



Unlimited access
to your world



SafeSign Identity Client

UZI snelstart gids.



Table of Contents

Document Information	3
About SafeSign Identity Client	4
About this document	5
About A.E.T. Europe B.V.....	6
1 Desktop settings	7
2 Server settings	9
3 USB Reader test	11
4 Connectie Internet Explorer.....	12
5 Internet Explorer op SBV-Z	17
6 Connectie Firefox.....	21
7 Firefox op SBV-Z.....	25



Title: SafeSign Identity Client UZI snelstart gids
Document ID: SafeSign-IC_UZI snelstart gids_rev1.docx
Project: SafeSign IC User Documentation

Document revision history

Version	Date	Author	Changes
1.0	1 Sept 2014	Ing. F.J. Hegge	Edited for SafeSign Identity Client UZI snelstart gids

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

SafeSign Identity Client (IC) is a software package that can be used to enhance the security of applications that support hardware tokens through PKCS #11 and Microsoft CryptoAPI.

The SafeSign IC package provides a standards-based PKCS #11 Library as well as a Cryptographic Service Provider (CSP) and CNG Key Storage Provider (KSP) allowing users to store public and private data on a personal token, either a smart card, USB token or SIM card. It also includes the SafeSign IC PKI applet, enabling end-users to utilise any Java Card 2.1.1 / Java Card 2.2 and higher compliant card with the SafeSign IC middleware.

Combining full compliance with leading industry standards and protocols, with flexibility and usability, SafeSign IC can be used with multiple smart cards / USB tokens, multiple Operating Systems and multiple smart card readers.

SafeSign IC allows users to initialise and use the token for encryption, authentication or digital signatures and includes all functionality necessary to use hardware tokens in a variety of PKI environments.

SafeSign IC comes in a standard version with an installer for Windows, MAC and Linux environments. It is also available for many other environments like mobile devices.



Figure 1: SafeSign Identity Client Smart card bundle

For more information, refer to the latest SafeSign IC Product Description on www.aeteurope.com.



Om een snelle implementatie van de UZI passen met SafeSign 3.0.80 en hoger te bevorderen is deze gids ontwikkeld die de belangrijkste stappen omvat om een installatie te testen.

Kort gesproken is SafeSign de schakel tussen de beveiliging van de certificaten op de UZI pas en de software op een computer. Het ontsluiten van de beveiliging komt tot uiting in het vragen van een PIN code. Hierbij zijn er diverse afhankelijkheden van het operating systeem van de desktop of de server. In dit document gaan we beknopt in op deze afhankelijkheden. Deze gids heeft niet het doel om volledig te zijn.

Het uitgangspunt is een configuratie waarbij de SafeSign software op een server wordt geïnstalleerd en er via een Windows 7 desktop (zonder SafeSign) met een Omnikey smartcard USB reader door middel van een Remote Desktop Connectie een verbinding gemaakt wordt. Het Microsoft remote desktop protocol zorgt ervoor dat de smartcard USB reader van de desktop doorgestuurd wordt naar de server. Werkt dit doorsturen niet correct dan zal het Token Beheer programma op de server geen smartcard reader tonen.



Note

This document is not intended to give a full or accurate overview of public key cryptography and how the process of encrypting / decrypting and verification of signed messages works, but tries to give the reader some background as to the why and how of public key cryptography and the use of tokens.



SafeSign
Identity Client

About A.E.T. Europe B.V.

No matter who you are or what you do; there is always a specific world you want, or need to access. AET makes this possible by creating the perfect technological solution in user identification, authentication and authorization: unlimited access, twenty-four/seven.

We do not only believe your world should be accessible anytime. We are also determined to make this access easy and secure. At a time when almost everything is digital, security has become our main focus. By creating unlimited, secure and convenient access to your world, we ensure that you have the power to control your own world. You, and nobody else.

In devising the best technological solutions, we need to be fast, smart and inventive. So that's exactly what we are. We are also passionate: about technology; about our business; about the possibility of providing convenient access to different worlds.

In our vision, everyone can benefit from the technology we offer. Because everyone deserves reliable, safe and unlimited access to the world he or she wants to enter. Which world do you want to access?

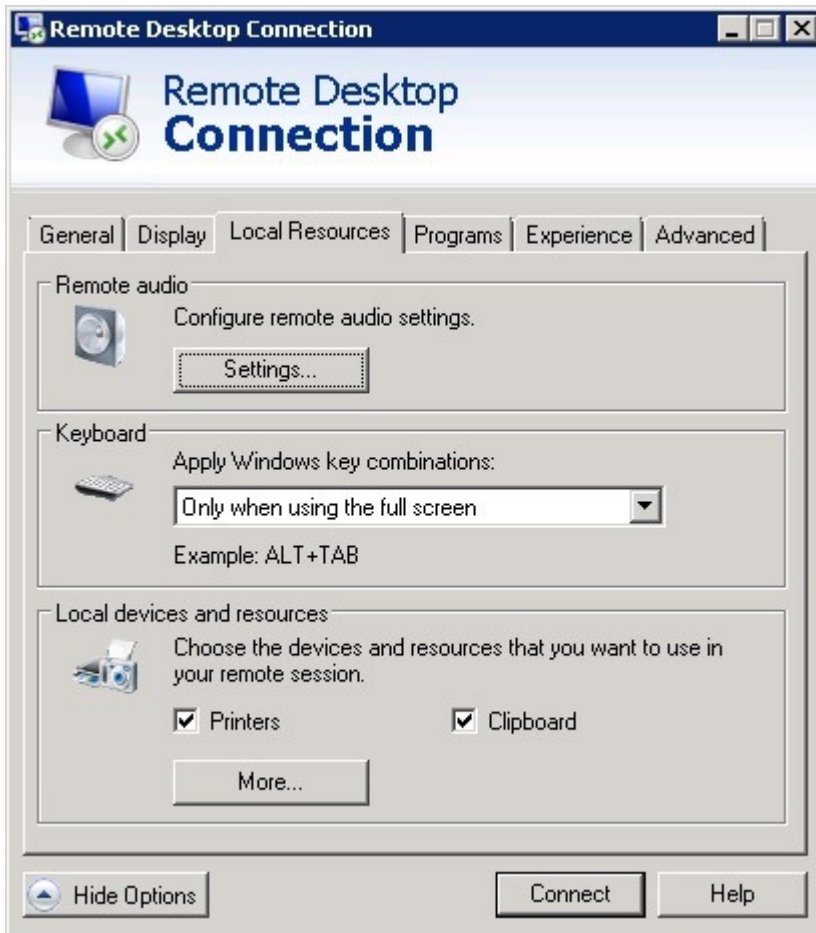


Unlimited access
to your world



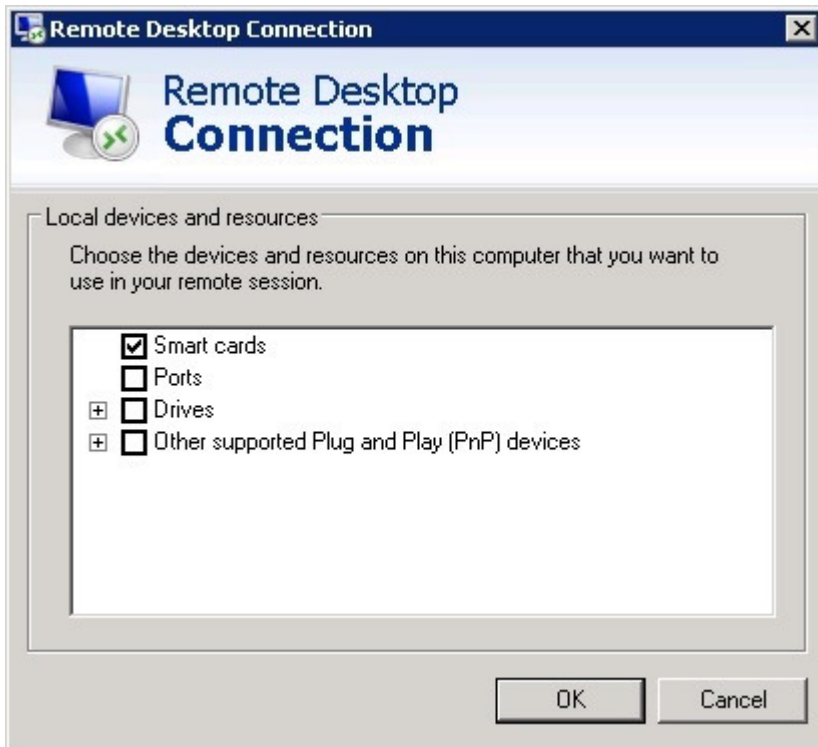
1 Desktop settings

Naast de juiste server settings is van belang dat de “smartcard” option aan staat. Deze vindt u onder de “More” knop in “Local devices and resources”.





