Sleutelbeheer: noodzaak bij een veilig Internet

Samenvatting
Voor het beveiligen van verkeersstromen over het Internet of een intranet is één van de mogelijke maatregelen encryptie. Met cryptografische technieken kunnen diverse doeleinden worden bereikt namelijk vertrouwelijkheid, integriteit en zelfs onweerlegbaarheid. Naast de meestal publiekelijk bekende en bewezen sterke mathematische algoritmen zijn de sleutels de belangrijkste factor in ieder systeem. Daarmee is het van belang dat de wijze waarop de sleutels worden beheerd voldoet aan strikte beveiligingseisen. Het beheer beslaat de gehele levenscyclus van de sleutels: generatie en registratie, distributie, opslag, gebruik en vernietiging.

1. Inleiding Cryptografie

Wat is het

Cryptografie is de kunst van geheimschrift. Het bestaat al eeuwen om de inhoud van berichten te verhullen voor mogelijke tegenstanders.

Er zijn vele en gevarieerde technieken beschikbaar ten behoeve van cryptografie maar ze zijn allen gebaseerd op een drietal elementen: een algoritme of een mathematisch proces om in combinatie met een sleutel de te beschermen data zodanig te verhullen dat uitsluitend door de bedoelde ontvanger er een boodschap van kan maken. Hiermee wordt vertrouwelijkheid bereikt.

Wat kan het

Met encryptie zijn een drietal voor business zeer belangrijke resultaten te bereiken:

1. vertrouwelijkheid - het zodanig verhullen van data dat deze alleen voor de bedoelde ontvanger waardevol is
2. integriteit - het beschermen van data door een controlegetal zodat iedere wijziging direct te onderkennen is
3. bericht authenticatie - het "digitaal tekenen" van een bericht zodat de afzender daarmee te herkennen is.

Door deze drie mogelijkheden te combineren zijn er zodanige waarborgen te creëren dat e-commerce mogelijk wordt.

Waarom heb je het nodig

Om zaken over het Internet te kunnen doen is het noodzakelijk om vertrouwen te hebben in het kunnen afronden van een transactie. Dit is niet anders dan in de papieren wereld. Cryptografie maakt het mogelijk een toereikend niveau van vertrouwen te bereiken.

Wie heeft ermee te maken

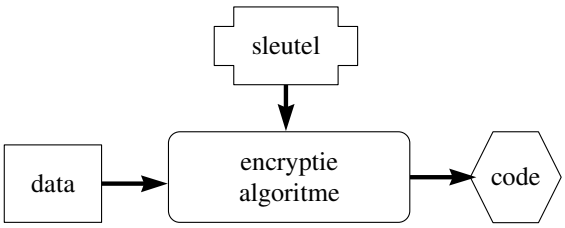
Binnen een organisatie hebben vaak meer personen met cryptografie te maken dan verwacht. Het zit bij de beleidsafdeling, deze dient aan te geven welke mate van bescherming dient te worden aangebracht, dan wel uit te drukken hoeveel belang een organisatie er aan hecht om de gegevens vertrouwelijk en integer te houden. Dit kan door een beveiligingsadviseur worden vertaald naar een of meer algoritmes, sleutelkwaliteit en procedures.
Daarnaast zit het bij de desktop-beheer en netwerk-beheer afdelingen. De desktop-beheerders krijgt te maken met onder andere browser-instellingen, de netwerkbeheerders mogelijk met (huur)lijn-encryptors, encrypting routers en/of virtuele prive netwerken.
Verder is er de applicatieontwikkelafdeling die een aantal maatregelen moeten treffen om de applicaties veilig te maken.

2. Sleutel systemen

Het aspect waar het meestal om gaat is niet de data noch de algoritmes, maar het sleutelbeheer. Het is van belang voordat er wordt ingegaan op sleutelbeheer eerst de globale werking van en de verschillen tussen de twee belangrijkste technieken te onderkennen, zijnde:

1) geheime sleutel systemen
2) publieke sleutel systemen

Uiteraard zijn beide systemen gebaseerd op de combinatie van een algoritme en een sleutel (zie figuur 1).

