

## ORGANISATIES IN STANDAARDISATIE VOOR INFORMATIEBEVEILIGING

### Auteur:

Ir Paul L. Overbeek  
Fysisch en Elektronisch Laboratorium TNO  
Postbus 96864  
2509 JG Den Haag  
tel 070 - 3264221

In deze publicatie introduceren we de belangrijkste internationaal werkende organisaties die actief zijn in de standaardisatie van informatiebeveiliging. Deze organisaties hebben, afhankelijk van hun doelgroep, zeer verschillende invalshoeken in hun activiteiten. Om hier inzicht in te bieden is voor iedere organisatie een korte beschrijving van de doelgroep en het werkprogramma opgenomen.

Informatie over standaarden is veelal beschikbaar via het Nederlands Normalisatie Instituut (NNI) in Delft.

### Internationaal

De belangrijkste internationaal werkende organisaties voor standaardisatie op het gebied van de informatie technologie zijn de International Organisation for Standardisation (ISO), de International Electrotechnical Commission (IEC) en het Comité Consultatif International Télégraphique et Téléphonique (CCITT). Het lidmaatschap van de ISO en de IEC is hoofdzakelijk voorbehouden aan nationale standaardisatie organisaties. In Nederland is dat het Nederlands Normalisatie Instituut (NNI), in België het Belgisch Normalisatie Instituut (BNI). Leden van de CCITT zijn de nationale PTT's.

Deze drie organisaties produceren ruwweg vier verschillende soorten documenten: basis standaarden (in het voornamelijk Engelse jargon: *base standards*), beschrijvingen van conformance testen, registratie procedures en documenten die dienen als achtergrond en uitleg. De nadruk ligt op de base standards.

### *ISO Technical Committee 68 'Banking and Related Financial Services'*

Zoals de naam als zegt richt ISO Technical Committee (TC) 68 zich op de bankwereld. Zo heeft TC68 standaarden ontwikkeld voor communicatie tussen banken onderling en voor communicatie tussen bank en klanten. Veel van de TC68-standaarden vinden hun oorsprong in 'American

National Standards Institute' (ANSI) standaarden en eveneens Amerikaanse 'Federal Information Processing Standard Publications' (FIPS PUBs).

### *ISO/IEC/JTC1*

ISO en IEC hebben een gemeenschappelijk forum, 'Joint Technical Committee 1' (JTC1), in het leven geroepen om standaarden op het gebied van de Open Systems Interconnection (OSI) tot stand te brengen. Op basis van OSI standaarden is het mogelijk om tussen ongelijksoortige computers informatie uit te wisselen via het (OSI) netwerk. Het werk van JTC1 wordt afgestemd met de CCITT.

Onder JTC1 zijn een aantal Sub Committees (SCs) actief. De meeste SCs hebben vroeg of laat wel wat met beveiliging te maken. De volgende zijn echter het meest actief op beveiligingsgebied:

#### SC6 'OSI Lower Layers':

SC6 ontwikkelt een model voor beveiliging op de lagere OSI lagen. Tevens werkt SC6 aan beveiliging op laag drie (Network Layer Security Protocol) en laag vier (Transport Layer Security Protocol) van het OSI model.

#### SC17 'Identification Cards':

SC17 houdt zich bezig met beveiliging van identificatie-middelen zoals de magneetkaart en de smart card.

#### SC18 'Text and Office Systems':

SC18 heeft aandacht voor veilige elektronische post, beveiliging van kantoortoepassingen in netwerken en beveiliging van elektronische documenten.

#### SC21 'OSI Architecture, Management and Upper Layers':

SC21 heeft de OSI Security Architecture ontwikkeld en is momenteel bezig om de Frameworks en Models, gebaseerd op de Security Architecture, te ontwikkelen.

Voorbeelden van andere activiteiten van SC21 zijn, beveiliging van: databases, beheer, zoek-hulpmiddelen als de 'Directory' (het telefoonboek in OSI-netwerken), toegang tot en transport van bestanden. SC21 steunt zwaar op bijdragen van de CCITT.