Vink hier de optie "Smart cards" aan. Zie onderstaand plaatje.



Op de server kan de SafeSign software met de standard opties geïnstalleerd worden.

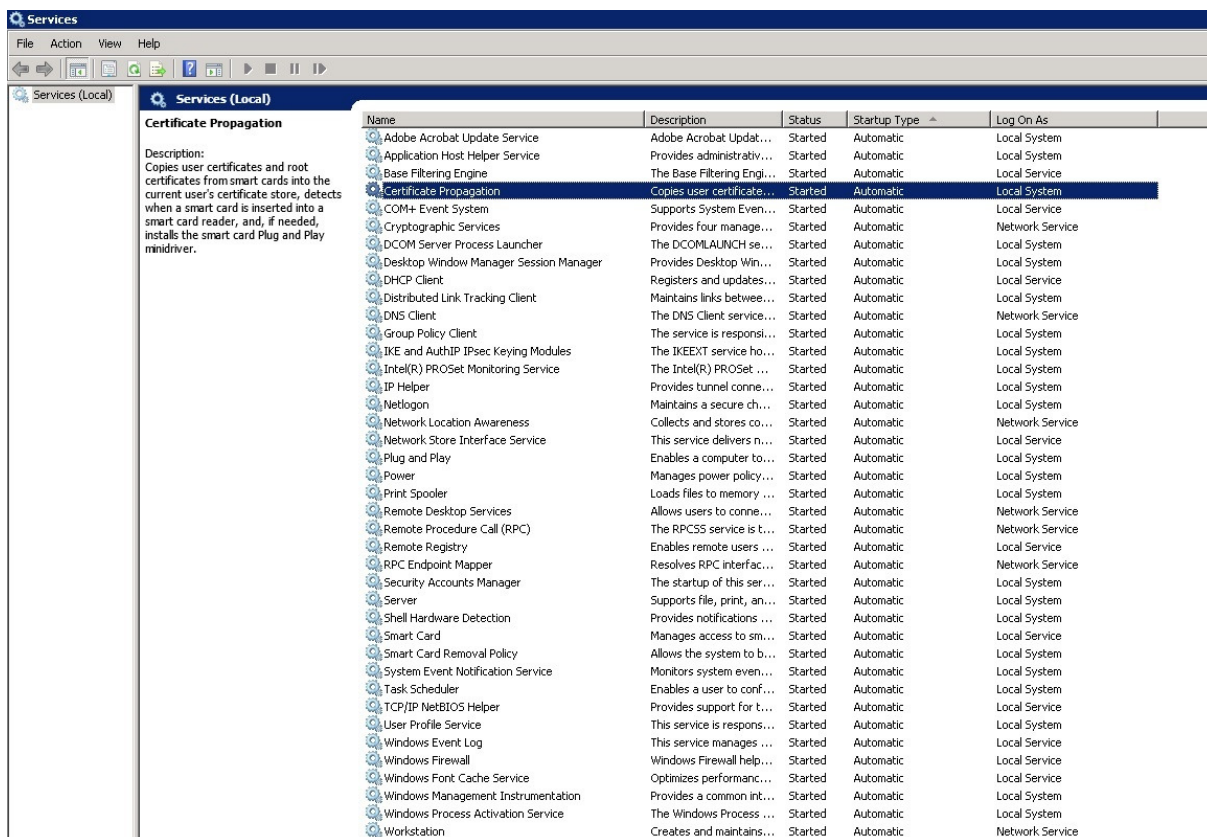
Het is makkelijker om de optie “install Firefox” uit te zetten en deze optioneel later via het menu van het Token Beheer programma uit te voeren. Hier komen we later nog op terug.

Het is zeer belangrijk voor de (indirecte) werking van SafeSign dat de volgende Microsoft services gestart zijn:

- “Certificate Propagation” (zorgt voor het doorzetten van certificaten naar de Microsoft Certificate Store)
- “Smart Card” (SafeSign werkt met smartcards)
- “Remote Procedure Call (RPC)” (heeft een afhankelijkheid in “Certificate Propagation”)

Optioneel is de service “Smart Card Removal Policy” indien u een desktop wilt “locken” na het verwijderen van een smartcard uit de reader.

Zie hiervoor de Services Management Console (“services.msc”) op de server.



In bovenstaand plaatje heeft de service “Certificate Propagation” de status “Started”.

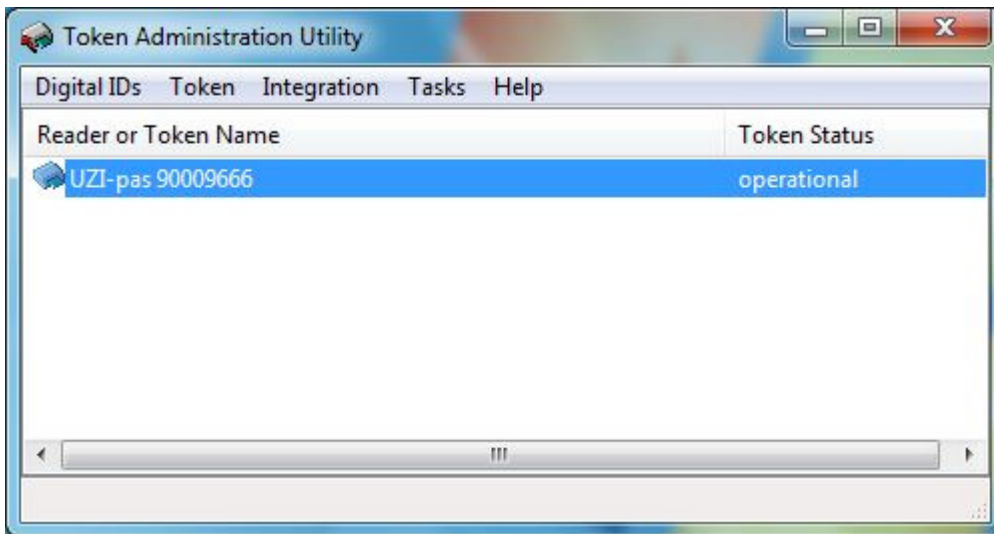


Indien er andere smartcard software op de PC draait kan deze service verstoord worden en zal SafeSign niet correct werken. Ook oudere SafeSign Software (pre versie 3.0.45) kan dit process verstoren.

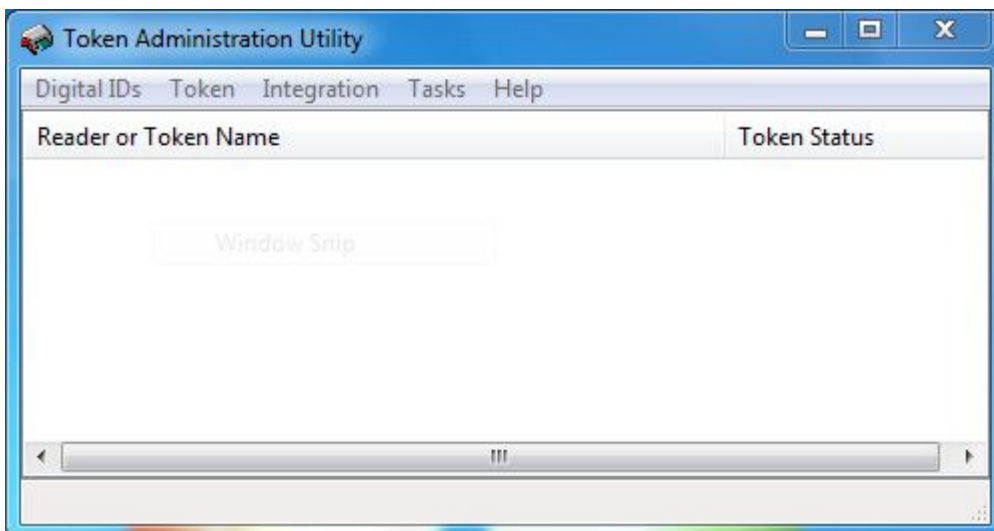
Het is dan ook van belang dat de SafeSign test op een schone machine uitgevoerd wordt.

Als eerste test is het van belang dat de SafeSign software de kaart goed kan benaderen. Hiervoor moet de UZI pas in de USB reader op de client gestoken worden en de SafeSign Token Administration Utility (Token Beheer programma) op de server opgestart worden.

