

AFSCHEID VAN OTP TOKENS

De toekomst is aan smartcards en hybride USB-tokens

OTP tokens zijn naar onze overtuiging een logische, maar tijdelijke stap in de natuurlijke ontwikkeling van sterke authenticatie. Door de acceptatie van PKI wordt bovendien in een sterk groeiend aantal landen het gebruik van OTP tokens in combinatie met AAA servers steeds minder serieus genomen. Ten opzichte van een met PKI geïntegreerde sterke authenticatie oplossing zijn de op OTP tokens gebaseerde systemen immers potentieel minder veilig, vaak duurder, lastiger en minder functioneel schaalbaar, om over 'vendor lockin' nog maar te zwijgen. ROB GREUTER EN LEON KUUNDERS

Vrijwel iedereen in deze maatschappij werkt regelmatig met één of andere vorm van zwakke dan wel sterke authenticatie. Vaak zelfs zonder te beseffen waarom voor het inloggen de ene keer een loginnaam en wachtwoord (zwak) volstaat en voor de andere keer een bankpas en PIN (sterk) nodig is. Met sterke authenticatie bedoelen we feitelijk elk authenticatieprotocol dat twee of meer van elkaar onafhankelijke manieren vereist om de juiste identiteit en privileges te verkrijgen. Die privileges worden vervolgens gebruikt om toegang tot een systeem of applicatie te krijgen. Veel toepassingen zijn gebaseerd op zogenaamde two-factor au-

een vingerafdruk, het stempatroon, de iris of de locatie waar je bent.

Het gebruik van alleen een loginnaam of een wachtwoord noemen we zwakke authenticatie (ook wel *single factor* genoemd). De voordelen van sterke authenticatie liggen voor de hand; gebruikers kunnen niet meer zomaar een wachtwoord 'uitlenen' waardoor misbruik van loginnamen moeilijker wordt. Daarbij wordt het risico op identiteitsdiefstal of misbruik fors gereduceerd, het gokken van een wachtwoord (denk Post-it) of het stelen van een smartcard is niet voldoende. Toch is sterke authenticatie niet zaligmakend. Je hebt immers nog altijd het risico op interventie door bijvoorbeeld

len komen overigens langzamerhand nieuwe, additionele technologische maatregelen beschikbaar (zie kader). Hoe dan ook, sterke authenticatie is en blijft belangrijk en daarmee zelfs een 'no-brainer' standaard authenticatieaanpak voor de meer volwassen organisaties. Een overzicht van de meest toegepaste vormen van sterke authenticatie:

Hardware Tokens

De meest toegepaste vormen van 'iets dat je hebt' zijn tokens en smartcards. Met name tokens zijn flink in ontwikkeling. Zo beschikken moderne USB-tokens, net als smartcards, tegenwoordig ook over een microprocessor, een (Java-) operating system, een encryptie applicatie en opslagruimte. De opslagruimte bij USB-tokens is veel groter dan die van smartcards. Deze zogenaamde hybride tokens (aangeboden door leveranciers als ActivIdentity, Aladdin, Giesecke & Devrient (G&D) en RSA Security) bieden dus de gecombineerde functionaliteit van USB tokens en smartcards in de vorm van een USB token. Daarnaast

De meeste smartcards zijn enkel bedoeld voor netwerkauthenticatie, bekend als smartcard logon

thenticatie. Dat is de combinatie van 1) iets dat je *weet* (de PIN of andere code) en 2) iets dat je *hebt* (bankpas, hardware token, PDA) of een *fysiek kenmerk* zoals

'trojans' en 'man-in-the-middle' aanvallen. In de praktijk brengt dit vooral risico's met zich mee bij authenticatie via het Internet. Tegen dat type aanval-

bestaan er zogenaamde One Time Password (OTP) tokens. Die laten via een LCD-display een getal zien dat om de zoveel seconden verandert. Dit getal wordt door het token berekend uit een statisch getal en de tijd. Doordat het statisch getal bekend is en gekoppeld aan de gebruiker kan het berekende getal worden gebruikt in het login proces. Meestal vervangt het dan het wachtwoord, hoewel het ook als extra verificatiecode gebruikt kan worden.

