Is internet-bankieren veilig?

Techniek en organisatie achter https

Internet is een open netwerk. Iedereen kan meekijken welk verkeer er over het lijntje gaat en berichtenverkeer zelfs muteren. Hoe zorg je er in zo'n omgeving toch voor dat je betrouwbaar zaken kan doen ? Over deze vraag gaat dit artikel.

Misschien ben je op feestjes wel eens gevraagd of jij als ICT-er kan aangeven hoe veilig internetbankieren nu eigenlijk is. Wat heb je toen geantwoord? Als het goed is heb je je gesprekspartner gewezen op de noodzaak van een goed beveiligde, spam- en virusvrije PC en het negeren van mailtjes waarin om toegangsgegevens wordt gevraagd. De campagne www.3xkloppen.nl brengt deze zaken nu landelijk onder de aandacht. En als je daar aan voldoet, hoe veilig is het dán nog? Want internet is een open netwerk. Iedereen kan meekijken welk verkeer er over het lijntje gaat en kan berichtenverkeer zelfs muteren.
We zullen het in dit artikel hebben over de techniek en organisatie achter de 's' van https, het protocol om gegevens over het internet te beveiligen tegen misbruik. We gaan het eerst hebben over de standaard beveiligingseisen en -technieken en over RSA-encryptie, het fundament van de internettransactiebeveiliging. Daarna gaan we in op het Secure Socket Layer-protocol (SSL) van https en op de Public Key Infrastructuur (PKI), een combinatie van maatregelen en technieken om in principe voor jou onbekende partijen, waarmee je over internet communiceert, toch te vertrouwen.

Beveiligingseisen en -technieken

In het geval van bankzaken regelen over internet moeten we voldoen aan alle eisen voor veilige communicatie. Deze zijn:

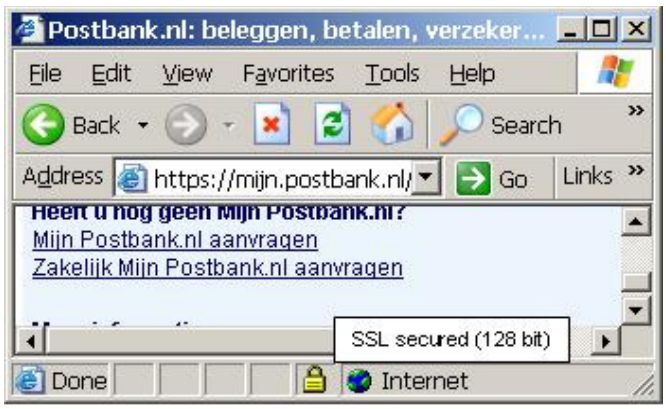
- authenticatie
  Vaststellen van iemands identiteit. Geldt zowel voor de bank als voor de klant.
- autorisatie
  Op grond van identiteit de bevoegdheid bepalen.
- geheimhouding
  Berichten kunnen niet door iemand anders gelezen worden.
- integriteit
  "Ik had er maar tien besteld in plaats van honderd."
- onweerlegbaarheid
  Beide partijen kunnen niet terugkomen op een transactie.

Ondanks het uitgebreide toepassingsgebied van beveiliging maken we goed beschouwd in de IT slechts gebruik van een viertal basistechnieken.