Een correcte herkenning van de UZI pas ziet er als volgt uit:



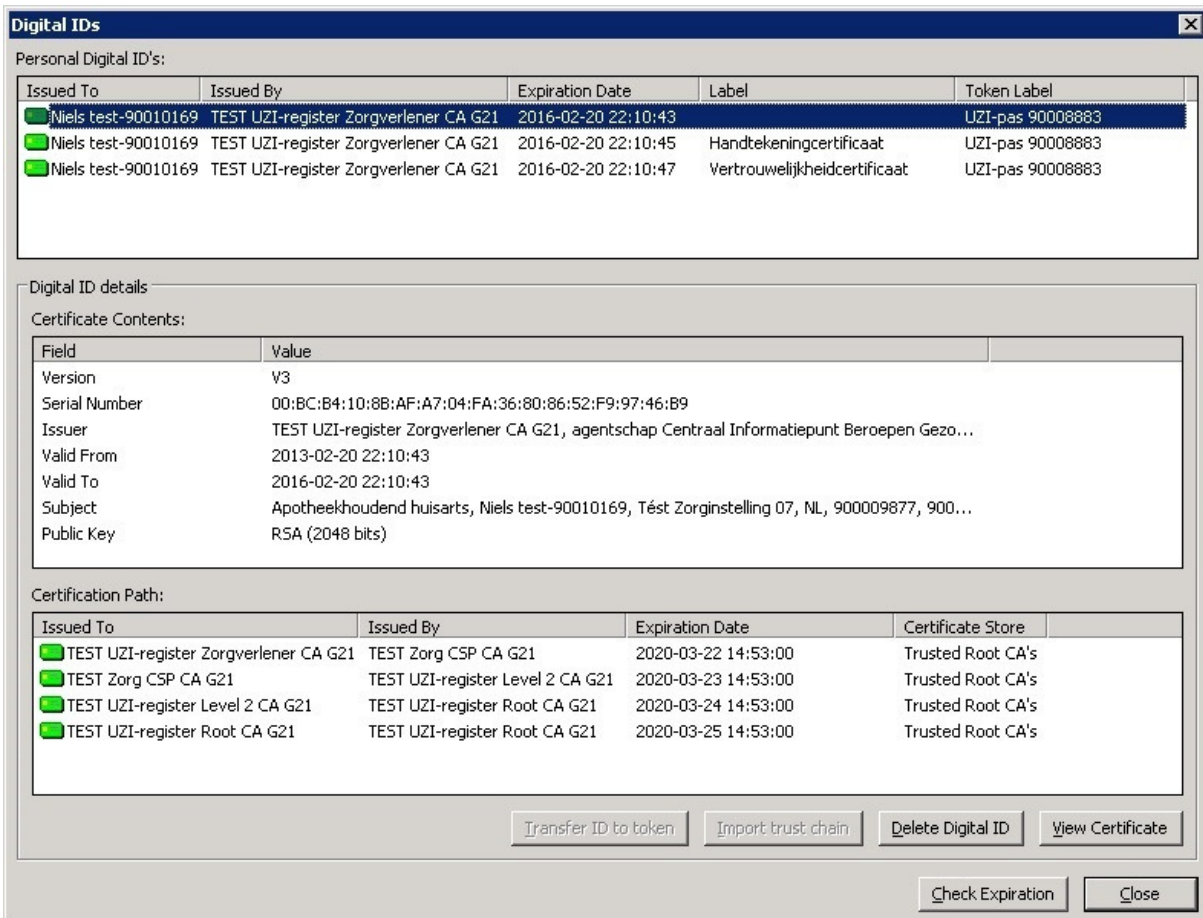
Ziet u onderstaand plaatje dan wordt de reader niet goed herkend en kan er geen PIN code gevraagd worden



Als volgende stap maakt u een connectie via Remote Desktop Connectie naar uw SafeSign test server.

Daarna start u het SafeSign Token Beheer Programma op via het start menu en bekijkt u de Digitale ID's ten behoeve van een Internet Explorer test.

Ziet u onderstaand plaatje dan zal de UZI pas waarschijnlijk correct werken.



Digital IDs

Personal Digital ID's:

Issued To	Issued By	Expiration Date	Label	Token Label
Niels test-90010169	TEST UZI-register Zorgverlener CA G21	2016-02-20 22:10:43		UZI-pas 90008883
Niels test-90010169	TEST UZI-register Zorgverlener CA G21	2016-02-20 22:10:45	Handtekeningcertificaat	UZI-pas 90008883
Niels test-90010169	TEST UZI-register Zorgverlener CA G21	2016-02-20 22:10:47	Vertrouwelijkheids-certificaat	UZI-pas 90008883

Digital ID details

Certificate Contents:

Field	Value
Version	V3
Serial Number	00:BC:B4:10:8B:AF:A7:04:FA:36:80:86:52:F9:97:46:B9
Issuer	TEST UZI-register Zorgverlener CA G21, agentschap Centraal Informatiepunt Beroepen Gezo...
Valid From	2013-02-20 22:10:43
Valid To	2016-02-20 22:10:43
Subject	Apotheekhoudend huisarts, Niels test-90010169, Test Zorginstelling 07, NL, 900009877, 900...
Public Key	RSA (2048 bits)

Certification Path:

Issued To	Issued By	Expiration Date	Certificate Store
TEST UZI-register Zorgverlener CA G21	TEST Zorg CSP CA G21	2020-03-22 14:53:00	Trusted Root CA's
TEST Zorg CSP CA G21	TEST UZI-register Level 2 CA G21	2020-03-23 14:53:00	Trusted Root CA's
TEST UZI-register Level 2 CA G21	TEST UZI-register Root CA G21	2020-03-24 14:53:00	Trusted Root CA's
TEST UZI-register Root CA G21	TEST UZI-register Root CA G21	2020-03-25 14:53:00	Trusted Root CA's

