




EUROPEAN COMMISSION

DIRECTORATE GENERAL XIII: Telecommunications, Information Market and Exploitation of Research  
DIRECTORATE B: Advanced Communications Technologies and Services



**Green Paper**  
on the  
**Security of Information Systems**

April, 1994

EO

# Table of Contents

Preface .....	1
Summary of Requirements for Action .....	3
Acknowledgement .....	7
1. Introduction .....	11
2. Scope .....	12
3. General issues .....	14
3.1. Globalisation of the economy and Mobility .....	15
3.2. Internal Market ("four freedoms") .....	15
3.3. Human Rights and the Protection of Communications .....	16
3.4. Social Acceptance of Identification and Authentication Methods .....	17
3.5. Human Rights and the Safety of Systems .....	19
3.6. Confidence in Communication Systems and Services .....	19
3.7. Management of Openness and Protection .....	21
3.8. Common Concerns of Commercial and National Security .....	23
3.9. Security and Law Enforcement on International Scale .....	23
3.10. Economics of the Security of Information Systems .....	24
3.11. Social Recognition of Information Crime .....	26
3.12. Human Factors .....	27
3.13. Safety Critical Environments .....	27
3.14. Embedding Systems .....	28
4. Demand Related Issues .....	30
4.1. Requirements for Enterprises and Individuals .....	31
4.1.1. Agreement on Security Requirements for Enterprises .....	31
4.1.2. Security Administration .....	33
4.1.3. Security Objectives for Enterprises .....	34
4.1.4. Exploiting Innovation .....	35
4.1.5. Sectoral Specifics .....	36
4.1.6. Security Domains .....	37
4.1.7. Security Labelling .....	38
4.1.8. Administration of Access to Security Related Data .....	39
4.1.9. Security Requirements for Individual Users .....	39
4.2. Requirements for Security Functions .....	40
4.2.1. Access Control .....	41
4.2.2. Requirements for Electronic Cash .....	42
4.2.3. Requirements for Security Services .....	43
4.2.4. Digital Signature .....	46
4.2.4.1. The Individual Right to Signature .....	46
4.2.4.2. Consistency of Legal Principles for Digital Signatures .....	47
4.2.4.3. Universal Acceptance of Digital Signatures .....	49
4.2.5. Privacy enhancement Issues .....	49
4.2.5.1. Perception of Requirements for Privacy Enhancement .....	49
4.2.5.2. The Case for the Provision of Public Confidentiality Services .....	52
4.2.6. Use of Names and Certifications of Credentials .....	54
4.2.7. Security of Electronically Stored Information .....	56
4.3. Requirements for the Safety of Communication Systems .....	57
4.4. Requirements for Evaluations .....	58
4.4.1. Trustworthiness of Communication Solutions .....	58
4.4.2. Motivation to Acquire Evaluated Solutions .....	60
4.4.3. Consistency of Procurement Practices .....	60
4.4.4. Operational Systems Accreditation .....	61

4.5.	Requirements for Security and Safety Methodologies .....	62
4.5.1.	Risk Analysis and Management .....	62
4.5.2.	Metrics for Loss Assessment .....	64
4.5.3.	Technology Assessment .....	64
4.5.4.	Analysis of Audit Trails .....	65
4.5.5.	Safety Specific Methodologies .....	66
4.6.	Requirements for Audits .....	67
4.7.	Information Valuation .....	67
5.	Supply Related Issues .....	69
5.1.	Supply Related Issues- Ways to meet the Security Demands .....	69
5.1.1.	Security Services .....	69
5.1.2.	Signature Schemes .....	73
5.1.3.	Confidentiality Schemes .....	74
5.2.	Supply Related Issues - Security Management .....	75
5.2.1.	Role of Trusted Third Parties (TTPs) .....	75
5.2.2.	Key Usage .....	78
5.2.3.	Key Management Service .....	79
5.2.4.	Distributed-Secret Escrow Systems .....	80
5.2.5.	Management Services for Names and Credentials .....	81
5.2.6.	The Management of TTPs .....	82
5.2.6.1.	Operating Principles of TTPs .....	82
5.2.6.2.	Interworking of TTPs .....	83
5.2.6.3.	Interworking of Autonomous Confidentiality Services .....	84
5.2.6.4.	Accreditation and Audit of TTPs .....	85
5.3.	Supply Related Issues - Evaluation of Trusted Solutions .....	86
5.3.1.	Evaluation of Products, Systems, Services and Applications .....	87
5.3.2.	International Harmonisation and Mutual Recognition .....	87
5.3.3.	Supplier Declarations .....	89
5.3.4.	Self-evaluation .....	89
5.3.5.	Evaluation of Applications .....	90
5.3.6.	Evaluation of Communication Services .....	91
5.3.7.	Trusted Network Management .....	92
5.3.8.	Evaluation of Methods and Tools .....	93
5.3.9.	Physical and Procedural Issues .....	94
5.3.10.	Modifications to Evaluated Products and Re-evaluation .....	94
5.3.11.	Performance Reporting for Trusted Products .....	95
5.3.12.	Rationalisation of Evaluations .....	96
5.4.	Maintenance of Safety and Assurance .....	97
5.5.	Technological Change .....	98
5.5.1.	Evolving technology .....	98
5.5.2.	Technology for trusted products .....	100
6.	Rights, Responsibilities and Liabilities .....	102
6.1.	Legal Framework .....	102
6.2.	Data held in Electronic Form .....	103
6.3.	Environment .....	107
6.4.	Interaction and Relationships between Private Parties .....	109
6.5.	Harm .....	110
6.6.	Eliminating and Mitigating Harm .....	110
6.7.	Legal Restrictions affecting Technical Solutions .....	112
6.8.	Limitations to Liability .....	112
6.8.1.	Recommendations for Liability Limiting Measures .....	112
6.8.2.	Information Security Audit .....	113
6.9.	Procedural Jurisdictional Issues .....	114
6.10.	Insurance Issues .....	115

7.	Spectrum of Measures to provide Information Security .....	117
7.1.	Policy Framework and Consensus .....	117
7.2.	Agreements .....	118
7.3.	Regulation and Legislation .....	118
7.4.	Accreditation .....	118
7.4.1.	Accreditation of Services .....	118
7.4.2.	Accreditation of TTPs .....	119
7.5.	Products and Services .....	119
7.6.	Common Practices and Codes of Conduct.....	119
7.7.	Awareness, Education and Training .....	121
7.8.	Specifications .....	121
7.9.	Standards .....	121
7.10.	Technology .....	122
8.	Cross Impact Analysis .....	123
Annex 1	Recalling the Action Lines.....	143
	Action line I - Development of a strategic framework for the security of information systems .....	143
	Action line II - Identification of user and service provider requirements for the security of information systems.....	144
	Action Line III - Solutions for immediate and interim needs of users, suppliers and service providers.....	144
	Action line IV - Development of specifications, standardisation, evaluation and certification in respect of the security of information systems .....	146
	Action line V - Technological and operational developments in the security of information systems.....	147
	Action line VI - Provision of security of information systems .....	148
Annex 2:	Recommendation of the Council of the Organisation for Economic Co-operation and Development (OECD) .....	151
Appendix A:	References .....	157
Appendix B:	Abbreviations .....	159
Appendix C:	Index .....	161

## **PREFACE**

The Council adopted in March 1992 a Decision in the field of the security of information systems<sup>1</sup> comprising the development of overall strategies for the security of information systems (action plan) and setting up a Senior Officials Group (SOG-IS) to advise the Commission on action to be undertaken. The Decision having as objective the development of overall strategies aiming to provide users and producers of electronically stored, processed or transmitted information with appropriate protection of information systems against accidental or deliberate threats.

The scope of the Decision foresees the following lines of action:

- I. Development of a strategic framework for the security of information systems
- II. Identification of user and service provider requirements for the security of information systems
- III. Solutions for immediate and interim needs of users, suppliers and service providers
- IV. Development of specifications, standardisation, evaluation, and certification in respect of the security of information systems;
- V. Technological and operational developments in the security of information systems; and
- VI. Provision of security of information systems.

Annex 1 recalls the Action Lines.

The Decision is implemented by the Commission, in close association with related actions in Member States and in conjunction with related Community research and development actions.

As a step towards the formulation of the "Action Plan" identified in the Council Decision and in accordance with the opinion of SOG-IS<sup>2</sup> a "Green Paper on the Security of Information Systems" has been prepared, which addresses, in accordance with the Annex of the Decision, an overall view of the

- requirements for action in summary form
- issues involved
- spectrum of measures that result from an analysis of the issues.

The present document sets out the background to the development of a consistent approach to Information Security in Europe taking into account common interests with other countries.

---

<sup>1</sup> OJ No L 123, 8.5.1992, p.19

<sup>2</sup> SOG-IS Opinion of 17.11.92 on objectives, scope and approach

## **Nature of Document**

**This document is consultative in nature and comments are invited to be addressed to the European Commission before August 1st 1994.**

**The purpose of the Green Paper is to share the insight and awareness obtained from the numerous contributions to the articulation of the Green Paper and to consult the parties concerned and interested on the actions and measures considered necessary to address the needs of the European Union in the field of information security.**

**The Green Paper states the main issues related to the security of information systems in their context, describes requirements, and summarises the requirements into a series of proposed positions and actions.**

**The proposed positions and actions address the needs identified for Trusted Services in Europe, International Developments and Technical Harmonisation in Information Security.**

# SUMMARY OF REQUIREMENTS FOR ACTION

## 1. Introduction

The trustworthiness and protection of information is essential for the functioning of a modern society.

Information Security threats are growing with the diversification and multiplication of communication services and use of electronic information by business, administrations and the individual.

In the last decade, the Community has been working progressively towards the creation of the Internal Market and led a policy of liberalisation and harmonisation in the field of communications services.

When the INFOSEC Decision was adopted it was recognised that the threat to information security would need a collective effort on the European level and it set as objective the formulation of an Action Plan to complement the national actions in a well understood spirit of subsidiarity as far as national and internal security was concerned.

The purpose of this section of the document is to set out the critical factors for future developments and the action required to ensure trustworthy information services and applications in Europe and in its relations with other parts of the world. It formulates options for future policy and identifies actions which promise to best meet the needs of the EC in the context of international developments and trends.

## 2. Proposed Positions and Actions

Based on the results of the enquiry having resulted in the Green Paper, needs for action on an EC-scale have been identified. These require a concerted approach within Europe and where possible internationally. The following proposed positions and actions are derived from the results of the work so far.

### ***General Position***

Democratic societies engaged in the global economy need to provide for adequate levels of information security. With the growing diversity of services and applications of telematics the security of information systems will need to evolve with demand and reduce the threats to security, privacy and safety while avoiding to obstruct innovation or economic and social developments.

### **A *Trust Services***

#### **Proposed Positions**

- In the emerging information society traditional techniques of securing information, such as signatures, envelopes, registration, sealing, depositing and special delivery need to be matched by electronic equivalents.

- The protection of the user, service provider, operator and the collectivity should be conserved and the balance between freedom and responsibility not changed in an uncontrollable manner.
- Service offerings need to cater for the needs for seamless information security for business, the general public, video and multimedia communications and teleworking, in the non-classified domain.
- The working of the Community Institutions and the EC-wide operation of public administrations of the Member States, can be expected to rely on a combination of these services, as appropriate.
- The definition of information crime and the rules governing the technical realisation and use of electronic evidence in civil and criminal court proceedings need to be harmonised within the EC to be able to address cases involving trans-European services and applications. In the absence of such harmonisation, “safe havens” for illegal activities can form to the detriment of the EC.
- As the economy becomes global, and the interrelationship among the different actors tighter, the accepted practices and rules to which these actors operate need to be well defined and transparent, implying a coherent codification of essential practices and relations.
- As Europe formulates and implements policies depending on, or affecting, information security, the consistency overall is demanding a greater attention. Specifically this relates to the new policies under the Maastricht Treaty, Internal Market, Competition, and Telecom Policies and specific actions such as Open Network Provision (ONP Directives) and Trans-European Networks (TENs).

### **Proposed Actions**

- to provide for the setting up of trust services and for consistent means to interact with these services. Trust services include digital signature, non-repudiation, claim of origin, claim of ownership in negotiable documents, fair exchange of values, untraceability, and time stamping
- to provide for the establishment of Europe-wide confidentiality services for non-classified information. These could include the following categories:
  - > *minimum IS assurance* to be maintained by all service providers (level of present letter mail and telephony under national privacy legislation)
  - > *enhanced IS assurance* for private and professional use (level of registered mail or courier delivery as needed for normal business transactions such as ordering and billing)
  - > *professional IS assurance* as needed for recognised categories of commercially (or otherwise) sensitive information
- to establish, accredit and audit a network of Trusted Third Parties for the administration of the service provisions such as for name assignment, key management, certification and directories
- to formulate a common EC-wide legal and regulatory Framework for the alignment of national conditions to meet the needs of the Internal Market and international developments in information security



- to establish the liability principles for information providers, intermediates, Trusted Third Parties, and value added service providers
- to put in place arbitration mechanisms to resolve liability conflicts
- to establish the common principles for legislation covering communication crime and for electronic evidence
- to develop generic codes of practice for the handling of non-classified information, including rules for security labelling
- to develop sector-specific codes of practice and base line controls.

## ***B International Developments***

### **Proposed Position**

- In view of the rapidly evolving international communication and security scene, the security needs of the European organisations and individuals must be safeguarded and the competitiveness of the European industry maintained.
- The creation of barriers to trade and services based on the control over security mechanisms and digital signature schemes needs to be avoided. In case acceptable international solutions can not be found a European option should be considered.

### **Proposed Action**

- to work towards international solutions for information security requiring global assurance
- to strengthen the support for international standardisation
- to formulate common positions swiftly with respect to international developments, as they arise
- consider offering European options for confidentiality and digital signature services internationally.

## ***C Technical Harmonisation***

### **Proposed Positions**

- Vendors and service providers need to innovate to survive commercially. They have a vital interest in ensuring that their products are adequately secure and safe.
- Electronic products, systems, services and applications must operate to generally recognised levels of trust.
- A differentiated approach to the evaluations of trusted solutions is needed which includes vendor declaration, self evaluation or formal evaluation. The choice of either of these mechanisms will depend on the costs and delays involved in formal certification processes, the level of assurance required and national constraints.
- The international character of service and product supply requires the establishment of mutual recognition of testing, validation, auditing and liability assessment.