#### SC22 'Languages':

SC22 houdt zich onder andere bezig met de POSIX interface set. POSIX is ontstaan als een initiatief van de IEEE (zie later).

**SC27 'IT Security Techniques':**

SC27 werkt aan standaardisatie van beveiligingstechnieken en -mechanismen al dan niet met gebruik van cryptografische technieken, richtlijnen voor het beheer van de beveiliging en aan methoden voor de evaluatie van beveiliging in IT-produkten.

**CCITT**

Zoals al gezegd zijn de activiteiten van CCITT nauw met die van ISO en IEC afgestemd. De beveiligingsactiviteiten van de CCITT zijn geconcentreerd in SubGroep (SG) VII, voornamelijk gericht op informatie technologie, en SG VIII, telematica. Onder deze SGs bevinden zich werkgroepen, aangegeven met de letter 'Q':

**SG VII Q18 'Message Handling Systems':**

Deze werkgroep heeft zich bezig gehouden met beveiliging in elektronische post (vastgelegd als opties en interfaces in de X.400 standaarden) en is nu bezig met beveiliging van Electronic Data Interchange (EDI).

**SG VII Q19 'Framework for Support of Distributed Applications':**

SG VII Q18 heeft de beveiligingsarchitectuur voor OSI ontwikkeld (OSI Security Architecture, ISO 7498-2 of X.800) en is nu, wederom in ISO SC21-verband, actief in de ontwikkeling van raamwerken en modellen voor beveiliging, onder andere voor gedistribueerde applicaties.

**SG VII Q20 'Directory Systems':**

Deze werkgroep heeft een raamwerk en methoden opgesteld voor authenticatie via de 'Directory' (Authentication Framework, X.509). Momenteel is deze groep bezig met methoden voor toegangsbeheersing die op dat raamwerk zijn gebaseerd.

**SG VIII Q28 'Security in Telematics Services':**

SG VIII Q28 werkt aan een raamwerk voor beveiliging van telematicadiensten.

**Europa**

***CEN/CENELEC en ETSI***

In Europa zijn de belangrijkste organisaties op het gebied van de standaardisatie voor beveiliging de Comite European de Normalization (CEN), de Comite European de Normalization Electrotechnique (CENELEC) en European Telecommunications Standards Institute (ETSI). De taakstelling van deze organisaties komt ruwweg overeen met wat ISO, IEC en CCITT mondiaal doen. Het lidmaatschap van CEN en CENELEC is voorbehouden aan de leden van de Europese

Gemeenschap en de Europese Vrijhandel Associatie (EVA). De beveiligingsactiviteiten binnen CEN en CENELEC worden gecoördineerd door de Advisory Expert Group on Information Security Standards (ITAEGV). CEN en CENELEC zijn verantwoordelijk voor het opstellen en ratificeren van Europese normen. Deze normen zijn vaak gebaseerd op base standards van ISO, IEC en CCITT. Dit zijn de bekende EN (European Norme) en ENV (European Norme Voraugabe) normen.

Het lidmaatschap van de ETSI staat open voor iedere organisatie die geïnteresseerd is in standaardisatie van telecommunicatie binnen Europa. Naast de PTT's zijn dit ook de aanbieders van producten en de groot-verbruikers van telecommunicatie. De ETSI maakt European Telecommunication Standards (ETSS). ETSI heeft verschillende werkgroepen op beveiligingsgebied. De belangrijkste activiteiten zijn: cryptografische algoritmen, beveiliging van elektronische post (samen met EWOS), beveiliging van teleconferencing, beveiliging van audiovisuele diensten en beveiliging van mobiele communicatie.