Smartcards

De meeste smartcards zijn enkel bedoeld voor netwerkauthenticatie, bekend als smartcard logon, of logische toegang. Daarnaast combineren steeds meer smartcard-fabrikanten deze functionaliteit met die van een proximity-card. Hierdoor kan met een smartcard zowel de toegang tot bedrijfsterreinen, gebouwen en ruimtes (bekend als fysieke toegang) als de netwerktoegang geregeld worden. De functionaliteit kan zelfs uitgebreid worden met bijvoorbeeld betaalfuncties voor de koffieautomaat en restaurant, kleding uitgifte-automaten, controle op gebruik van kopieerapparaten, 'employee benefit' zaken en natuurlijk als ID Badge.

Token- smartcard combinatie

Steeds meer fabrikanten van OTP tokens zijn overigens al bezig om de link tussen OTP en PKI te leggen. Een mooi voorbeeld hiervan is de Vasco DP850 die het beste uit beide werelden combineert: ▶

Internetbankieren met beide billen bloot

Sterke authenticatie is het standaardantwoord voor het verkrijgen van vertrouwen van miljoenen klanten in vele financiële Internetproducten zoals Internetbankieren. Een nog onbekend aantal klanten van Citibank's Citibusiness service heeft dat onlangs geweten. Een ijzersterk georganiseerde phishing aanval gecombineerd met een zogenaamd 'man in the middle' scenario heeft het vertrouwen in Two-factor authenticatie met het Internet als medium krachtig aangetast. De noodzakelijke extra en unieke code die het token van de Citibank klanten genereert, werd door de klant gewoon ingevoerd maar door de aanvaller netjes doorgegeven aan het originele loginscherm van Citibank. Ook hield de aanvaller rekening met foutmeldingen om zo authentiek mogelijk over te komen en het gewonnen vertrouwen van de gebruiker te behouden. Iedere zichzelf respecterende bank wist echter dat dit ging gebeuren, de vraag was enkel wanneer en met welke financiële instelling. Bruce Schneier (Counterpane) voorspelde deze aanval voorjaar 2005, ir. Barbara Oosterveld (NedSecure Solutions) deed dat begin 2005.

Uiteraard zijn er allerlei tegenmaatregelen bedacht om dit te

kunnen voorkomen. Bijvoorbeeld door de sterke authenticatie via een ander medium zoals SMS te laten verlopen. Tegen een 'man in the middle'-aanval werkt dit echter niet; de aanvaller zit toch tussen de gebruiker en de website. Meer over deze two-factor spoofing: http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html.

Welke lessen trekken wij hieruit?

1 (Remote) two-factor authenticatie is wel nuttig, maar lost goed beschouwd vooral problemen op die we tien jaar geleden hadden.

2 Het aanpassingsvermogen van cybercriminelen is vele malen hoger dan wij denken en hopen.

Ook klanten van Nederlandse financiële dienstverleners zullen slachtoffer (kunnen) worden van identiteitsfraude. Zijn dit type dreigingen dan op geen enkele manier tegen te gaan? Gelukkig wel! Als je bijvoorbeeld two-factor authenticatie technologie combineert met kort levende client certificaten en het bovendien clients mogelijk maakt om 'phishing sites' te blokkeren op basis van een actuele database is er geen speld meer tussen te krijgen.

- ▶ Smartcard voor cryptografische toepassingen en digitale handtekeningen.
- ▶ OTP generator op basis van het op de smartcard aanwezige 'secret' voor authenticatie.

Hierdoor authenticiseer je op basis van drie factoren (smartcard, PIN en OTP). Let wel, om dat hier sprake is van twee maal 'wat je hebt' blijven we dit two-factor authenticatie noemen.

Sterke authenticatie en PKI

De verschillende authenticatiemiddelen hebben ieder hun eigen specifieke voor- en nadelen. Die zijn afhankelijk van de fabrikant en het toepassingsgebied. Te denken valt dan aan beperkingen door de combinatie van sterke authenticatie met diskencryptie technologie waarbij pre-boot authenticatie vereist is, of de vereiste dat men niet vast wil zitten aan één fabrikant ten aanzien van functionele schaalbaarheid, centrale beheeraspecten of prijstechnische zaken. Een essentieel aspect hierin is de keuze voor de authenticatieserver. Wil men werken met een AAA server (die gebruikt wordt voor authenticatie, autorisatie en administratie) of de sterke authenticatie integreren met een PKI (gebaseerd op de digitale handtekening)?

waardoor PKI eindelijk in staat is bij te dragen aan de zakelijke doelstellingen. Betrouwbare authenticatie is één van die doelstellingen, omdat men wil weten wie gebruik maakt van de informatiebronnen op het netwerk.

