

# Cryptografie in Nederland.

## Auteur

Leon Kuunders is security consultant en managing partner bij NetSecure Nederland.  
E-mail: [leon@netsecure.nl](mailto:leon@netsecure.nl)

## Introductie

Cryptografie wordt algemeen beschouwd als één van de middelen om het vertrouwen in het internet groter te maken. Door het versleutelen van informatie kan voorkomen worden dat gegevens tijdens transport en opslag onbedoeld in handen komen van derden en kan onweerlegbaarheid worden verkregen. In voorafgaande afleveringen zijn primair zaken behandeld rondom de betrouwbaarheid van informatie (artikel 1: PGPdisk en artikel 3: Windows 2000 EFS). Daarnaast is in artikel 2 (OpenPGP versus S/MIME) kort gesproken over de integriteit en authenticiteit van informatie.

In dit vierde en laatste artikel over cryptografie wordt eerst ingegaan op het gebruik van de elektronische handtekening, de wettelijke basis hiervoor en de privacy aspecten die ermee gemoeid zijn. Vervolgens zullen de overeenkomsten tussen versleuteling en elektronische handtekeningen worden besproken en uiteindelijk worden de diverse toepassingsgebieden voor cryptografische technieken nader toegelicht. In de conclusie wordt ingegaan op het Encryptie Kennis Centrum Nederland (EKCEN), een platform dat als doelstelling heeft het promoten van en voorlichting geven over cryptografische technologie en producten.

## De elektronische handtekening

De Europese Gemeenschap heeft in december 1999 de richtlijn 1999/93/EG [1] geaccepteerd die betrekking heeft op elektronische handtekeningen. Een Nederlands wetsvoorstel dat strekt tot uitvoering van de richtlijn is in Mei 2001 gepubliceerd [2]. De wet maakt een verschil tussen gewone en gekwalificeerde (geavanceerde) elektronische handtekeningen.

Een gewone elektronische handtekening wordt omschreven als "*elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie*" (authenticatie is een verbastering van het franse woord *authentication* en wordt gebruikt voor het aangeven van de verbintenis tussen identificatie en authenticatie). Dit kan een ingescande handtekening zijn, bijvoorbeeld een opdrachtbevestiging die na ondertekening wordt gefaxt naar de leverancier.

Een gekwalificeerde elektronische handtekening moet:

1. op unieke wijze aan de ondertekenaar zijn verbonden;
2. het mogelijk maken om de ondertekenaar te identificeren;
3. tot stand zijn gekomen met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
4. op dusdanige wijze zijn verbonden aan de gegevens waarop ze betrekking heeft dat elke wijziging achteraf kan worden opgespoord.

Minister van Boxtel (Grote Steden- en Integratiebeleid) heeft steeds voor ogen gehad dat er één elektronische identificatie moet komen die voor het totale gegevensverkeer tussen de overheden en de burger gebruikt kan worden. Hiermee wordt voorkomen dat de burger wordt lastiggevallen met allerlei typen smartcards en verschillende soorten handtekeningen voor verschillende diensten van de overheid [3]. Deze keuze heeft tot gevolg dat de elektronische handtekening die gebruikt zal worden voor burger-overheid communicatie pas vanaf eind 2002, 2003 beschikbaar zal zijn. Het digitale paspoort, een combinatie van paspoort en chipkaart (eventueel uitgebreid met biometrische technieken voor identificatie), is de meest waarschijnlijke optie.

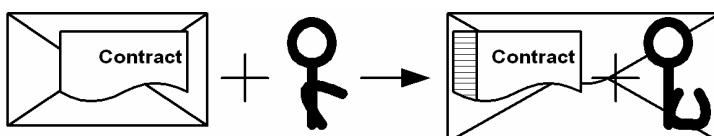
De wens om te komen tot een multifunctionele chipkaart, niet alleen te gebruiken voor overheidsdiensten, wordt door meerdere partijen uitgesproken [4]. Met zo'n kaart wordt voorkomen dat de gebruiker een meervoud aan chipkaarten moet gebruiken voor het kunnen plegen van diverse transacties in de publieke en private sector. Vanuit beveiligingsoogpunt is een groot aantal persoonsgebonden kaarten een ongewenste ontwikkeling omdat de controle op het gebruik ervan (op zowel economisch als privacy gebied) een onmogelijke taak wordt.