Transfer ID to token Import trust chain Delete Digital ID View Certificate

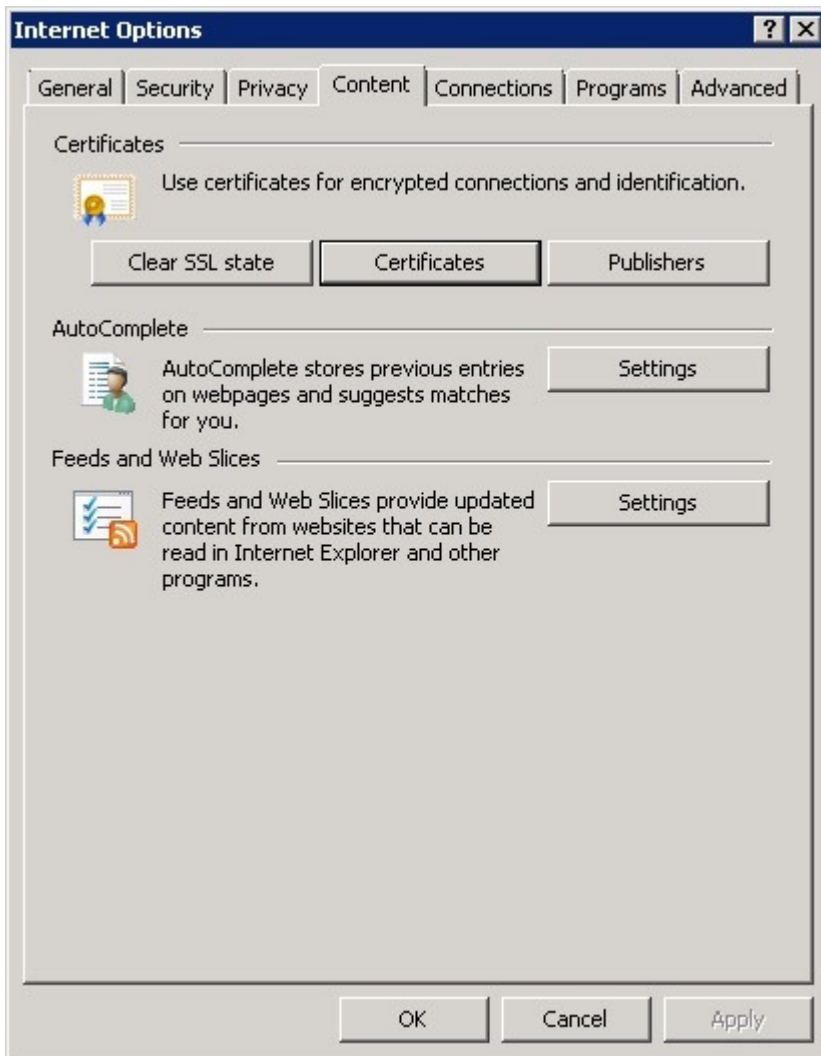
Check Expiration Close

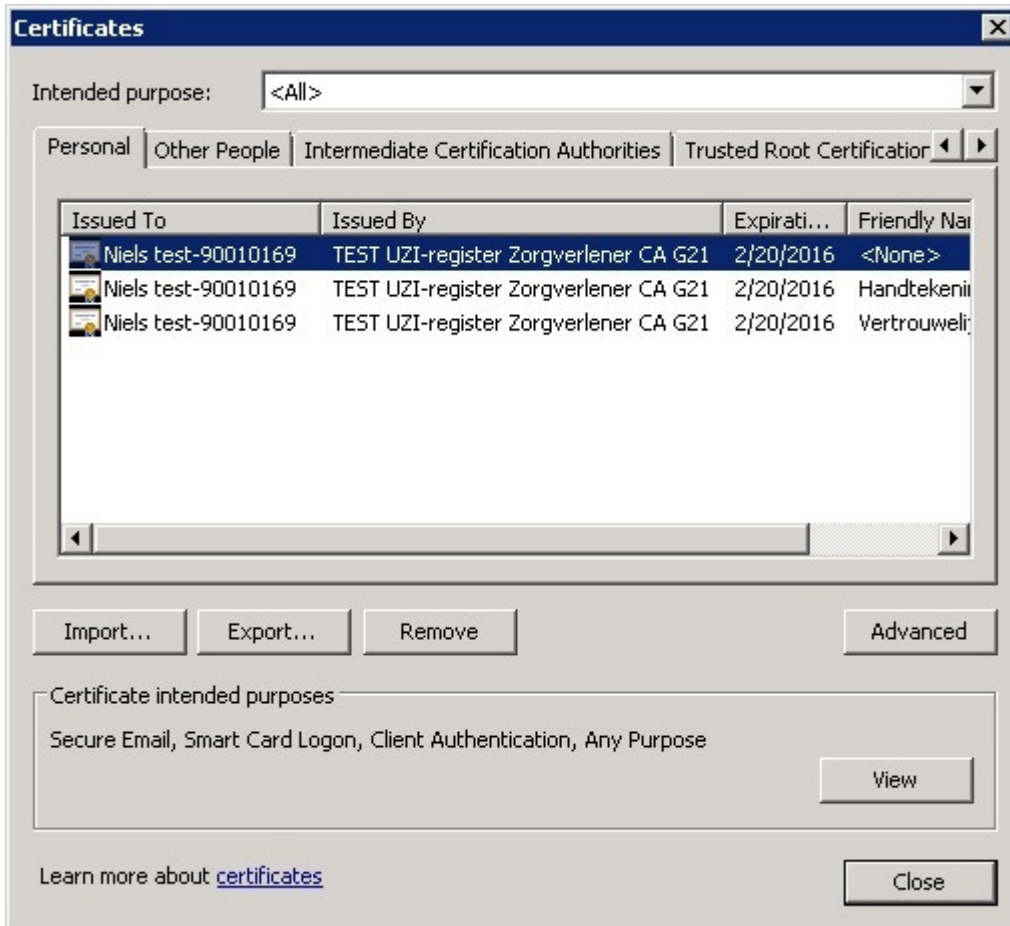
Hierbij is het van de belang dat de iconen aan de linker kant groen zijn.



Mogelijk ziet u andere Digitale ID's. Deze staan in de zogenaamde Microsoft Certificate store.

Via de "Internet Options" van Internet Explorer kun u deze beheren.
Zie hiervoor de tab "Content" en de knop "Certificates"





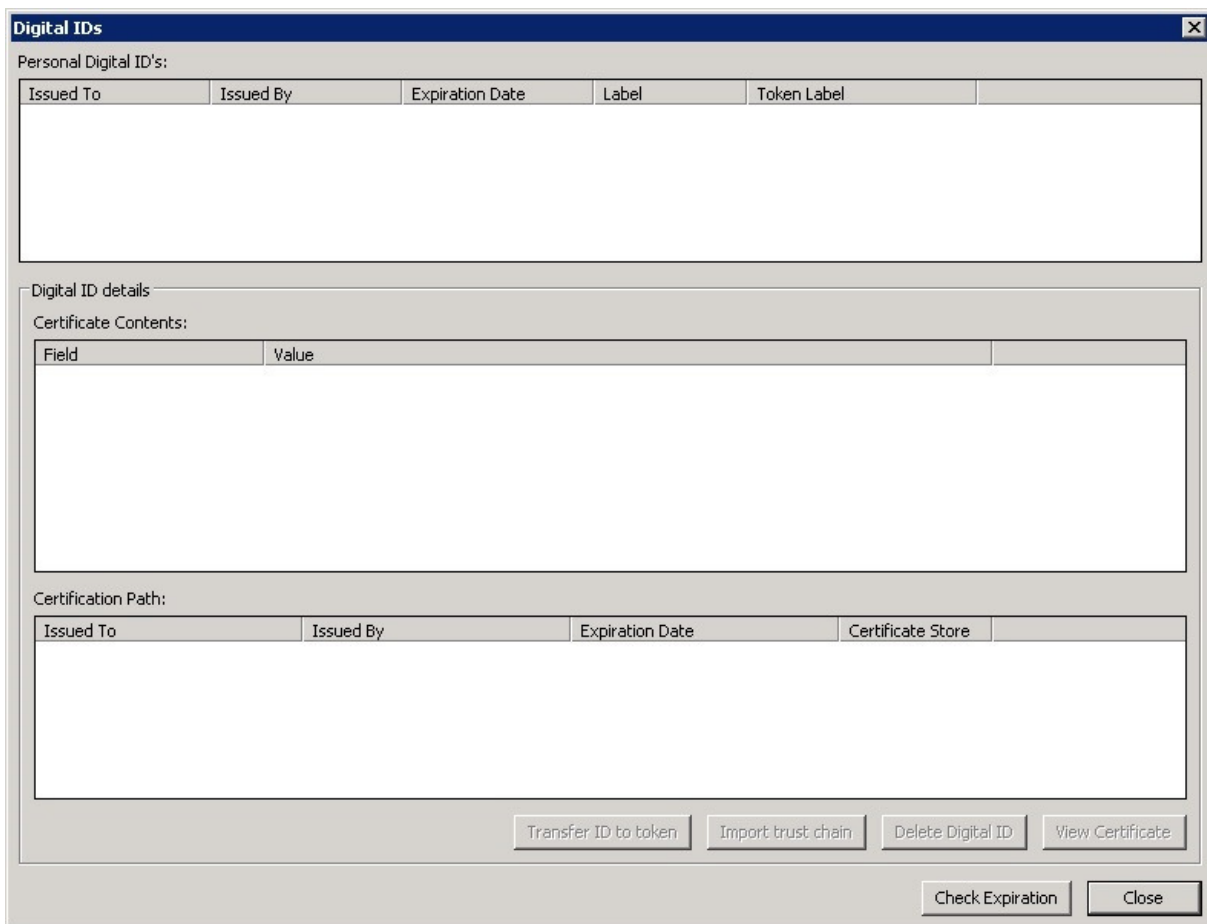
Via de knop "Remove" kunt u de certificaten verwijderen.

Op het moment dat u een smartcard in de USB reader steekt, zal Microsoft de certificaten via de Certificate Propagation Service in de Microsoft Certificate Store zetten.

Via het wisselen van de Tabs "Personal" en "Other people" bijvoorbeeld wordt het scherm ververst. Gebeurt dit niet (hier kunnen diverse externe oorzaken aan ten grondslag liggen) dan zal hier nader onderzoek door Microsoft Support of een consultant verricht moeten worden.



Ziet u onderstaand plaatjes na het verwijderen van alle certificaten en het insteken van een UZI pas dan zal SafeSign geen PIN code via Internet Explorer laten zien.





Certificates [X]

Intended purpose: <All>

Personal | Other People | Intermediate Certification Authorities | Trusted Root Certification

Issued To	Issued By	Expirati...	Friendly Na
-----------	-----------	-------------	-------------