#### *ECMA, EWOS*

Voorts zijn binnen Europa de ECMA en EWOS actief. De European Computer Manufacturers Association (ECMA) is, om het oneerbiedig te zeggen, een club van Europese computer- en netwerk-leveranciers. Onderdeel van de belangenbehartiging namens die leveranciers vormt de steun aan het standaardisatiewerk, ook op beveiligingsgebied. Immers, goede standaarden zijn ook in het belang van de ECMA-leden. De ECMA heeft een aantal Task Committees (TCs). Voor beveiliging zijn de belangrijkste:

#### TC22:

Beveiliging van database systemen;

#### TC29:

Beveiliging van gestandaardiseerde documenten in de kantooromgeving (Office Document Architecture, ODA, bijdrage via SC18 van ISO/IEC/JTC1);

#### TC32:

Deze TC heeft verschillende werkgroepen, genoemd Task Groups (TGs). De onderwerpen van de werkgroepen zijn:

- TG2: Beveiligingseisen voor interactief werken via netwerken;
- TG6/10: Beveiliging op de lagere ISO lagen (bijdrage via SC6 van ISO/IEC/JTC1)

- TG9: Beveiliging in 'Open' systemen. TG9 heeft een raamwerk voor beveiliging ontwikkeld. Daarop werden data structuren voor beveiliging en beveiligingsdiensten gebaseerd. Nu is deze groep bezig met de ontwikkeling van protocollen, methoden voor authenticatie en andere bouwstenen voor beveiliging.
- TG36: Criteria voor de evaluatie van beveiliging (bijdrage voornamelijk via SC27 van ISO/IEC/JTC1, maar ook rechtstreekse beïnvloeding van de ontwikkeling van de ITSEC).

De European Workshop for Open Systems (EWOS) is opgericht door de ECMA en gebruikersorganisaties met de steun van CEN, CENELEC, ETSI en de Europese Commissie (EC, het 'kabinet' van de Europese Gemeenschap). EWOS richt zich op het definiëren van *profielen* (functional profiles). Een profiel is een doorsnede van een base standard en een keuze uit de vele opties. Profielen zijn nodig omdat de base standards, vanwege die vele opties, vaak niet direct bruikbaar zijn. De EWOS stelt ook profielen voor beveiliging op. Het werk op beveiligingsgebied binnen de EWOS wordt gecoördineerd door de EWOS Experts Group on Security (EWOS EGSEC).

#### *De rol van de Europese Commissie*

In dit overzicht van activiteiten binnen Europa mag de Europese Commissie (EC) niet ontbreken. De EC begint steeds meer activiteiten op beveiligingsgebied te ontplooiën, voornamelijk in een coördinerende rol. Een goed voorbeeld hiervan is het INFOSEC-initiatief. INFOSEC heeft als doel om op Europees niveau een aantal taken op beveiligingsgebied van de grond te brengen en te coördineren. Dit betreft met name activiteiten op juridische gebied (o.a. wetgeving binnen Europa op het gebied van de privacy en de bescherming van IT-produkten), technisch gebied (via de Europese onderzoeksprogramma's, zie verderop) en de meer procedurele, op afstemming gerichte activiteiten (zie o.a. EPHOS). De EC heeft inmiddels een orgaan in het leven geroepen (per april 1992 officieel) waarbinnen de taken op beveiligingsgebied gestuurd worden en waarin tevens een groot deel van de beleidsvoorbereiding op het gebied van de Europese informatiebeveiliging plaats vindt. Dit orgaan, met vertegenwoordigers van alle EG-landen, heet de Senior Officials Group on Information Security (SOGIS).

Eén van de belangrijkste activiteiten van de EC is de coördinerende rol in de totstandkoming van de Information Technology Security Evaluation Criteria (ITSEC). De ITSEC is een initiatief van Nederland, Engeland, Duitsland en Frankrijk. Deze vier landen ontwikkelden een gezamenlijke standaard voor de evaluatie van beveiliging in informatietechnologie produkten. Dit initiatief

wordt ondersteund door de EC. De ITSEC wordt tot 1994 binnen Europa uitprobeerde. Daarna wordt de ITSEC op basis van de opgedane ervaringen bijgesteld. Inmiddels wordt er ook door SC27 van ISO/IEC/JTC1 aan de ITSEC gewerkt en heeft ook het Amerikaanse NIST serieuze interesse getoond.