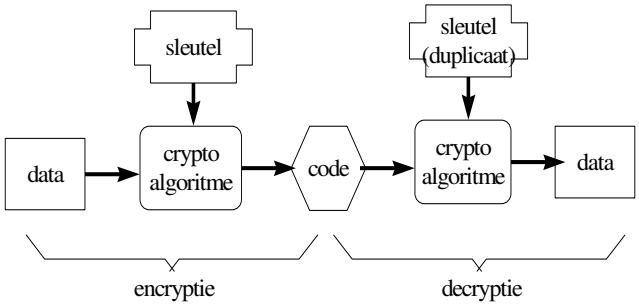


Figuur 1 Basisproces cryptografie

Geheime sleutel systemen

De essentie van een cryptografisch systeem gebaseerd op geheime sleutels is dat dezelfde sleutel wordt gebruikt om een bericht te encrypten en om het te decrypten. Zodoende dat deze systemen ook wel worden aangeduid als "symmetrisch".

De meest gebruikte algoritmes zijn hierbij DES (Data Encryption Standard, IDEA (International Data Encryption Algorithm) en RC4 (Rivest Cipher 4). Vele financiële instellingen krijgen door hun nationale toezichthouder de verplichting om DES of de zwaardere uitvoering ervan 3DES te gebruiken. RC4 is een onderdeel van de door Netscape ontwikkelde SSL (Secure Socket Layer) bescherming van HTTP.



Figuur 2 Encryptie en decryptie met geheime sleutel systemen

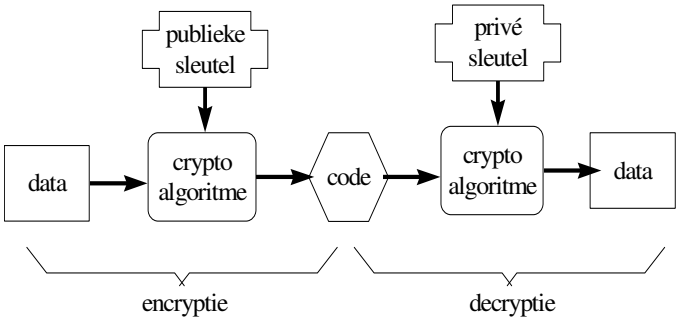
Essentieel aan een geheim sleutelsysteem is dat een ieder die in een berichtuitwisseling deelneemt over een exemplaar van de sleutel moet beschikken, maar dat deze geheim blijft voor anderen. Daarnaast moet deze sleutel zo lang zijn dat de gewenste mate van bescherming wordt bereikt. Verder is het noodzakelijk regelmatig van sleutel te wisselen om de hoeveelheid onthulde data te beperken in het geval dat een sleutel wordt gekraakt.

Publieke sleutel systemen

Deze systemen zijn gebaseerd op andere mathematische principes en er worden dan ook andere sleutels gebruikt voor encryptie en decryptie. Vandaar dat deze systemen ook wel worden aangeduid met "asymmetrisch".
Het concept van publieke sleutel cryptografie werd in 1976 geïntroduceerd door Whitfield Diffie and Martin Hellman om hiermee het sleutelbeheer probleem op te lossen.

De twee sleutels worden samen een sleutelpaar genoemd, waarvan er één als "privé" wordt beschouwd en uitsluitend in bezit is van de houder. De andere sleutel is "publiek" en bedoeld om mee te geven aan een ieder die vertrouwelijk met de houder te wenst te communiceren.
Sterker nog: het systeem wordt pas dan interessant als de publieke sleutels vrij beschikbaar zijn voor iedereen. De behoefte van een zender en de ontvanger om geheime sleutels te delen is verholpen: alle communicatie is gebaseerd op alleen publieke sleutels, en geen enkele privé sleutel hoeft ooit verzonden of gedeeld te worden.

De bekendste en meest gebruikte algoritmes zijn: RSA (naar de uitvinders Rivest, Shamir en Adleman), en DSA (Digital Signature Algoritme). Van recentere datum zijn de algoritmes ECC (Eliptic Curve Crypto) en RPK (Raike Public Key). En er is nog meer te verwachten: een 16-jarige jongedame uit de UK heeft een zeer sterk algoritme ontworpen.



Figuur 3 Encryptie en decryptie met een publiek sleutel systeem

Praktijk
In de praktische toepassingen worden de sterke kanten van de bovenstaande sleutelsystemen benut.

Hoewel encryptie mogelijk is met zowel een geheim als een publiek sleutel systeem, zijn de geheime sleutel systemen meestal sneller tot veel sneller en worden ze dan ook gebruikt voor real-time encryptie van bijvoorbeeld een huurlijn, of bulkdata voor opslag.
Echter om de geheime sleutel te distribueren kunnen bij uitstek de mogelijkheden van een publiek sleutelsysteem worden aangewend.