Import... Export... Remove Advanced

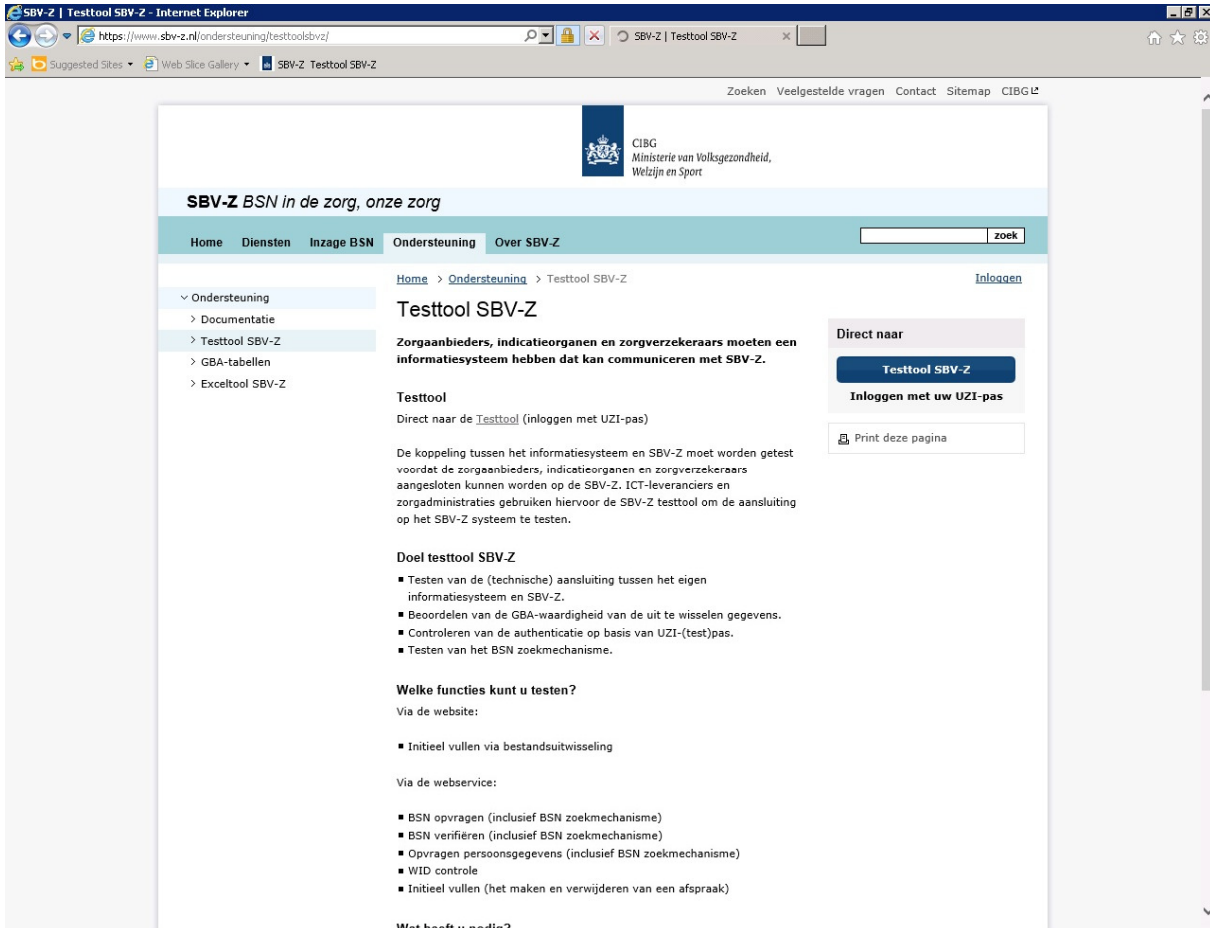
Certificate intended purposes

View

Learn more about [certificates](#) Close

Om de UZI-pas te testen met Internet Explorer gebruiken we de volgende test:

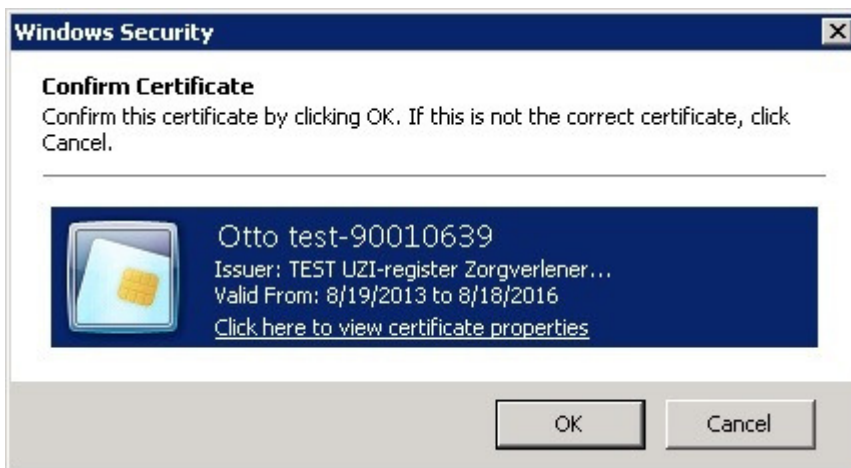
Ga naar URL : <https://www.sbv-z.nl/ondersteuning/testtoolsbvz/default.aspx> (terwijl u een verbinding heeft via RDP) op uw server.



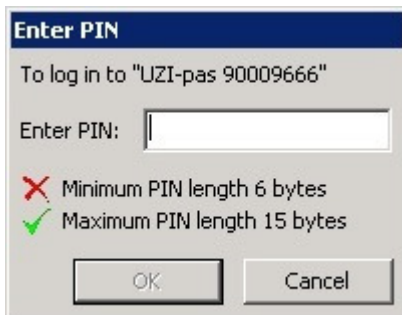
Klik op de knop "TestTool SBV-Z".



Als het certificaat van de UZI pas correct in de Microsoft Store staat, dan komt er een venster met een soortgelijke inhoud als hieronder. Er kunnen meerdere certificaten getoond worden. Kies de juiste en klik op OK



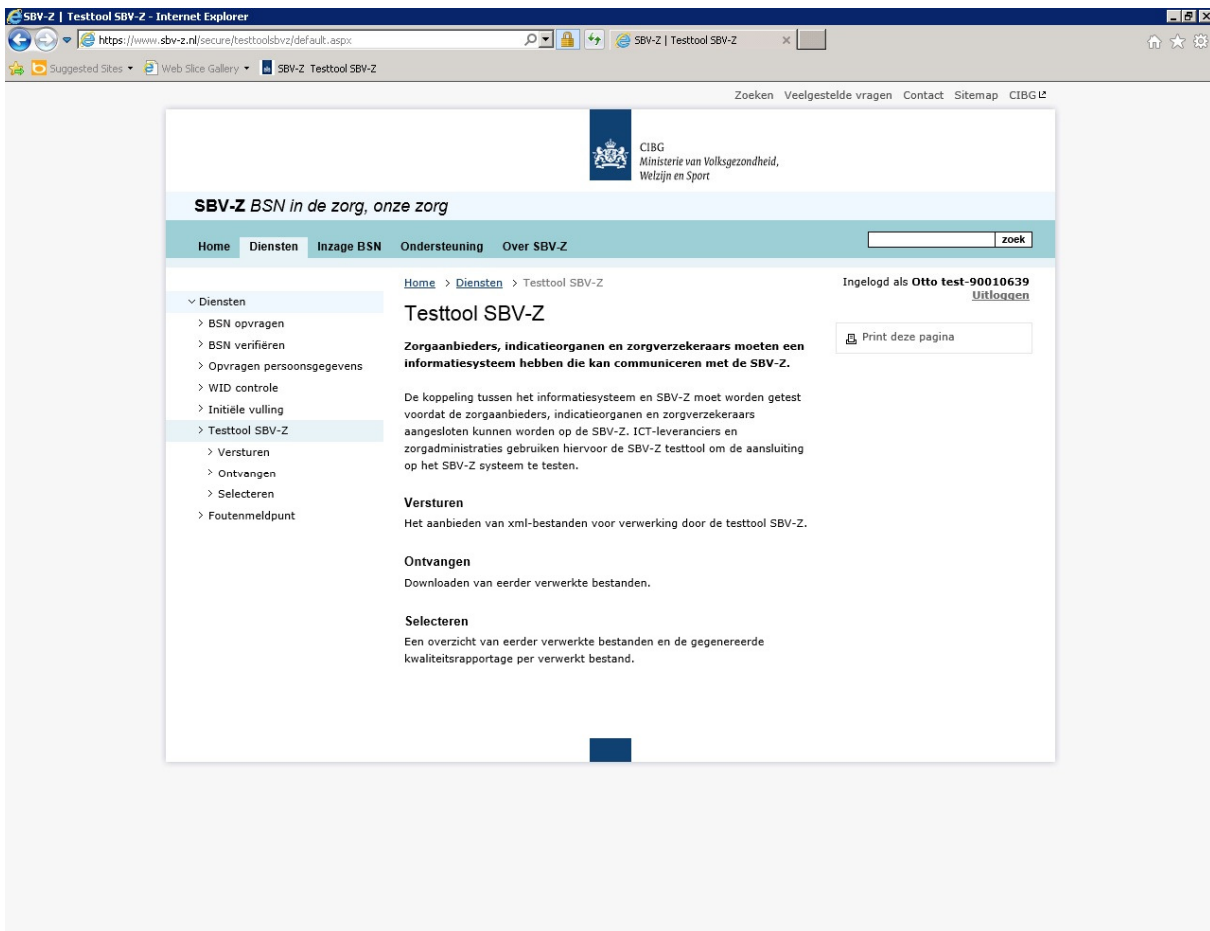
SafeSign zal nu het certificaat op de smartcard gaan “openen” en om een PIN code vragen.