Logischerwijs stevenen we af op een kaart die èn persoonsgebonden is èn geaccepteerd zal worden door diverse instanties die op dit moment nog eigen kaarten uitgeven. Het nieuwe Nederlandse paspoort lijkt bij uitstek geschikt om deze voorkeurkaart te worden. De identificatie van de gebruiker wordt bij het afgeven van een paspoort geregeld door de lokale overheid (gemeente) en geeft daarmee een basis voor het binden van de elektronische identiteit aan de werkelijke identiteit.

Om deze multifunctionele kaart mogelijk te maken zullen service verlenende organisaties er toe over kunnen gaan om de door de overheid uitgegeven kaart te *vertrouwen* in plaats van het uitgeven van een eigen kaart. Vergelijk als voorbeeld het laten zien van het paspoort bij een bank alvorens een rekening geopend kan worden en een bank kaart wordt verkregen. Indien het paspoort wordt voorzien van een chip met daarop de elektronische identificatie van de gebruiker zou deze kaart ook kunnen worden geaccepteerd door de bank en vervalt de behoefte aan een extra kaart.

### **Anonieme Transacties**

Het gebruik van de elektronische handtekening voor transacties zou er als volgt uit kunnen zien: de serviceverlener verstuurt via e-mail aan de servicenemer het contract waarin de voorwaarden staan (zoals kosten en dergelijke) waaraan de af te nemen dienst onderhavig is. Na lezing wordt door de servicenemer het document van een elektronische handtekening voorzien (met behulp van de privé sleutel) en (samen met zijn/haar publieke sleutel) teruggestuurd via e-mail aan de serviceverlener (zie figuur 1).



figuur 1.

Indien de publieke sleutel van de serviceverlener in het bezit is van de servicenemer dan kan het versturen van het elektronisch getekende contract middels versleutelde e-mail gebeuren. Hiermee wordt voorkomen dat derden achter de inhoud van het contract kunnen komen en op die manier alsnog kennis kunnen nemen van de persoonsgegevens van de servicenemer.

De serviceverlener verifieert de geldigheid van de elektronische handtekening aan de hand van de (meegestuurde) publieke sleutel van de servicenemer (bijvoorbeeld in de Gemeentelijke Basis Administratie (GBA) [5], [6]) en geeft na goedkeuring in zijn systeem aan dat de aangeboden dienst gebruikt kan worden.

De toegang tot het daadwerkelijk gebruik van de dienst kan vervolgens geregeld worden door bij een transactie door de serviceverlener een unieke *transactie code* te laten versturen die door de servicenemer wordt voorzien van een elektronische handtekening en terug wordt gestuurd ter verificatie. De serviceverlener geeft vervolgens goedkeuring aan de transactie nadat de handtekening succesvol is geverifieerd (figuur 2).



figuur 2.

Een dergelijke transactie zou het online bestellen van een CD kunnen zijn, maar ook het offline kopen van een CD in een winkel. Het betalen met creditcard (online) of PIN pas (offline) heeft tot gevolg dat de tussenpersoon (winkelier) de identiteit, of een gedeelte van de identiteit van de koper te weten komt. Denk bijvoorbeeld aan de nieuwe mogelijkheid die Albert Heijn heeft geïntroduceerd rondom het sparen met behulp van je bankkaart. Waar vroeger nog een aparte AH-pas nodig was om van aanbiedingen te kunnen genieten, is het tegenwoordig mogelijk om deze gegevens te laten koppelen aan je PIN-pas. Als je gebruik maakt van je pas om te betalen bij de supermarkt is een eenvoudige druk "op de groene knop" voldoende om je aankoopgedrag (en je kortingen en je Air Miles en je bonuspunten) te laten registreren door de AH computer. Deze transacties zijn dus niet anoniem en een adequaat controlemechanisme (hoe weet ik zeker dat mijn gegevens niet alsnog worden geregistreerd?) op het gebruik van deze techniek ontbreekt.