## Amerika

In Amerika zijn de belangrijkste organisaties de American National Standards Institute (ANSI) en de Institute of Electrical and Electronics Engineers (IEEE). Zowel ANSI als IEEE zijn actief op beveiligingsgebied via de ISO en IEC.

ANSI houdt zich intensief bezig met de ontwikkeling van standaarden voor de bankwereld. Daarnaast besteedt ANSI aandacht aan beveiliging van EDI en draagt ANSI bij aan het werk van de ISO op het gebied van de beveiliging.

IEEE heeft als beveiligingsactiviteiten ondermeer het project 'Standard for Interoperable LAN Security' (SILS) dat zich richt op lokale netwerken waarin veelal niet alle OSI lagen geïmplementeerd hoeven te zijn. Verder is de IEEE de motor achter 'Portable Operating System Interface for Computer Environments' (POSIX). POSIX is een interface tussen applicatie en operating system en heeft als doel de overdraagbaarheid van applicaties te bevorderen. POSIX heeft ook een (beperkte) interface voor beveiligingsfuncties. Een derde activiteit van IEEE is 'Medical Data Interchange' (MEDIX), een project dat zich richt op beveiliging van medische gegevens.

Naast ANSI en IEEE zijn gedrieën het Amerikaanse Department of Defense (DoD) met het USA National Computer Security Center (NCSC) en het USA National Institute of Standards and Technology (NIST) zeer actief op beveiligingsgebied. De bekendste standaarden van deze organisaties zijn:

- Trusted Computer System Security Evaluation Criteria (TCSEC, beter bekend naar de kleur van de kaft als het *Orange Book*). Het Orange Book beschrijft evaluatie criteria voor de beveiliging van IT-producten. De nadruk ligt daarbij op beveiliging van besturingssystemen.
- Trusted Network Interpretation of the TCSEC (TNI of *Red Book*). Het Red Book richt op beveiliging in netwerken.

Overigens zijn er veel meer standaarden van DoD/NCSC/NIST.

Voorts is de Open Implementors Workshop (OIW) in Amerika het gemeenschappelijk forum voor leveranciers van OSI-produkten. De OIW definieert profielen van de OSI-standaarden, ook op beveiligingsgebied, en is hiervoor de Amerikaanse tegenhanger van de Europese EWOS.

### Overige organisaties

De in de voorgaande secties genoemde organisaties hebben allen activiteiten die rechtstreeks gericht zijn op informatiebeveiliging. Daarnaast zijn er nog een groot aantal organisaties die vaak zijdelings, maar wel noodzakelijk, betrokken zijn bij informatiebeveiliging. Ook zijn er clubjes die invloed proberen uit te oefenen op andere organisaties of leveranciers zonder daarbij perse zelf standaarden te definiëren.

Hierna bespreken we deze bonte verzameling.

#### *Gericht op de overheid*

### GOSIP

Government OSI Profiles (GOSIP) zijn profielen van de OSI standaarden, vergelijkbaar met die van EWOS en OIW. Een GOSIP is een door de overheid gekozen profiel voor eigen gebruik. Als U aan een overheid met een eigen GOSIP wilt leveren dan moet U aan de betreffende GOSIP voldoen. Er zijn GOSIPs van verschillende landen. Met name in de GOSIPs van Engeland, Amerika en Canada wordt redelijk veel aandacht aan beveiliging besteed. Nederland en België hebben geen eigen GOSIP.

### EPHOS

Het European Procurement Handbook for Open Systems (EPHOS) moet een GOSIP voor de EG worden. Het is de bedoeling dat in de toekomst alle nationale overheden zich richten naar de standaarden van dit handboek bij de aanschaf van informatie- en telecommunicatie produkten. EPHOS wordt ontwikkeld door Frankrijk, Duitsland en Engeland. De eerste fase van EPHOS is in maart 1992 afgerond en omvat voornamelijk richtlijnen voor communicatie volgens de X.25 standaard, MHS (message handling systems, onder andere voor electronic mail) volgens de X.400-84-standaard (feitelijk nu al wat verouderd) en richtlijnen voor het gebruik van FTAM (File Transfer, Access and Management). Deze eerste fase bevat nog geen beveiliging. In de tweede fase, die zich onder andere richt op Electronic Data Interchange (EDI), lokale netwerken en documentuitwisseling volgens de Office Document Architecture-standaard (ODA) zal wel enige aandacht voor beveiliging zijn.

