Veilig en comfortabel: thin en zero clients met smartcards

Door de toenemende afhankelijkheid van IT-systemen en cloudservices wordt databeveiliging voor interne en externe communicatie steeds belangrijker. Gecombineerd met smartcards bieden thin en zero clients van IGEL op betrouwbare wijze bescherming tegen manipulatie, gegevensdiefstal en andere bedreigingen.

Inhoud:

- Waartegen bieden smartcardoplossingen bescherming?
- Wat zijn de typische toepassingsscenario's?
- Welke smartcardtypen en -oplossingen zijn er?
- Hoe kunnen geheugen- en processorkaarten zinvol en efficiënt worden gecombineerd met thin en zero clients?
- Welke voordelen zijn er op het gebied van mobiliteit en productiviteit?

IGEL® TECHNOLOGY

Thin resp. zero client met geïntegreerde smartcardlezer: de IGEL UD3 / IZ3

Veel werkgevers veronachtzamen de bescherming tegen computercriminaliteit en laten hun medewerkers in de steek als het gaat om IT-beveiliging. Tot deze conclusie komt een representatief onderzoek, uitgevoerd in opdracht van de Duitse hightech-organisatie BITKOM. Bijzonder alarmerend is het feit dat 40 procent van de medewerkers niet weet hoe zij met wachtwoorden of externe media zoals USB-sticks moet omgaan. Om bedrijfskritieke gegevens afdoende tegen onbevoegde toegang te beveiligen, voldoet de combinatie van gebruikersnaam en wachtwoord vaak niet meer en een goedbedoelde aanscherping van de richtlijnen voor wachtwoorden strandt steeds vaker op de bijkomende neveneffecten van complexe IT-omgevingen.

Gevaarlijke wachtwoordchaos

Een grotere kans op gevaren, de toenemende complexiteit van het gebruik van IT en externe of mobiele toegang tot het bedrijfsnetwerk, maken het proces van authenticatie steeds ingewikkelder. Een diversiteit aan toepassingen, desktops en cloudservices vraagt om een eenduidige procedure om de toegangsrechten te regelen. E-mailclients, databases, bedrijfstoepassingen als SAP of CRM, centrale IT-omgevingen, veilige "virtuele ruimtes" voor projectdeelnemers of het intranet hebben geleid tot een onoverzichtelijke en riskante hoeveelheid aan wachtwoorden, pincodes en toegangs-ID's, die gebruikers bovendien met net als fysieke beveiligingsobjecten als sleutels, chipkaarten, badges of tokens moeten bewaken. Het gevolg hiervan is dat de overbelaste gebruikers hun wachtwoorden op memoblaadjes schrijven of ze op slaan op hun mobiele telefoon.

In veel sectoren worden thin en zero clients gebruikt...

Met name voor organisaties die te maken hebben met persoonsgegevens of andere gevoelige, bedrijfskritieke informatie, is de noodzaak hoog om actief op te treden, zodat tevens de authenticatie-data afdoende tegen spionage en diefstal wordt beschermd – zowel van binnenuit als van buitenaf. Onder deze sectoren vallen bijvoorbeeld banken, verzekeringsmaatschappijen, administratieve dienstverleners en de gezondheidszorg. Maar ook specifieke afdelingen binnen organisaties zoals controlling, de boekhouding, research en development, verkoop en personeelszaken vallen onder deze categorie. Om de gegevensopslag consequent te centraliseren en lokale opslagmedia zoals USB-sticks eenvoudig en afdoende te reglementeren, kiezen steeds meer organisaties voor cloud-omgevingen met thin of zero clients, die in vergelijking met werkplek-PC's grote voordelen op het gebeid van beveiliging bieden. Zo staan de kosten- en energie-efficiënte apparaten bijvoorbeeld geen lokale gegevensopslag toe. Bovendien verhinderen het read-only geheugen en het besturingssysteem dat virussen, trojaanse paarden en andere malware zich op de apparaten nestelen.