Georganiseerde semi-anonieme transacties zoals in het voorbeeld [7] voorkomen dat tussenpersonen die de dienst aanbieden wetenschap moeten hebben van de daadwerkelijke identiteit van de servicenemer. Anonimiteit kan worden bereikt doordat de tussenpersoon alleen de beschikking heeft over de transactiecode en de geassocieerde *hash* waarde (oftewel de handtekening die is gegenereerd door de servicenemer voor de eenmalige transactie code) en niet over zaken als de naam van de kaarthouder en zijn bankrekeningnummer.

## Versleutelen en handtekening

Er zijn duidelijke overeenkomsten tussen het gebruik van cryptografische technieken voor het coderen en decoderen van bestanden (vertrouwelijkheid) en het gebruiken van elektronische handtekeningen (integriteit, authenticiteit). De basis voor deze technieken ligt namelijk in het gebruik van sleutelparen bestaande uit een publieke

en een privé sleutel (*public key* cryptografie, zie ook deel 2 uit deze serie). Waar de elektronische handtekening een juridische basis vraagt is dit bij het coderen en decoderen van bestanden niet nodig. De reden hiervoor is eenvoudig: een gecodeerd bestand waarborgt alleen de vertrouwelijkheid van de informatie en dit valt niet in juridische termen vast te leggen. Wil men echter weten of de communicatiepartner werkelijk diegene is die hij zegt te zijn en of de gegevens in ongewijzigde vorm zijn ontvangen, dan is het gebruik van een elektronische handtekening noodzakelijk.

Wil men dus op een veilige *en zekere* manier communiceren via bijvoorbeeld e-mail dan is de werkwijze als volgt:

- 1) coderen van bijlagen en de informatie in de e-mail;
- 2) genereren van een elektronische handtekening voor het gecodeerde bestand;
- 3) toevoegen van de elektronische handtekening aan het gecodeerde bestand.

Om te voorkomen dat een gecodeerd bericht (waarvan de authenticiteit op zichzelf niet kan worden aangetoond) wordt voorzien van een valse handtekening is het verstandig om in het bericht de naam van de verzender en de ontvanger op te nemen [8].

## Toepassingsgebieden

Zoals reeds gemeld zijn de toepassingsgebieden voor cryptografie legio. Naast het gebruik ervan voor het beveiligen van informatie kan er ook zekerheid rondom communicatie mee worden verkregen. Het belang ervan wordt door alle partijen (overheid en commercieel) ingezien. De ontwikkeling rondom de elektronische handtekening en de wens om een groot gedeelte van de transacties tussen burger en (lokale) overheden via elektronische weg af te handelen zullen voor een enorme toename gaan zorgen.

Thuiswerken neemt dankzij de mogelijkheid om via internet een verbinding te leggen met het bedrijfsnetwerk, een steeds grotere vlucht. Dit vraagt om een gedegen beveiliging, van het verkeer tussen de thuiswerker en het bedrijfsnetwerk (vertrouwelijkheid) tot aan de toegang tot het bedrijfsnetwerk (identificatie en authenticatie). Zowel het bedrijfsnetwerk als de PC of laptop van de thuiswerker moeten dus beveiligd worden.

Producten als Windows 2000 EFS en PGPdisk voor bestandsencryptie gebruiken als basis dezelfde techniek als die voor de elektronische handtekening nodig is. Het opzetten van VPN verbindingen tussen verschillende bedrijfsonderdelen en thuiswerkers is een ander voorbeeld van de inzet van cryptografie. Ze maken beide deel uit van een breed scala aan technieken die door bedrijven worden ingezet om hun informatie te beveiligen.

Voorwaarde voor de (eind-)gebruikersacceptatie van al deze technieken is dat deze [9]:

1. eenvoudig zijn in het gebruik;
2. op meerdere punten zijn in te zetten;
3. bewezen veilig zijn;
4. zichtbaar zijn voor de gebruiker; en
5. relatief niet meer tijd vragen.

De mate van beveiliging van informatie is afhankelijk van de technische en organisatorische maatregelen die er rondom de omgang met informatie zijn getroffen. De technische maatregelen komen allemaal direct dan wel indirect voort uit, of in aanraking met, cryptografische technieken.