- **Safety, security and quality have many commonalities: these must be exploited to reduce cost and delays in evaluations.**

### **Proposed Actions**

- **to establish an international scheme for evaluation, certification and mutual recognition, that provides for integrated security, safety and quality evaluations for applications, services, systems and products**
- **to raise the general level of information security and safety by promoting development assurance**
- **to establish the principles for incident reporting obligation for evaluated solutions, and their dissemination**
- **to establish principles for incident containment**
- **to establish a scheme for service provider and vendor self-evaluations and declarations**
- **to specify community-wide quality criteria for the safety of systems, incl. methodologies for the assessment of threats, vulnerabilities, and hazards for safety critical systems**
- **establish rules for the assurance of embedded systems.**

## ACKNOWLEDGEMENT

The present document is the result of numerous contributions received from experts, working in the framework of IBAG, SRI, ETNO, the Security Investigations and SOG-IS (over 200 contributions received). To develop the thinking on specific groups of issues, the SOG-IS Advisory Group, reinforced by other experts, were consulted and contributed to the development of the document. In a spirit of openness, qualified contributions were accepted from all parties ready to contribute and to discuss their input in the context of international workshops<sup>3</sup>, that served to consolidate the views into a coherent presentation.

While the experts acted in a personal capacity, their affiliation is included in the list below as an indication of the range of experience which was drawn upon.

The contributions and active involvement in the preparation of this document of the following personalities is gratefully acknowledged:

C.	Amery	Zergo Consultants Ltd.	UK
K.	Anstötz	BIFOA	D
Mr.	Auer	Siemens Nixdorf	D
G.	Axelsson	Swedish Agency for Administrative Development	S
E.	Barrêto	CEC DGIII/B	
M.	Baum	Independent Monitoring	USA
T.	Benjamin	Défence Research Agency	UK
E.	Bible	Cameron, Markby and Hewitt	B
H.J.	Bierschenk	IBAG	D
D.	Birch	Hyperion	UK
J.	Birenbaum	France Telecom	F
J.	Blackwell	CEC DGXIII/C	
C.	Blatchford	Panacea Ltd	UK
R.E.	Bloomfield	ADELARD	UK
K.	Brady	Unix Operating System Engineering	USA
A.	Brignone	Protexarms	F
S.E.	Brummel	Akin, Gump, Strauss, Hauer, Feld & Dassel	B
A.J.	Butcher	MOD - Royal Air Force	UK
L.	Cabirol	SCSSI	F
R.	Cadwallader	ENACT Ltd.	UK
P.	Carriot	France Telecom	F
S.	Castell	CASTELL	UK
E.	Cauvin	Agence pour la protection des programmes	F
D.	Cerny	Bundesministerium des Innern	D
B.J.	Chorley	NPL	UK
J.	Christensen	CEC DGXIII/C	
C.	Clark	IBAG	UK
R.	Clark	University of Dublin	IRL

---

<sup>3</sup> A previous draft of the document (draft 4.0) was made widely available through paper copies and electronic means. It was scrutinised by over 1000 experts in the field.

A workshop was held on December 15, 1993 to which interested parties were invited to:

- a) comment on the conclusions and recommendations (section "Summary of Requirements for Action")
- b) identify existing work and activities that could contribute to the implementation of some or all of the recommendations
- c) formulate suggestions for the implementation of the recommendations
- d) signal interest to participate in the implementation of the recommendations.

A wealth of information was communicated prior and during the workshop, but no clearly defined solutions to the problems were identified. There are no apparent ready-made solutions that can be applied in an international context.

B.	Collins	PCSL Consulting	UK
J-F.	Cornet	ECOLORG	F
C.J.	Coumou	Coseco International BV	NL
J.M.	Court	Institute of Chartered Accountants	UK
E.	Daclin	Acatel Alsthom Recherche	F
H.	Daniel	BSI	D
P.	Daniel	GEC Marconi Secure Systems Ltd.	UK
J.	De Decker	IBM	B
D.	De Geest	ESN	B
B.	De Schutter	Free University of Brussels	B
M.	De Soete	Philips I.T.S.	B
D.	De Winter	Siemens Nixdorf AG	D
Mr.	de Kervasdoue	CAP SESA	F
A.	de la Torre Prados	Ministerio de Industria	E
E.R.	de Lange	Ministry of Transport, Public Works and Water Management	NL
P.	de Lauzanne	GSIT	F
T.	de Vries	KPMG Management Consultants	NL
P.	Dellios	Ministry of Transports and Communications	GR
Y.	Deswarte	LAAS-CNRS & INRIA	F
R.	Dierstein	DLR	D
G.	Dietzel	CEC DGXIII/C	
R.	Dunkel	IBM Europe	F
D.	Duthil	Agence pour la protection des programmes	F
G.	Eisen	IABG	D
G.	Endersz	Telia Research AB	S
R.A.	English	Communications Security Establishment	UK
G.	Enste	CAP debis GEI	D
A.	Eriksen	Ministry of Justice	N
P.	Fagan	Secure Information Systems Ltd.	UK
A.	Fisher	Fischer International Systems Inc.	USA
Mr.	Fravezzi	Ministry of Defence	B
A.	Fujioka	NTT Laboratories	Japan
P.	Furberg	c/o Swedish Agency for Administrative Development	S
S.	Gaskill	Dibb Lupton Broomhead	UK
M.	Gasparinetti	CEC Consumer Policy Service	
H.P.	Gebhardt	CEC DGXIII/A	
S.	Geyres	VERILOG	F
L.	Glanert	Deutsche Telecom	D
S.E.	Greenfield	NIST	USA
H.	Hagemann	FernUniversität Hagen	D
A.	Hallan		L
R.	Hanouz	CEPME	F
N.G.L.	Harding	Health Systems Co-ordination	UK
G.	Hardy	Touche Ross & Co.	UK
N.	Harwood	BT	UK
P.	Haufman	SPRI	S
S.	Herda	GMD	D
V.	Heyvaert	Akin, Gump, Strauss, Hauer, Feld & Dassel	B
N.	Higham		UK
G.	Hoberg	BELGACOM	B
P.	Hoving	TeleTrust S	S
E.	Humphreys	XiSEC	UK
D.	Hurley	OECD	
F.	Iribarne Navarro		E
K.	Iversen	Norwegian Centre for Medical Informatics	N
E.	Jahren	Ministry of Government Administration	N
C.	Jansen	Philips Crypto B.V.	NL
M.	Jones	DTI	UK
L.	Kahn	ETNO - Telia AB	S
M.	Kemna	CEPIS Task Force	NL
M.	King	CESG	UK
H.M.	Kluepfel	Bellcore	USA
P.	Knopf	Swiss Mission to the E.C.	B

T.	Knowles	DMR Group Ltd.	UK
M.	Kopecky	SNCF	F
S.	Kowalski	Stockholm University	S
M.	Krimizis	G&K Multimedia	GR
H.	Kurth	IABG	D
S.	Kurzban	PACE	USA
D.	Lafont	SCT-DPusers	F
R.	Lampard	NPL	UK
P.	Landrock	Cryptomathic A/S	DK
J.	Lang	Perihelion Software Ltd.	UK
C.	Laske	Free University of Brussels	B
Y.	Le Roux	Digital Equipment	F
J.	Leach	Zergo Consultants Ltd.	UK
A.	Legait	SYSECA	F
O.	Leiberich		D
E.	Lemmens	Programmation de la Politique Scientifique	B
J.M.	Lemuzeau	Alcatel Alsthom Recherche	F
K.	Lindup	SRI	UK
W.	London	Cameron, Markby and Hewitt	UK
F.	López Crespo	Ministerio para las administraciones publicas (MAP)	E
C.P.	Louwerse	CEN/TC251/WG6 - Leiden University Hospital	NL
M.	Mackenbrock	BSI	D
W.	Madsen	Computer Sciences Corporation	USA
N.P.	Mansfield	Shell Internationale Petroleum Maatschappij B.V.	NL
L.	Martin	National Security Agency	USA
S.	Mathews	PCSL Consulting	UK
M.	Mavis	ETNO - OTE	GR
R.A.J.	Middleton	British Computer Society	UK
M.	Miloikovitch	Thomson-CSF	F
S.	Mohammed	European Parliament	
R.	Moses	Information Systems Ltd.	UK
G.	Moustakas	G&K Multimedia	GR
P.	Müller	Bull Ingénierie	F
M.	Nasrullah	Ministry of Transport, Public Works & Water Management	NL
S.-I.	Nilsson	ECITC	B
J.	Norman	SGS-Thomson Microelectronics	F
M.	Ohlin	Swedish Defence Material Administration	S
T.	Olhede	Spri	S
T.	Osvald	ECTIC - CEN	B
K.W.	Ott	Ott Technology Software sprl	B
A.	Parondo	ISDEFE	E
A.	Patel	Teltec	IRL
L.	Pauwels	Belgacom	B
A.	Peralta	Univ. Politecnica de Cataluna	E
P.	Perrot	France Telecom	F
H.	Peuckert	Siemens AG	D
C.	Pfleeger	Trusted Information Systems (UK) Ltd.	UK
F.	Piau	Pari Mutuel Urbain	F
E.	Pimentel Saraiva	Banco Totta & Acores	P
D.	Pinkas	Bull	F
R.	Pizer	Certification Body, UK ITSEC Scheme	UK
D.	Poelmans	EDS B nv	B
R. I.	Polis	Groupe de Management Genève	CH
K.	Prestun	Alcatel	F
G.R.	Price	The Institute of Internal Auditors - Glynwed Group Services	UK
M.	Purser	Baltimore Technologies Ltd.	IRL
G.	Rabe	Technischer Überwachungs-Verein Nord e.V.	D
K.	Rannenber	Universitaet Freiburg	D
R.	Rehorst	Telecommunications and Post Department	NL
K.	Rihaczek	DuD	D
E.	Roback	Computer Systems Laboratory	USA
G.	Roelofsen	PTT NL	NL
T.	Roraas	Norwegian Telecommunication Regulatory Authority	N

C.	Rossi	FTI	I
R.A.	Rueppel	R3 Security Engineering AG	CH
G.	Ruggiu	Bertin	F
G.	Rumi	ETNOTEAM SpA	I
M.	Salmon	Thomson CSF	F
E.H.	Schäfer	Deutsche Telecom	D
I.	Schaumüller-Bichl	Genesis GmbH	A
T.	Schoeller	BSI	D
G.	Shuringa	Radobank	NL
U.	Sieber	Universität Würzburg	D
H.	Siebert	IBM Deutschland	D
F.	Simoes	European Parliament	
R.	Slegtenhorst	Organisation and Technology Research NV	B
S.	Smith	EDS B	B
J.	Sneep	COSSO	NL
J.W.	Steed		UK
H.	Strack	EISS - Universität Karlsruhe	D
W.	Suchun	FUNDP	B
C.	Sundt	ICL Secure Systems	UK
M.	Tuset		E
R.	Urry	Digital Equipment Corp.	B
I.	Uttridge	Logica Defence & Civil Government Ltd.	UK
P.	van Dijken	Shell International Petroleum	NL
P.W.J.	van Dok	Cooperative Centrale Raiffeisen-Boerenleenbank B.A.	NL
H.	van Dorp	Bazis Foundation	NL
W.	van Gils	Intercai	NL
M.	van Lith	KPMG EDP Auditors	NL
N.	van Zuuren	Prodata Systems	B
A.	Veller	Cullen International	B
A.	Verrijn-Stuart	CEPIS - Leiden University	NL
M.	Volpe	STET/SIP	I
L.	Voorham	CEC Security Office	
M.	Waidner	E.I.S.S. - Universität Karlsruhe	D
C.	Weber	Tandem Computers GmbH	D
H.	Weerd	Coopers & Lybrand	NL
W.	Whitehurst	IBM Corporation	USA
K.	Wiessing	The Dutch Government Centre for Information Security	NL
G.	Williams	ACT/BIS Information Systems Ltd.	UK
D.	Willis	DTI	UK
S.	Winkelmann	Hochschule für Technik u. Wirtschaft	D
H.	Wirth	Auswärtiges Amt	D

## 1. INTRODUCTION

Individual, corporate and national wealth expresses itself increasingly in the form of information. The growth and performance of an estimated 2/3 of the economy relies on manufacturing or services heavily dependent on information technology, telecommunications and broadcasting, and therefore depends critically on the accuracy, security and trustworthiness of information. This is of as great importance and interest for individuals as for commerce, industry and public administrations. Correspondingly, the protection of information in all its aspects, here referred to as Information Security<sup>4</sup>, has become a central policy issue and a major concern world-wide.

The Council Decision of March 31, 1992<sup>5</sup> in the field of security of information systems recognises this situation and calls for the "development of strategies to enable the free movement of information within the single market while ensuring the security of the use of information systems throughout the Community".

A consistent approach at European level could help to promote the interoperability of systems, lower existing barriers and avoid the formation of new ones between the individual Member States and with other countries<sup>6</sup> in compliance with the competition rules and the Internal Market policies. Therefore, there is an urgent need to address requirements and options for action in the field of security of information systems at national, Community and international level in close collaboration with sector actors and national governments. Any action must take into account both national and international commercial, legal and technical developments.

The key issue is to provide effective and practical security for information held in an electronic form to the general users, the business community and administrations without compromising the interests of the public at large.

Since information security is involved in the protection not just of property and people, but even of society itself, Member States regard it as a topic which, like defence, touches on national sovereignty.

---

<sup>4</sup> Information Security is concerned with the protection of information stored, processed or transmitted in electronic form, against deliberate or accidental threats.

Information is acquired, communicated, processed and stored by Information Services. Electronic Information services need a secure communication infrastructure, secure terminals (including processors and data bases) as well as secure usage. The management of the service provision itself must also and foremost be secure. Therefore the approach to information security starts from an analysis of the needs of an individual or organisation for Information Services.

<sup>5</sup> 92/242/EEC

<sup>6</sup> This danger has already been identified and OECD Member Countries have, in the context of Protection of Privacy and Transborder Data Flow of Personal Data, recognised the risk of new technical barriers forming. They have therefore agreed to endeavour to remove and to avoid to create in the name of privacy protection, unjustified obstacles to transborder flows of personal data, co-operate in the implementation of the Guidelines and agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

## 2. SCOPE

Security is a pervasive subject that arises whenever information is being used in private, business and public life. The scope of the subject and a clear distinction of the of the different dimensions needs to be kept in mind throughout. The diagram below provides a statement of the scope in an aggregate form.

