Beveiliging van gegevens op internet

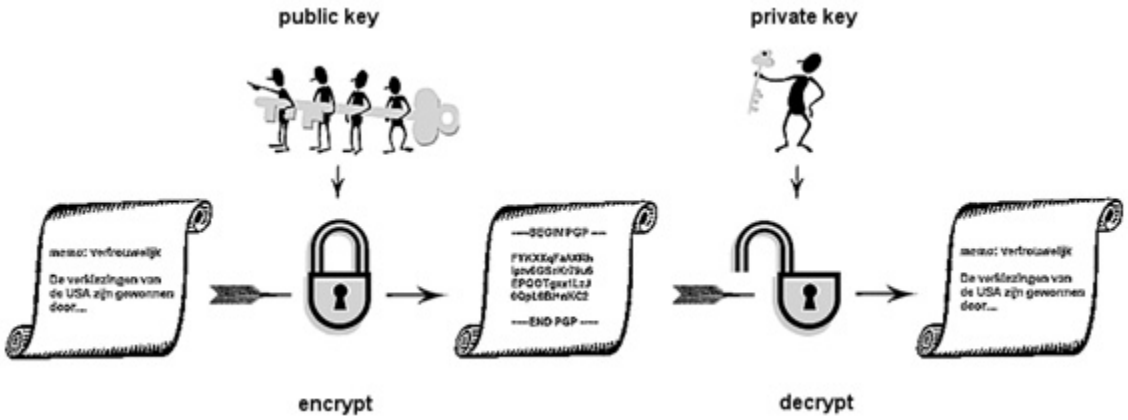
PKI: Public Key Infrastructure bij de RUG

Frans Velthuis f.j.velthuis@rc.rug.nl
Anke Breeuwsma j.c.breeuwsma@rc.rug.nl

Iedereen kent het nog wel van vroeger, geheime briefjes uitwisselen met vriendjes, die niemand verder mocht lezen, alleen die paar vriendjes voor wie het bestemd was. Wij deden het meestal op de manier van het verschuiven van letters, waar een ?A? hoorde te staan kwam een ?D? en waar een ?B? hoorde te staan kwam een ?E?. Maar er waren vast ook wel andere methodes.
Bij ons ging het vroeger natuurlijk niet om belangrijke zaken, maar met de opmars van het internet en zeker nu steeds meer mensen gebruik maken van bijvoorbeeld telebankieren en creditcards, wordt het veilig versturen van gegevens steeds belangrijker. In dit artikel meer over cryptografie, digitale handtekeningen en hoe authenticatie en versleuteling van gegevens bij de RUG en daarmee samenhangend bij SURFnet geregeld is met behulp van PKI (Public Key Infrastructure).

Versleutelen van berichten

Het versleutelen van berichten/bestanden met behulp van een wiskundige berekening wordt *cryptografie* genoemd. Op deze manier kan vertrouwelijke informatie opgeslagen over een netwerk (of internet) verstuurd worden zonder dat iemand anders dan degene voor wie het bestemd is, het kan lezen.
Het versleutelen van informatie waardoor het niet meer leesbaar is (je ziet in plaats van tekst een code) wordt *encryptie* genoemd. Het terughalen van die informatie tot een leesbaar stuk heet *decryptie*.



Public Key-encryptie

Public Key-cryptografie

Voor het versleutelen van tekst heb je een zogenaamde sleutel (*key*) nodig. Er kan gebruik worden gemaakt van cryptografie met zowel 驮 als twee sleutels. Bij 驮 sleutel heeft zowel verzender als ontvanger dezelfde geheime sleutel nodig. Dit is natuurlijk handig als je elkaar kent en dicht bij elkaar woont, maar bij onbekenden die ook nog ver uit elkaar wonen, is dit niet handig. De geheime sleutel moet dan over het internet verstuurd worden en wie kan dan nog garanderen dat de sleutel geheim blijft? Een betere manier is het versleutelen met twee sleutels. De zogeheten *public key cryptografie*.
Bij *public key cryptografie* maak je gebruik van een paar *keys*. De *public key* wordt gebruikt voor encryptie en de *private key* voor decryptie. De *public key* kan uitgedeeld worden aan personen via internet (of met behulp van een *keyserver* waarin sleutels opgeslagen zijn).
De *private key* (het woord zegt het al) hou je voor jezelf. Wil iemand jou een beveiligde tekst over internet sturen, dan encrypt hij die tekst met jouw *public key*. Je krijgt de versleutelde tekst via het internet gestuurd en met behulp van je eigen *private key* kun je de tekst ontcijferen en lezen wat diegene je toegestuurd heeft.