Verschillen tussen beide systemen

Zoals uit het kader blijkt zijn de verschillen tussen OTP-authenticatie en PKI-authenticatie aanzienlijk. De vendor lockin die bij OTP bestaat is het eerste verschil. De toepasbaarheid van PKI-authenticatie het tweede. Verder wordt de PKI-smartcard ook gebruikt voor de digitale handtekening. Dat kan niet bij OTP, want een OTP-systeem is (in PKI-termen) gebaseerd op het delen van de privé sleutel. Een digitale handtekening die gebaseerd is op een

die bovenaan de wensenlijst staat bij organisaties. Smartcards hebben daarvoor wel de goede (en gestandaardiseerde) afmetingen. De sterke groei van draadloze toepassingen zorgt ervoor dat contactloze smartcards over enkele jaren de positie van hybride USB tokens zullen overnemen.

Wat betreft gebruikersvriendelijkheid: gebruikers moeten algemeen bekend zijn met smartcards, met als in het oog springend voorbeeld de bankpas en de chipknip. De daarvoor gebruikte magneetstrip en contactchip worden op dit moment al vervangen door korte afstand draadloze technologie. Door het samengaan van fysieke en logische toegangsbeveiliging worden de beheerlasten lager. En dankzij de voorstellen voor open standaarden

| Type organisatie | Land | Authenticatiemiddel | Aantal |
|----------------------------|-------------|-------------------------|------------|
| Verzekeraar | Duitsland | Smartcards | 20.000+ |
| Verzekeraar | Duitsland | Smartcards + USB tokens | 40.000+ |
| Internet bank | China | Smartcards + USB tokens | 500.000+ |
| Internet bank | China | USB tokens | 60.000+ |
| Internet bank | China | USB tokens | 10.000+ |
| Internet bank | China | Smartcards + USB tokens | 5.000+ |
| Internet bank | China | USB tokens | 10.000+ |
| Oliemaatschappij | Noorwegen | Smartcards | 30.000+ |
| Industrie | Spanje | Smartcards | 12.000+ |
| Electronisch stemmen pilot | Spanje | Smartcards | 4.000+ |
| Bank | Spanje | Smartcards | 7.000+ |
| Nationale ID kaart | Taiwan | Smartcards | 1.000.000+ |
| Hypotheekbank | Zwitserland | Smartcards + USB tokens | 5.000+ |

Overzicht van enkele authenticatieprojecten waarbij smartcard/USB-tokens geïntegreerd worden met PKI.

Traditioneel zijn OTP-tokens gekoppeld aan een AAA-server en smartcards aan zowel een AAA-server als een card management systeem

Traditioneel zijn OTP-tokens gekoppeld aan een AAA-server en smartcards aan zowel een AAA-server als een card management systeem (van dezelfde fabrikant uiteraard). Sinds enkele jaren beweegt de trend zich richting integratie van smartcards in een PKI. PKI is immers volwassen geworden qua technologie, standaardisatie, internationale acceptatie en prijsstructuur. De PKI-componenten zijn door de brede ondersteuning inmiddels een integraal onderdeel geworden van de technische infrastructuur. De focus in de PKI-markt is daardoor gewijzigd van technologie naar ondersteuning

dergelijk systeem voldoet dus niet aan de wettelijke vereiste dat de privésleutel enkel bekend is aan en te gebruiken door de eigenaar.

Over de hybride USB tokens kan nog worden gezegd dat ook dit feitelijk een overgangstechnologie betreft. Enerzijds komt dit doordat een hybride toepassing aan meer risico's bloot staat. Er zijn al virussen ontwikkeld specifiek voor de 'slimme' USB flash drives. Dat is onwenselijk voor een authenticatietechnologie. Verder kan zo'n hybride token niet als ID-badge worden gebruikt. Het kunnen personaliseren van een token is belangrijke functionaliteit

(zie het OATH-platform) voor sterke authenticatie kan het aantal passen dat gebruikt moet worden omlaag.

Smartcard gebaseerde authenticatiesystemen kennen uiteraard ook nadelen, deze wereld is immers niet zwart/wit. Zo kun je een smartcard natuurlijk niet aan je sleutelbos hangen wat nu net wel zo gemakkelijk kan bij OTP- en USB-tokens. Van grotere impact zijn de feiten dat smartcard systemen altijd een smartcard reader nodig hebben (al of niet ingebouwd) en altijd client software vereisen. Essentiële zaken waarop niet iedere organisatie zit te wachten.