Vul de PIN code van de UZI-pas in en druk op OK.

U bent nu ingelogd op de test website.

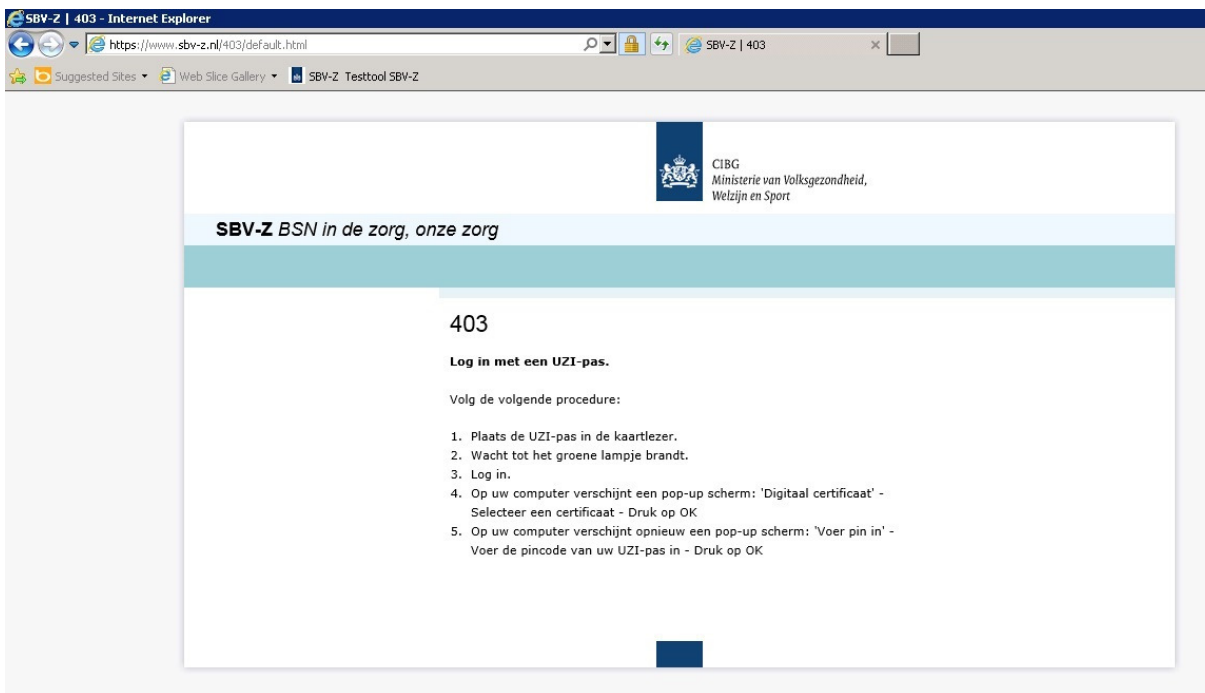
Dit kunt u zien aan de tekst aan de rechter bovenkant van de pagina: "Ingelogd als". De pas werkt nu correct.



The screenshot shows the Internet Explorer browser window displaying the SBV-Z Testtool SBV-Z website. The address bar shows the URL: <https://www.sbv-z.nl/secure/testtoolsbvz/default.aspx>. The page header includes the CIBG logo and the text "CIBG Ministerie van Volksgezondheid, Welzijn en Sport". The main navigation menu includes "Home", "Diensten", "Inzage BSN", "Ondersteuning", and "Over SBV-Z". The "Diensten" menu is expanded, showing options like "BSN opvragen", "BSN verifiëren", "Opvragen persoonsgegevens", "WID controle", "Initiële vulling", "Testtool SBV-Z", "Versturen", "Ontvangen", "Selecteren", and "Foutmeldpunt". The "Testtool SBV-Z" section is selected, displaying the title "Testtool SBV-Z" and the text: "Zorgaanbieders, indicatieorganen en zorgverzekeraars moeten een informatiesysteem hebben die kan communiceren met de SBV-Z." Below this, there is a paragraph explaining the connection between the information system and SBV-Z. The user is logged in as "Otto test-90010639" and there is a "Uitloggen" link. A "Print deze pagina" button is also visible.

Afhankelijk van de rechten van de pas op de website kunt u ook andere meldingen krijgen.

Klikt u op een andere link als "Versturen" of "Ontvangen" in de testtool, dan krijgt u mogelijk onderstaand scherm met een 403 error. Deze meldingen worden niet door SafeSign gegenereerd maar door de website.



Binnen Internet Explorer 10 en 11 kunt u via de Developer Tools optie (F12) ervoor kiezen om uw IE versie aan te passen. Zie hiervoor de Emulation mode (Ctrl-8). Afhankelijk van uw omgeving geeft dit mogelijk een verbetering met betrekking tot inlog problemen.



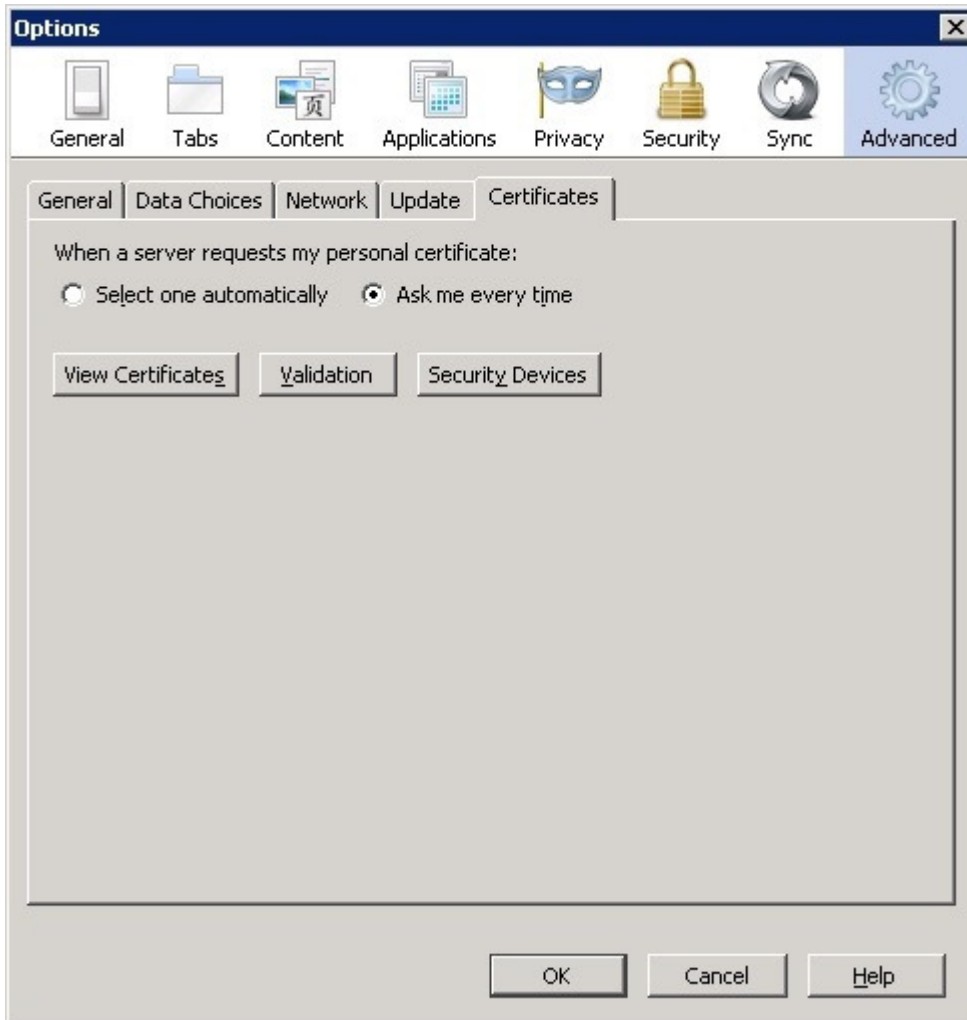
Voor Firefox is het belangrijk dat de PKCS#11 bibliotheek geladen is.

Voer de Firefox installatie uit via het Integratie Menu van het Token Beheer programma.



De Firefox versie kan verschillen met de hierboven getoonde versie. Selecteer uw versie en druk op de knop "Install" en op "Close".