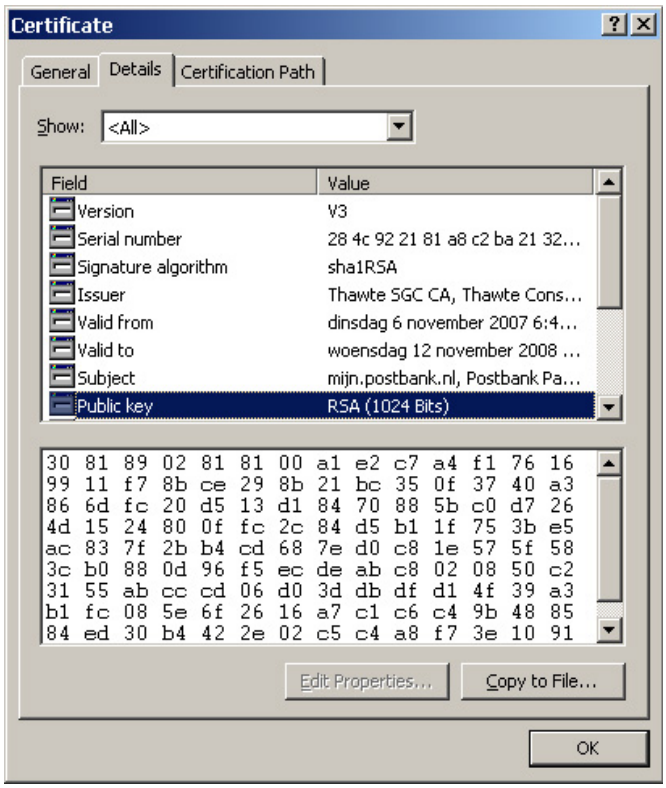
1. Hashing: de uit te wisselen informatie krijgt een 'vingerafdruk'.
2. Symmetische encryptie: berichten worden met een sleutel *k* ge-encrypt. De ontvanger kan het bericht decrypten met dezelfde sleutel *k*.
3. Asymmetrische encryptie: de encryptiesleutel *e* is totaal verschillend van de decryptiesleutel *d*.
4. Geheime sleuteluitwisseling.

Al deze technieken worden gebruikt als je een https-site benadert. Alle vier komen in dit artikel ook aan de orde.

Bij het bezoeken van een https-site wordt het SSL-protocol opgestart. Principe van dit protocol is dat het via asymmetrisch encryptie een beveiligde verbinding opzet en dat de onderlinge communicatie vervolgens via symmetrische (session key) encryptie verloopt. Als gebruiker kun je dit zelf zien (figuur 1).



Figuur 1. De beveiligde site van de Postbank, getoond met Internet Explorer 6



Figuur 2. De informatie over de asymmetrische encryptie volgens het RSA-protocol onder het tabblad "Details"

Bij een https-site verschijnt er altijd een slotje in de browser. Beweeg je er met de muis overheen, dan wordt de pop-up "SSL secured (128 bit)" getoond. Dit is informatie over de symmetrische encryptie. Dubbelklik je op het slotje, dan verschijnt een venster met op tabblad "Details" informatie over de asymmetrische encryptie volgens het RSA-protocol (figuur 2).

We gaan nu in op de betekenis van het veld "Public key", RSA (1024 Bits).

RSA: een prachtig stukje wiskunde

Het RSA-systeem werd in 1978 ontwikkeld door de cryptografen Rivest, Shamir en Adleman. Het is gebaseerd op het principe dat het vermenigvuldigen van twee priemgetallen eenvoudig en snel kan, maar het ontbinden van dat product in de twee priemgetallen bijzonder moeilijk is. Verder maakt het systeem gebruik van de modulo rekenen en machtsverheffen (voor wie het vergeten was: bij modulo rekenen kan de uitkomst niet groter worden dan de modulo: 7 modulo 10 is 7, maar 27 modulo 10 is ook 7). De geniale RSA-formule en pijler van de internetbeveiliging luidt:

$(K^e \text{ Mod } PQ)^d \text{ Mod } PQ = K$ waarbij $e*d = (P-1)(Q-1)+1$ en P en Q priemgetallen zijn.

Hier staat de essentie van encryptie: je start met 'bericht' *K*, en gaat die machtsverheffen met *e modulo PQ*. Het resultaat is je ge-encrypte *K*, die we even *C* noemen. Vervolgens ga je *C* nogmaals machtsverheffen, maar nu met *d modulo PQ* en je komt weer terug bij de oorspronkelijke *K*.

