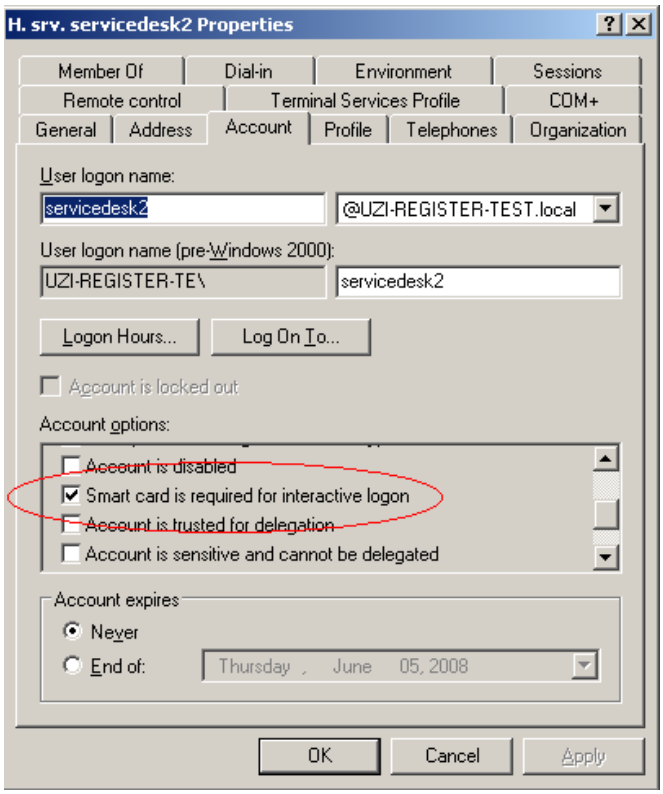
Indien een nieuwe gebruiker wordt toegevoegd dient bij de "User logon name" de juiste UPN suffix geselecteerd te worden. Verder dient het gebruikersdeel gevuld te worden met het UZI-nummer van de UZI-pas.

De complete "User logon name" dient overeen te komen met de UPN waarde in het desbetreffende certificaat: uzinummer@abonneenummer zoals hieronder weergeven:



Open daarna in de Active Directory het nieuw aangemaakte account.

Zet in het tabblad Account bij Account Options de optie voor Smart Card logon aan: Smart Card is required for interactive logon.



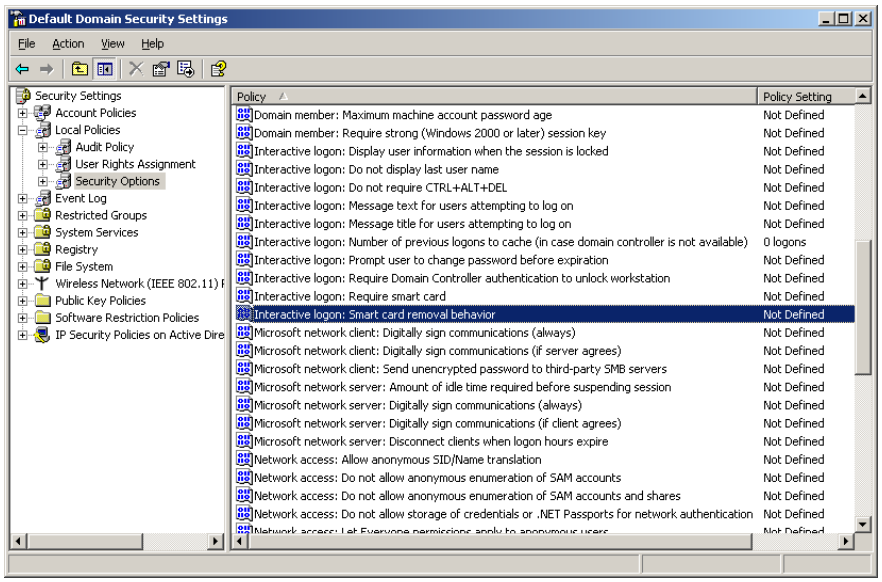
3.3 Aanpassen bestaande gebruiker

De “User logon name” van een bestaande gebruiker kan op dezelfde wijze worden aangepast als hierboven beschreven. Let hierop op dat de optie Requires Smart Card Logon aan wordt gezet.