## IPSIT

De International Public Sector IT Group (IPSIT) is een informeel verband tussen verschillende organisaties uit de publieke sector (overheid, semi-overheid, PTT). Ook de IPSIT definieert OSI profielen. De IPSIT fungeert tevens als een soort pressiegroep.

### *Onderzoek*

Er zijn binnen Europa verschillende grote onderzoeksprogramma's. Deze programma's hebben tot doel om de Europese samenwerking te bevorderen en een technologische voorsprong op te bouwen. Uit de grote onderzoeksprogramma's komen vaak *de facto* standaarden voort. In de volgende Europese onderzoeksprogramma's zijn taken opgenomen die mede aandacht besteden aan informatiebeveiliging:

- RACE: Research and Development in Advanced Communications
- ESPRIT: European Strategic Programme for Research and Development in Information Technology
- TEDIS: Trading EDI Systems
- AIM: Advanced Informatics in Medicine
- ENS: European Nervous System
- ANSA: Advanced Network Systems Architecture
- SESAME: Secure European System for Applications in a Multivendor Environment

Informatie over Europese onderzoekprogramma's is verkrijgbaar via Directoraat Generaal (DG) XIII van de Europese Commissie. In principe zijn de resultaten uit de onderzoekprogramma's openbaar. In praktijk blijkt enige volhardendheid in de jacht naar informatie noodzakelijk te zijn.

Er zijn niet alleen in Europa samenwerkings- en onderzoeksprogramma's. Ook in Amerika en in Japan zijn er grote programma's. Een goed voorbeeld is het Athena project. Dit is een samenwerkingsprogramma tussen het Amerikaanse Massachusetts Institute of Technology (MIT) en verschillende computerleveranciers waaronder Digital en IBM. Als onderdeel van het Athena project is Kerberos ontwikkeld. Kerberos is een authenticatie-server voor gebruik in netwerken. Authenticatie van zowel gebruikers, programma's als computersystemen is mogelijk. Kerberos is in korte tijd zeer populair geworden aangezien het in aanvang kosteloos beschikbaar was. Helaas is er nu een export-licentie nodig, hetgeen voor de Europese markt een nadeel is.



### *Initiatieven van gebruikers*

#### MAP

Het Manufacturers Automation Protocol (MAP) is een verzameling OSI standaarden en profielen voor gebruik in een productie omgeving, b.v. besturing in een produktiehal. Eén van de stuwende krachten achter MAP is General Motors. Er is een gemeenschappelijke MAP/TOP-groep die kijkt naar de beveiligingseisen.

#### TOP

De Technical and Office Protocols (TOP) richten zich meer op de kantooromgeving. Ook TOP is een verzameling OSI standaarden en profielen. Eén van de belangrijkste krachten achter TOP is Boeing.

#### NIUF

De North American ISDN Users Forum (NIUF) heeft een werkgroep 'ISDN en Beveiliging'. Deze werkgroep richt zich op gebruikerseisen voor beveiliging in ISDN, een beveiligingsarchitectuur voor ISDN en het ontwerp en de ontwikkeling van veilige ISDN applicaties.

#### DECUS

De DEC User Society (DECUS) is een vereniging van gebruikers van Digital apparatuur. In verschillende landen zijn er Special Interest Groups en Working Groups die zich specifiek met beveiliging bezig houden, echter niet beperkt tot Digital producten. DECUS Europe neemt tevens deel in de EWOS Experts Group on Security.

### *Initiatieven van leveranciers*

#### SPAG

De Standards Promotion and Application Group (SPAG) is een groep van Europese leveranciers die profielen, ook voor beveiliging, ontwikkelt vanuit het standpunt van de leveranciers.