Provision of enhanced information systems security for	Concerning	For systems and telematic services dealing with	General requirements	Realisation
<div style="border: 1px solid black; padding: 5px; width: fit-content;">           General public            Business            Special groups            Administrations            Products            Systems            Services            Applications         </div>	<div style="border: 1px solid black; padding: 5px;">           Availability and utility            Integrity and authenticity            Confidentiality and possession            Authentication            Authorisation            Non-Repudiation            Auditability            Safety            Fail-safe            Robustness            Data protection            Legal Evidence            Timeliness         </div>	<div style="border: 1px solid black; padding: 5px; width: fit-content;">           Audio            Data            Image            Multi-media         </div>	<div style="border: 1px solid black; padding: 5px;">           Openness            General interest            Global/international            General acceptance            General availability            Free competition            Economically viable            Easy to use            Feasible            Conform to different legal conditions            Safeguard legitimate interests            Harmonious development            Intermediaries         </div>	<div style="border: 1px solid black; padding: 5px;">           Consensus formation, agreements and frameworks            Awareness, education and training            Common practices and conduct            Standards and Specifications            Products, services and technology            Regulation and legislation            Certification and accreditation         </div>

### Structure of this document

The core of the document is describing issues and the resulting requirements for action. It was felt necessary to state the problems clearly and concisely before attempting to define solutions. In this sense, the document, in its present form, represents a rather comprehensive analysis of the problems, without being a work programme. The requirements for actions are stated in a general form, without implying any particular organisational responsibility. These issues are grouped under the following headings:

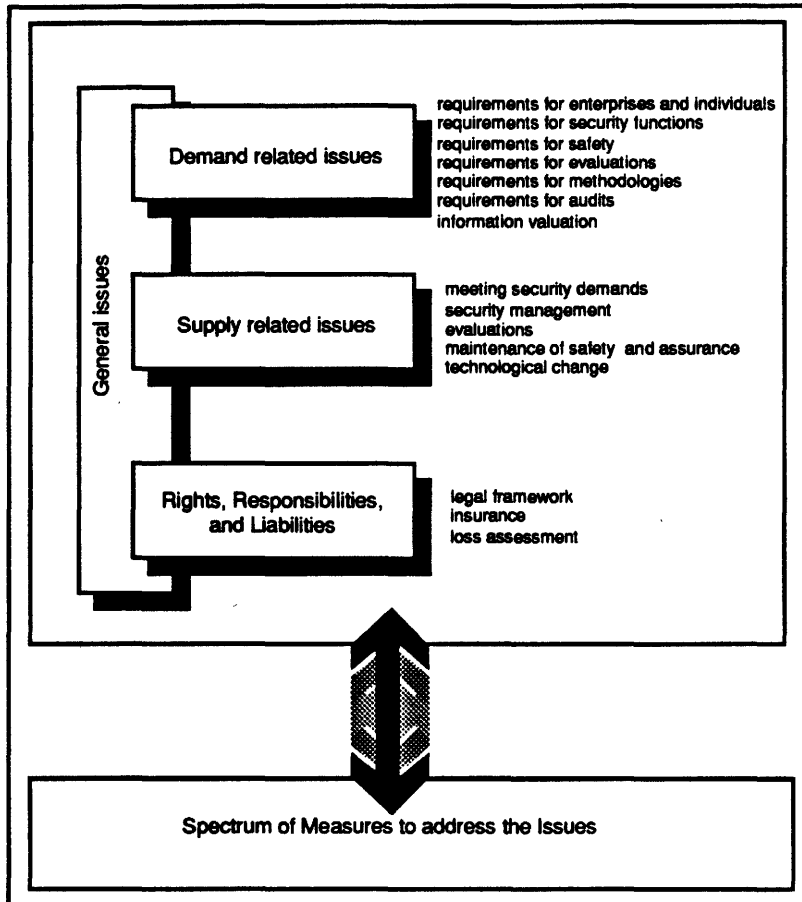
- *General issues.* Here some of the basic issues relating to the security of information systems are described. These place security into a fast evolving world economy and states issues like rights and obligations, human rights, openness and protection.
- *Demand related issues.* Issues under this section are concerned with requirements, security objectives, Codes of Practice, and the needs for digital signature and privacy enhanced communications.



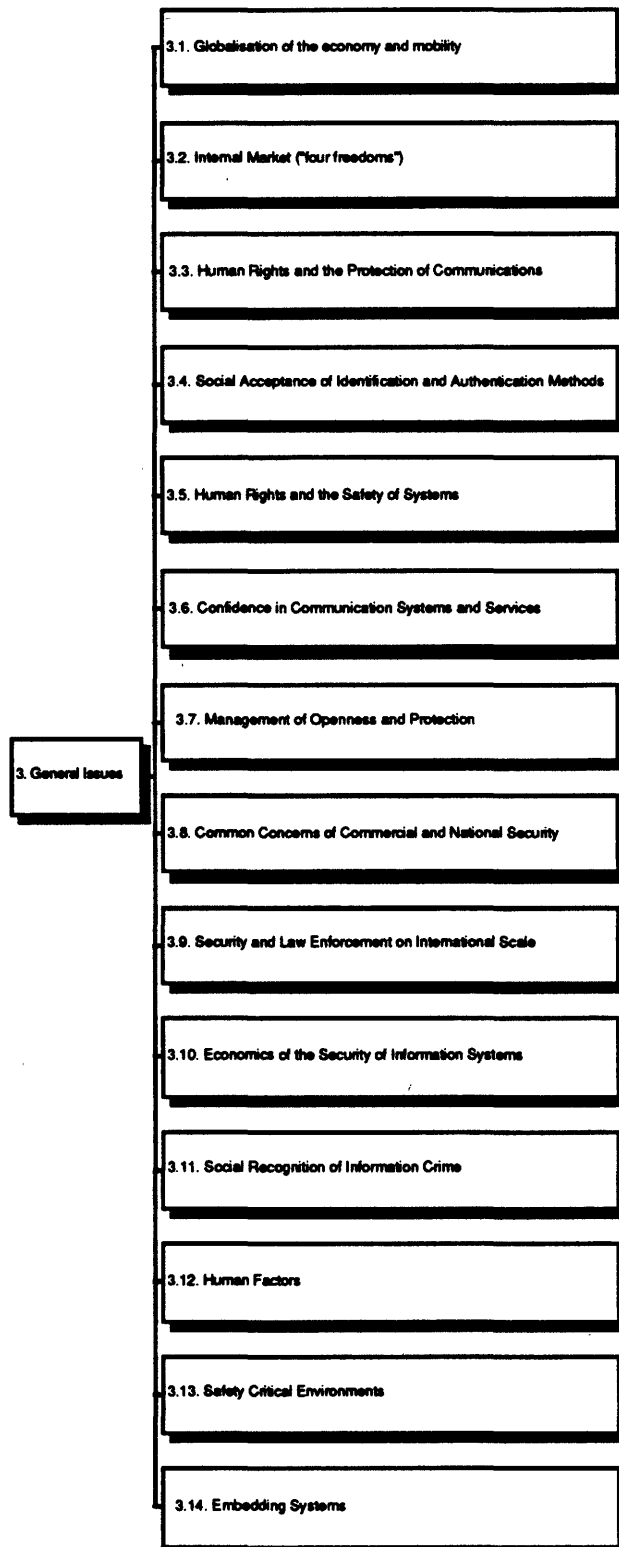
- *Supply related issues.* Under this heading, issues are identified which arise when meeting the demand for security and include security services, Trusted Third Parties, evaluation and R&D.
- *Rights, responsibilities and liabilities issues.* Under this heading issues relating to the consequences of security breaches are dealt with. These include civil law and insurance.

The measures one can consider addressing the issues identified are aggregated in a separate section. This presentation is used to accentuate the profile of issues which can be addressed by the same kind of measures.

The diagram below depicts this structure.



### 3. GENERAL ISSUES



#### 3.1. Globalisation of the economy and mobility

## **Issue**

The internationalisation, diversification, pluralisation and popularisation of the use of communications and information systems.

## **Discussion**

The unprecedented increase in mobility and the provision of global communications has resulted in manufacturing, trade and leisure activities extending world-wide. Distributed manufacturing, publishing, and financial operations form the back-bone of the modern economic system. Travelling and communications for business or pleasure are common place. This is being supported, and sometimes driven, by a spectacular development in the field of communications and by the proliferation of affordable and easy to use information systems. In the last decade the cost-performance of long-distance transmission has improved by 5 orders of magnitude. This change is providing the basis for a rapid diversification of world-wide services customised to provide access to a full range of information services and utilities wherever and whenever required. Terrestrial, satellite and mobile networks provide the physical infrastructure and an unrestrained number of service applications provide the customised applications.

The nature and scope of provision of Information Security in this new world of open, multi-service and multi-media communications with a multitude of alternatives to routing, management and access has profoundly changed the requirements and options for Information Security (IS).

Flexibility of access, openness of the network and the service environment have to be balanced against the requirement of accountability of the user and the service provider and the protection of possible third parties involved. Associated with this is a new network of responsibilities and liabilities.

## **Requirements**

- Revision of the scope and approach to information security to reflect the new conditions, challenges and requirements brought about by globalisation
- adaptation of the respective policies and regulations
- clearly defined conventions on the expectations, responsibilities, duties and liabilities, related to levels of security, harm, and good practices.

## **3.2. Internal Market; ("four freedoms")**

### **Issue**

Alignment of the national conditions relating to Information Security with the requirements of the functioning of the Internal Market.

### **Discussion**

The Internal Market, as adopted in the "Single Act", provides for the "four freedoms" within the Community, ie free movement of goods, capital, services and people. The legislation of Member States provides for the internal needs for information security, however the requirements in the case of trans-European communications remains to be addressed. Inconsistent or incomplete provisions of information security and safety represents a technical obstacle to the working of the Internal Market.

The measures taken to establish confidence in systems should not adversely affect the flow of goods and services. Standardisation, certification, mutual recognition and administrative procedures should provide for the unobstructed working of the Internal Market. This requires standards that are valid but not overly restrictive on technological solutions, and certification regimes that recognise the international aspects of many of the markets (eg in avionics, motor vehicles), the costs of certification, and the likely acceptance by the market of any certification regimes put in place.

Beyond the technical aspects, the administration of information security needs to reflect the realities of the needs of the Internal Market. Services are to be increasingly provided on the principle of "one-stop" and "pay-per-use". Information security, as an integral part of services, needs to be provided in a seamless manner throughout the Community and support EC actors in their business world-wide.

Related are the issues of liability and insurance. The impact of different states legal systems and the associated liability issues needs to be understood.

### **Requirements**

- Adaptation of the existing provisions with respect to their conformance to the Internal Market policy of the EC implying the removal of existing internal barriers and the avoidance of the formation of new technical barriers due to divergent application of security and safety rules, regulations and legislation
- provision to business and the public of solutions available throughout the Community and preferably at the international level respecting the "one stop" and "pay-per-use" principles
- consistent deployment of standards and certification where critical for the working of the Internal Market
- certification and standards that reflect the needs of the different market segments.

## **3.3. Human Rights and the Protection of Communications**

### **Issue**

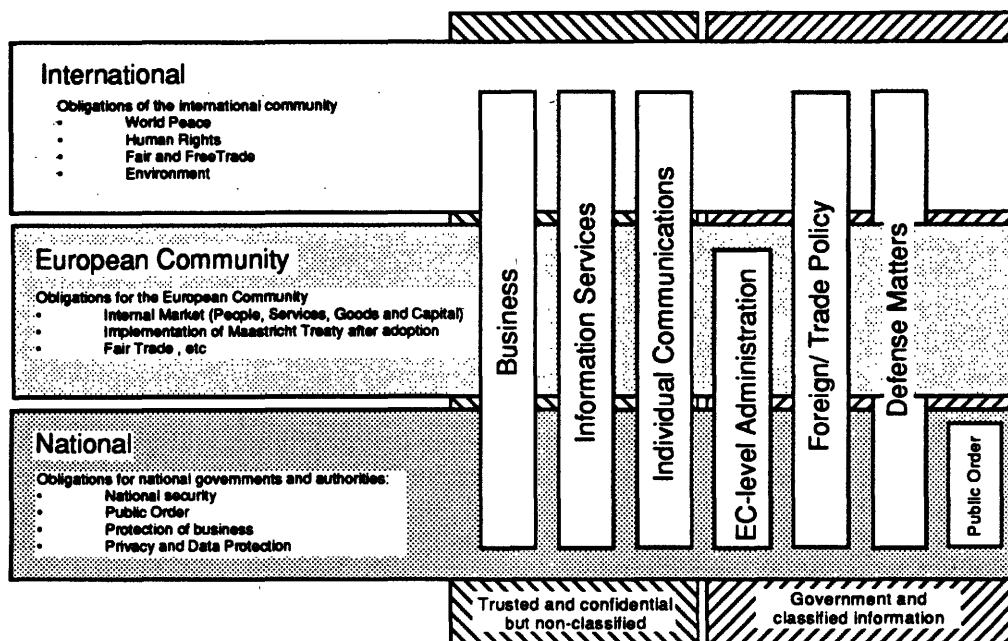
To reconcile the human right to privacy and the obligations of law enforcement to protect public order.

### **Discussion**

Privacy and the protection of private information is considered one of the fundamental human rights of individuals and is protected to varying degrees in Member States. The European convention on Human Rights states "Everyone has a right to respect for his private and family life, his home and his correspondence". Individuals have the legitimate expectation that this right is respected and that solutions are made available to him that ensure the safeguard of this right. This applies to conversation in the home and to a lesser degree when telecommunications is being used. However, prevailing national solutions do not, at present, provide for trans-European services and communications and this lack can be exploited, inter alia, by organised crime. With the rapid growth and diversification of communication services the rights and duties of individuals and law enforcement are being reviewed and redefined, eg FBI supported legislation and the proposal of the government to provide US business and citizens with cryptographic devices including explicit provision for intercept by law enforcement agencies.

As the safety and security of the individual provided by the process of law and order is also related to human rights, reconciling these objectives represents a delicate political issue.

The diagram below gives an overview of international, Community and national responsibilities for different application categories.



## Requirements

- Common approach defining rights, responsibilities and duties of individuals, business and of the authorities.

## 3.4. Social Acceptance of Identification and Authentication Methods

### Issue

To reconcile the human right to privacy and protection and the use of identification and authentication methods for access control, authentication and accountability.

### Discussion

The use of biometric methods and smart cards is technically feasible and becoming more economically feasible as an identification technique and access control.

Biometric methods rely on a system of machine recognition of a set of personal characteristics to verify the identity of an authorised user in order to allow access to some physical environment. Such personal characteristics are categorised into physiological - hand geometry (faceprints, fingerprints, non-retinal and retinal blood vessel analysis, palm prints) and behavioural - voiceprints (signature dynamics, keystroke dynamics). Methods being researched include machine phrenology, lip prints and the response of the skeleton to a physical stimulus. Many other different personal characteristics and recognition techniques are being investigated. Some of these affect the human right for privacy more than others and some are socially unacceptable.