… in combinatie met smartcards

Om daarnaast grip te krijgen op het wachtwoordrisico, worden wereldwijd als technische oplossing zogenaamde smartcards geïntroduceerd – kunststof kaarten in creditcardformaat, die doorgaans een chip met

TOEPASSINGSVOORBEELDEN

SECTOR	PROCESSORKAART	GEHEUGENKAART
Universiteiten	—	Toegangskaarten
Bankwezen	Chipknip	—
Ziektekostenverzekeraars	Gezondheidszorgkaarten	Ziekteverzekeringskaarten
Overheid	Legitimatiebewijzen	—
Betaaltelevisie	Decoderkaarten	—

hardwarelogica, geheugen of zelfs een microprocessor bevatten. Vergeleken met magneetstripkaarten zijn deze “minicomputers” breed inzetbaar en gaan ze veel langer mee. Smartcards kunnen tot 100.000 keer worden gelezen. Ze zijn ongevoelig voor magnetische velden en – dankzij een ingebouwde bescherming tegen overspanning – ook tegen ontladingen. Voor het gebruik van de smartcard is een smartcardlezer noodzakelijk, die ofwel in de computerbehuizing is ingebouwd of via USB (eventueel ook serieel) met het systeem wordt verbonden. De smartcardlezer heeft tot taak de microprocessor van de kaart van stroom te voorzien. Via het stuurprogramma communiceren de toepassingen op het systeem vervolgens met de betreffende smartcard.

Slim en programmeerbaar

De belangrijkste eigenschap van een smartcard is de “intelligentie”, oftewel de programmeerbaarheid. De kaart kan bijvoorbeeld voor externe applicaties onleesbare keys bevatten, die alleen bruikbaar zijn voor de toepassingen die op de smartcard zelf worden uitgevoerd. Moderne authenticatieprocedures maken gebruik van het zogenaamde “challenge/response-mechanisme”. Daarbij moet telkens op een andere vraag het juiste antwoord worden gegeven. Smartcards hebben in principe voldoende intelligentie en geheugen om ook complexe beveiligingsprocessen zoals identificatie- en authenticatieprocedures alsmede de modernste versleutelingstechnologieën aan te kunnen. Afhankelijk van de profielschets worden daarbij kaarten met verschillende capaciteiten ingezet.

Geheugen- en processorchipkaarten...

Het goedkoopste basistype smartcard is de zogenaamde geheugenchipkaart (ook wel synchrone chipkaart). Deze bestaat in feite uit meerdere keren te beschrijven geheugen, met cellen die de smartcardreader sequentieel uitleest via de bijbehorende interface. Geheugenchipkaarten zijn te kopiëren en worden daarom alleen gebruikt voor opslag van gegevens, niet voor beveiliging tegen onbevoegd uitlezen of manipulatie. Het meest intelligente type smartcard, de processorchipkaart (ook wel asynchrone chipkaart), werkt anders. De microprocessor die in het binnenste van de plastickaart is gelast verhindert door middel van cryptografische procedures onbevoegde toegang tot de opgeslagen gegevens. Veelgebruikte worden bijvoorbeeld betaalkaarten, gezondheidspassen en identiteitsbewijzen met persoonsgegevens, maar ook decoderkaarten, die via een certificaat televisiesignalen decoderen.

…maken thin en zero clients nog veiliger

Als het gaat om snel, veilig en makkelijk wisselende personen toegang te bieden tot centrale gegevens, zijn de goedkopere geheugenkaarten meestal de eerste keuze. Daarmee krijgen bijvoorbeeld artsen of verpleegkundigen in ziekenhuizen zonder veel authenticatie-inspanning op verschillende plaatsen en afdelingen toegang tot de voor hen vrijgegeven patiëntengegevens, het ziekenhuisinformatiesysteem of inventarisdatabases. Hetzelfde geldt voor bibliotheken waarbij bezoekers specifiek toegang nodig hebben tot gebruikersafhankelijke zoekomgevingen en toch gebruik maken van algemeen toegankelijke thin clients, zero clients of softwarematige thin clients – waarbij een thin client-besturingssysteem van een gestandaardiseerde pc of notebook effectief een thin client maakt.