e en *d* zijn encryptie/decryptie-'sleutels" die je via een zeer eenvoudige berekening kunt genereren uit een gegeven *P* en *Q*. Hiervoor gebruik je bijvoorbeeld het vrij beschikbare 'keytool'-programmaatje. Bij een *P*=17 en *Q*=23 'passen' bijvoorbeeld e=7 en *d*=151. De combinatie *e,PQ* noemen we nu de privé-sleutel, de combinatie *d,PQ* de publieke sleutel, maar dat mag ook omgekeerd. De hacker ziet alleen het product *PQ* =391 en/of e of *d*. Zijn uitdaging is uit te zoeken uit welk product van twee priemgetallen *PQ* bestaat. Want alleen dan kan hij de andere e of *d* bepalen en is de encryptie gekraakt. Nu vormt dat voor het getal 391 niet zo'n probleem, maar voor een getal bestaande uit 1024 bits wordt dat een stuk lastiger. Dat is namelijk een getal met 300 cijfers, bijvoorbeeld:

3748927459194857994857909875298375590789459873445597109873597345185784390175019789459873539570978175509874755135873748927459194857994857909875298375590789459873445597109873597345185784390175019789459873539570978175509874755135873748927459194857994857909875298375590789459873445597109873597345185784390175019789459873539570978175509874755135873748927459194857994857909875298375590789459873445597109873597345185784390

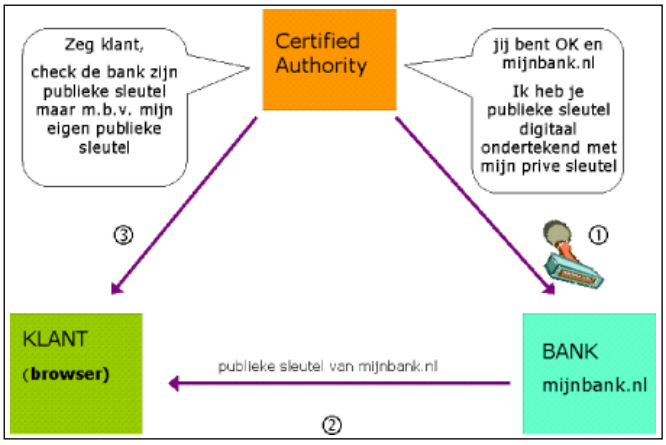
Zelfs met de hedendaagse computers is dit nog steeds een onmogelijke zaak. Conclusie: bij het opzetten van een beveiligde https-verbinding wordt een zeer zware encryptie gebruikt, die men met de huidige IT-middelen normaliter niet kan kraken.

Is internetbankieren veilig? Technisch gezien: ja

Na deze geruststellende constatering gaan we nader in op PKI en SSL. Public Key Infrastructuur (PKI) staat voor een combinatie van maatregelen en technieken om in principe voor jouw onbekende partijen waarmee je over internet communiceert, tóch te vertrouwen. Het Secure Socket Layer-protocol (SSL) is één van die gehanteerde technieken.

PKI

In figuur 1 heeft een klant al contact gelegd met de https-site van de Postbank. Dubbelklikken op het slotje resulteert in het