As an example, the retinal blood-vessel pattern of a human eye (retinal vasculature) is highly characteristic of the individual. A typical system might work as follows. The individual is re-

quired to look into an optical device and through a process of optical adjustment fixate on a crosswire whereby the recognition machine will locate the fovea of the individual, and scanning with a low intensity infra-red beam detect the nodes and branches of the retinal pattern falling within the scanned area. The measured pattern is compared with the stored pattern of the individual and access is granted or denied depending on the result of the comparison. This method of machine recognition may or may not be considered socially acceptable on the grounds of hygiene, due to the type of information being stored about the individual (a record of which may be built up which may reveal other information relating to a persons health condition) or the general problem of protection of medically relevant information.

There are systems under trial for the recognition of human profiles eg the human face. Again these systems may not in general be socially acceptable and the issue of privacy and human rights may come into play. The use of voice-prints has been introduced in Australia and does not require the consent of the persons concerned. It is used to scan calls for individuals.

The banking industry in the UK has extensively researched the whole range of biometrics and has recently published tough criteria for biometric systems in point-of-sale applications. At present it is believed that no existing biometric product can meet every aspect of these criteria. Nevertheless in other application environments biometric products have been successfully trialled and are in operational use. The use of fingerprint recognition at Expo'92 in Seville for all season ticket holders demonstrated public acceptance of the methodology. Likewise the use of hand geometry systems (which originated back in 1971) by the US Immigration & Naturalisation Service as a means of verifying regular visitors at selected major US airports is being extended to include other major airports in North America and Europe (Frankfurt). Earlier studies confirmed that to be successful in an "Open" application - involving large public user populations, any verification process has to satisfy a number of criteria:

- operational simplicity
- ease of use
- robust and error free
- safe use
- no health risk for eye or other physical contacts
- potential cost savings, for both the user and the system operator
- greater security
- long-term acceptability
- avoiding major system changes.

In addition to biometric controls, the role of smart cards containing megabytes of personal data may potentially represent an issue. Even a magnetic stripe on a passport or national identity card may contain around 200 characters of information. Security and privacy controls should reflect national conventions and practices. Smart identity cards and national identification numbers may serve as conduits to greater amounts of personal data contained in data bases. Member States treat such technology differently. As identity cards and passports become machine readable embedded chips or magnetic/optical stripes, privacy and security controls must be incorporated to prevent abuse of the personal data they contain.

Progress in bio-technology raises new questions as to the definition of privacy and as to the rights of the individual over information relating to his person and the assurances required for its use. Information relating to genetic defects are of obvious sensitivity and implies corresponding measures for protection. Work may need to be undertaken to set out a clear definition between things that are biometric and things that are medical. At the present time there is low confidence by the general public in the honesty of commerce or government in the field of bio-technology.

## **Requirements**

- Clarification of the ownership and privacy issues related to the use of biometric data

- agreed classification of biometric data and conditions requiring secure handling of such data
- definition of the rights of and responsibilities of individuals, business users, corporations and administrations using biometric techniques.

### **3.5. Human Rights and the Safety of Systems**

#### **Issue**

To reconcile the human right to expect the supply of goods and services that are not life threatening, with the vendors commercial needs to supply goods and services that exploit information systems in safety critical functions.

#### **Discussion**

Safety critical systems differ from security critical ones in that if they fail death or serious injury to people may result. The law treats the liability of suppliers in this situation differently from that where information is lost or property damaged. Suppliers are held strictly liable. Codes of practice for the development of safety critical systems exist in order to reduce the chance of failure and design techniques are invoked to analyse all possible hazards. Nevertheless risks remain.

At a Community level, harmonisation of such codes of practice and design techniques would enable citizens to rely on a consistent level of safety in any Member State, and it would reduce the costs of development of codes of practice and design techniques in each country. Community-wide procurement would be facilitated, as would the development of safety critical systems by Community-wide consortia.

#### **Requirements**

- Community wide standard for design practices and codes of conduct
- harmonised legal environment for vendors and users of safety critical systems.

### **3.6. Confidence in Communication Systems and Services**

#### **Issue**

To establish confidence in communication services and systems for all the parties involved (users, public, service providers etc.). This includes confidence in the general ability of the technology as well as confidence in specific solutions and the way they are managed.

#### **Discussion**

Confidence in the security and safety of communication services and systems is a basic requirement if regulators are to discharge their duties, if service providers and vendors are to be able to operate in the communication market, and if consumers and users are to benefit from the technologies. In considering confidence we need not only to address it from an idealised objective viewpoint but also to take into account the behaviour of users, their perception of risks and its volatility. It might only take one incident to undermine user confidence with substantial financial and political repercussions. eg reluctance to use air travel, rejection of certain makes of cars.

Confidence is therefore a key notion. It is achieved through the integration of disparate sources of evidence from the process used to develop the system, properties of the system as revealed by analysis and testing, and through experience with the particular systems and other similar ones. The confidence in a service or system should be rigorously and scientifically based: the confidence should not be misplaced. There is a need to understand this integration of evidence and engineering judgement and to develop procedures and techniques for it.

An important contributor to confidence is the experience with the system under consideration and similar systems. While many suspect that software and design errors are important factors undermining confidence in systems this is normally supported by anecdotes rather than by statistically significant evidence. There is a need to establish what dependability is being achieved in practice, the relative importance of different parts of the computer systems and how the dependable computer systems are compared with other components in the wider system. Mechanisms should be put in place for feeding this data back to the development of systems and for providing early warning of problems before these develop into incidents. Ideally, the experience with systems should be related back to the techniques and procedures used to develop them.

There is also the issue of how confidence in a service or system can be expressed and communicated.

While undoubtedly independent diverse viewpoints are important in the verification and validation of systems and in motivating vendors and service providers the issue of whether these practices need to be codified into formal requirements for third party evaluation and certification needs careful consideration and evaluation of the costs, risks and benefits. The alternatives of self-evaluation, supplier declarations and of using other mechanisms such as liability and the insurance market may be more appropriate.

Linked to the concept of confidence is the need to anticipate whether a system could potentially meet the requirements and to prevent the development of unassurable systems. It may be possible to develop simple rules (eg the notion of claim limits used in parts of the nuclear industry to disallow claims of reliability greater than  $10^{-5}$  failures per demand for a single system) that, while not restricting innovation unduly, prevent delimiting what is assurable.

## **Requirements**

- Real-time indication for the user of the trustworthiness of a service or system
- feedback mechanisms for security and safety related incidents involving communications
- independent assessment of the levels of trustworthiness being achieved
- investigation of the reasons why the security and safety of systems are compromised
- understanding of the relative importance of the different system components and the components of the wider system and usage context
- methods/frameworks for evidence reporting
- role (costs, benefits) of certification in providing confidence and communicating this in the market place
- establishment of agreed claim limits to establish assurability.



## 3.7. Management of Openness and Protection

### Issue

Openness and protection are partially contradictory user requirements, which need to be reconciled depending on the specific circumstances. The user must be able to define the security controls based on need, consistent with national, international and regulatory constraints. These controls need to be managed in a way that provides protection in an open environment and do not unduly impede the functioning of the service or usage.

### Discussion

In considering management, one must introduce the concept of a user of an Information System, and the role that they perform in using that system. At any time the user of an Information System will be performing a role, which could be one of: system owner, administrator, auditor, investigator, data provider, or user. It is quite possible for the requirements of these roles to be logical in conflict with each other. Openness of access may be in conflict with protection from general availability. There may also be national, international or regulatory constraints which impose role requirements beyond those needed to satisfy the operational use of the Information System. An open environment must be provided with controls that are capable of providing protection without technical limitations.

A single, isolated computer may be effectively protected, as far as confidentiality is concerned, against threats from outside by physical separation and human administration. This does not apply in the context of telematics. Telecommunications and telematics applications are increasingly being designed for maximum openness and inter-operability since the utility of ITT&B-based services and applications depends largely on the possibility of users worldwide being able to freely inter-operate over communication links. Major international efforts are underway to establish standards permitting this, in particular through Open System Interconnection (OSI), Open Distributed Processing (ODP) and Open Network Provision (ONP).

The acceptance and use of telematics services depends on meeting the justifiable interests of all parties: in particular to be able to choose trade-offs between "openness" and "protection"<sup>7</sup>.

The comparison with the way this dilemma is traditionally addressed leads to some observations which also apply when information is handled electronically. These include, for example

- The User/Originator requires the freedom to decide over the degree of openness/protection depending on his appreciation of the requirement or the applicable rules of conduct for the given activity.
- Profiles exist setting out the needs of both openness and protection that need to be supported. A single level profile will not support the requirements of all the users involved, and there may need to be mechanisms which allow for negotiation between profiles to determine temporarily agreed common profiles.

---

<sup>7</sup> Openness necessitates the following requirements

- 1) Accessibility to anyone
- 2) Accessibility at any place
- 3) Accessibility at any later time
- 4) Transparent functionality
- 5) Standardised modes of use
- 6) Formalised legal evidence

These requirements must be met and protected by appropriate security measures.

- Infrastructure, services, applications and organisation have to be adapted to provide the openness/protection.
- To the role holders, both the visibility of and the transparency of the degree of openness/protection is crucial.
- Accountability for the application of appropriate levels of openness/protection require objective records, which are themselves protected.
- The management of the openness and the protection of Information Systems requires the definition of security domains. These correspond to the security policies which are in force for the Information Systems in use, as modified by the constraints of the role holders. It should be remembered that computers which are not directly under human supervision may form part of the security domains involved.

The development of a generic framework for the management of open and protected communications in a user/business oriented environment must include:

1. Reinforcement of the options to define security domains

Terminal users, servers and other computer based resources link into business processes to provide information domains which require corresponding security domains. Such facilities must not only promote the correct degree of openness, but must also provide filters against unauthorised access. This needs to be possible not only at one site eg on LAN-Based applications, but also via MANs and other communication-links. The definition and management of such security domains needs to be possible either from within the user group or provided by a trusted third party. Virtual Private Networks have some of the features, but these would also need to be available in the context of public network based applications.

2. User Interface for the management of openness/protection

The normal usage requires the ability to communicate either with specific correspondents, a select group, an open group or indiscriminately. The choice being determined by the nature of the information, its function and the applicable rules. The user-interface needs to cater for this as well as the underlying services and applications.

3. Objective records and procedures for the accounting of open/protected transactions

Processes must be available that provide non-refutable evidence of the origin of, and delivery of, information to all involved partners.

**Requirements**

- Generic framework for the management of open and protected communications in a user/business oriented environment:
  - definition of agreed security domains
  - user interface for the management of openness/protection
  - objective records and procedures for the accounting of open/protected transactions

### **3.8. Common Concerns of Commercial and National Security**

#### **Issue**

Information Security is a common concern of business, administrations, citizens, law enforcement and defence.

#### **Discussion**

Though not to the same degree, commercial and personal information security shares many aspects with the defence and other classified governmental affairs. This provides an opportunity for commercial and personal applications to build on experience and expertise from the defence and classified government area.

The reverse is also true. As commercial security advances and becomes available at a large scale, governments and defence organisations may wish to take into account this body of experience. In addition governments themselves are, of course, in the need of adequate protection of their non-classified information and will wish to make use of public services of this kind.

#### **Requirements**

- Common requirements of business, citizens and authorities to adequately protect commercial and personal information and its communication.

### **3.9. Security and Law Enforcement on International Scale**

#### **Issue**

Crime is exploiting weak information security to further its ends. Strong information privacy may also be used to escape investigation by law enforcement.

#### **Discussion**

Crime, and here organised crime and terrorism in particular, are relying on weak information security to prepare and execute their operations. As quite powerful means for information security have been published and are freely available, their increased use in protecting such operations is perceived as a growing problem. Public authorities have in the past used legal and regulatory powers to restrict the use and dissemination of related technologies. With the growing availability of computing power and open networks, this approach is getting less effective, as organised crime, contrary to the legitimate user, feel free to use products that are not authorised. The overall result is that business is seriously constrained in meeting its security requirements, particularly in international communications and in its relations with other organisations. If business requires the legal and regulatory powers to relinquish total control over these security related technologies, business has a "duty of care" to manage and control their use for their commercial and business purposes, including the policing and auditing of management environments. Correspondingly, authorities maintaining control carry the responsibility for the potential damage to business, individuals and the economy at large.

Privacy and security are impacted by the growth in interconnected law enforcement/criminal information systems; There is an increasing availability of criminal and law enforcement information from a variety of national data bases (eg, United Kingdom's Police National Computer 2 - PNC2; Germany's INPOL; France's fichier des personnes recherchées - FPR; the United States' National Crime Information Centre - NCIC; Canada's Canadian Police Information Centre - CPIC and Australia's Law Enforcement Access Network - LEAN) and

international data bases (eg, Schengen Information System; INTERPOL's X.400 distributed data base network and the EUROPOL/Trevi Information System). Incorrect information can lead to false arrests and a general denial of civil liberties. Non-vetted information can result in individuals being arrested and/or investigated for spurious and non-criminal reasons such as political, trade unionist and religious activities.

### **Requirements**

- Effective, internationally agreed, economic, ethical and usable solutions to meet business, administration and personal needs
- mechanisms for authorised interception for law enforcement
- reporting of incidents and crimes, adjusted to the conditions of the Internal Market
- equipment, software and an infrastructure of trusted third parties.

## **3.10. Economics of the Security of Information Systems**

### **Issue**

The use of information security impacts on costs, performance and availability. It may also be used to achieve a competitive advantage.

### **Discussion**

The cost of security is an integral part of cost of ownership of an information system. The cost of protection against breaches of security needs to be commensurate with the costs (both direct and indirect) that may be incurred from a breach in security. A security breach may have short term (and perhaps, localised) implications such as loss of sales and revenue or fraud or theft. It may also have longer term (and wider) impacts on business communities through loss of confidence and consequential loss of business.

The costs of detection, resistance and recovery can be both tangible and high, and although there are techniques available to quantify risks there are no generally applicable methods for estimating the potential costs arising for example from denial of service or loss of integrity. The application of security measures may also make it harder to use and may constrain overall performance. However, where the security risk is high enough to cause an unacceptable level of compromise, leading to considerable commercial and financial loss, then security measures must be given high priority commensurate with the nature and value of the business in question.

If information security is too expensive, clumsy, not effective in the context of actual usage or not available in time its use is avoided and high risks are taken until something drastic happens. The issue for information security is therefore, not only to be effective but also to address other requirements which impact the acceptability and application of information security.

In particular, countermeasures may have to be put in place that meet specific regulatory or legislative requirements, with associated mandatory assurance needs.