DOOR IGEL ONDERSTEUNDE SMARTCARDOPLOSSINGEN EN LEESAPPARATEN (KEUZE)

AANBIEDERS	SMARTCARDS/LEZERS
A.E.T. Europe B.V.	SafeSign
Aladdin	Aladdin eToken en Smartcard
Athena	IDProtect
Deutscher Sparkassen Verlag	Smartcards/lezers
IGEL Technology	IGEL Smartcard
Gemalto	IDPrime .NET
geNUA	GeNUCard
HID	Omnikey (alleen leesapparaat)
Reiner SCT	cyberJack (leesapparaat)
SecMaker	NetID
TeleSec	TCOS

Ingebouwde en externe smartcardlezers

Omdat veel van deze toepassingen overeenkomen met de inzetscenario’s van thin en zero clients, integreren enkele fabrikanten smartcardlezers direct in de devices. Een pionier op dit gebied is IGEL Technology. De huidige thin client-modellen van IGEL - UD3, UD5, UD9 en UD10 - en de zero client IZ3 zijn indien nodig verkrijgbaar met een ingebouwde smartcardlezer. Dankzij de PC/SC-interface (personal computer/smartcard) zijn de geïntegreerde lezers geschikt voor alle soorten smartcards en een veelvoud aan oplossingen. Daarnaast ondersteunt IGEL voor de meeste IGEL-modellen, en voor met IGEL Universal Desktop Converter 2 (UDC2) samengestelde systemen ook veel externe PC/SC-lezers (zie tabel).

Efficiënt en veilig: de IGEL Smartcard

Een bijzonder betaalbare oplossing voor authenticatie is de IGEL Smartcard. Deze is gebaseerd op een geheugenkaart waarop verschillende gegevens, zoals de authenticatiegegevens van gebruikers, worden opgeslagen. Vóór de uitgifte wordt de betreffende kaart door de netwerkbeheerder via de Setup op de juiste wijze ingesteld, zodat de gebruiker bijvoorbeeld meerdere gebruikersspecifieke sessies kan openen zonder telkens een wachtwoord te moeten invoeren. Hiermee worden voor gebruikers al enkele belangrijke en comfortabele oplossingen voor toegang tot IT-omgevingen ondersteund, zoals Citrix XenApp/XenDesktop, VMware Horizon of Microsoft Remote Desktop Services (RDS). Zo kunnen bijvoorbeeld lokale, virtuele of cloud-toepassingen automatisch worden gestart op het moment dat de IGEL Smartcard in de lezer wordt geschoven. Bij het verwijderen van de IGEL Smartcard, wordt de thin of zero client automatisch geblokkeerd. De lopende sessie op basis van Citrix HDX, PCoIP (VMware) of Microsoft RDP respectievelijk RemoteFX, worden ontkoppelt en er verschijnt een screensaver met loginscherm, waarin de gebruiker zich opnieuw kan aanmelden met de smartcard en pincode om terug te komen in de eigen sessie.

Een hoge mate van beveiliging met processorkaarten

De meest gebruikte toepassingen voor identificatie en authenticatie door middel van processorkaarten zijn elektronische identiteitsbewijzen, zoals het Duitse persoonsbewijs met elektronisch identiteitsbewijs (ePerso), het Nederlandse UZI-pas of het Belgische eID. In de Duitse gezondheidszorg wordt veel gebruik gemaakt van de elektronische gezondheidskaart (eGK), in combinatie met een in een Cherry-toetsenbord geïntegreerde smartcardlezer. In de financiële dienstverlening zijn naast Cherry- ook DESKO-toetsenborden populair. In het hoger onderwijs zorgen externe smartcardlezers en processorkaarten voor toegang tot datacenters, netwerkprinters en bibliotheken. De verschillende gebruikersgroepen van de servergebaseerde IT-architectuur – studenten, bezoekers of externe wetenschappers – krijgen daarbij verschillende toegangsrechten tot het intranet, verschillende databases, gevirtualiseerde toepassingen en bureaubladen of afdrukfuncties. De op certificaten gebaseerde authenticatie van de betreffende gebruikersgroep vindt puur via de smartcard plaats of wordt als tweeweg-authenticatie aangevuld met een pincode, die bij bijzonder hoge beveiligingsvereisten op een van het eindapparaat gescheiden terminal moet worden ingevoerd.