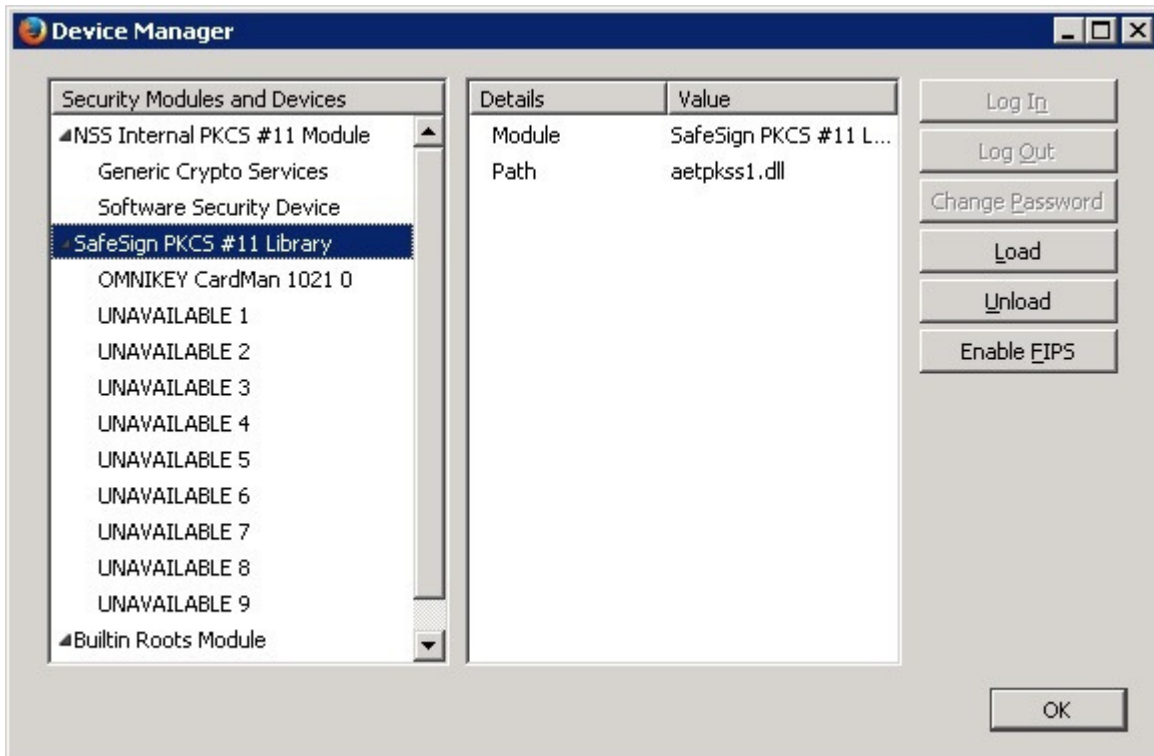
Om te controleren of de Firefox installatie correct is, gaat men naar de Advanced Options van Firefox en bekijk hierbij de "Security Modules" via de knop "Security Devices" in de tab "Certificates". Zie het voorbeeld hieronder.



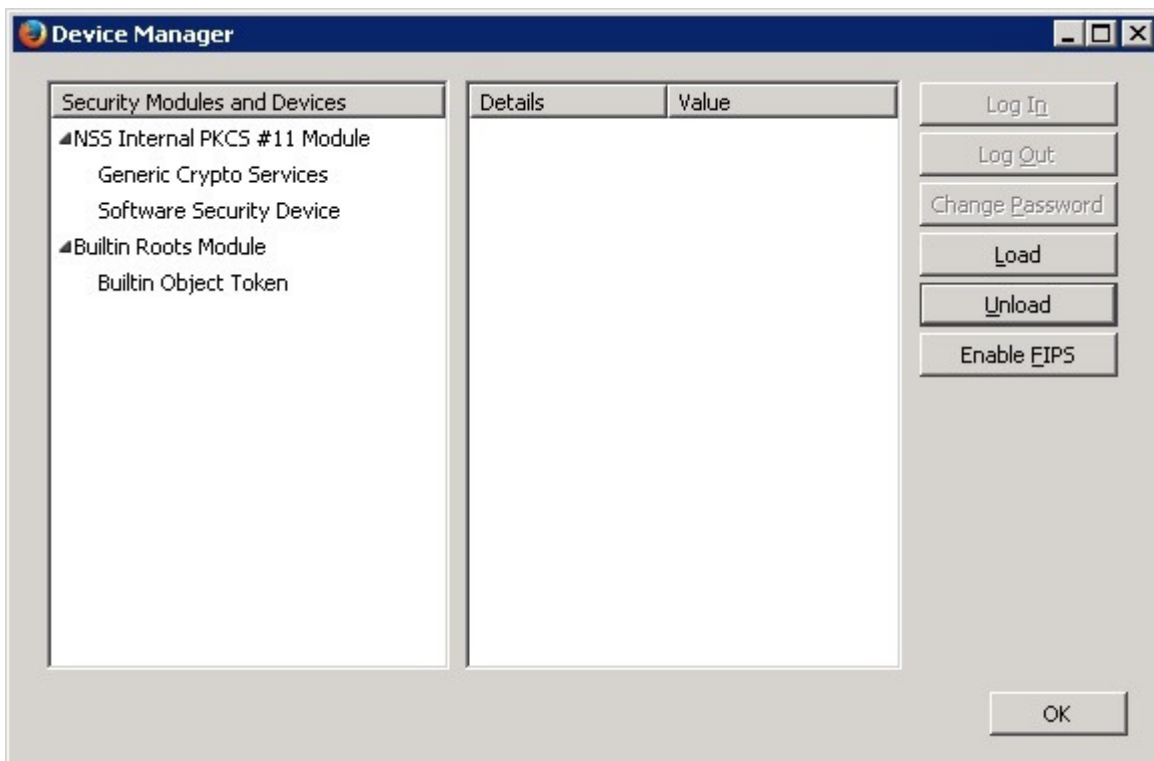
Ziet men onderstaand plaatje (met mogelijk een andere Omnikey of andere (USB) reader) dan is Firefox goed geconfigureerd voor SafeSign en zal de UZI pas waarschijnlijk werken.



Onderstaand scherm toont een correct geladen SafeSign module.



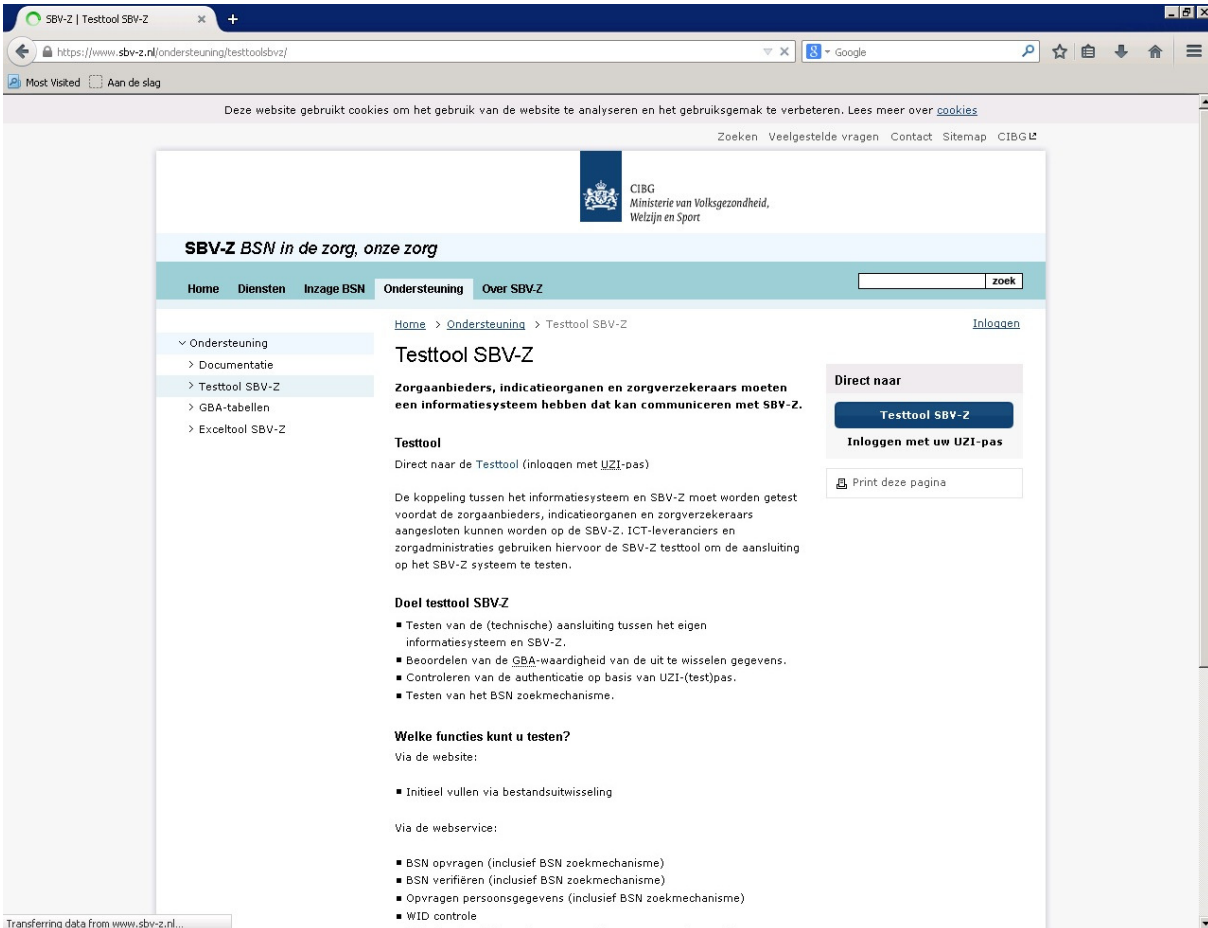
Ziet men onderstaand plaatje na een herstart van Firefox dan is de SafeSign module niet goed geladen en zal SafeSign geen PIN scherm tonen via Firefox.