To a business, securing information can be thought of as being like an insurance policy - the cost of protection must be balanced against the likely consequences of the perceived threat occurring. This cost is made up of a number of elements, including:

- the life-cycle costs of implementing the countermeasures in relation to likely and worst case
- impact on business performance
- liability of management for incidents and relationship with customer confidence
- legal costs.

An important experience from the past two years shows that, in commercial applications, the aspects of cost and ease of use are critical for the introduction of information security. For this reason a number of enterprises, including many Governments, are looking to procure Commercial Off The Shelf (COTS) security products to meet their needs, rather than developing bespoke systems.

The unit cost of security is affected by market volume. Market volume is unlikely to be achieved without commoditisation of security products to the point where they are part of the IT infrastructure rather than a separate cost factor (on cars, ABS was expensive until it became generally fitted).

High volume and commoditisation can be achieved by:

- the provision of a common architecture and security building blocks which can be used across the widest possible community so that low prices can be achieved
- development of world-wide standards for secure systems
- raising awareness of security risks in order to stimulate demand
- common or mutually recognised security evaluations world-wide
- supplier self-certification, with appropriate liabilities
- agreed protection levels with corresponding sets of protection measures (to focus products onto common needs). Current work on baseline controls could provide a basis for an agreed minimum protection level. Other protection levels may be needed for more sensitive or critical information.

It may be that separate security evaluation criteria and methods need to be developed to allow for low assurance assessments to be carried out at low cost.

### **Requirements**

- “IS-to-cost” techniques for business and private users
- incorporation of good information security design practice in the development of products and services
- definition of information security as business and marketing factor
- identification of acceptance levels for insurers, regulators and the commercial courts
- specification of duties and responsibilities of parties to the use of information systems and their security requirements

- security architecture and "building blocks" specifications and standards, with a view to minimising the cost of providing commonly needed levels of security.

### **3.11. Social Recognition of Information Crime**

#### **Issues**

Negligence, ignorance and recklessness are some of the causes of many security breaches and create the opportunity for information crimes.

#### **Discussion**

Information security breaches, like failures to observe safety rules, can in many instances be attributed to a lack of care or ignorance. This is compounded by the fact that the loss of immaterial goods, for example information, is not considered as serious as the loss of material goods. This is due in part to the fact that electronically stored information can be reproduced at close to zero costs without the loss of the original. Stealing information is therefore often considered as a gain for the thief without a loss to the owner. It is perceived by many to be a game rather than a real problem because people are unable to relate the electronic world to the real one. This has the double effect of inciting negligence by the owner of the information and little concern for the illegal acquisition of information. Because of the widely practised back-up of information resources, this applies even to the intentional or accidental destruction of information.

There is much work in establishing and reinforcing "ethical principles" as applied to specific actions of information ownership, creation, dissemination, etc. These need to be related to sector actors, their control perspective and the assets over which they exercise either explicit or implicit authority. This needs to be related to codes of practice and conduct, legislation and regulation to establish the extent to which protection is dependent upon a formal or informal control environment or can rely on the enhancement of ethical and professional standards. Changes to traditional programming techniques have made it possible for non-IT professionals to deliver programming and systems analysis methods. In many smaller enterprises such work would often be done by non-IT professionals.

Two examples of computer crime illustrate the diversity of situations which may arise:

#### *Example 1*

In a German company (belonging to the "Association for Security") a programmer - unsatisfied with his salary - caused damage by a specific computer-programme. This program modified the data of a data bank by randomly controlled write operations. The programme was intricately hidden among other programme-parts. Within two years the data-bank became more and more defective and damaged. The costs of damages and of reconstructing the data bank were about 500 000 ECU.

#### *Example 2*

In an office of the German Government a huge computer-system, comprising various storage means and terminals was installed. Suddenly the computer-execution-times and the response times became much longer than expected. After a difficult investigations it turned out, that a programmer, who had founded together with his wife a shop for sending out photo-equipment, has done his complete accounting, mailing, etc. for his shop on the computer in a hidden area. He had camouflaged or suppressed the protocolling of this programme. He caused damage of about 100 000 ECU.

## **Requirements**

- Education and training on the information security requirements and concepts needed to operate in a secure manner in the Information Age
- clarification of "Info-Ethics" for the professional and individual user in its relationship to information security
- clarification of responsibilities of the sector actors in general and in their relations within each other, with particular reference to open and distributed applications.

## **3.12. Human Factors**

### **Issue**

Human interference with information systems constitutes the biggest risk factor to security and the most difficult to address.

### **Discussion**

The largest potential threat to IT systems arises from the people involved in them be they designers, programmers, operators or users. And more security breaches are caused by human error, often by well intended people, than any other causes.

Apart from providing "fool-proof" system and services, there is thus a need for organisations to give due consideration to the non technical techniques which they should consider to meet this threat. Such techniques could come under the heading of personnel policies and forced users - positive vetting, removal on notice, monitoring changes in life style, avoidance of collusion, job organisation, contracts of employment, etc. And the role of good supervision.

Allied to this is the need to emphasise that controls in a system must not only relate to the technical mechanisms but to the system overall, including the clerical and manual workforce. And, of course, they must relate to the overall objectives of the organisation.

"Security is an attitude of mind, practice and discipline."

### **Requirements**

- Adjustment of personnel management practices and organisational procedures to reduce the vulnerability by the actions of staff and other people
- greater use of non-technical management controls.

## **3.13. Safety Critical Environments**

### **Issue**

Protection of information in safety critical environments.

### **Discussion**

Safety and security have a common technological basis, but differ in their objective. In complex systems there is in many cases a duality of objectives. Safe systems need also to be secure. The reverse is not necessarily the case.

Safety is defined in terms of hazards and risk. A hazard is a set of conditions (a state) that can lead to an accident, given certain environmental conditions. The analysis of the safety environment involves identifying the hazards within a safety critical environment and then either verifying that hazardous states cannot be reached or that the risk is acceptable. Risk is defined as a function of the probability of a hazard occurring, the probability that the hazard will lead to an accident, and the worst potential loss associated with such an accident. You can diminish risk by reducing any or all of these factors, and there are environmental-safety techniques that focus on each.

There is an increase in the use of information systems within various areas of application which are considered as part of a safety critical environment. For example in the area of healthcare (eg medical databases), air traffic control, transportation of hazardous and dangerous goods, industrial processes etc. The increased reliance on electronic information in these various areas of application specifically related to the control and management of safety, has resulted in an increased need for the protection of the information system supplying such information. Therefore the protection of information systems used in safety critical environments is a factor to be addressed when considering hazards and associated risks in such environments.

Consideration needs to be given to the common requirement of security and safety, common methods for analysing the threats, vulnerabilities and hazards, and the role of security evaluation for safety-critical systems.

### **Requirements**

- Common approach to the handling of security and safety critical requirements
- methodologies for threat, vulnerability and hazard analysis for the protection of information systems used in safety-critical environments
- methodologies for the design, development and procurement of safety critical systems, covering project management, development environment, auditing of process, configuration management and change control
- common approach to security evaluation of information systems in safety-critical environments
- common approach to information systems recovery in safety critical environments.

## **3.14. Embedding Systems**

### **Issue**

There is a marked trend to embed information systems in other products. This raises particular security and safety issues.

### **Discussion:**

Increasing use of computers and information processing is occurring in a manner that incorporates information/computers into other products to make those products more usable, flexible, etc. These embedded systems, that are usually hidden from the user, depend upon the accuracy of the programs they contain and the information inputs/outputs to preserve the usefulness of the products in which they are placed. Failure of the processor or corruption of



the programs or information contained may cause failure or destruction of the device or hazard to the user.

Embedded systems are already being used in automobiles for controlling ignition and carburettor systems or braking systems, in television sets and VCRs, in microwave ovens, and so on. As embedded systems proliferate they create potentials for physical hazard to users beyond simple loss of the functionality of the devices in which they are embedded. The potential will also exist that such embedded systems could constitute a hazard to the well-being of bystanders or property.

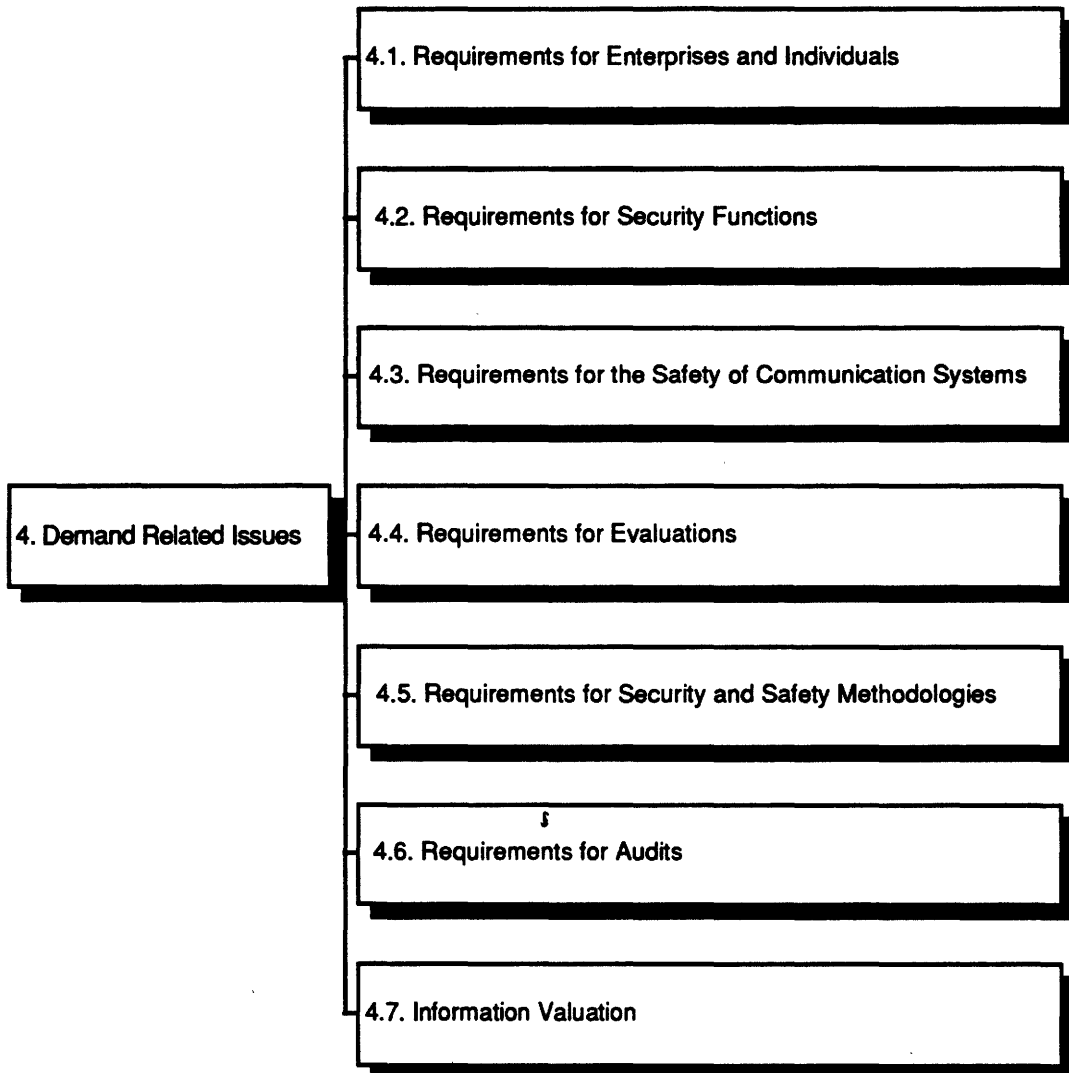
Security hazards can be introduced quite unwillingly. For flexibility reasons, suppliers of communication systems are moving towards installable firmware in the field. They may thereby overlook the fact that such a facility may create an undefined platform. IEEE standard 1149.1 calls for standard test access ports and also foresees the possibility of remote diagnosis. It is therefore possible to extract data flowing between the components on a printed circuit.

To some extent, liability laws will cover product failures which create damage to users. However, there may need to be some added means of ensuring the reliability of embedded systems and the integrity of the systems as they leave the factory.

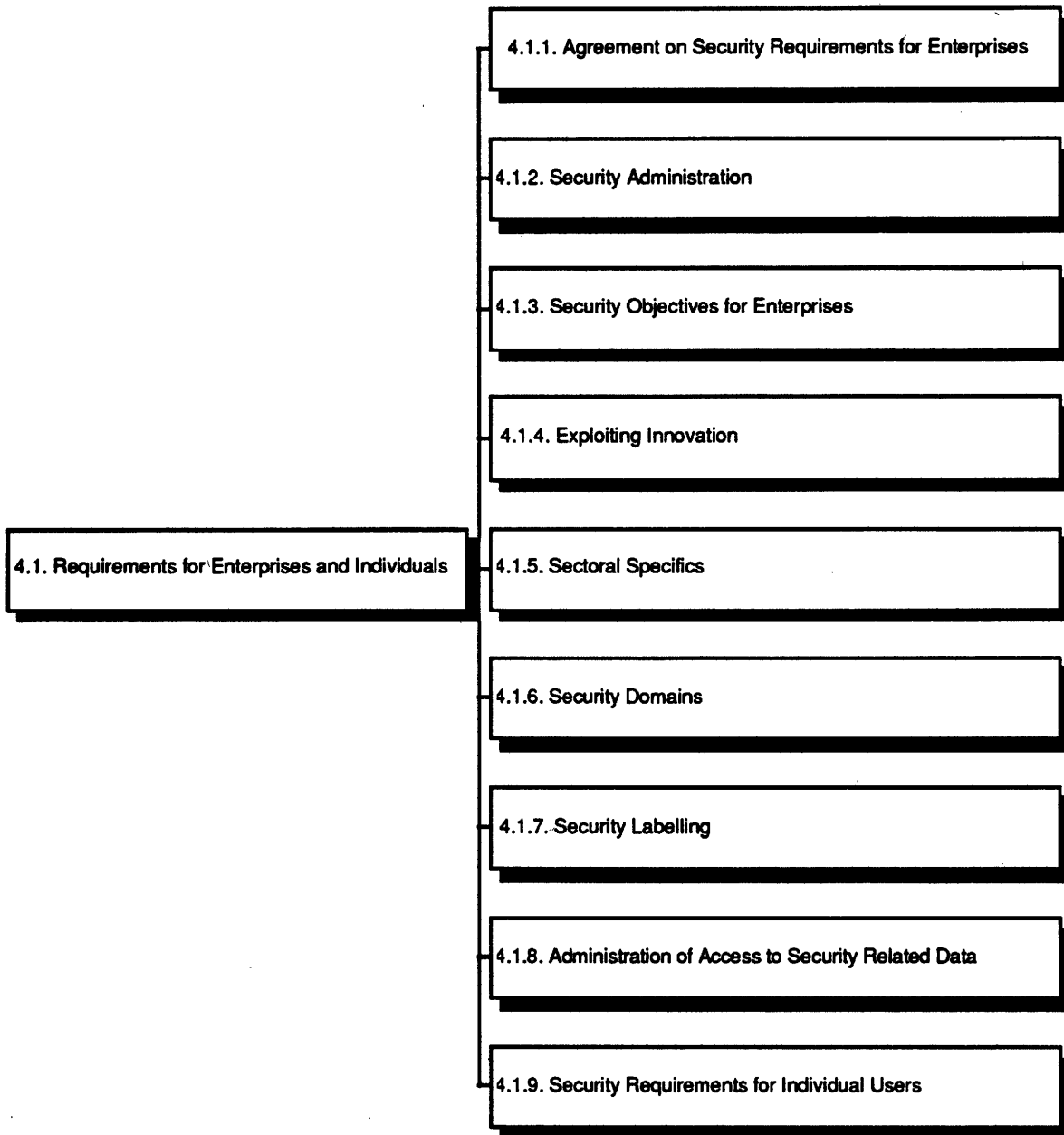
### **Requirements**

- **Methods of testing that enable standards of reliability to be ensured, including tests to destruction where appropriate**
- **approach for the certification of safe products**
- **definition of requirements for fail-safe system architectures and implementations**
- **anti-tampering and protection specifications and standards**
- **quality label, that indicates the quality level of the embedded system**
- **awareness of designers of the potential impact of innovation in the validity of test technology.**

## 4. DEMAND RELATED ISSUES



## 4.1. Requirements for Enterprises and Individuals



### 4.1.1. Agreement on Security Requirements for Enterprises

#### Issue

Identification of real world security requirements and objectives for business and administration. The derivation of security requirements from business requirements is complex and not well understood.

