

Elektronische communicatie speelt een steeds grotere rol in onze samenleving. Ook in de zorg. De Wet gebruik burgerservicenummer in de zorg (W-bsnz) helpt er bij elektronische communicatie zeker van te zijn dat het om de juiste patiënt gaat. Het Zorgverzekeraars identificatie en authenticatie register, kortweg ZOVAR, is ontwikkeld om de zorgverzekeraars en zorgkantoren te kunnen voorzien van een authenticatiemiddel waarmee zij het BSN (burgerservicenummer) bij de SBV-Z (Sectorale Berichten Voorziening in de Zorg) kunnen opvragen.

ZOVAR is onderdeel van het CIBG, agentschap van het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Dit is een factsheet van ZOVAR.

Een overzicht van alle factsheets vindt u op de website www.zovar.nl.

ZOVAR geeft servercertificaten uit. Met behulp van deze servercertificaten kunnen zorgverzekeraars en zorgkantoren veilig elektronisch communiceren. Een servercertificaat mag niet op ieder systeem worden geïnstalleerd. Niet alleen het systeem zelf, óók de omgeving waar het systeem staat moet aan een aantal voorwaarden voldoen. Het moet praktisch onmogelijk zijn om de sleutels ongemerkt te stelen of te kopiëren. Met deze factsheet zet ZOVAR de voorwaarden voor u op een rij.

Voor de beveiliging van het ZOVAR Servercertificaat moeten in de praktijk bijvoorbeeld de volgende elementen minimaal op de server aanwezig zijn:

- Een virusscanner voorzien van de laatste updates (virus signatures).
- Een spyware scanner voorzien van de laatste updates (voor Macintosh computers is dat op dit moment niet noodzakelijk).
- Een firewall zo ingericht dat alle communicatiekanalen zijn afgesloten met uitzondering van die, die noodzakelijk zijn voor de bekende applicaties.
- Het besturingssysteem moet voorzien zijn van de laatste updates.
- Het servercertificaat mag alleen door het administrator account benaderd worden. Dit wordt ook wel het systeembeheerders account genoemd.
- De private sleutel moet versleuteld zijn. Dit om te voorkomen dat de private sleutel onversleuteld op een backup komt te staan.
- Als er voor de versleuteling geen gebruik wordt gemaakt van een Certificate Store, dan moet voor de versleuteling een gangbaar versleutelingsalgoritme voor private sleutels gebruikt worden. Daarnaast moet het bestand met daarin de private sleutel zo beveiligd worden dat alleen de applicatie toegang krijgt tot dit bestand. De consequentie is dat bij het herstarten van een systeem of applicatie, er altijd een activeringscode ingegeven moet worden voordat het servercertificaat gebruikt kan worden.
- De activeringscode bestaat minimaal uit 6 karakters. Het is geen bestaand woord (of naam) en bestaat uit:
 - hoofdletters
 - kleine letters
 - en tenminste 1 cijfer
- Voor de activeringscode moet er een zogenaamde passphrase gebruikt worden. Dit is een voor de gebruiker makkelijk te onthouden zin (b.v. Ikvindmelknietlekker2006).
- Er moeten minimaal 2 lagen van fysieke toegangsbeveiliging zijn voordat er toegang is tot het systeem met de private sleutel. Denk hierbij aan bijvoorbeeld een afgesloten ruimte en een afgesloten serverkast waarin het systeem met de private sleutel zich bevindt.
- En tot slot, een schermbeveiliging die bij het verlaten van de ruimte geactiveerd moet worden.

Als u gebruikt maakt van een HSM (Hardware Security Module) voor het genereren van het sleutelpaar en de beveiliging van de private sleutel die bij het servercertificaat hoort, is een aantal beveiligingseisen direct al ingevuld.

Naast de genoemde minimale set is het ook noodzakelijk om een goede risicoanalyse uit te voeren op basis van de NEN7510 norm (www.nen7510.org).