U kunt dan eventueel handmatig de PKCS#11 bibliotheek toevoegen via de "Load" knop. Zie hiervoor de handleiding voor de desbetreffende SafeSign versie.

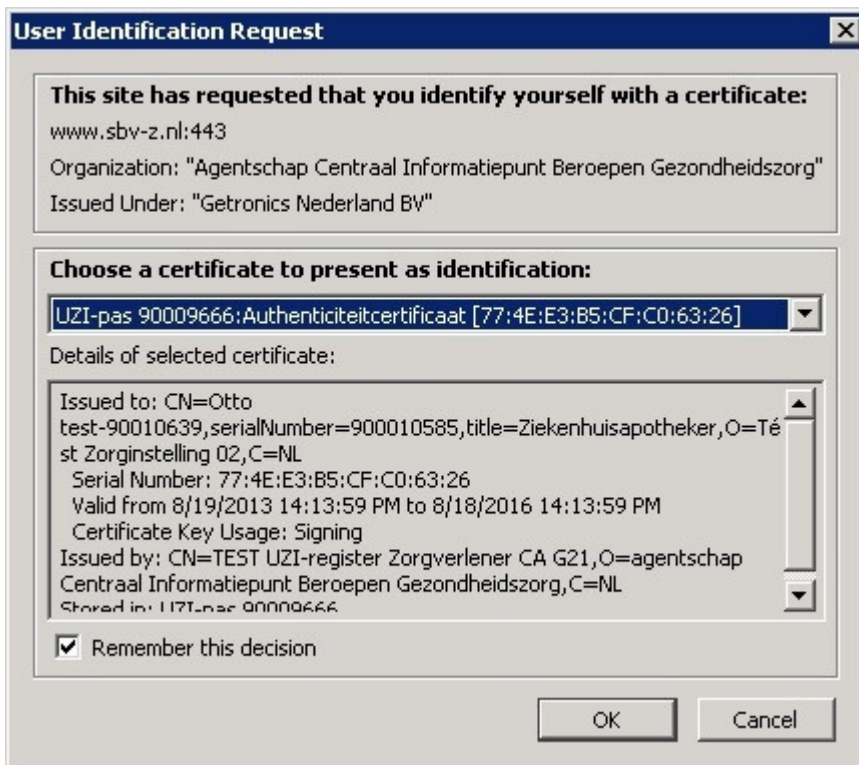
Om de UZI-pas te testen met Firefox gebruiken we de volgende test:

Ga naar URL : <https://www.sbv-z.nl/ondersteuning/testtoolsbvz/> (terwijl u een verbinding heeft via RDP) op uw server.



Klik op de knop "TestTool SBV-Z".

Vervolgens zal SafeSign via de geladen module, de UZI-pas benaderen en het certificaat tonen.



Kies het juiste certificaat en klik op OK

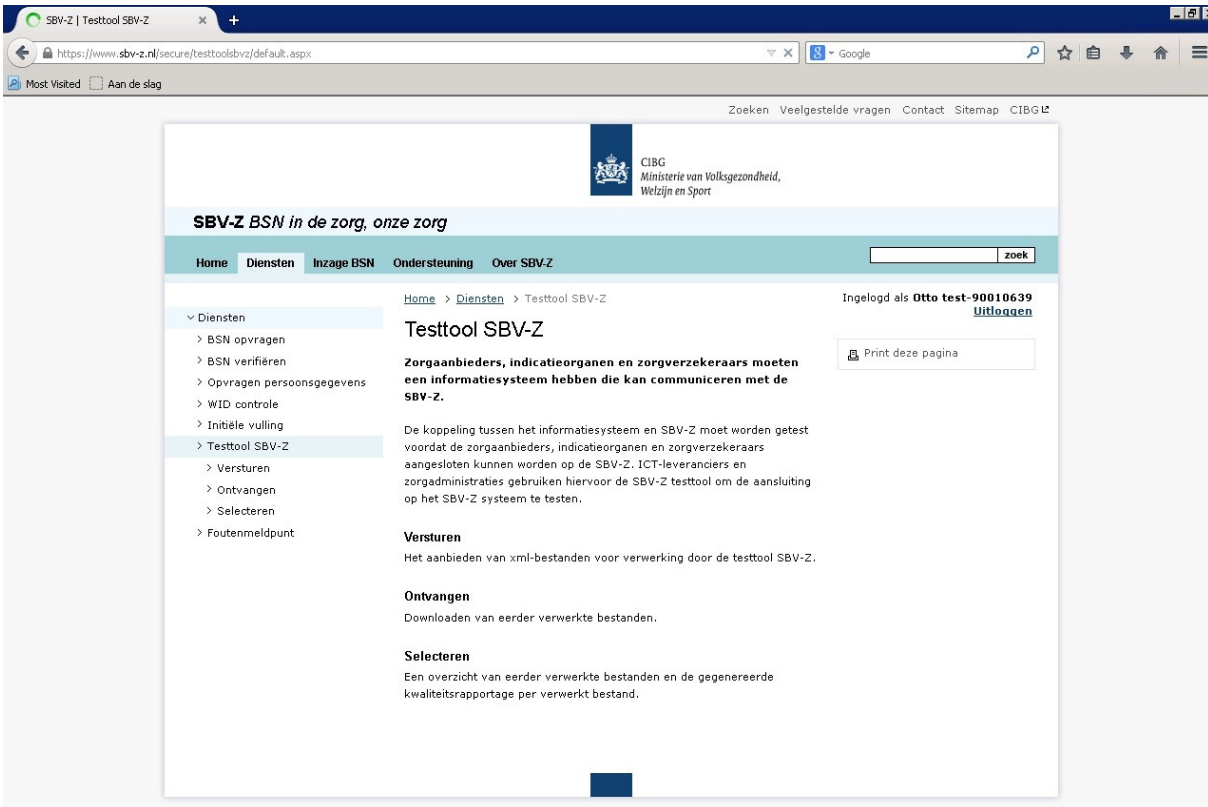
SafeSign zal nu het certificaat op de smartcard gaan “openen” en om een PIN code vragen. Firefox noemt dit een “master password”.



Vul de PIN code van de UZI-pas in en druk op OK.

U bent nu ingelogd op de test website.

Dit kunt u zien aan de tekst aan de rechter bovenkant van de pagina: "Ingelogd als". De pas werkt nu correct.



The screenshot shows a Firefox browser window displaying the SBV-Z Testtool website. The browser's address bar shows the URL <https://www.sbv-z.nl/secure/testtoolsbvz/default.aspx>. The website header includes the CIBG logo and the text "CIBG Ministerie van Volksgezondheid, Welzijn en Sport". Below the header, there is a navigation menu with options: Home, Diensten, Inzage BSN, Ondersteuning, and Over SBV-Z. A search bar is located to the right of the navigation menu. The main content area is titled "Testtool SBV-Z" and contains the following text:

Zorgaanbieders, indicatieorganen en zorgverzekeraars moeten een informatiesysteem hebben die kan communiceren met de SBV-Z.

De koppeling tussen het informatiesysteem en SBV-Z moet worden getest voordat de zorgaanbieders, indicatieorganen en zorgverzekeraars aangesloten kunnen worden op de SBV-Z. ICT-leveranciers en zorgadministraties gebruiken hiervoor de SBV-Z testtool om de aansluiting op het SBV-Z systeem te testen.

Versturen
Het aanbieden van xml-bestanden voor verwerking door de testtool SBV-Z.

Ontvangen
Downloaden van eerder verwerkte bestanden.

Selecteren
Een overzicht van eerder verwerkte bestanden en de gegenereerde kwaliteitsrapportage per verwerkt bestand.

In the top right corner of the page, it says "Ingelogd als Otto test-90010639" with a link to "Uitloggen". There is also a "Print deze pagina" button.