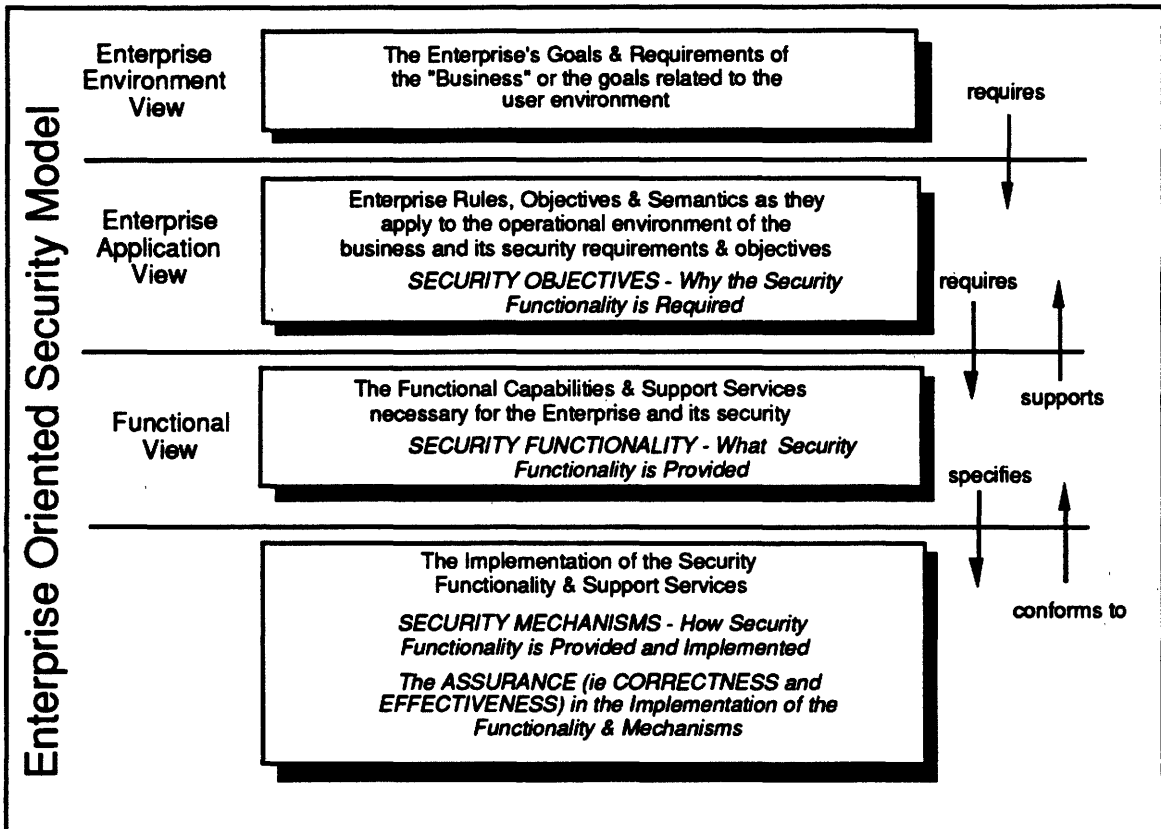
#### Discussion

The protection of information systems must include all relevant aspects. Consideration must be given to requirements from the view point of the enterprise, taking into account corporate and organisation plans, goals and strategies of the business or administration. Requirements at this level can be then translated into "Security Objectives", ie why the security functionality is required as it applies to the operation of the business or administration environment.

There are two elements to this:

- identifying business requirements which have a security dimension
- relating that security dimension to security objectives.

These security objectives need then to be supported by a definition of the security functionality and related services required necessary to support the user/business.



The security model has not included legal, accounting or regulatory requirements which may be imposed upon enterprises rather than forming any integral part of the Enterprise requirements.

Given the complexity and diversity of user/enterprise requirements for such protection it is necessary to classify the requirements in some structured way consistent with real world business and operational environments.

The protection of information systems needs to consider the enterprise requirements of the "business". These requirements not only include functionality that is "owned" by the enterprise but must include inter-enterprise requirements as well. It must consider the functionality and assurance of IT building blocks, end user applications, integration enablers (such as electronic mail), operating systems, communication services and protocols, and basic hardware and software platforms.

The balance of functionality (what it does) and assurance (how well it does it), both generic and application specific, will determine the extent to which electronic information systems are accepted as an integral part of both the public and corporate IT infrastructure to underpin business actions.

The prime requirement for any secure system must be a set of architectural principles that can be effectively translated into an overall design framework. Secure systems must be created at different "grades of assurance" from a set of policies, standards and procedures.

Specific security requirements relating to open systems will come from a threat assessment and risk analysis which will form part of the overall system security policy process.

The cost of security is an integral part of the cost of ownership of an IT system. The cost of protection against breaches of security needs to be commensurate with the costs (both direct and indirect) that may be incurred from a breach in security. A security breach may have short term (and perhaps, localised) implications such as loss of sales and revenue or fraud. It may also have longer term (and wider) impacts on business communities through loss of confidence and consequential loss of business.

The cost of detection, resistance and recovery can be tangible and high, and although there are techniques available to quantify risks there are no generally applicable methods for estimating the potential costs arising for example from denial of service or loss of integrity. The provision of security measures may also make it harder to use and may constrain overall performance. However, where the security risk is high enough to cause an unacceptable level of compromise, leading to considerable commercial and financial loss, then security measures must be given high priority commensurate with the nature and value of the business in question. Sectoral requirements vary widely, as do requirements by size of enterprise within a sector. Sectoral requirements may be varied by regulation, bilateral international agreements, general trading agreements or conventions.

Increased demand for Electronic trading from all kinds of businesses, both public and private sector, will place requirements for security on the communal service infrastructure that provides the capability for such business activities. The regulatory and legal environment within which such service organisations work will become a factor for economic growth in the community, and security of service provision an element of such services.

## **Requirements**

- Taxonomy and directory of user requirements and security objectives derived from experience with practical applications.

### **4.1.2. Security Administration**

#### **Issue**

Security administration operates within the overall management. It should not compromise its mission.

#### **Discussion**

Security administration is an indispensable function for the normal working of any organisation and falls within the "control" aspect of management's activities.

The function's objectives will be to ensure the existence and maintenance of security of:

- hardware, firmware, software
- personnel
- communications and networks
- physical environment.

It will also be concerned about disaster recovery and contingency planning; compliance with legislation such as data protection and privacy laws, and maintaining auditability. Corporate

governance issues are now starting to require directors of listed companies in UK to state publicly whether they consider that their companies' system of internal control has been working, and this specifically includes information security consideration.

Security administration represents a non-negligible cost factor in an enterprise. It may also unduly restrict personnel to do their job. Therefore, security administration and management needs must be reconciled.

Personnel in the security administration function need not only to have adequate awareness, information and training in order to recognise threats and vulnerabilities and to be aware of appropriate counter-measures, but also to understand the enterprise's mission.

Management is responsible for reviewing audit reports and taking corrective action where necessary. Audit is responsible for ensuring that security technology has been implemented in accordance with the organisation's security policy.

Specific items to be considered under this area also include control over safety critical and process control information, and security logs and the need for real-time alarms to detect intruders, where appropriate. It is important to be realistic about controls and not overlook simple matters such as the possibility of passwords being sold.

### **Requirements**

- Guidelines for establishment of security administration function
- recommendation on moving towards commonality of laws on data privacy and protection, particularly relating to individuals
- means to provide increased awareness and relevant education and training
- guidelines for consideration of balanced security, taking account of level of risk in different areas (physical, personnel, hardware, software, data, etc).

### **4.1.3. Security Objectives for Enterprises**

#### **Issue**

Definition of Security Objectives for enterprises.

#### **Discussion**

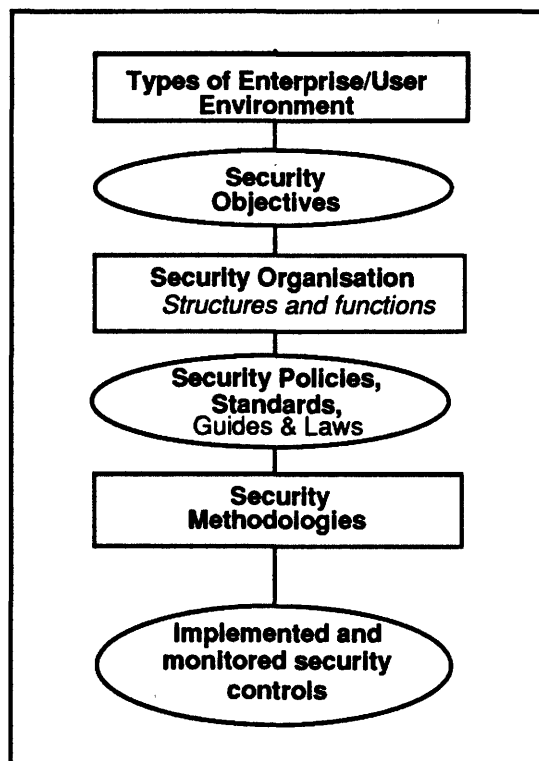
A security objective is a description of what security the enterprise is trying to achieve eg why this security control/function is wanted. It is a mission statement of the user/enterprise which describes why an aspect of security is needed. It is a user/business target or purpose to which security is being addressed. For example, consider the subject of data integrity and the objective "Prevent unauthorised modification to data". The security objective has the purpose to ensure that appropriate mechanisms should exist to preserve the integrity of data. For example this may be related to data held on a medical database, on a company financial database, in airline reservation system or a geography information system.

The organisation of security within enterprises in terms of business control structures or in the case of some user environment (eg legal, accounting, audit etc.) and functions (eg IT, human resources, insurance) needs to be integrated with a set of security policies, standards (both public and in-house), and made compliant with laws and regulations (eg computer crime manual), guidelines and codes of practice etc.

The process of producing a security policy may require the use of a set of security methodologies, tools and evaluation criteria. For example risk analysis methods, baseline controls, and evaluation criteria (eg ITSEC, Federal Criteria etc.).

Security objectives thus encompasses a set of objectives (and possibly sub-objectives) and a set of related issues that reflect specific points of concern, problems, questions relative to business requirements, controls and applications.

The diagram below shows the relationship between Security objectives, Security organisation, and Security methodologies. Laws apply to the user environment directly. Their presence generates some of the security objectives. Standards may be both mandatory and discretionary, and may incorporate methodologies. The final box covers security methods and techniques.



## Requirements

- Standard techniques for drawing-up security policies for typical situations
- methods and techniques for agreeing levels of security and security objectives.

### 4.1.4. Exploiting Innovation

#### Issue

To establish how service providers and vendors could exploit the benefits of innovation without compromising security and safety.

## **Discussion**

Vendors and service providers need to innovate to survive commercially. They have strong vested interest in ensuring that their products are adequately secure and safe. Businesses by their very nature need to take risks to survive and this commercial imperative for a risk taking culture has to be reconciled with the needs for an inherently risk averse security and safety culture in a way that is effective yet does not stifle innovation.

There are many aspects to innovation. On the one hand there is innovations which change the technology that is being used to implement systems (eg from electrical or electronic to programmable). Other innovations concern the domains of application (new forms of command and control, remote diagnosis and maintenance, ultra-critical applications) and other innovations concern the technology. This can either be in the technologies deployed (eg new forms of fault tolerance, different types of open systems) or in the technologies used to develop systems (eg code generation, novel testing regimes, formal methods, neural nets).

These innovations are likely to continue the trend for greater integration and internationalisation of systems, a convergence of dependability, safety and security problems, a blurring in the distinction between hardware and software. Systems are likely to be more open than in the past, be the result of evolution, and make extensive use of components already deployed in other applications. The safety and security concerns will change as a system evolves, and changes in the environment of a system (eg organisational changes, removal of other systems ensuring safety) can cause a system to evolve into a higher level of criticality.

There is a need that the measures taken to provide confidence in systems can cope with these innovations and that businesses have predictable certification or regulatory costs where these are relevant. This has a number of implications for the regulatory and certification regimes and poses challenges to the standards making process.

Innovation can bring with it new hazards. There is a need to identify these and either remove them via redesign, provide measures to tolerate them or at worst, measures to mitigate their consequences.

## **Requirements**

- Assessment methods for impacts of changes on systems
- procedural and regulatory frameworks need to address convergence of safety and security (implications for standards)
- methods for identifying early on where innovations are likely to be unacceptable from a safety perspective or will result in such economic penalties that they are not viable commercially.

