# COLUMN

Ir. Teus van der Plaat, IVENT Research en Innovatie Centrum

**Iedereen die in actieve dienst is geweest bij Defensie of allen die dat nog steeds zijn, weten wat de twee eerste afkortingen betekenen. De PSU, de Persoonlijke Standaard Uitrusting, is de set van middelen die aan elke militair standaard wordt verstrekt. Toen ik in dienst was, was dat onder andere het handboek soldaat, een plunjebaal en andere spullen als een helm, een schepje, een mok etc. Op een zeker moment kreeg ik een brief dat ik alles mocht houden en daarna heeft mijn zoon in de straat nog vele jaren 'oorlogje' gespeeld met de overblijfselen. Recenter is de verstrekking van de PGU, de Persoonlijke Gevechtsuitrusting.**

## NA DE PSU EN DE PGU, DE PDU?

Aangezien we momenteel het tijdperk naderen van de oorlogsvoering en verdediging in cyberspace, wordt het tijd dat we ons assortiment uitbreiden met een PDU, een Persoonlijke Digitale Uitrusting. Elke defensiemedewerker, militair of burger dient zich te beschermen tegen de dreigingen van cyberspace. In de pers staan continu verhalen over alle succesvolle hackpogingen en dit is slechts het topje van de ijsberg, want vele bedrijven lopen er absoluut niet mee te koop als hun digitale omgeving het slachtoffer is geworden van een of andere actie. Ook de politiek heeft ingezien dat cyber een belangrijke factor aan het worden is, want dat is zo ongeveer het enige onderdeel van Defensie waarop intensiveringen gepland staan. Formeel is er binnen Defensie nog niet besloten over te gaan tot het verstrekken van de PDU, dus dan leent een column zich er goed voor om hier eens over te filosoferen.

Waar zou dan een dergelijk **Persoonlijke Digitale Uitrusting** (PDU) uit moeten bestaan?

Allereerst is belangrijk te bedenken dat het allemaal zo voordelig en goedkoop mogelijk moet zijn, want geld is een schaars goed bij Defensie. Een belangrijke component van de PDU is de bestaande defensiesmartcard. Deze kaart is recent weer door de zware overheidscertificeringstest gekomen en is dus geschikt als authenticatiemiddel voor een geclassificeerde *trusted* omgeving. Ze bevat naast de contact chip ook een public key en is beschermd met een pincode. Er is nog maar een zeer beperkt aantal overheidspartijen, dat succesvol door de bijbehorende audit heen gekomen is. Elke defensiemedewerker bezit in principe een smartcard, die ook visueel zichtbaar gedragen moet worden. Op dit moment zijn er ruim 80.000 van deze gecertificeerde kaarten in omloop en worden deze naast visuele identificatie ook voor allerlei andere toepassingen gebruikt.

Als tweede element van de PDU wordt gedacht aan het verstrekken van een telestick. Inmiddels zijn er in de pilot die hiermee loopt ruim 4.000 in gebruik en zijn de kinderziektes er wel uitgehaald. Rond het tijdstip van uitkomen van dit blad moet hij officieel in productie zijn. Aangezien de telestick bestaat uit een goedkope standaard USB stick van enkele euro's en een opvouwbare smartcardreader, zijn de extra kosten hiervan gering. Mede omdat het op de privé PC en internetverbinding gebruikt moet worden of in de toekomst binnen Defensie op een zogenaamd Thin Client Device, dat ook opgestart kan worden met een telestick. Uit reacties van de pilotgebruikers blijkt, dat men er in het algemeen zeer tevreden mee is. Omdat elke defensiemedewerker standaard ook beschikt over een digitaal account gekoppeld aan de centrale directory en peoplesoft, zijn de extra kosten relatief gering. Vermeldenswaardig, zeker in het blad van de verbindingsofficieren, is het feit dat de nieuwste versie van de telestick als proef is uitgerust met een Open Source voice- en videoclient, die verbonden is met de Open Source telefooncentrale Asterisk. Alle gebruikers van de telestick kunnen hierdoor op departementaal vertrouwelijk niveau met elkaar bellen en een videosessie opzetten. Aangezien de telestick naast internet ook werkt over broadband UMTS, WiFi en Satcom verbindingen biedt dit allerlei goedkope communicatiemogelijkheden.

Als derde element van de PDU wordt voorgesteld iedereen uit te rusten met een SIM-kaart (*Subscriber Identity Module*). De productiekosten van een SIM-kaart geproduceerd in flinke aantallen, zijn in de orde van enkele euro's, er worden er immers wekelijks miljoenen wereldwijd verstrekt door mobiele operators. Omdat Defensie beschikt over een eigen mobiele netwerkcode (204 22), heeft Defensie ook het recht om zelf SIM's te laten drukken. Aangezien een SIM gewoon een chip is waar naast de gestandaardiseerde zaken ook vele andere zaken op gezet kunnen worden, ontstaat er een potentiële zeer krachtige combinatie. Uiteraard wordt de SIM ook gekoppeld aan de centrale directory en de smartcard. Een SIM alleen is uiteraard niet genoeg. Er openen zich grote mogelijkheden door deze SIM te gaan gebruiken in commerciële en operationele (GSM, UMTS, LTE) netwerken. Ten aanzien van de te gebruiken *devices* is de keuze onbeperkt. Er zijn momenteel meer dan 1.000 verschillende typen telefoons en smartphones in gebruik. Ook m2m (*machine to machine*) communicatie kan gebruikt worden op deze infrastructuur. Omdat Defensie zelf de architectuur van de SIM kan bepalen, kunnen er ook additionele beveiligingsmaatregelen genomen worden die op een normale commerciële SIM niet aanwezig zijn.

## BRING YOUR OWN DEVICE

Met een SIM alleen zijn we er niet, hij dient geplaatst te worden in een telefoon, smartphone, tablet of laptop. Naar keuze of noodzaak kan dit een 'eigen' device zijn, onder het motto BYOD (*Bring Your Own Device*) of een door Defensie verstrekt exemplaar. Vele alternatieven zijn mogelijk en ook ten aanzien van wel of niet privé gebruik zal nog het nodige uitgezocht moeten worden. Op welke commerciële en eigen operationele netwerken deze apparatuur gaat werken, is ook nog de vraag. Een ding is duidelijk, de PDU biedt voor Defensie naast grote besparingsmogelijkheden ook allerlei nieuwe mogelijkheden voor operationeel gebruik. Op de innovatiekalender staan diverse proeven en pilots om deze mogelijkheden samen met de industrie te testen.