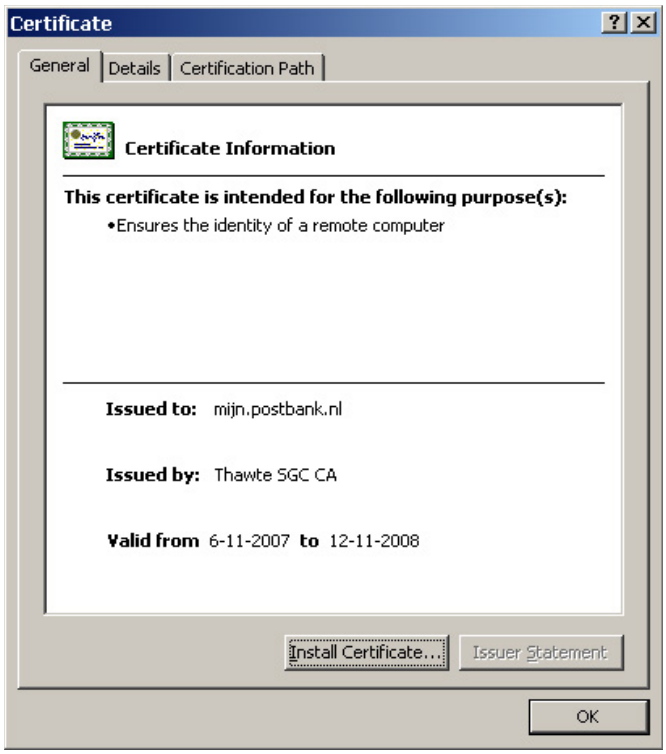


Figuur 3. Weergave van de centrale rol die de Certified Authority speelt

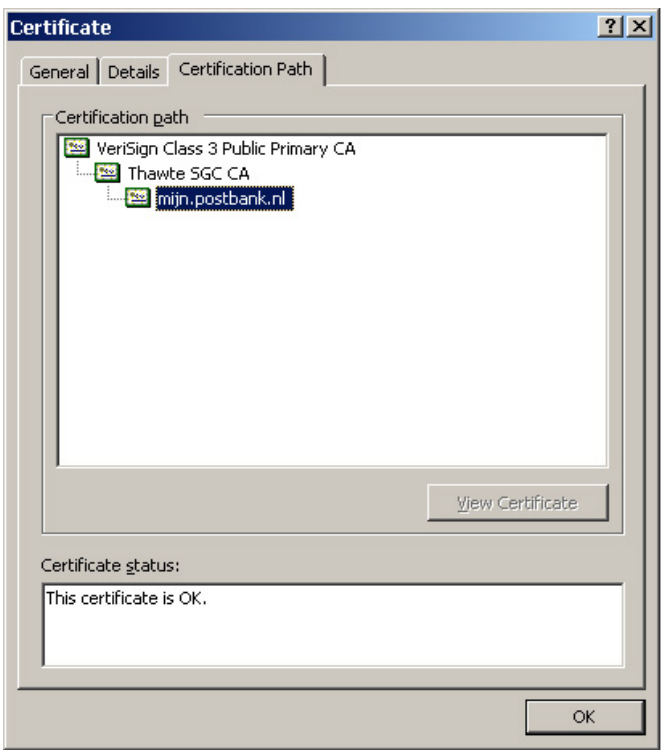
'Certificate'-venster (figuur 2). Onderdeel van het certificaat is de Public Key, RSA 1024 bits.
De browser heeft via het SSL-protocol deze publieke sleutel van de bank gekregen. Met deze publieke sleutel (**e**PQ) kan je vertrouwelijke informatie versleutelen (**e**ncrypten) en naar de bank sturen. Dit versleutelde bericht kan alleen met de privé-sleutel (**d**PQ) van de bank worden ge**d**ecrypt. Die privé-sleutel houdt de bank strikt geheim, dus je hebt de garantie dat je met je eigen vertrouwde bank communiceert. Maar ... is dat wel zo? Die privé-sleutel is misschien wel in handen gekomen van een frauduleuze bankmedewerker. Of die publieke sleutel die ik heb ontvangen is van een criminele organisatie! Oftewel, communiceer ik wel met de instantie met wie ik wíl communiceren?
Om die vraag positief te kunnen beantwoorden worden PKI's ontworpen. Centraal daarbij is een derde partij, de 'Certified Authority' (CA), die garandeert dat ik communiceer met mijn eigen vertrouwde bank.
Dit verloopt via een uitgebreid proces. Op hoofdlijnen gaat dit als volgt (zie ook figuur 3):

- De bank verzoekt CA om de publieke banksleutel ePQ te certificeren.
- De CA stelt de identiteit van de aanvrager vast aan de hand van strikte procedures (bijvoorbeeld Kamer van Koophandel-controle, controle bij de Nederlandsche Bank).
- Als alles goed is bevonden, plaatst de CA een digitale "echtheidsstempel" op de openbare sleutel van de bank. Voor die echtheidsstempel wordt een combinatie gebruikt van hashing-techniek (zie Field "Signature Algorithm" van figuur 2) en RSA-encryptie met de privé-sleutel van de CA.
- De gangbare browsers zijn 'voorgeladen' met tientallen publieke sleutels van wereldwijd erkende CA's. Als de klant contact legt met de bank, ontvangt de browser de gecertificeerde publieke sleutel van de bank. Met de publieke sleutel van de CA kan de browser nu de echtheid van de digitale handtekening en daarmee de echtheid van de openbare banksleutel verifiëren en dus ook de gebruiker waarschuwen als er iets mis is.