## Conclusie

Het inzetten van cryptografische technieken is nog niet eenvoudig genoeg. De ontwikkelingen op het gebied van smartcards maken het gebruik echter wel steeds gemakkelijker. Gebruiksvriendelijkheid zal een belangrijke voorwaarde zijn voor het uiteindelijke succes van cryptografie. Door de enorme hoeveelheid informatie die er op dit gebied te verkrijgen is en de toevoegingen van nieuwe technieken zoals ECC (Elliptic Curve Cryptography – versleuteling gebaseerd op andere wiskunde algoritmes) is het moeilijk om een helder en volledig beeld te krijgen van wat wel en niet mogelijk is.

Het succes van de elektronische belastingaangifte geeft aan dat de acceptatie en dus ook het vertrouwen in cryptografische technieken steeds beter wordt. De informatie- en telecommunicatietechnologie geeft ongekende decentralisatiemogelijkheden die door steeds meer grote en kleine ondernemingen worden herkend en ook dit zal voor een belangrijke *push* zorgen.

Gedegen voorlichting op dit gebied is en blijft essentieel. Dat wil zeggen: voorlichting die niet gestuurd wordt door commerciële belangen, maar gericht is op het belang van de eindgebruiker. De overheid draagt hierin haar steentje bij, onder andere door het geven van voorlichting over de mogelijkheden van ICT aan het MKB [10]. Eerder dit jaar is het Encryptie Kennis Centrum Nederland opgericht [11], een non-profit organisatie die kennis over encryptietechnologie, -producten en -diensten verzamelt en presenteert. Geheel in lijn met de voorstellen van de taskforce ICT-en-kennis [12] zal middels het EKCEN initiatief informatie over cryptografische ICT toepassingen met ondernemend Nederland worden gedeeld. Dit is beslist een aanzienlijke stap in de goede richting. Ik nodig alle vakbroeders van harte uit om dit initiatief te steunen, nadere informatie is bij ondergetekende op te vragen door een e-mail te sturen naar [leon@ekcn.nl](mailto:leon@ekcn.nl).

Augustus 2001  
Leon Kuunders

Achtergrond:

[1] Richtlijn 1999/93/EG Europese Gemeenschap, December 1999  
<http://www.kub.nl/sobu/eec/weh-1-2.pdf>

[2] Wet elektronische handtekeningen, Mei-Juli 2001  
Zoek bij [www.overheid.nl](http://www.overheid.nl) op "wet elektronische handtekeningen"

[3] Verslag algemeen overleg; kamerstukken 26387.10, Maart 2001  
<http://overheid-op.sdu.nl/cgi/showdoc/pdf/of:22581/5/0/KST52466.pdf>

[4] Cards and personal identification, Juli 2001  
<http://www.iso.ch/iso/en/commcentre/pdf/Smartcards0003.pdf>

[5] Eindrapport GBA in de toekomst, Maart 2001

<http://www.gba.nl/downloads/Eindrapport%20'GBA%20in%20de%20toekomst'.pdf>

[6] Kabinetsreactie modernisering GBA, Juni 2001

<http://overheid-op.sdu.nl/cgi/showdoc/pdf/of:22581/6/0/KST54734.pdf>

[7] New Rules for Anonymous Electronic Transactions. An Exploration of the Private Law Implications of Digital Anonymity, Jan Grijpink & Corien Prins, Juli 2001

<http://elj.warwick.ac.uk/jilt/01-2/rfts/grijpink.rtf>

[8] Defective Sign & Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP and XML, Don Davis, Mei 2001.

[http://world.std.com/~dtd/sign\\_encrypt/sign\\_encrypt7.html](http://world.std.com/~dtd/sign_encrypt/sign_encrypt7.html)

[9] Digitalisering van de leefwereld, Sociaal en Cultureel Planbureau, Mei 2000

<http://www.scp.nl/boeken/cahiers/cah167/nl/acrobat/cah167totaal.pdf>

[10] Plan van Aanpak: Het MKB in de Digitale Delta, Juli 2001

<http://overheid-op.sdu.nl/cgi/showdoc/pdf/of:22581/1/0/KST54529.pdf>

[11] Encryptie Kennis Centrum Nederland

<http://www.ekcn.nl>

[12] Rapport Taskforce ICT-en-kennis, Juli 2001

<http://taskforce-ict-en-kennis.nl/Eindrapport-task-force.pdf>