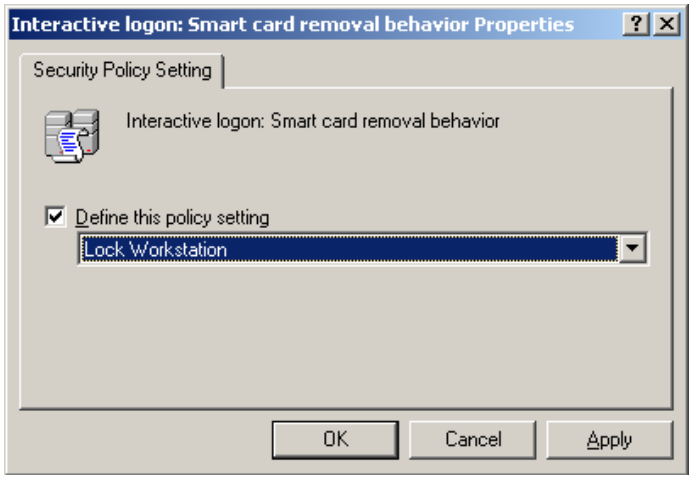
3.4 Aanpassen Group Policy m.b.t. “Smartcard Removal Behaviour”

Stel deze group policy zodanig in dat, zodra de smartcard wordt verwijderd, het systeem automatisch wordt gelocked.

Ga naar **All Programs -> Administrative Tools -> Domain security policy -> Local Policies Select Security Options**. Selecteer **“Interactive Logon: Smart card removal behaviour”**:



Activeer deze policy: **“Lock workstation”**:[1]



1 Indien gebruik wordt gemaakt van een Microsoft Vista werkstation, dient de service “Smart Card Removal Policy” gestart te zijn.

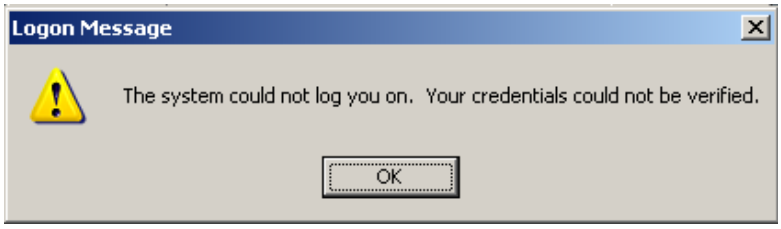
4 Probleemoplossing

4.1 Mogelijke foutmeldingen bij aanmaken eigen smartcards

Tijdens de configuratie van smartcard logon kunnen er op een aantal momenten foutmeldingen komen. In deze paragraaf staan een aantal voorkomende fouten vermeld die met name betrekking hebben op het zelf aanmaken van smartcards.

4.2 Foutmeldingen bij gebruik UZI-pas voor smartcard logon

4.2.1 CA's not trusted



Als de Certificate Authority certificaten niet zijn geïnstalleerd komt er een foutmelding dat de Credentials niet geladen kunnen worden. Deze melding komt ook in beeld als er wordt geprobeert om te inloggen met een UZI-pas afkomstig van een andere abonnee (en dus een afwijkende Domain suffix.

4.2.2 CRL's onbeschikbaar

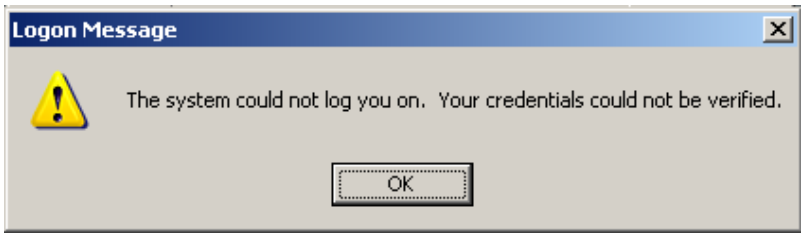
Bovenstaande foutmelding komt als er geen verbinding beschikbaar is met de CRL's. Dit kan bijvoorbeeld gebeuren als er geen internet verbinding beschikbaar is. De UZI-pas heeft als eis dat er altijd een geldige CRL kan worden benaderd. Dit om vast te stellen of de UZI-pas is ingetrokken of niet.