Door gebruik te maken van een publiek sleutelsysteem is het mogelijk een bericht te voorzien van de identiteit van de verzender. In het geval van bijvoorbeeld een bestelling levert dit de noodzakelijke zekerheid op aan de kant van de ontvanger. Door het bericht door het encryptie algoritme te halen en daarbij gebruik te maken van de privé sleutel en de eindwaarde aan het bericht toe te voegen, kan de ontvanger de identiteit van de verzender verifiëren met de publieke sleutel. Het is daarbij dan wel nodig dat er zekerheid is over de natuurlijke persoon die de houder is van de privé sleutel.

3. Sleutelbeheer

Scope
Sleutelbeheer omvat de gehele levenscyclus van de crypto-sleutel: vanaf de generatie via registratie, distributie, opslag en gebruik tot en met de vernietiging. Op deze gehele cyclus dient een security officer toe te (kunnen) zien.
Het doel van sleutelbeheer is zorgvuldig met de sleutels om te gaan. Alle cryptosystemen zijn afhankelijk van een adequaat opgezette wijze van sleutelbeheer. Dit is vaak van even groot belang als de kwaliteit van het algoritme.

Voorschriften
Voor een beperkt aantal organisaties zijn er strikte voorschriften. Zo schrijft De Nederlandse Bank voor hoe banken in het financiële verkeer met crypto-sleutels dienen om te gaan. Andere organisaties dienen zelf de richtlijnen en procedures uit te werken hoe er met sleutelmateriaal omgegaan dient te worden. Bij voorkeur sluit het aan bij de wijze waarop de beheerorganisatie werkt. Er zijn handboeken en richtlijnen vanuit diverse organisaties zoals bijvoorbeeld het European Security Forum.

Sleutelgeneratie
Bij de generatie van de sleutel dient de vertrouwelijkheid gegarandeerd te kunnen worden, vandaar dat dit dikwijls geïsoleerd plaatsvindt. Daarnaast mag er geen mogelijkheid zijn om in een systeem een nieuwe gegenereerde sleutel middels een intelligent algoritme te voorspellen. Dit is een behoorlijk lastig mathematisch proces omdat "random number generators" bewijsbaar snel vervallen in een cyclus, ook al kan de cyclus duizenden iteraties groot zijn. Verder moet een sleutel geen zwakke combinatie van tekens zijn (een reeks of een serie gelijke tekens).
Om de kans op onthulling en fraude te verminderen dient de generatieprocedure twee of meer deskundige personen te betrekken in de uitvoering.

Gegeven de steeds krachtiger wordende pc-werkstations en de mogelijkheid rekenkracht in het internet te gebruiken, moeten sleutels van voldoende lengte (lees: kracht of kwaliteit) worden genomen.

Sleuteldistributie
Om conventionele symmetrische systemen te kunnen gebruiken, delen de partijen de sleutel. Omdat er wensen/eisen zijn om de risico's van onthulling te verminderen dient de sleutel regelmatig te worden vervangen. Dit impliceert een sleutel distributie mechanisme, waarmee een gegenereerde sleutel kan worden afgeleverd bij de gebruikers.

Er zijn voor twee partijen A en B een aantal manieren waarop sleuteldistributie kan plaats vinden:

1) A maakt/kiest een sleutel en laat deze bezorgen bij B.
2) Een derde partij maakt/kiest een sleutel en laat deze bij zowel A als B bezorgen.

3) Gebruikmakend van een reeds bestaande sleutel kan een nieuwe door of A of B worden gemaakt/gekozen en naar de ander worden verzonden, geëncrypt met de bestaande sleutel.
4) Indien A en B een sleutelrelatie hebben met een derde partij kan deze een nieuwe sleutel maken/kiezen en deze naar en A en B geëncrypt verzenden.

Voor de opties 1 en 2 is een fysieke bezorging nodig, en ook dit heeft zo zijn problemen. Er mag geen onderschepping of kennisname mogelijk zijn. Hiertegen zijn dan fysieke maatregelen te treffen, zoals "tamperproof" enveloppen. Verder is het opsplitsen in N delen van de sleutel en het verspreiden van de delen over meer zendingen en/of meer personen een toereikend gebleken methode.