SLIM MAAKT MOBIEL: SESSIE-ROAMING EN DELEN VAN HET BUREAUBLAD

- De IGEL Smartcard en andere geheugenkaarten worden vaak gebruikt in combinatie met werkplek-roaming. Als de kaart uit de lezer wordt gehaald, onderbreekt het systeem de actuele sessie met de centraal beschikbaar gestelde toepassingen, virtuele workspaces of cloudservices. De sessie draait echter centraal op de achtergrond verder en kan heel eenvoudig op een willekeurige andere thin of zero client in het netwerk worden voortgezet door simpelweg de kaart weer in de lezer te steken. De met sessie-roaming aangeduide functionaliteit vormt een goede invulling van moderne kantoorconcepten zoals het flexkantoor, om mobiliteit van medewerkers, samenwerking en uiteindelijk productiviteit te bevorderen. Andere toepassingsgebieden voor sessie-roaming zijn bijvoorbeeld te vinden bij ziekenhuizen en bibliotheken.

PKI, digitale handtekening en single sign-on (SSO)

Processorkaarten worden ook gebruikt voor uiterst veilige authenticatie binnen een Public Key Infrastructure (PKI). In tegenstelling tot traditionele versleuteling, waarbij beide partijen van het legitimatieproces dezelfde key nodig hebben, zijn de keys voor encryptie- en decryptie bij het public key-proces verschillend. Voor decryptie zijn een openbare en een privé sleutel vereist (public en private key). De openbare sleutel is voor iedereen toegankelijk en wordt gebruikt voor het versleutelen van informatie en het versturen ervan naar de ontvangende personen. Deze decoderen de ontvangen gegevens uiteindelijk met hun privésleutel. Op

UITERST VEILIGE THUISWERKPLEKKEN

- Voor een zeer goed beveiligde externe toegang tot IT via een smartcard, kan gebruik worden gemaakt van de combinatie van een IGEL thin client met de niet-manipuleerbare oplossing “Mobile Security Device geNUCard”. Aansluiten en stroomvoorziening gebeurt via USB, de authenticatie en key-handling door middel van een smartcard. Een geïntegreerde firewall garandeert veilige VPN-datacommunicatie via DSL, ISDN, UMTS of WLAN. geNUCard is door het Duitse “Bundesamt für Sicherheit in der Informationstechnik (BSI)” goedgekeurd voor de versleutelde uitwisseling van geclassificeerde gegevens en is in combinatie met IGEL thin en zero clients gecertificeerd. De oplossing voldoet aan de verschillende eisen voor geheimhoudingsplicht VS-NfD, NATO Restricted en Restreint UE. Bovendien maakt geNUCard ook een absoluut veilig thin client-beheer mogelijk, omdat de oplossing de bij alle IGEL thin, zero en software-thin clients meegeleverde IGEL Universal Management Suite (UMS) voor beheer op afstand ondersteunt.

deze wijze worden digital signature fraudebestendige “handtekeningen” gemaakt, die de echtheid van documenten bevestigen. Naast een veilige authenticatie vormt de digitale handtekening ook de basis voor een tijdsbesparende single sign-on (SSO). SSO-oplossingen geven gebruikers na een eenmalig bewijs van hun identiteit toegang tot alle toepassingen en hulpbronnen die voor hen zijn vrijgegeven. Natuurlijk moet de privésleutel altijd geheim worden gehouden. Opgeslagen op een smartcard is deze aanzienlijk beter beveiligd dan met een wachtwoord.

Smartcards – gewoon veiliger

100 procent beveiliging is natuurlijk ook met smartcards niet gegarandeerd. Geheugenkaarten kunnen worden gekopieerd en processorkaarten kunnen aan derden worden doorgegeven. Maar de criminele inspanningen om onbevoegd toegang te krijgen, zijn aanzienlijk groter dan in omgevingen met uitsluitend wachtwoordbeveiliging. Met thin en zero clients biedt IGEL de ideale omstandigheden voor een efficiënte en effectieve inzet van smartcards. Naast de veilige tweefactor-authenticatie zorgen deze met single sign-on en sessie-roaming voor een hogere productiviteit bij de dagelijkse computerwerkzaamheden. Welke smartcardoplossing de juiste is, hangt ook af van het vereiste beveiligingsniveau. Met de IGEL Smartcard en optionele ingebouwde smartcardlezers toont de fabrikant tevens aan dat een goede smartcardoplossing niet veel hoeft te kosten.