4.2.3 Certificaat is ingetrokken

Als een UZI-pas is ingetrokken kan deze ook niet meer gebruikt worden om in te loggen met Smartcard logon. Op het moment van inloggen vindt er communicatie plaats tussen de UZI-pas en de CRL's. Tijdens het inloggen zal hiervan een melding worden weergegeven.

Het is uiteraard wel mogelijk om (tijdelijk) voor de betreffende UZI-pashouder het account aan te passen zodat het account beschikbaar is om zonder UZI-pas in te loggen. Dit dan bijvoorbeeld tot het moment dat de pashouder de beschikking heeft over een nieuwe UZI-pas.

4.2.4 *Verkeerde UPN ingevoerd*

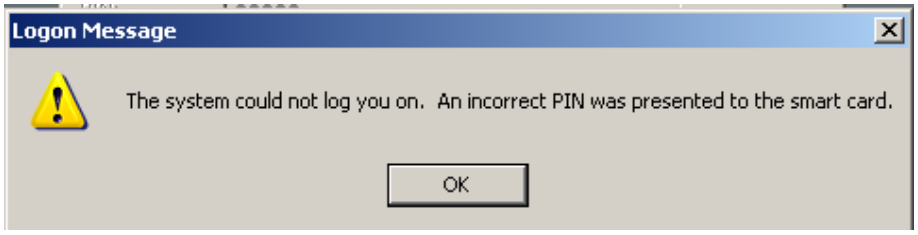


Bovenstaande foutmelding kan ontstaan als er een onjuiste UPN Suffix is opgegeven. Controleer of het opgegeven Suffix gelijk is.

4.2.5 *Pas geblokkeerd*

Als er met een UZI-pas wordt ingelogd die is geblokkeerd komt Safesign met bovenstaande melding. Hierin staat vermeldt dat met de Token Manager de pas kan worden gedeblokkeerd. Gebruiker hiervoor een systeem dat beschikt over de Token Manager, maar waarop niet hoeft te worden ingelogd met een Smartcard.

4.2.6 *Verkeerde pincode*



Bovenstaande foutmelding komt in beeld zodra er een onjuiste pincode wordt opgegeven. LET OP: deze foutmelding komt ook als er wordt ingelogd met een UZI-pas die niet geschikt is voor Smartcard logon en als de pas afkomstig is van een andere abonnee.

BIJLAGE 1: Microsoft Smart card logon architecture and process

http://www.microsoft.com/technet/security/topics/identitymanagement/scard.mspx

This section describes the recommended authentication protocol for smart card logon (Kerberos) and the smart card logon process.

The Kerberos protocol is the primary authentication mechanism in the Microsoft Windows 2000, Windows XP, and Windows Server 2003 operating systems. At the heart of the protocol is a trusted server called a Key Distribution Center (KDC). When the user logs on to the network, the KDC verifies the user's identity and provides credentials called "tickets," one for each network service that the user wants to use. Each ticket introduces the user to the appropriate service and optionally carries information that indicates the user's privileges for the service.

Microsoft's implementation of the protocol uses extensions to enable smart card logon, which offers the twin advantages of strengthening the authentication process and providing seamless entry into the PKI. Smart card logon works only with Kerberos; you cannot use NT LAN Manager (NTLM), the authentication method of Windows NT 4.0, and earlier versions of Windows NT, for smart card logon.