Een dergelijke manier van distributie is een redelijke oplossing voor het encrypten van een vaste lijnverbinding omdat er slechts één partij is waarmee er wordt gecommuniceerd. De sleutelrelatie is daarmee één op één. Wanneer er meer partijen in een schema zitten wordt het al zeer snel onhoudbaar om op basis van één op één encryptie te werken. Wanneer er N hosts zijn er dan (n*(n-1)/2) sleutels te onderhouden.

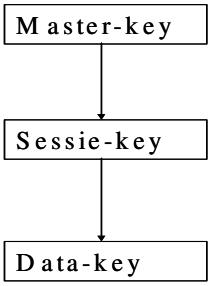
Voor optie 3 wordt gebruik gemaakt van een sleutelverloop. Eenmaal een sleutel op z'n plek (fysiek) worden de andere sleutels aangereikt. Als een sleutel echter in handen valt van een derde dan zijn ook alle daarna volgende sleutels automatisch voor deze derde beschikbaar. Dit is niet gewenst.

Door het inzetten van een extra indirectie kan dit worden voorkomen. Er wordt een hiërarchie van sleutels gebruikt: voor sleuteluitwisseling (masterkey), voor sessies (sessiekey), voor data (datakey). Gevolg: het aantal waarnemingen op data waarbij de masterkey is gebruikt is erg klein geworden namelijk alleen bij de uitwisseling van sessiesleutels. De masterkey wordt fysiek uitgewisseld, de overigen kunnen via het datakanaal in geëncrypte vorm uitgewisseld worden, en worden bijvoorkeur zo vaak verwisseld als nog verantwoord is gegeven hun verwachte levensduur. Uiteraard kan deze hiërarchie naar behoefte worden verdiept, naarmate de behoefte aan bescherming van de masterkey en de geëiste levensduur ervan toeneemt.

Wanneer er een gemeenschappelijk sleuteldistributie centrum (SDC) wordt gebruikt (optie 4) wordt de proportie van het N hosts probleem veel beter. Ieder van die N hosts heeft een (1) masterkey waarmee met het SDC wordt gecommuniceerd, en de sleutels worden aangereikt. Toetreden tot het SDC impliceert een afstemming en fysieke distributie en handmatige installatie van deze masterkey.

In het geval dat de aantallen hosts en netwerken groot zijn kan er worden overgegaan naar het uitvoeren van een hiërarchie van distributiecentra. Een SDC zou bijvoorbeeld per lokaal netwerk kunnen worden uitgevoerd. Voor lokale communicatie is de lokale SDC gezaghebbend. Wanneer er buiten het verzorgingsgebied van de SDC wordt gecommuniceerd dienen de betrokken SDC's een gemeenschappelijke hiërarchisch hogere SDC te vinden. Hoewel ieder van de drie betrokken SDC's de sleutels kan toewijzen zal meestal de hiërarchisch hoogste SDC hiervoor de aanwijzingen geven.

Bij een publiek sleutel systeem op basis van een trusted third party (TTP) die de identiteit van de sleutelhouder garandeert, is deze problematiek weer heel anders: de sdc's kunnen komen te vervallen. Daarvoor in de plaats komt de distributie van de public key van de TTP. Verder dienen de hulpmiddelen beschikbaar te zijn om te achterhalen of de aangegeven identiteit correct is, dat wil zeggen past bij de publieke sleutel. De TTP heeft een publiek te raadplegen registratie. Vervolgens kunnen de sessiesleutels met behulp van asymmetrische algoritmen veilig worden uitgewisseld.



Sleutelopslag
Sleutels dienen op een veilige manier te worden opgeslagen. Dat dit in software niet eenvoudig is, is wel af te leiden uit de moeite die het heeft gekost om passwords veilig op te slaan, en deze kennen een vele lichtere eis: ze hoeven nooit meer in klare taal beschikbaar te zijn; vergelijken kan prima in geëncrypte vorm. Bij sleutelopslag geldt echter dat sleutels wel beschikbaar moeten blijven.

Ongeacht hoe goed het betreffende platform (en diens besturingsysteem) ook is, de sleutels worden bijvoorkeur in specifieke hardwarematige beveiligingsmiddelen opgeslagen. Deze zijn onderworpen aan bijzonder zware standaarden, waardoor bijvoorbeeld de sleutel automatische wordt gewist als de omhulling wordt geopend. Verder is meestal een eis dat het openen niet onopgemerkt kan blijven. Hier zijn ISO en FIPS standaarden van toepassing.