Bewijsmateriaal

Het is natuurlijk altijd gemakkelijk om meningen en trends als harde feiten neer te zetten. Daarom is enige bewijsvoering op zijn plaats: de tabel toont een overzicht van enkele authenticatieprojecten waarbij smartcard/USB-tokens geïntegreerd worden met PKI. Dit lang niet uitputtende overzicht geeft duidelijk aan dat het hier beslist niet gaat om een niche in de authenticatiemarkt. Integendeel, het gaat – in toenemende mate en onomkeerbaar – om grote projecten van grote genommerde organisaties en vaak in landen waarvan wij al snel denken dat ze daar achterlopen. Als je bedenkt dat een goed deel van deze projecten al medio 2002 zijn gestart, zijn wij het juist die achterlopen!

Voor de goede orde, het betreft hier ter illustratie projecten met de smartcard/USB token middleware-oplossingen van partijen zoals AET Europe, Getronics PinkRocade en TrustAlert, deels in samenwerking met het Duitse G&D, een van de grootste fabrikanten wereldwijd van smartcards en USB tokens. De toegepaste functionaliteit binnen deze projecten beslaat zo'n beetje iedere functionaliteit die je kunt bedenken, van eenvoudige netwerkauthenticatie tot e-mail versleuteling tot digitale handtekeninggestuurde workflow alsmede Electronische Nationale Identiteitskaart (ENIK).

Conclusie

OTP-tokens en traditionele AAA-servers hebben hun diensten bewezen. De onafwendbare volgende stap is het gebruik van smartcards en hybride USB-tokens in combinatie met PKI, en waar mogelijk het combineren van fysieke en logische toegangscontrole. Deze vervolgroute zal voor veel organisaties drempelverlagend werken bij het gebruik van sterke authenticatie.

Rob Greuter is Senior Adviseur Informatiebeveiliging bij NedSecure Solutions en per e-mail te bereiken via rob.greuter@nedsecure.nl.

Leon Kuunders is Senior Adviseur Identity Management bij Trusted-ID en per e-mail te bereiken via leon@trusted-id.nl.

OTP systemen

OTP systemen worden door diverse leveranciers aangeboden, zoals Aladdin, ActivIdentity en RSA Security. Deze tokens hebben als een belangrijk voordeel dat ze platformonafhankelijk zijn: ze werken onafhankelijk van aanwezige hardware, behoeven geen client software en kunnen dus overal gebruikt worden.

Een OTP systeem werkt met een 'shared secret'. Dit statische getal, zoals het eerder werd genoemd, is zowel opgenomen in het token als in de centrale database van de authenticatie server. Hiermee is direct duidelijk welke nadelen aan een OTP systeem kleven. Doordat het systeem is gebaseerd op een geheim is het niet mogelijk het OTP token op plaatsen buiten de eigen organisatie in te zetten. Hierdoor ontstaat vendor lockin. Daarbij bestaat het risico dat de centrale database wordt gekraakt, waardoor de betrouwbaarheid van het authenticatieproces aanmerkelijk verlaagd wordt.

PKI-systemen

Van hype naar realiteit is het motto bij PKI. Deze technologie werd jaren geleden gebruikt om enorme investeringen in Internet goed te praten. PKI was het toverwoord voor veilige en betrouwbare online transacties. Bijna risicoloos. Leveranciers van certificaten deden goede zaken, niet in de laatste plaats door de

onwetendheid bij de afnemers. PKI-ontwerpen waren per definitie gedreven door de technologie. Zakelijke doelstellingen werden daardoor nogal eens uit het oog verloren. Trusted-Third-Parties deden hun best de PKI markt in hun greep te krijgen. Ze faalden. Erger nog, ze bleken al snel het single-point-of-failure in het PKI-vertrouwenssysteem te zijn.

Inmiddels is er veel veranderd. De technologie an sich is op de achtergrond geraakt terwijl de praktische toepassing juist integraal onderdeel is geworden van de infrastructurele componenten. Ook heeft het geholpen dat PKI is gebaseerd op open standaarden die daadwerkelijk interoperabel zijn. Wetgeving heeft een extra impuls gegeven aan de toepassingsgebieden van deze technologie. Door deze veranderingen is de focus van PKI gewijzigd naar het gebruik ervan. Ook wordt duidelijk waar PKI wél goed voor is: authenticatie.

Identity- & access-management

Respect moet je verdienen, zoals PKI heeft ondervonden. PKI is dan ook allang niet meer de fonkelende ster aan het firmament maar wel een solide belichtingsplan; het is een gewillige bouwsteen geworden van het vakgebied Identity & Access Management. In dit vakgebied speelt authenticatie een belangrijke rol en kan PKI eindelijk zijn waarde laten zien.