Typically, Kerberos uses symmetric key encryption. The certificate on the smart card, however, is based on asymmetric public key encryption.
As Figure 1 shows, Windows 2000, Windows XP, and Windows Server 2003 use a layered approach for local and domain logon,

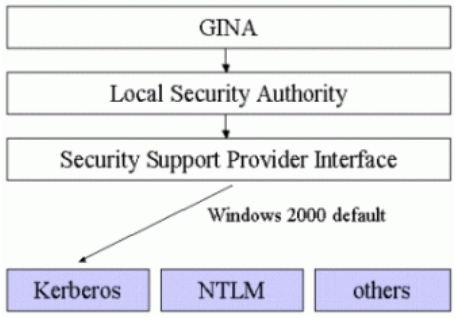


Figure 1: Smart Card Logon Architecture

The smart card logon process includes the following steps (see Figure 2):

1. After the user inserts a smart card, the Windows logon service (WINLOGON) dispatches this event to the GINA.
2. The user is prompted to enter a PIN (rather than a username and password).
3. The GINA sends the PIN to the Local Security Authority (LSA).
   Note: There is no logon domain information required, because the user is logged on with a User Principal Name (UPN).
4. The LSA uses the PIN to access the smart card and extract the certificate with the user's public key.
5. The Kerberos security service provider sends the signed user's certificate with the user's private key to the KDC.
6. The KDC compares the UPN in the certificate with the UPN on the user object in

the directory. The KDC also verifies the signature on the certificate to ensure that it was issued by a CA that's trusted in the Active Directory forest, such as an Enterprise CA.

7. The KDC encrypts the logon session key and the TGT for the ticket granting service with the public key from the client certificate. This step ensures that only the client with the appropriate private key can decrypt the logon session key.
8. The client decrypts the logon session key and presents the TGT to the ticket granting service. After this process is complete, all other communication in Kerberos uses symmetric encryption.

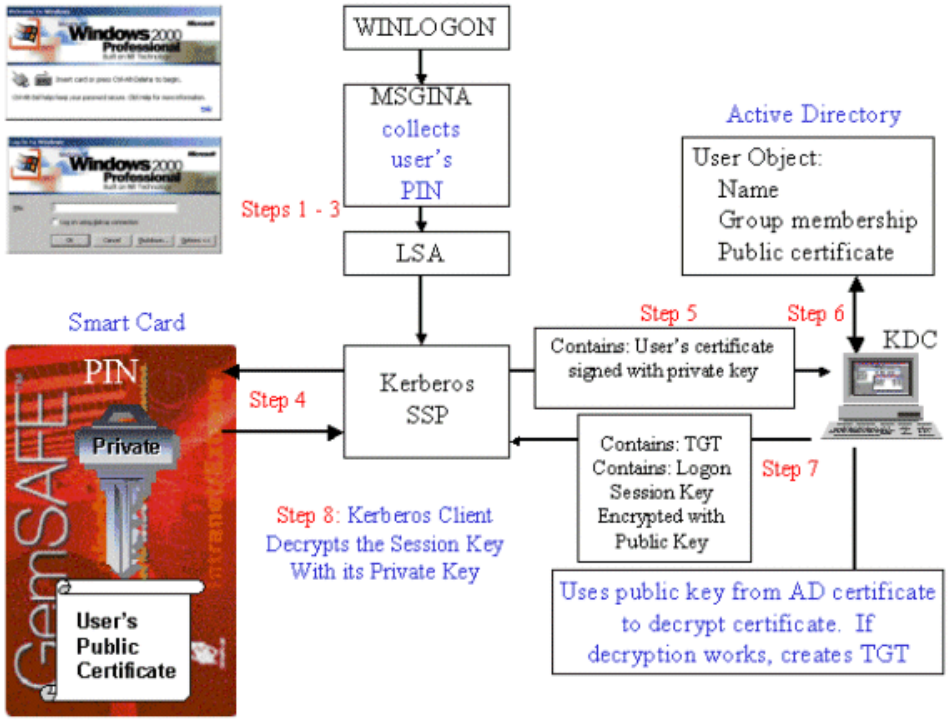


Figure 2: Smart Card Logon Process

BIJLAGE 2: Aandachtspunten Registry settings m.b.t. CRL

In http://support.microsoft.com/kb/887578 staan een aantal register settings beschreven die betrekking hebben op het gebruik van de CRL:

HKEY_Local_Machine\System\CurrentControlSet\Services\KDC\CRLValidityExtensionPeriod

This DWORD value lets you to extend the CRL validity period by a specified number of hours. When you set this value to a non-zero value, the certificate status checking code for smart card logons ignores any validity period errors as long as the CRL is not expired by more than the number of specified hours. This extension of the validity period only applies to CRLs that are used during the evaluation of certificates used for smart card logon. For example, this extension would apply to a certificate that is issued by a certification authority (CA) that is populated in the NTAuth store and to any certificates that are part of the trust chain used to verify the NTAuth store certificate.