### **4.1.5. Sectoral Specifics**

#### **Issue**

Beyond the normal requirements common to different business sectors and user environments there may also be additional requirements and priorities specific to the operational nature and commercial mission of a particular business. These specific requirements can be normally expressed in terms of codes of practice and baseline controls.



## **Discussion**

Legal and regulatory provisions can be supported by Codes of Practice in an attempt to achieve due care and diligence. There are those of general application and those that are industry specific. A general Code of Practice may be achieved by the establishment of a security management handbook, maybe based upon the approach taken for achieving a Quality code of practice (ISO9000). The application of information security is a prerequisite for the successful conduct of business for particular sectors, especially when these sectors are highly interactive. The traditionally prominent among them are:

- Finance
- Trade
- Medical
- Telecommunications
- Manufacturing industry
- Process industry
- Administrations.

There may be other market led requirements, that will result in a different security based segmentation.

## **Requirements**

- Consolidation and development of a set of Codes of Practice and baseline controls addressing specific business sector requirements.

### **4.1.6. Security Domains**

#### **Issue**

Openness and protection.

#### **Discussion**

In practice, the level of information security is dynamically adapted to a given situation. This leads to the concept of Dynamic IS Management and the need to be able to define domains, in which information security is applied homogeneously.

Domains are user groupings sharing some of their functions and support. For some activities they operate as virtually closed user groups, but have the possibility to interwork with other domains as long as certain minimum requirements ensure no loss of trust or a transparent downgrading.

The notion of a security domain is therefore important for two reasons. Namely,

- It can be used to describe how security is managed and administered, and
- It can be used as a building block in modelling security relevant activities that involve elements under distinct security authorities.

Examples of domain activities are:

- accesses to elements (eg a database for network management)
- provision of a communication links
- operations relating to a specific management function

- non-repudiation operations involving a notary.

The organisation of security within enterprises in terms of business control structures or in the case of some user environment (eg legal, accounting, audit etc.) and functions (eg IT, human resources, insurance) needs to be supported by a set of security policies, standards (both public and in-house), laws and regulations (eg computer crime manual), guidelines and codes of practice etc.

The security policy defines what is meant by security within the domain, the rules by which security may be obtained to the satisfaction of the security authority, and the activities to which it applies. The security policy may also define which rules apply in relations with other security domains in general, and in relations with particular other security domains.

The management of inter-domain openness and protection may be different depending on similarities in purpose, and agreements will be needed to achieve appropriate levels of assurance. Mechanisms by which TTPs achieve efficient, coherent management of policies, procedures and controls between domains need development:

### **Requirements**

- Mechanisms for management of policies, procedures and controls between domains for TTPs
- generation of guidelines for domain creation, management and control
- development of a common framework for domain interworking
- agreement on management, TTPs, accreditation, auditing and relations with law enforcement agencies.

#### **4.1.7. Security Labelling**

##### **Issue**

Transfer of information among domains requires agreements on the expression of the sensitivity of information, ie the syntax and semantics of the associated security labels, and of the procedures and mechanisms for handling labelled information.

##### **Discussion**

The basis for the trustworthiness of a domain and the trust between domains is the assurance that the processes that are used to manipulate information behave in a way that corresponds to the protection requirements of the information in terms of confidentiality and possession, integrity and authenticity, and availability and utility.

Labels are a method for expressing the sensitivity of information. They can be based on different scales, like the value of information or the impact of a security breach affecting the information.

The need for comprehensive labels has become acute because of the increasing degree to which organisations interoperate electronically. This has led to increased reliance on technical measures to achieve adequate security. It is quite feasible for trusted systems to switch on or off technical measures automatically providing that the label adequately expresses the security requirement associated with a piece of information. Labels could then be used to make decisions on information routing, transmission enveloping, requirements for confirmation and so on.

However, decisions on information routing etc. cannot be made without user labelling, that is, some indicator of the categories of information which can be allowed into end-systems or to users.

Organisations have to agree on the range of options that do meet any particular security requirement. Part of the solution to the handling of labelled information lies in the development of Codes of Practice specifying procedures and mechanisms. There is also a need for accreditation and audit of communicating partners. The introduction of independent third parties avoids the pairwise interactions that would otherwise be necessary to establish trust.

### **Requirements**

- Guidelines for security labelling.
- standard on how to express labels and on the meanings of a basic set of security labels
- Codes of Practice and accreditation methods for domains claiming to support standard labels, and their mutual recognition.

#### **4.1.8. Administration of Access to Security Related Data;**

##### **Issue**

Support of functions for the administration of security related data.

##### **Discussion**

Management of rights is an administrative function available to both security administrators and resource owners. While management functions reserved to security administrators can be rather sophisticated, functions available to resource owners have to be kept simple and easy to use. The management of rights can be separated into security information related to users (eg privileges, keys and/or passwords) and security information related to resources (eg access control lists, labels; keys). Management functions need to be performed from the place where the administrator/resource owner is sitting and apply to a number of remote resources. It is therefore important that the management of access rights is done in a secure fashion (eg using appropriate security protocols).

##### **Requirements**

- Easy to use tools for access right management and key management
- secure solutions for remote administration
- awareness for control issues concerning security related data, and implications of non-action.

#### **4.1.9. Security Requirements for Individual Users**

##### **Issue**

Individuals and small companies have "enterprise requirements" but often have little opportunity to choose appropriate security protection when dealing with large organisations (eg equipment and software suppliers, service suppliers, banks).

## Discussion

The individual user, in their role as a private citizen or as a member of a liberal profession (eg a lawyer or medical doctor), has a natural interest, and sometimes a legal requirement, to protect some of their information. Unlike in the case of the enterprise, the individual user will not normally go through a systematic process of establishing goals, definition of security objectives, etc., unless they are subject to professional standards of conduct.

The individual normally has at his disposal a PC (or small network of PCs) and some communication links, eg telephone, fax, e-mail. Often physical security is likely to be weak.

Most liberal profession work under some codes of practice or conduct. These codes are of a general nature and do not normally specify particular security arrangements.

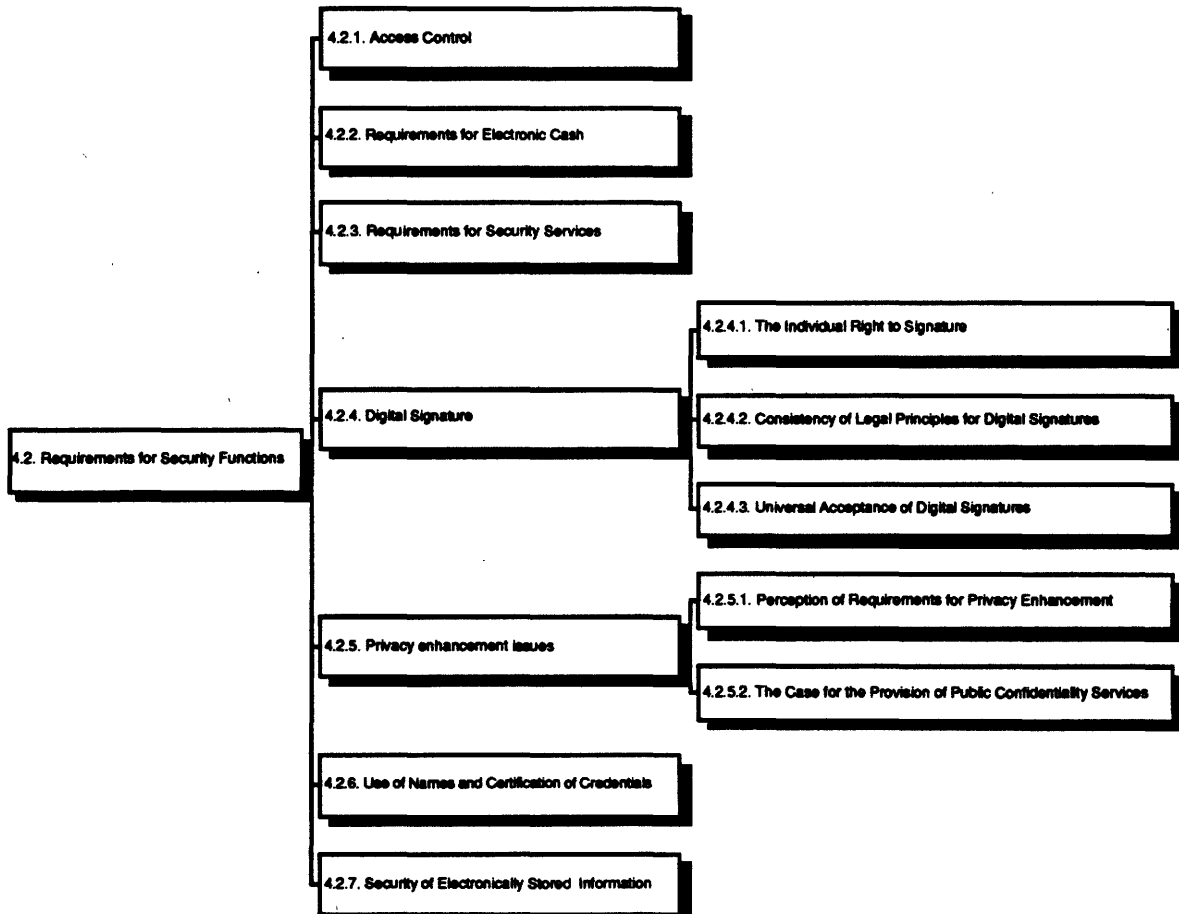
The common and specific requirements of individual users, with regard to the protection of their computer installation (physical and electronic), the protection of their data (against accidental and deliberate loss) and the protection of their communications (eg signed communications, privacy enhanced communications) must be established.

The individual user has also an interest that the totality of processing of any matters relating to the user is correct and confidential to the extent required.

## Requirements

- User profiles identifying standard types of users together with typical requirements.

## 4.2. Requirements for Security Functions



## **4.2.1. Access Control**

### **Issue**

Access control procedures to many systems need to be standardised and well managed to meet their objectives.

### **Discussion**

Computer systems and services impose control procedures on persons (or other systems) attempting to access them directly or over local or wide-area networks. These access control procedures apply to "connections"; that is, they determine whether or not a connection, association or session is allowed to be established. These control procedures have been often primitive and relatively insecure, as the occurrence of "hacking" demonstrates.

The requirement for secure access control is not confined to access to host computers by persons at terminals. Reciprocal (mutual) access control is often needed between two (or sometimes more) systems. Access control can apply across general telecommunication networks, determining (for example) who may call whom by telephone; or who may receive which programme on a cable TV network. In addition to applying to end-to-end (trans-network) communications, access control also applies to users and (even more importantly) operators accessing the network and to access by human users to terminal devices.

Although the importance of access control is widely recognised, the practical application of security techniques in solving the problem is more limited. This is for a variety of reasons including technical complexity, lack of agreed standards and lack of user acceptability.

Secure access control relies on a mixture of:

- identification mechanisms (authentic naming) identifying the remote person or system
- authorisation mechanisms, determining the authority of the remote person or system to carry out different types of actions
- random (unpredictable) components, affording protection against the re-use of once-valid access control messages under invalid circumstances (replay)
- cryptographic techniques to protect the above from modification, copying, etc.

The automation of physical or logical access control procedures based on biometrics has been in use for a number of years, most notably utilising voice verification techniques. These latter focus on the vocal characteristics that produce speech and not on speech itself. Today there are several organisations that are actively marketing and/or developing voice verification systems. There are two basic types of voice verification system - telephone-based systems and stand-alone equipments which can be networked within a discrete building or group of buildings. A further distinction exists between those systems which are text-dependent, where a pre-registered word, phrase or number is used for verification, and text-independent, which can handle a fuller vocabulary.

Without some analysis of access control scenarios, followed by some outline standardisation work, users and systems are going to find themselves having to implement and use (depending on their current application) a range of incompatible techniques, which in turn rely on only partially interoperable infrastructures (such as naming and identification authorities, certification authorities, key management systems, directory services, etc.).

Access control very often involves only two parties: one making the access and one granting/denying the access. In some environments this is however inadequate as some intermediaries cannot do the access on their behalf but on the behalf of someone else. This

applies in a number of cases, in particular for distributed applications or transaction processing. For example, in a distributed service the requester addresses its request to the nearest server able to fulfil the service and then the request has to be forwarded so that it can be honoured by the appropriate server within the service. This problem is called delegation.

For the server point of view different policies may apply: it may be interested only by the privileges of the initial requester and by the privileges of all the intermediaries. The access control decision may then be based on the properties of the initial requester only or on all of the entities involved. In addition restrictions about what intermediaries are or are not allowed to do may be specified by the initial requester.

There is a need for widely accepted solutions to the most common access control scenarios.

### **Requirements**

- Group access control scenarios and schemes based on levels of commonality
- techniques, products, specifications and standards addressing access control matched to the scenarios identified
- parameters common to most or all of the above techniques, products, specifications and standards and the feasibility of establishing common formats for them
- identification of the key features for coherence in the supporting infrastructure
- basic access control mechanisms for pilot implementation
- development of delegation scenarios
- identification of techniques, products, specifications and standards addressing delegation and their association with the identified scenarios.

#### **4.2.2. Requirements for Electronic Cash**

##### **Issue**

A general purpose system is needed for providing electronic cash.

##### **Discussion**

The securing of electronic cash shares some problems with negotiable documents, and may also need additional properties such as privacy (untraceability) and dividability.

Large scale solutions already exist for paying small amounts of money in special situations, such as special cards for telephones and travel. Other systems exist for large amounts of money - prepayment and credit cards. Between these two, there is a need for a system to make general purpose payments for relatively small amounts of money. This means that the system must have low transaction costs, and will thus be able to compete with existing special cards.

The system should ideally include the following properties:

- unlimited transferability (from one user to another)
- dividability into any sub-amount required
- independence from on-line TTP services

- privacy / untraceability
- security and uniqueness - ie cannot be forged or copied.

It should give users complete control over the amount transferred in each transaction, and allow them to know the amount remaining. It should be relatively easy to refill the device with electronic money, possibly via unsecured network services.

### **Requirements**

- Agreement on the concepts underlying electronic cash
- international standards.

### **4.2.3. Requirements for Security Services**

#### **Issue**

Various security services have been identified. Agreement on their requirements must be established.

#### **Discussion**

A variety of security services has been identified. Although several of these are used in practice at a limited scale, their general requirements have not yet been agreed and their availability to the general user is not yet established. Some of the more important services are described below.

#### *Non-Repudiation Services*

Non-repudiation of origin respectively receipt means that a particular user, called the originator respectively the receiver, cannot repudiate (ie deny) to have signed respectively received a particular electronic document. It does not prove who has actually created the document. We have exactly the same problem with paper documents: the fact that someone puts his signature on a hand-written transcript of music does not mean he is the composer.