Welke oplossing een organisatie uiteindelijk ook kiest, de investering betaalt zich vaak alleen al terug doordat het vertrouwen sterk toeneemt. Met name wanneer hiermee imago-schade of misschien wel boetes vanwege gegevensverlies worden voorkomen.

DE

DUITSLAND (HOOFDKANTOOR)
IGEL Technology GmbH
Hanna-Kunath-Str. 31
D-28199 Bremen | Duitsland
Telefoon +49 421 52094-0
info@igel.com | www.igel.de

AU

AUSTRALIË
IGEL Technology Pty. Ltd.
Level 32 | 101 Miller Street
North Sydney, NSW, 2060 | Australia
Telefoon +61 432103599
info@igel.com | www.igel.com

AT

OOSTENRIJK
IGEL Technology
Zweigniederlassung Österreich
Wienerbergstraße 11/A12
Vienna Twin Towers
1100 Wenen | Oostenrijk
Telefoon +43 1 99 460-6238
info@igel.com | www.igel.com

BE

BELGIË
IGEL Technology BVBA
Researchpark Haasrode 1820
Interleuvenlaan 62
3001 Leuven (Heverlee) | België
Telefoon +32 16 39 47 57
info@igel.com | www.igel.com

CH

ZWITSERLAND
IGEL Technology GmbH
Zweigniederlassung Schweiz
World Trade Center
Leutschenbachstraße 95
8050 Zürich
Telefoon +41 44 308 37 41
info@igel.com | www.igel.com

CN

HONG KONG
IGEL Technology
Care of: Melchers (H.K.) Ltd.
1210 Shun Tak Centre | West Tower
168-200 Connaught Road C.
Hong Kong | China
Telefoon +852 2546 9069
infohk@igel.com | www.igel.com

BEIJING
IGEL Technology
Care of: Melchers Beijing Ltd.
Beijing Tower | Room 503-504
10 Changan Ave. (East)
Beijing 100006 | China
Telefoon +86 10 65257775
info@igel.com | www.igel.com/cn

SJANGHAI
IGEL Technology
Care of: Melchers (Shanghai) Ltd.
13 Floor | East Ocean Centre
588 Yanan Road (East)
Sjanghai 200001 | China
Telefoon +86 21 6352 8848
info@igel.com | www.igel.com/cn

GUANGZHOU
IGEL Technology
Care of: Melchers Guangzhou Ltd.
Room 1108 | T.P. Plaza
9/109 Liu Hua Road
Guangzhou 510010 | China
Telefoon +86 20 8666 8700
info@igel.com | www.igel.com/cn

FR

FRANKRIJK
IGEL Technology
57, Esplanade du Général de Gaulle
92081 PARIS LA DEFENSE CEDEX
Telefoon +33 1 46 96 56 89
france@igel.com | www.igel.fr

NL

NEDERLAND
IGEL Technology
Orteliuslaan 850
3528 BB Utrecht
Telefoon +31 30 767 1055
benelux@igel.com | www.igel.nl

SE

ZWEDEN
IGEL Technology
Fridhemsgatan 94D
854 61 Sundsvall | Zweden
Telefoon +46 70 267 16 16
info@igel.com | www.igel.com

SG

SINGAPORE
IGEL Technology
Care of: C. Melchers GmbH & Co.
Singapore Branch | 101 Thomson Road
24-01/05 United Square
Singapore 307591
Telefoon +65 6259 9288
info@igel.com | www.igel.sg

UK

GROOT BRITTANIË
IGEL Technology Ltd
Merlin House, Brunel Road
Theale | Reading | Berkshire
RG7 4AB | Groot Brittanië
Telefoon +44 118 340 3400
info@igel.com | www.igel.co.uk

US

VERENIGDE STATEN
IGEL America Sales Corporation
616 Corporate Way, Suite 2-3263
Valley Cottage | NY 10989 | USA
Telefoon +1 610 420 7470
info@igel.com | www.igel.com

IGEL Technology America, LLC
2106 Florence Avenue
Cincinnati | OH 45206 | USA
Telefoon +1 954 739 9990
Gratis (alleen in de VS): +1 877 GET IGEL
info@igelamerica.com | www.igel.com