HKEY_Local_Machine\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters\UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors

After you set this DWORD value to 1, the Kerberos clients (in this case it is Smartcard logon client) will ignore revocation unknown errors that are caused by expired CRL.

HKEY_Local_Machine\System\CurrentControlSet\Services\KDC\CRLTimeoutPeriod

This DWORD value lets you to specify the CRL time-out period to reduce false positives. The Key Distribution Center (KDC) passes this value to the certificate policy checking code. By default, the KDC specifies a time-out value of 90 seconds even if this registry value is not set.

HKEY_Local_Machine\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters\CRLTimeoutPeriod

This DWORD value lets you to specify the CRL time-out period to reduce false positives. The Kerberos client passes this value to the certificate policy checking code. By default, the Kerberos client specifies a time-out value of 90 seconds even if this registry value is not set.

Note The HKEY_Local_Machine\System\CurrentControlSet\Services\KDC\CRLValidityExtensionPeriod registry entry and the HKEY_Local_Machine\System\CurrentControlSet\Services\KDC\CRLTimeoutPeriod registry entry should be set on the logon domain controller.

The HKEY_Local_Machine\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters\CRLTimeoutPe
http://support.microsoft.com/kb/887578

BIJLAGE 3: Third party certificaten op Domain Controller(s)

Ten behoeve van de Windows smartcard logon functionaliteit dient elke Domain Controller in het netwerk voorzien te worden van een Domain Controller certificaat. Bij installatie van Microsoft Certificate Services gebeurt dit automatisch. Het is ook mogelijk om de Domain Controller certificaten aan te vragen bij een externe Certificate Service Provider. Deze bijlage beschrijft welke informatie hiervoor nodig is en hoe op de domain controller(s) certificaten geïnstalleerd moeten worden. Het aanvragen van Domain Controller certificaten bij een certificeringinstantie is niet opgenomen in dit document zelf. Zie ook [4] "Requirements for Domain Controller Certificates from a Third-Party CA, support Q291010".

Benodigde informatie t.b.v. aanmaken van de DC certificaten

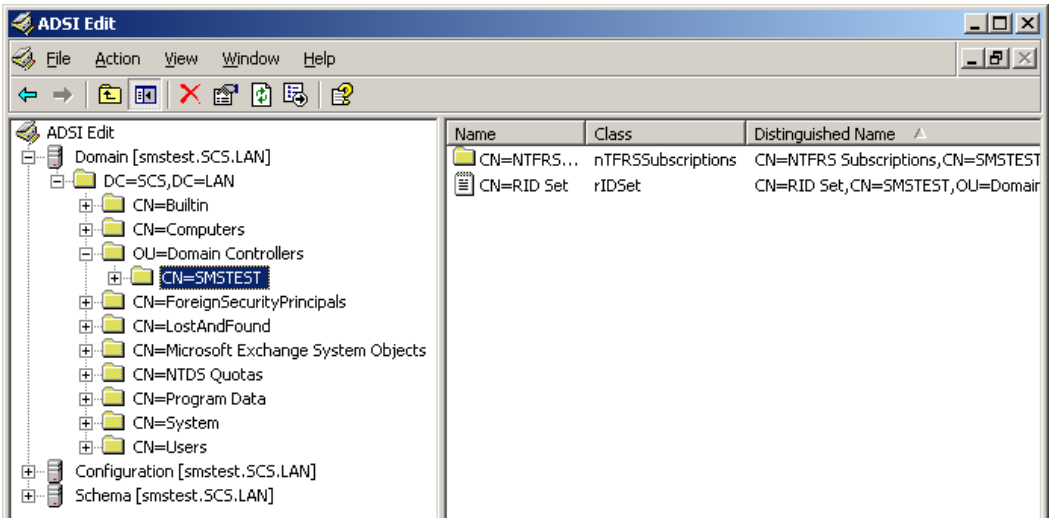
Elke Domain Controller wordt voorzien van een eigen certificaat. Per Domain Controller is onderstaande informatie nodig (deze informatie wordt in het certificaat opgenomen):