Betrouwbare afzender: digitale handtekening

Versleuteling zorgt ervoor dat het bericht niet door anderen gelezen kan worden als het verstuurd wordt via internet. In sommige gevallen wil je nog meer zekerheid, dan wil je weten of het bericht dat verstuurd is inderdaad afkomstig is van diegene die als afzender genoemd is.

Even een voorbeeld om dit duidelijk te maken. Pieter heeft gesolliciteerd bij een bedrijf, laten we het Symtechnic noemen. Hij krijgt van de directeur van Symtechnic een e-mail waarin staat dat hij aangenomen is met daarbij een salarisaanbieding. Pieter wil wel graag weten of de e-mail inderdaad afkomstig is van de directeur van Symtechnic.

Een digitale handtekening zou hier uitkomst kunnen bieden. Dit is voor de ontvanger het bewijs dat het bericht daadwerkelijk van de afzender afkomstig is en dat het onderweg niet gewijzigd is. Een digitale handtekening kan afzonderlijk van encryptie gebruikt worden. Soms is het voldoende om te weten of het bericht inderdaad van diegene afkomstig is zonder dat het bericht zo belangrijk is dat niemand het mag lezen. De digitale handtekening staat onder het bericht dat verstuurd is.

```
-----BEGIN PGP SIGNATURE-----
iQA/AwUBOrYOKGAs/Ud4ZaHfEQJnBwCfa
FIS7MO+vhteJcRjU/BC2FXgC1YAmwZ4
S7WBb4Eg5N2IRqP7+ace/IGD
=wAp4
-----END PGP SIGNATURE-----
```

Voorbeeld van een digitale handtekening

Met behulp van een encryptie-programma (bijv. PGP, *Pretty Good Privacy*) wordt een samenvatting gemaakt van het bericht. Deze samenvatting wordt met behulp van de *private key* versleuteld. De versleutelde samenvatting is de digitale handtekening, die vervolgens onder het bericht wordt geplaatst.
De ontvanger van het bericht haalt de oorspronkelijke samenvatting met behulp van de public key weer tevoorschijn. Daarna wordt met behulp van hetzelfde encryptie-programma opnieuw een samenvatting van het bericht gemaakt. Als deze twee samenvattingen gelijk zijn, is dat het bewijs dat er niets aan het oorspronkelijke bericht gewijzigd is.

Betrouwbaarheid

Het bovenstaande voorbeeld werkt alleen als Pieter de directeur van Symtechnic persoonlijk kent en de *public key* van hem heeft gekregen. Alleen dan kan Pieter zeker weten dat hij de juiste *public key* heeft. Maar wat als je die persoon niet persoonlijk kent en je wilt wel belangrijke geheime informatie uitwisselen? Daarvoor heb je een zogenaamde derde persoon nodig die de *public keys* van beide partijen signeert en die door beide partijen vertrouwd wordt. Deze derde persoon kan een kennis of een collega zijn, maar het kan ook een instelling zijn die een algemeen vertrouwen geniet. Voor dit doel is de zogenaamde *Public Key Infrastructure* (PKI) in het leven geroepen.
Er zijn steeds meer instellingen die PKI als dienst aanbieden en daarmee als derde persoon optreden. Even terug naar het voorbeeld. Pieter had dus gebruik kunnen maken van PKI om de *public key* van de Symtechnic-directeur op te halen en zo te kijken of de e-mail inderdaad van de directeur afkomstig was.

Certificaten

Een *public key* wordt, voordat het verspreid wordt, verpakt in een certificaat. Behalve de *public key* bevat een certificaat persoonsgegevens van de eigenaar en de digitale handtekening van 驮 of meer personen die er voor instaan dat de persoonsgegevens inderdaad bij deze *public key* horen. Verder bevat een certificaat o.a. nog een geldigheidsduur.
Er zijn twee soorten certifcaten: PGP- (*Pretty Good Privacy*) en X.509-certificaten. De eerstgenoemde worden vooral gebruikt binnen mail-programma?s terwijl laatstgenoemde bijvoorbeeld ook gebruikt worden bij de communicatie tussen een webserver en een webclient.

