



Complexiteit maakt per definitie onveilig

# Beveiligings- techniek: het doekje voor het bloeden

*Auteur: Frans M. Kanters* > Frans Kanters is security watcher en freelance journalist. Hij publiceert regelmatig over kwesties rond informatiebeveiliging (e-mail: Frans@Le-Platane.nl).

*Identificatie en authenticatie vormen een steeds belangrijker aspect binnen beveiliging. Is het zo dat dit met certificaten überhaupt wel zin heeft? Een aantal organisaties ziet op tegen de hoge eisen ten aanzien van PKI overheid voor de elektronische handtekening. (smartcard, FIP140 certificering, EAL4 et cetera). Zal de PKI in de toekomst dan niet alleen gebruikt gaan worden voor authenticatie doeleinden. Om maar met de deur in huis te vallen: is er een alternatief voor PKI?*

"Om met het laatste deel van de vraag te beginnen, 'ja', op zich wel. Het ligt eraan hoe je het opzet. Een PKI wordt op dit moment veelal opgezet als een centrale autoriteit, die zaken controleert, en aan de hand van het resultaat van deze controleslag een certificaat al dan niet toekent. Een certificaat is een set gegevens behorend bij een persoon of computersysteem, gekoppeld aan een sleutelpaar. Voorheen werd

Het invoeren van beleid ten aanzien van informatiebeveiliging kan niet zonder de inzet van technologie. De complexiteit van technische beveiligingsproducten en de snelheid waarmee innovaties zich opvolgen, maken deze invoering lastig. In combinatie met het onjuist ontwikkelen van software wordt een fors aantal beveiligingsincidenten veroorzaakt. Beveiligingstechniek wordt daardoor een soort doekje voor het bloeden. Als technisch beveiligingsconsultant en ethisch hacker komt ing. Hans van de Looy, CEO van Madison Gurkha BV, dit scenario maar al te vaak tegen. Het aanbod aan beveiligingstechniek is enorm; er is echter ook veel techniek die in feite onnodig is. De echte problemen ontstaan pas als mensen met de techniek om moeten (leren) gaan. Daarnaast wordt er een cruciale fout gemaakt: tijdens de ontwikkeling van software wordt te weinig aandacht besteed aan security, en ontstaat er per definitie onveilige programmatuur.

elke PKI (Public Key Infrastructuur) geïmplementeerd als een soort piramidestructuur waarbij de CA (Certificate Authority) aan het hoofd staat, en waaronder alle overige onderdelen hangen. Als je certificaten gaat gebruiken voor het veilig uitwisselen van e-mail dan zijn er al veel langer alternatieven, namelijk het veilig uitwisselen van e-mail gebaseerd op een web of trust. Dit was al beschikbaar voordat PKI bestond. PGP (Pretty Good Privacy) is wel het bekendste voorbeeld hiervan. Momenteel is er een andere open source variant, genaamd GPG (GNU Privacy Guard). Hierbij is er

geen centrale autoriteit. Het vertrouwen naar elkaar uitspreken, van mensen onderling, vormt hierbij de basis. Dit doe je door elkaars publieke sleutel te ondertekenen. Wil je op dit moment op basis van X.509 certificaten iets of iemand authenticeren en veilig informatie uitwisselen, dan kom je al snel terecht bij organisaties als Verisign. Deze hebben een complete structuur ingericht om certificaten uit te delen. Een PinkRoccade en Diginotar zijn in feite onderaannemers van Verisign. De masterkey van Pink is namelijk weer ondertekend door Verisign. Hier zie je dus ook die pirami-