- FQDN (=Fully Qualified Domain Name)
- ObjectGUID

De objectGUID kan op de volgende wijze achterhaald worden:

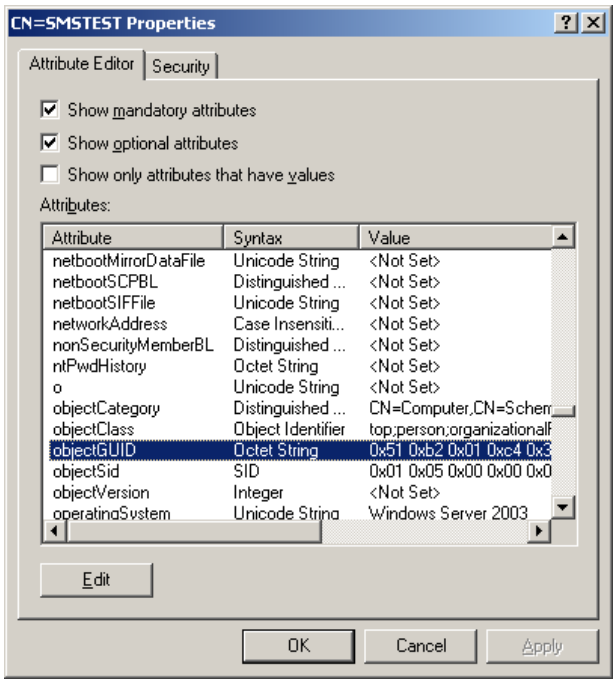
1. Open the ADSI Editing Tool. You can open the ADSI Edit tool by entering adsiedit.msc in the command line.

2. Under **Domain NC [...]**, click on **DC=<abc>..DC=<def> -> OU=Domain Controllers -> CN=<DomainControllerMachineName>**[2]

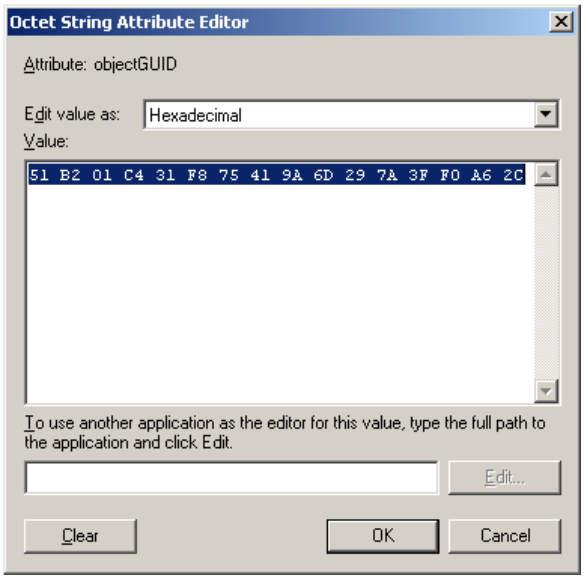


2 Hieronder kunnen andere subcontainers vallen. Negeer deze.

3. Right-click on this node in the left pane and select **Properties**. The Properties dialog box opens.



4. On the **Attribute Editor** tab, select the **Show optional attributes** checkbox and the **objectGUID** property in the **Attributes** list.



Aanvragen DC certificaat

Dit is verder niet uitgewerkt en hangt af van de Certificate Service Provider.

Installeren Domain Controller certificaat
Onderstaande actie dient uitgevoerd te worden op alle Domain Controllers, waarbij het desbetreffende Domain Controller certificaat wordt geïnstalleerd.

Importeer het ontvangen DC certificaat (.pfx) op Domain Controller middels MMC:

1. Start MMC (type **mmc** in de command prompt)
2. **Add Snap-in certificates**
3. Kies **Local Computer Store** en vervolgens **Add**
4. Rechter muisklik op **Personal** → kies **All tasks** → **Import** het .PFX bestand → voer **password** in en klik op **finish**.