#### COS

De Corporation for Open Systems (COS) is een groep leveranciers in Amerika die het gebruik van 'Open' systemen en van OSI standaarden in het bijzonder wil stimuleren.

### POSI

Ook de Promoting Conference for OSI (POSI) beoogt het gebruik van OSI standaarden te stimuleren.

### OSI NMF

Netwerkmanagement is een probleem dat gelukkig steeds meer aandacht krijgt. Het OSI Network Management Forum (OSI NMF) richt zich op management in OSI netwerken. Bijzondere aandacht krijgen de beveiliging van het management, en het management van beveiliging.

### X/Open, Unix International, Open Software Foundation (OSF)

Deze groepen, gevormd door voor een deel dezelfde leveranciers, beogen een internationaal erkende verzameling *de facto*-standaarden te definiëren om de ontwikkeling van open systemen te bevorderen. Ook voor beveiliging worden zo keuzes gemaakt. Het is echter niet de bedoeling van deze groepen om zelf nieuwe standaarden aan de toch al ruime verzameling toe te voegen.

### EUROBIT

De European Business in Information Technology (EUROBIT) groep is een belangengroep van leveranciers in Europa. EUROBIT maakt zich vooral sterk voor de belangen van niet-Europese leveranciers en probeert eventuele handelsbelemmeringen weg te nemen. Beveiliging is in toenemende mate een verkoopargument geworden. Daarnaast kan beveiliging ook een reden zijn om de export en import van IT-producten te bemoeilijken. Dit zijn twee redenen waarom EUROBIT zich sterk maakt voor duidelijke, algemeen erkende, regels voor de evaluatie van beveiliging in IT-producten.

### IBAG

De INFOSEC Business Advisory Group (IBAG) is een belangenvertegenwoordiging, zeg maar pressiegroep, van het Europese bedrijfsleven (vooral aanbieders van IT-producten), gericht op het INFOSEC initiatief van de Europese Commissie en meer specifiek op de ITSEC.

### EurOSInet, OSIONE

EurOSInet is een organisatie van leveranciers die gemeenschappelijk de acceptatie van OSI standaarden in Europa willen stimuleren door demonstratieprojecten waarin de mogelijkheden van OSI getoond wordt. OSIONE, een acroniem van OSI Organisation for Network Establishment, is een vergelijkbaar initiatief maar dan mondiaal. Het OSIONE consortium koppelt bij voorbeeld

de demonstratienetwerken van OSInet en EurOSInet. Er moeten ook demonstratieprojecten op beveiligingsgebied komen.

### *Defensie*

#### NATO

De North Atlantic Treaty Organisation (NATO) heeft intern een geheel eigen standaardisatieproces. De NATO volgt zoveel mogelijk de internationale civiele standaarden. Een voorbeeld hiervan is de NATO OSI Security Architecture (NOSA). NOSA is een inperking van de OSI Security Architecture. Slechts voor bijzondere toepassingen worden militaire voorzieningen geïmplementeerd.

#### SDNS

Het Secure Data Network System (SDNS) is een project dat het gebruik van beveiligde OSI standaarden binnen defensie wil stimuleren. Dit OSI beveiligingsproject wordt grotendeels gefinancierd door het Amerikaanse DoD. Aandachtspunten zijn: veilige berichtbehandeling (secure message handling, onder andere electronic mail), beveiliging op OSI-laag 3 en 4, beveiliging door toegangsbeheersing en beheer van cryptografische technieken en sleutels.

### *Diversen*

Voorts zijn er enkele initiatieven die enigszins buiten de hierboven geschetste kaders vallen. Zo zijn er binnen Europa enkele initiatieven op juridisch gebied die de beveiliging betreffen. Drie initiatieven springen er uit:

Allereerst wordt er op Europees niveau gewerkt aan de afstemming van de wetten op het gebied van de privacy. Ten tweede moeten in de toekomst alle IT-producten onder de bescherming van de (vernieuwde) Europese auteurswetten vallen. Ten derde wordt er gewerkt in de richting van Europese wetgeving met betrekking tot (grensoverschrijdende) computercriminaliteit. Ook deze initiatieven worden door de EC gecoördineerd.