Organisatie van de PKI bij de RUG

Een *Public Key Infrastructure* is een hi벡rchische boomstructuur van personen (*Certification Authorities*) die gerechtigd zijn binnen hun eigen organisatie certificaten te signeren. De Rijksuniversiteit Groningen maakt deel uit van de PKI die opgezet is door SURFnet en waarvan SURFnet ook de top van de PKI vormt. De *Certification Authority* (CA) van de RUG, een medewerker van het RC, is weer gemachtigd om binnen

faculteiten en diensten personen aan te wijzen die de identiteit van personen vast kunnen stellen en hun certificaten kunnen voordragen ter certificering.
Het certificaat van de hoogste CA binnen een PKI heet een *root*-certificaat. PKI-organisaties kunnen onderling elkaars *root*-certificaten signeren (*cross-certification*) en zodoende impliciet alle certificaten van de andere organisatie accepteren. Binnen Nederland zijn er ook andere PKI-organisaties opgezet, o.a. door de overheid en door de notarisorganisatie (www.diginotar.nl). De verwachting is dat in de nabije toekomst diverse van deze organisaties zullen gaan integreren tot een groter geheel.
De hoogste *Certification Authority* van een PKI (in ons geval SURFnet) signeert de certificaten van de CA's in het daaronderliggende niveau van de PKI. Die signeren weer de certificaten van de CA's in het niveau daaronder, etc. Een certificaat dat gesigneerd is door een CA binnen een PKI is daarom altijd te herleiden tot het *root*-certificaat en in feite is alleen d certificaat nodig om te kunnen bepalen of een willekeurig certificaat deel uitmaakt van een PKI.
Hoe kun je nu bepalen of een certificaat inderdaad van de root-CA is? Daarvoor is het handig gebruik te maken van de *fingerprint* van het certificaat. Een *fingerprint* is een getal van enkele bytes dat gegenereerd wordt uit het certificaat door middel van een zgn. *one way function*. Dit is een functie met de eigenschap dat er geen methode bestaat om vanuit het gegenereerde getal een ander bestand te construeren dat hetzelfde getal genereert.
De *fingerprint* van een CA-certificaat wordt gepubliceerd op de website van een CA, in offici뮗 publicaties van de CA-organisatie en kan altijd telefonisch *gechecked* worden bij een medewerker van de CA-organisatie. Op de PKI-site van de RUG (http://certs.rug.nl) staan de *fingerprints* van de SURFnet- en RUG-CA-certificaten.

E47B 87E5 7997 D4CE F71C 2D19 602C FD47 7865 A1DF

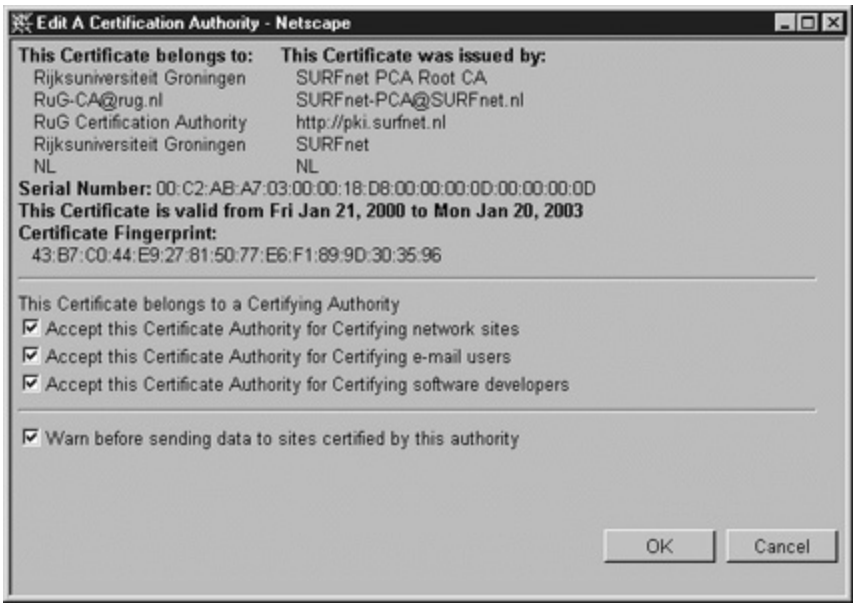
Voorbeeld van een fingerprint

Voordat SURFnet overgaat tot certificering van de CA van een instelling, wordt gecontroleerd of er voldaan wordt aan de eisen die SURFnet stelt. Deze eisen betreffen o.a. de procedures die gevolgd worden en de werkomgeving waarbinnen het signeren van een certificaat plaatsvindt. Alle eisen die SURFnet stelt aan een instellings-CA zijn te vinden op: http://pki.surfnet.nl/policies.html

Soorten certificaten die door de RUG-Certification Authority verwerkt kunnen worden

Hieronder volgt een opsomming van de soorten certificaten die verwerkt kunnen worden en de toegevoegde waarde van signering door de RUG-CA.