De bank wil ook graag weten of achter de browser een echte klant van de bank zit. Voor de authenticiteit van de klant gebrui-



Figuur 4. Het Postbank-certificaat is uitgegeven door de CA "Thawte SGC"



Figuur 5. De hiërarchische opbouw (trust chain) van CA's

Figuur 6. Voorbeeld van de dialoog tussen browser en bankserver

ken de banken verschillende systemen. In het voorbeeld van de Postbank moet de gebruiker een gebruikersnaam/wachtwoord opgeven en bij transacties een zogenaamde TAN-code. Dit alles natuurlijk over een beveiligde SSL-verbinding.

Alles staat of valt met het vertrouwen dat de uitgever van certificaten geniet

PKI-infrastructuren hanteren meestal een zeer uitgebreid stelsel van voorzieningen op organisatorische en technisch niveau. Voor de geïnteresseerden: kijk bijvoorbeeld eens op www.pkioverheid.nl. Of in je Internet Explorer-browser onder menu Tools, Internet Options, tabblad "Content", buttons voor certificaten. Of op de site van de grootste 'root' CA ter wereld: www.verisign.com.

SSL

Het Secure Socket Layer-protocol is een essentieel onderdeel van PKI-infrastructuren over internet. Zodra iemand op de inlog-site van een bank komt, is het beveiligingsslotje te zien en heeft er al een dialoog tussen browser en bankserver plaatsgevonden (figuur 6).

De essentie van het SSL-protocol is om via zware asymmetrische RSA-encryptie een beveiligde verbinding met lichte symmetrische encryptie op te zetten. De lichte symmetrische encryptie met een 128bits-sleutel is zeer veilig, gezien de beperkte duur van een internetbankieren-sessie. De SSL bepaalt de symmetrische encryptie via voorkeurslijstjes in de browser en de server.

Conclusie

En dan nu terugkomend op de openingsvraag: is internetbankieren veilig? Technisch gezien: ja. Het SSL-protocol met 1024bits RS- sleutels en 128bits-sessiesleutels valt praktisch niet te kraken. Organisatorisch gezien: alles staat of valt met het vertrouwen dat de uitgever van certificaten (de CA dus) geniet. Praktisch adviseer ik bij internetbankieren en -winkelen de volgende twee regels te hanteren.

1) Controleer het "general" tabblad van het certificaat. Staat daar een goede url en is de CA een bekende partij? 'Google' desnoods op de naam van de CA voor meer informatie.

2) Geef persoonlijke data zoals creditcardnummer of wachtwoord alleen op als de site "https" is. Voor banken is dit altijd het geval, maar bij sommige winkels niet. In die laatste situatie weet je dat je gegevens onbeveiligd over het internet reizen en dus in handen kunnen vallen van kwaadwillenden.

Gerrit Smink is ICT-architect bij ATOS-Origin.

Atos Origin wint 'Partner of the Year 2008 technology'-award

Oracle kent elk jaar Partner Awards toe aan partners die zich in het afgelopen jaar door hun prestaties en inzet hebben onderscheiden. Dit jaar ging de prijs naar Atos Origin. Caroline Wouters, Alliances & Channels Director Benelux binnen Oracle, reikte de Oracle Award uit tijdens de jaarlijkse Oracle Partner Networking Day. Volgens Wouters was Atos Origin afgelopen jaar zeer succesvol in het aanbieden van Oracle-oplossingen die deels zijn gebaseerd op het Utility Based Grid Concept. Wouters: "Zij investeert pro-actief in Oracle-technologie en standaardoplossingen én in trainingen en skills van haar consultants. Voor deze laatste groep heeft Atos Origin een compleet vernieuwd studiehuis met opleidingen in Jdeveloper, Fusion Middleware en de traditionele Oracle Database opgezet. Bovendien is Atos Origin Certified Advantage Partner en maakt zij actief gebruik van alle mogelijkheden die het Oracle Partner Netwerk biedt."