Bij de mainframe-platformen (zoals IBM OS/390, Siemens BS2000, Compaq/Tandem Hymalaya) dient aan coprocessoren en insteekmodules te worden gedacht. Overigens zijn er ook uitstekende netwerkversies van crypto-modules die voldoen aan de standaarden en geschikt zijn voor een veel groter bereik aan platforms. Aan de gebruikerskant is de smartcard een te voorzien opslagmechanisme. Het zal nog moeten blijken hoe veilig de combinatie van smartcards wordt met pc's die kwetsbaar zijn voor virussen en trojaanse paarden (en er zijn voortdurend nieuwe ontwikkelingen). Alle overige apparaatjes die aan gebruikers worden overhandigd zijn offline van aard: ze gaan niet in/aan de pc. Bij sommige van deze apparaatjes worden de sleutels tijdens configuratie er in gezet. De ontvangende gebruiker dient de uitgever te vertrouwen voor het geheim houden van de sleutels.

Wordt de sleutel op papier opgeslagen dan dient deze uit twee of meer delen te bestaan, waarbij soms de sleutel zelf niet eens wordt onthult door deze op een soort pin-brief af te drukken. Dan raakt alleen bij herstel het betreffende sleuteldeel bekend. Om efficiëntie te bereiken in geval van een noodsituatie, kan een N-uit-M opdeling worden gehanteerd. Dat wil zeggen dat er minimaal N aanwezige delen moeten zijn van een maximum van M om de bedoelde sleutel uit de delen te kunnen samenstellen. Voorbeelden uit de praktijk zijn 2-uit-3, 2-uit-4 en 3-uit-5. Naarmate het belang groter wordt, zijn er meer personen bij betrokken.

Sleutelgebruik
De sleutel dient niet langer gebruikt te worden dan verantwoord is voor de risico's die de organisatie wenst te nemen. Verder mogen geen extra risico's ontstaan doordat het nodig is de sleutels te gebruiken. Uitvoeren van het encryptie- en decryptieproces mag op geen enkele manier de sleutels onthullen, ook niet in de log van het platform- en besturingssysteem.

Sleutelvernietiging
Als de periode is verstreken waarvan de organisatie vindt dat sleutels veilig kunnen worden gebruikt, dienen deze sleutels te worden vernietigd. Dit kan echter niet zomaar: als het ging om een sleutel waarmee gegevens waren opgeslagen dienen al deze gegevens te worden gedecrypt en weer geëncrypt met de nieuwe sleutel. Dit kan een uiterst kostbare zaak zijn als het gaat om veel gegevens. Daarnaast is er tijdens deze activiteit altijd een kans op onthulling, tenzij het volledig gescheiden gebeurd van de normale verwerking. Verder moet de wettelijke bewaartermijn in aanmerking worden genomen. Wat te doen als er binnen die periode een gerechtelijk bevel komt waarin wordt gevraagd om een e-mailtje te decrypten? Het is noodzakelijk de betreffende wetgeving na te gaan, en deze veranderd met de ambities op het Europese vlak met enige regelmaat. Met de concept richtlijnen met betrekking tot digitale handtekeningen (waarin tenslotte ook sleutels zijn betrokken) worden de mogelijkheden voor vernietiging er niet beter op. Let wel: TTP's krijgen hiermee de plicht om (in potentie enorm grote) sleutel- of certificaatarchieven aan te leggen.

Er zijn encryptiesystemen waarbij de vernietiging eenvoudig met een commando is geregeld. In het andere geval dient alles te worden gewist en alleen de geldige sleutels te worden herladen, een duidelijk minder veilige opzet. In ieder geval is de kans op verstoring zo groot dat er strakke procedures nodig zijn, waarin minimaal met een twee-personen (resp. vier-ogen) principe wordt gewerkt.

Indien er reservekopieën waren gemaakt op een drager dienen deze veilig te worden vernietigd. Deze drager kan van alles zijn: magnetisch, optisch maar ook papier. Denk hierbij ook aan de exemplaren die op een uitwijklocatie kunnen zijn opgeslagen.

4. Organisatie van sleutelbeheer

Uit de hoeveelheid aspecten die er bij sleutelbeheer komen kijken, kan worden afgeleid dat de organisatie ervan van groot belang is. Voor de reguliere taken dienen er weloverwogen procedures te zijn. Hierbij wordt ook vastgelegd hoe de controle op de uitvoering en op de uitvoerders plaatsvindt.