LET OP:
Nadat bovenstaande actie is ingevoerd dient de **Domain Controller** te worden **herstart**.

Installatie CA certificaten
De hiërarchie waaronder de Domain Controller certificaten uitgegeven worden dient ook geïnstalleerd te worden (naast de hiërarchie waaronder de smartcard logon certificaten uitgegeven zijn). Gebruik hiervoor

```
certutil -dsPublish -f  [filename]  rootca
certutil -dsPublish -f  [filename]  ntauthca
```

Zie ook paragraaf 2.2.1.

Check Domain Controller certificaat
Controleer of de Domain Controller een certificaat heeft en of alle CA's geïnstalleerd zijn middels het commando:

```
certutil -dcinfo
```

Zie ook paragraaf 2.2.1.

BIJLAGE 4: SHA-2 i.c.m. Windows 2003

Met een standaard SP1 of SP2 installatie van Windows 2003 server is het niet mogelijk om gebruik te maken van SHA-2 certificaten. Dit is een bekend issue bij Microsoft.

Voor de Clientproducten Vista en XP SP3 zijn er geen problemen. Windows XP ondersteund vanaf SP3 SHA-2 certificaten en Windows Vista ondersteund vanaf basis SHA-2.

Microsoft heeft dit probleem onderkend en beschreven in onderstaande KB.

http://support.microsoft.com/kb/938397

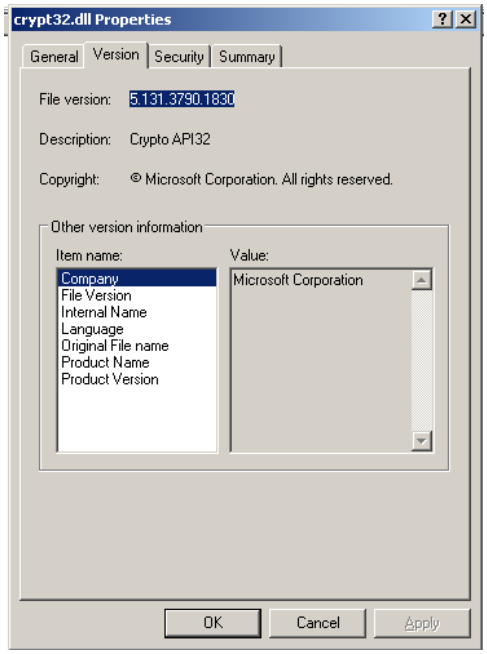
De huidige installatie (Windows 2003 R2 SP1) bevat een verouderde versie van de CryptoAPI 32 dll.

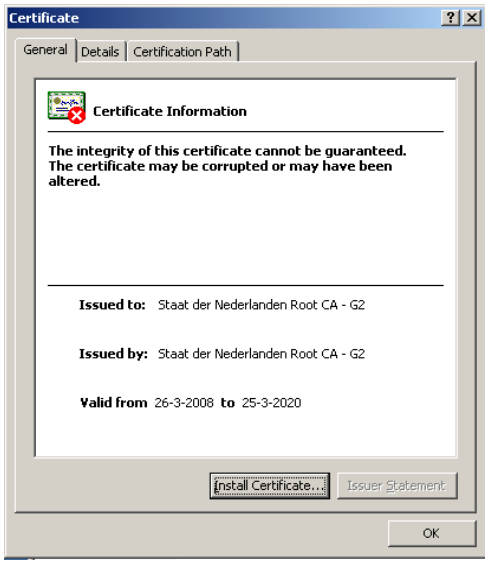
Binnen kb938397 is een hotfix beschikbaar gesteld. Hiervoor is SP1 of SP2 minimaal noodzakelijk.

Een upgrade naar SP2 is vanaf SP1 dus voor installatie van de in KB938397 genoemde hotfix niet noodzakelijk.