- *PGP-certificaten*
  Bij gebruik binnen mail geeft een gesigneerd certificaat de ontvanger van het bericht de zekerheid dat de verzender daadwerkelijk is wie hij pretendeert te zijn. Bij gebruik binnen PGP-net (waarmee een zgn. *Virtual Private Network* (VPN) opgezet kan worden) geeft een gesigneerd certificaat de andere kant van de beveiligde verbinding de zekerheid dat hij contact heeft met de pc van de juiste persoon.
- *X.509 client-certificaten*
  Bij gebruik binnen mail en binnen een VPN geeft certificering dezelfde toegevoegde waarde als bij PGP-certificaten. X.509 client-certificaten kunnen verder gebruikt worden om de toegang tot een WWW-server te regelen. Een WWW-server kan bijvoorbeeld zo ingesteld worden dat toegang alleen toegestaan wordt aan degenen die in het bezit zijn van een certificaat dat gesigneerd is door de RUG-CA en dat aangeeft dat de bezitter deel uitmaakt van een bepaalde faculteit en bijv. een bepaalde werkgroep.
- *X.509 server-certificaten*
  Deze certificaten worden gebruikt op *secure*-servers die gebruik maken van het SSL-protocol (*Secure Sockets Layer*-protocol). Een gesigneerd server-certificaat geeft een gebruiker de zekerheid dat hij contact heeft met een server die daadwerkelijk beheerd wordt door een RUG-organisatie zoals die in het certificaat wordt omschreven en dat de naam waarmee de server zich bekendmaakt daadwerkelijk de naam is, waaronder het is geregistreerd.
- *X.509 applet signing-certificaten*
  Deze certificaten worden gebruikt om Java-*applets* te signeren die in een internetprogramma gedownload en uitgevoerd kunnen worden. Een certificaat dat gesigneerd is geeft de gebruiker de zekerheid dat de *applet* daadwerkelijk afkomstig is van de organisatie die vermeld is in het certificaat en dat die organisatie deel uitmaakt van de RUG.



X.509-certificaat van de RUG-CA

Aanvragen van PGP-en X.509-certificaten bij de RUG

Op de RUG-PKI-site staan alle stappen omschreven voor het aanvragen van een PGP- of X.509-certificaat (onder andere *key* aanmaken, aanvraagformulier certificaat invullen). Als u de aanvraagprocedure heeft doorlopen, dient u zich te legitimeren bij de Helpdesk van het RC. Dat kan met paspoort en rijbewijs.
Het legitimeren is een eis van de SURFnet- PKI-organisatie; de identiteit van een gebruiker moet *face-to-face* vastgesteld worden. Na bovenstaande aanvraagprocedure krijgt u van de RUG-CA een gesigneerd PGP-certificaat of X.509-certificaat. De RUG-CA geeft uw certificaat door aan de SURFnet-keyserver zodat anderen uw certificaat (incl. *public key*) daar vandaan kunnen halen. Een certificaat heeft een geldigheid van vijf jaar. Na die vijf jaar kan het certificaat niet meer gebruikt worden.
Het kan ook voorkomen dat een certificaat voortijdig ingetrokken moet worden (bijvoorbeeld wanneer u vertrekt naar een andere werkgever). Het certificaat komt dan op een CRL (*Certificate Revocation List*) te staan, een lijst van ingetrokken certificaten. Op de PKI-site van de RUG-CA kunt u de RUG-CRL vinden.

Meer informatie:

RUG-PKI-site: https://certs.rug.nl
Helpdesk RC: http://www.rug.nl/rc/organisatie/pictogram/archief/rc/frhelp.htm
Brochure Veilig communiceren op het Internet: www.surfnet.nl/publicaties/brochures/beveiliging
PGP-software: www.pgpi.org/

Begin pagina

index Pictogram 2