## BIJLAGE A ACRONIEMEN

De volgende acroniemen en afkortingen zijn gebruikt:

AIM	Advanced Informatics in Medicine
ANSA	Advanced Network Systems Architecture.
ANSI	American National Standards Institute
ANSI	American National Standards Institute
BNI	Belgisch Normalisatie Instituut
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CEN	Comite European de Normalization
CENELEC	Comite European de Normalization Electrotechnique
COS	Corporation for Open Systems
DECUS	DEC User Society
DG	Directoraal Generaal
DoD	Amerikaanse Department of Defense
EC	Europese Commissie
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
EN	European Norme
ENS	European Nervous System
ENV	European Norme Vorausage
EPHOS	European Procurement Handbook for Open Systems
ESPRIT	European Strategic Programme for Research and Development in Information Technology
ETS	European Telecommunication Standards
ETSI	European Telecommunications Standards Institute
EUROBIT	European Business in Information Technology
EWOS	European Workshop for Open Systems
EWOS EGSEC	EWOS Experts Group on Security
FIPS PUBs	Federal Information Processing Standard Publications
GOSIP	Government OSI Profiles
IBAG	INFOSEC Business Advisory Group
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPSIT	International Public Sector IT Group

ISO	International Organisation for Standardisation
ITAEGV	Advisory Expert Group on Information Security Standards
JTC1	Joint Technical Committee 1'
MAP	Manufacturers Automation Protocol
MEDIX	Medical Data Interchange
MIT	Massachusetts Institute of Technology
NATO	North Atlantic Treaty Organisation
NCSC	USA National Computer Security Center
NIST	USA National Institute of Standards and Technology
NIUF	North American ISDN Users Forum
NNI	Nederlands Normalisatie Instituut
NNI	Nederlands Normalisatie Instituut
NOSA	NATO OSI Security Architecture
ODA	Office Document Architecture
OIW	Open Implementors Workshop
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSIone	OSI Organisation for Network Establishment
OSI NMF	OSI Network Management Forum
POSI	Promoting Conference for OSI
POSIX	Portable Operating System Interface for Computer Environments
RACE	Research and Development in Advanced Communications
SCs	Sub Committees
SDNS	Secure Data Network System
SESAME	Secure European System for Applications in a Multivendor Environment
SG	SubGroep
SILS	Standard for Interoperable LAN Security'
SOGIS	Senior Officials Group on Information Security
SPAG	Standards Promotion and Application Group
TC	Technical Committee
TCs	Task Committees
TEDIS	Trading EDI Systems
TGs	Task Groups
TOP	Technical and Office Protocols

BIBLIOTHEEK

FEL-TNO

seminar

ER 97 316  
GRAVENHAGE 16

# INFORMATIE BEVEILIGING

Het verzekeren van de integriteit van  
onmisbare gegevens in computers



dinsdag 28 april 1992, Beurs-World Trade Center Rotterdam

No:

36043

Ex:

1

Met medewerking van:

VU AMSTERDAM  
ABN-AMRO BANK  
PHILIPS CRYPTO BV  
SCOLL IT SECURITY  
COSECO INTERNATIONAL BV  
KPMG KLYNVELD EDP AUDITORS  
IBM INFORMATION NETWORK EUROPE  
MINISTERIE VAN BINNENLANDSE ZAKEN  
CENTRALE RECHERCHE INFORMATIEDIENST  
FYSISCH EN ELEKTRONISCH LABORATORIUM TNO  
NEDERLANDS GENOOTSCHAP VOOR INFORMATICA

Dagvoorzitter  
Prof.Dr.Ir. R. Paans RE  
Vrije Universiteit Amsterdam en IBM Nederland NV

MCNL  
Postbus 359  
5600 AJ Eindhoven

Port betaald  
Port Payé  
Eindhoven



**mikrocentrum** nederland