Bij de meeste taken zal er sprake zijn van taakscheiding, naast de platform- of besturingssyteem-beheerder zal bijna altijd de security officer betrokken zijn. Om de kans op fraude te verkleinen hebben de betrokken personen geen hiërarchische gezagsverhouding. Indien er specifieke encryptiehardware wordt gebruikt, is er aanleiding voor een gescheiden beheer(groep). Deze kent haar eigen procedures voor plaatsing, veranderingen op of aan, en verwijdering van de encryptiehardware.

Om door een onafhankelijke partij (bv EDP-audit) de controle te kunnen laten plaatsvinden dient er een verslaglegging te zijn van alle (pogingen tot) activiteiten van sleutelbeheer: wie deed wanneer wat met welke sleutel. Dit verslag mag niet door beheerders te beïnvloeden zijn zonder dat ook dat gemeld wordt, en het verslag wordt op een strikt gescheiden beheerd systeem opgeslagen. Iedere waarneming van ongewone (combinaties van) activiteiten zal moeten leiden tot een onderzoek naar de gang van zaken, en mogelijk tot aanvulling of aanpassing van procedures.

Voor grotere en striktere dan wel formeler geregelde sleutelbeheeromgevingen zijn er ook voorschriften te verwachten in personele en fysieke sfeer.

Van iedere medewerker die optreedt als sleutelbeheerder wordt er een antecedentenonderzoek gedaan en worden referenties nagegaan. Zo ook voor de security officer. Is beveiliging een hoofdtaak dan wordt het onderzoek intensiever en diepgaander.

De fysieke voorschiften spreken zich uit voor de noodzaak van fysiek gescheiden locaties van activiteiten en gescheiden opslag van (reservekopieën van) sleutels en het verbod op gelijktijdige aanwezigheid in een locatie van deelnemers aan een deelactiviteit. Niet te vergeten: gescheiden netwerken voor beheer en gebruik van de encryptie systemen.

Verder valt onder organisatie de wijze waarop de certificeringseisen dan wel standaards voor de gebruikte hardware en software wordt vastgesteld. Hieronder vallen dan niet alleen de centrale delen maar ook de clients waarmee gebruikers de mogelijkheden van encryptie kunnen benutten, zoals een mail-client (SMIME), filetransfer-client (SSH) en tegenwoordig ook een terminal-emulatie client (TN-E).

Hoewel veel aandacht in de vakpers uitgaat naar de kracht van een algoritme in relatie tot de lengte van een sleutel, is in de dagelijkse praktijk het goed organiseren en uitvoeren van sleutelbeheer de meest essentiële factor.

Veel voorkomende afkortingen

DSA - Digital Signature Algorithm
DES – Data Encryption Standard
ECC - Eliptic Curve Crypto
HTTP – HyperText Transport Protocol
IDEA – International Data Encryption Algorithm

ISO – International Standardization Organization
KEK – Key Exchange key
RNG – Random Number Generator
RPK - Raike Public Key
RSA – asymmetric encryption invented by Rivest, Shamir, Adleman
SSL – Secure Socket Layer
SDC – Sleutel Distributie Centrum
SMIME – Secure Multipurpose Internet Mail Extension
SO – Security Officer
SSH – Secure Shell
TN-E – Telnet Enhanced
TTP – Trusted Third Party

Literatuur

A Framework for Using Cryptography, European Security Forum, December 1997. (available to ESF-members)

Cryptography In Business, A Briefing Paper, European Security Forum, Oktober 1997. (available to ESF-members)

Sleutelmanagement in de praktijk, veilig communiceren en zaken doen, W. Huurman en J. Jaarsma, Praktijkjournaal Informatiebeveiliging, september 1999, Ten Hagen Stam, issn 1388-5383

Cryptography and Network Security, Principles and Practice, 2nd edition, W. Stallings, 1999, Prentice Hall, isbn 0-13-869017-0

De Auteur
Ir. Ernst J. Mellink is IT Security Architect en eigenaar van More-Secure BV. Hij adviseert grotere en kleinere organisaties over de wijze waarop IT-beveiliging (technisch en organisatorisch) een onderscheidende factor kan zijn in de markt en in de bedrijfsvoering. Hij is bereikbaar op e.j.mellink@more-secure.nl

Contact

More-Secure BV
Da Costalaan 14
3767GH Soest
T: +31 (0)6 5357 9338
F: +31 (0)35 524 7587
E: info@more-secure.nl
W: www.more-secure.nl