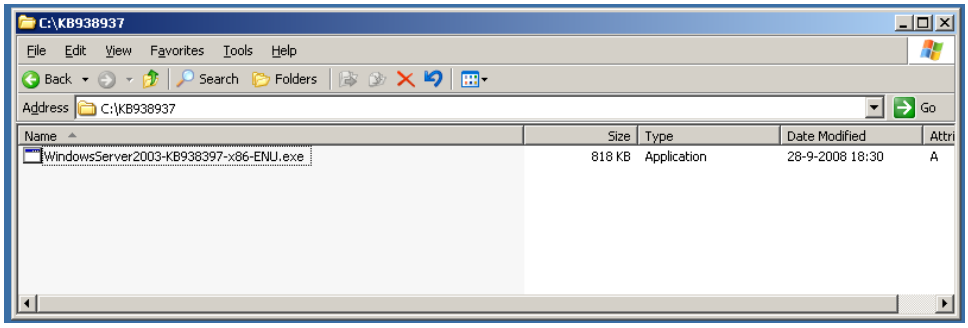
Vaststellen versienummer Crypt32.dll

Versie 5.131.3790.1830 herkend geen SHA-2

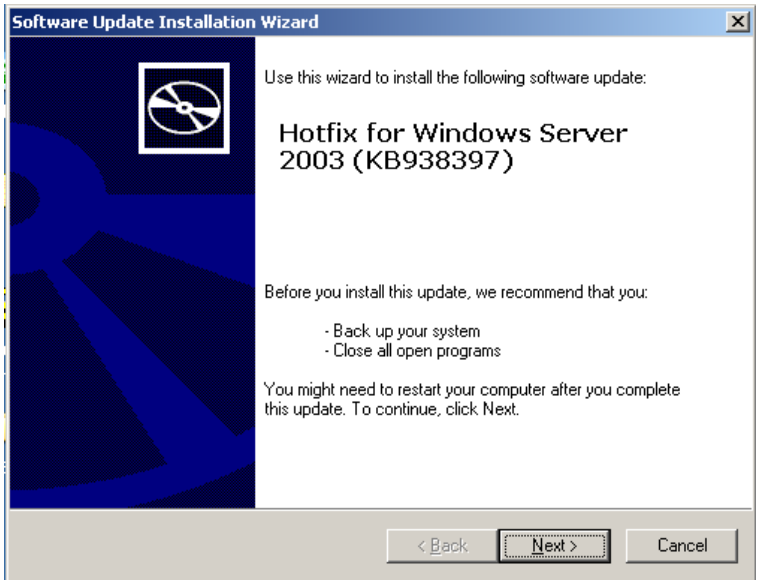




Starten van de Windows Server2003-KB938397-x86-ENU.exe

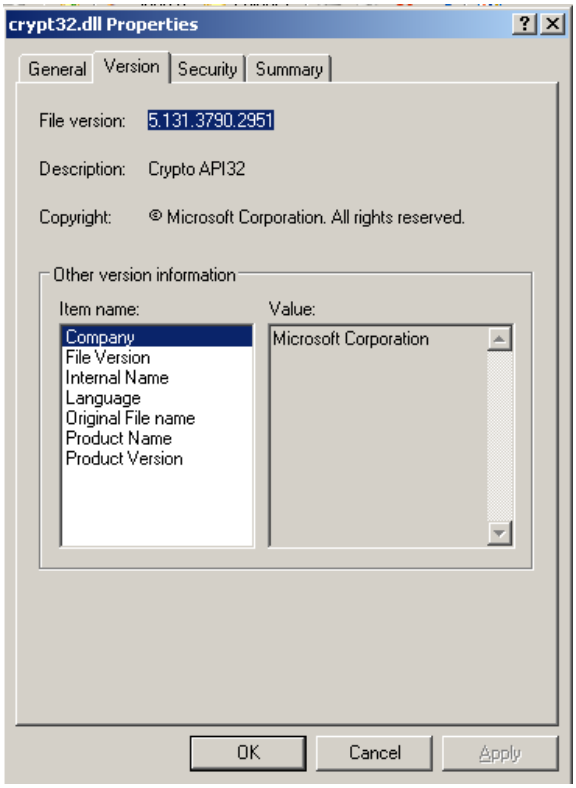


Default keuzes volgen via de Software update Installation Wizard.



Vaststellen versienummer Crypt32.dll

Versie 5.131.3790.2951 herkend SHA-2



Het signature Algoritme wordt herkend binnen het OS.