Non-repudiations services are precisely the services which in electronic communication can cover all legal functionalities of a hand-written signature, but in a much more secure way: The main difference is that the digital signature which supports the non-repudiation provides a logical connection to the message.

#### *Claim of Origin*

Copyright is a very important security service in the electronic handling of a document. The major problem with enforcing copyright of, say, a software program, is that of two different versions it is difficult to decide which one is the original. This problem is of course not restricted to electronic documents only. In fact, one runs into exactly the same kind of problems as in the paper world.

The service required here is "claim of origin". This is the counterpart to non-repudiation in the sense that the point is to allow the creator to prove who created the document, as opposed to non-repudiation of origin, which allows everybody to prove that someone has signed a particular document (which typically commits him to something). The difference is that with non-repudiation services, the receiver is able to prove something, whereas claim of origin pertains to the transmitter.

### *Claim of ownership*

Some conventional physical documents, such as eg the bill of lading and the bill of exchange, must be negotiable. The possession of the document must allow to give title to anybody who can present it. The electronic equivalent is also needed.

The goal to achieve here is that an electronic document at any particular time can be proved to be the (temporary) property of a particular user.

With ordinary paper documents, the problem is solved by giving the original of a document certain physical attributes that are difficult to reproduce. With this precaution, it makes sense to speak of the original of a document, and define the owner simply as the person holding the original.

Negotiable documents entail that their physical uniqueness must be protected against duplication; it must be easy to distinguish a copy from its original. This is the case with hand signed paper documents; the hand-written signature cannot be copied such that the copy could not be distinguished from the original. Although a digital signature does protect the integrity of the signed electronic document, it can, however, easily be copied so that the physical original cannot be distinguished from its copies.

This impedes the usage of electronic communication eg in maritime trade. The sender of a cargo produces a unique document, the bill of lading, hands a copy to the shipper and sends the protected original to the receiver. The receiver may trade the original and its title or keep it. Whoever presents the original to the shipper will be handed over the cargo.

The shortcoming of the paper bill of lading is the fact that it takes time to transport it, particularly as it is a piece of value and must be well protected. Therefore, an electronic substitute should be found that protects the uniqueness of the original document, and which can be transacted over communication systems. The technique should support recovery after equipment or communication failure.

Besides issuing negotiable documents there are other ways of securing correct title to property. Instead of a person proving his claim by the presence of a token, the claim may be addressed to a distinct person who then is expected to prove his identity. This is the case with the freight bill, which is another way to deliver a cargo to the authentic receiver. However, the freight bill cannot be traded as effectively as the bill of lading.

The provision of electronic negotiable documents must include:

- document uniqueness, ie a document should only exist in one single valid copy (and can therefore not be sold more than once by an owner)
- document authenticity, ie a document should not be able to alter, and the origin of a document should be possible to identify
- transferability, ie the document should be possible to transfer through communication networks
- fail-safe storage and communication, ie recovery after failure should be possible both when the document is stored or transferred between parties.

One should expect that, unless proper electronic documents will be available, the use of paper for negotiable documents will be continued at the expense of effectiveness and more paper.

Transaction of negotiable documents are often a part of a larger business transaction, eg the seller of a document receives a payment, or negotiable documents are exchanged between the parties. When such transactions are taking place over a telecommunication network, there



might be a need for a service giving fair exchanges of values, ie a service that can guarantee that either will the whole exchange be performed or it will perform no exchange. Such a service will secure fraud during exchange of values.

### *Fair Exchange of Values*

When negotiable trade documents change hands, they are often handed over in exchange for something else, for example another negotiable document, some form of payment, or simply some piece of information that may be of sufficient value to the receiver.

The party who gives a document away may of course be concerned with the possibility that he may not receive in exchange the object or the information he was supposed to.

If the parties meet physically and exchange ordinary documents, this concern may not be very serious; an attempt of abuse is likely to be detected early enough to prevent a successful fraud. In the world of (interactive) EDI, however, the problem can be more serious. Efficient communication is possible over great distances with parties to which there may be little or no existing business relations. Such parties may well be found worthy of less trust than those with which physical meetings can be arranged.

### *Untraceability*

As electronic registration and transportation of data becomes more common, there are an increasing number of scenarios where individuals face new threats against their privacy. Since many types of personal data can easily be traced to particular individuals, the fact that the data are electronically stored introduces the possibility that someone could efficiently collect comprehensive dossiers on individuals, even without this becoming known to the users themselves.

In its most general form, anonymity or untraceability is a service with the goal of preventing such personal data from being traced and collected.

The issue is therefore to allow accesses, calls or transactions to be performed without revealing the identity of the user.

In some cases, anonymity of the user is required or identification of the user is unnecessary. Examples where anonymity is required are about electronic cash or electronic shopping where this is related to the privacy of the user. Practical cases are about road toll systems and mobile phone billing without revealing location history of user. Examples where identification of the user is unnecessary by the target system is where a service is opened to thousands of users but where subscription to the service is not managed directly by the service but by another company: The service manager is only interested in the fact that charges can be paid when the service is used. Who is using the service is not relevant. In some cases the user would also like to know that the service manager is not able to trace back the user.

Another category where anonymity is required is non-traceable calls. Reporting fraud or corruption will only happen if the call (either phone or e-mail) is not traceable to the caller.

There is a need to have mechanisms able to fulfil these needs. However these kinds of techniques should not be used when there is at the same time a requirement of auditability. For cases where both requirements exist there can be solutions where tracing an event can only be achieved by co-operation between different auditors.

### *Time-Stamping*

In electronic communications, a digital equivalent is required for the date and time stamp in the paper world. Such a time stamp must be issued by an organisation that is trusted. If time

stamps are simply attached internally by the sender or receiver of a message, then, in case of litigation, it will be difficult to establish if these were erroneous or have been forged.

In direct communications, both parties may agree on a mutual time reference, but in store-and-forward type communications time stamping by a third party is particularly important .

Depending on sectoral differences, different granularities of time stamps may be needed. Some sectors may be content with the date, some with the nearest second.

## **Requirements**

- Scenarios for the use of electronic security services
- user specifications for electronic security services
- establishment of international application rules that can operate under the different legal frameworks and that ensure international communicability
- identification of different scenarios where it is appropriate for the public interest to mask or hide the identity of the end user, taking into account the balance between full anonymity and audit.

### **4.2.4. Digital Signature**

#### **4.2.4.1. The Individual Right to Signature**

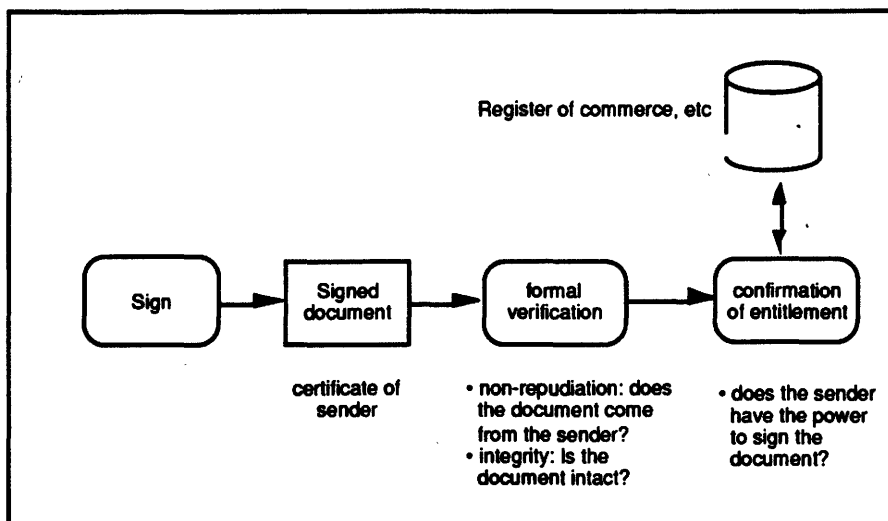
##### **Issue**

Individuals have the right to sign any information.

##### **Discussion**

Like with hand-written signatures, anybody is entitled to use a digital signature. Therefore, the distribution of keys for the purpose of signature must be non-discriminatory and non-restrictive. Separate from the signature is the question of entitlement, ie if a certain person is empowered to sign a certain element of information, document or transaction.

Signature verification is therefore a two step process: formal verification of the signature and verification of the entitlement of the sender. This process is depicted below.



It is assumed in this simple model, that the sender adds his certificate (name plus his public key) to the signed document. The formal verification then establishes that a person with a certain name has correctly applied his signature and that the document has not been modified in transfer. Verification of entitlement checks that the name has the legal power to sign a particular document.

Note that as a consequence, the powers given to a person should not be included in the attributes of the certificate, otherwise any change in these powers would invalidate the certificate.

The situation maybe further complicated by the fact that several signatures maybe required for certain documents, eg husband and wife plus notary, two company directors.

### Requirements

- Clarification of the right to signature and the attached entitlement.

### 4.2.4.2. Consistency of Legal Principles for Digital Signatures

#### Issue

The legal functions have to be clearly identified for the authority of digital signatures, before a code-of-practice can be developed and introduced.

#### Discussion

In legal practice security and functional requirements for hand-written signatures differ widely. In some cases a hand-written signature is only to indicate that the signer has concluded his train of thought or his expression of will; under the given circumstances its authenticity may be obvious and needs not be provable. In other cases, for evidence, the signature must be provably authentic. In yet other cases authenticity requirements may demand attestation or even ask for more than one person's signature or for public notification. Another important case are "process signatures", where a process and not a natural person is the signer.

The spectrum of legal requirements can be matched by the spectrum of technical realisations which may differ with respect to security provisions just as widely as legal requirements. Yet the signing process must be transparent to the signer. For this reason it must follow

standardised rules; specific man-machine interfaces must be familiar to the signer; ie they must follow a standardised layout principle.

For ease of transition (in judicial thinking) from hand-written to digital signatures traditional functional requirements for hand-written signatures should be met by the technical implementation of digital signatures as closely as possible.

A particular problem is the validity period of a digital signature. One must distinguish the validity period of the signature itself and the validity period of the entitlement.

The validity period of the digital signature itself may have to be limited for technical reasons. These reasons include:

- Insufficient key length. One may discover that some years from now, new progress in mathematics and technology makes it plausible that keys of the originally chosen limited length can be broken. (For instance, several European banks have introduced remote banking with RSA keys of length 512 bits. One cannot guarantee that this will be safe in 10 years, or even less, from now.)
- Poor key generation. One cannot be sure that programs at the desired quality level will be used by all key management centres. Hence users of those key management centres may find that their keys are breakable, and they have to cancel their certificates.
- Weak protection of workstation. The secret key of a user may be compromised accidentally or through negligence. It may also be possible to tap the password of a user through a Trojan horse on his PC and subsequently get access to the secret key. (Fraudulent users may even claim this happened, and give away their key on purpose, in order to dispute that a certain signature did originate from them.)

Taking the necessary precautions, and taking a differentiated approach to the validity period of signatures, then most digital signatures would fall inside the scope of applicability of hand written signatures

The entitlement attached to a signature normally changes much faster. The authority given to a person should therefore not be included in the attributes of the certificate, otherwise any change in entitlement would invalidate the certificate.

However, in all the work that has been carried out so far, there is no solution offered to the following problem: If messages have been signed with a key and needs to be kept for a number of years, and that key is denounced by the user as being compromised, how can the value of the already calculated signature be left intact? One possibility might be to use a TTP for time stamping, but further study into this problem seems in place. An example may illustrate this point.

If a user A signs a message in 1993, which has legal consequences to user B until 2003, and A then cancels his certificate in year 1995, claiming that his key has been compromised, he will probably claim that the signed document from 1993 was falsified in 1995 by B, who could have bought a copy of A's secret key. However, if B upon receipt in 1993 had gone to a TTP and had the signature of A time stamped and signed by the TTP, or even registered, he can prove that A in fact did produce the said signature back in 1993.

For some sectors and/or applications the granularity of the time stamping will be critical. It is conceivable that trusted time down to one second accuracy will be needed.

## Requirements

- EC-wide/international agreement on the legal functions of signatures

- clarification of the conditions of acceptance of the authority of a digital signature, eg for legally binding purposes, ie as substitute for hand-written original signatures
- recommendation for the implementation for a public digital signature scheme for use by business, administrations and the general public
- legislative rules and, where appropriate, liabilities, for keys, certificates and TTPs to cover revocation of any or all the entities involved in the “chain of proof” needed in the signature technique.

#### **4.2.4.3. Universal Acceptance of Digital Signatures**

##### **Issue**

For digital signatures to become a full alternative to hand-written signature universal acceptance is required.

##### **Discussion**

All functions of the hand-written signature should also apply to digital signatures.

Where legal functions are carried out by digital signature, consensus with the legal profession is essential.

Enterprises and individuals require greater legal certainty with regard to the use of Digital Signatures, and all transactions involving computers.

##### **Requirements**

- Development, together with the legal profession, of recommendations for the practical use of digital signatures as a full equivalent to hand-written signatures in legal transactions including the conditions required for evidence
- demonstration, through pilot projects, that digital signatures can be used as equivalent to hand-written signatures
- inclusion in the curriculum of relevant educational institutes (eg engineering, law and business schools) the use of digital signature.

#### **4.2.5. Privacy enhancement Issues**

##### **4.2.5.1. Perception of Requirements for Privacy Enhancement**

##### **Issue**

Confidentiality is, at times, essential for the good functioning of administrations, business and human relations.

##### **Discussion**

Business user of telecommunications and information systems cannot obtain full business benefit without confidentiality services being available. There is a clear need for confidentiality services in the exchange of information in the business as well as in the private use. Today the exchange of sensitive information requiring confidentiality is often done in

non-electronic form because for electronic transmission "confidentiality" is either not available or its use not permitted. With the increasing demand for fast exchange of all kind of data, demand for "confidentiality" will become pressing. It is already present in some applications such as medical information systems.

Most business and private users of communication systems are aware of the conflict between their confidentiality requirements and national security issues which require the possibility to intercept the communication in a way regulated by national laws. They accept the national authorities ability for this interception provided there are adequate safeguards to prevent unauthorised interception even by government employees.

Expectations of confidentiality of electronic message services can currently not be met in the absence of international standards or internationally accepted methods. Uptake of these services by commercial users to support business processes will therefore have a natural limit, ie to those messages that someone usually writes on a postcard. Examples of commercially sensitive information includes pricing and bidding strategies, mergers and take-overs, or from a privacy point of view (transmission of personnel and medical data).

#### *User needs for confidentiality,*

In analogy with confidentiality offered by existing physical mail and archiving services, ie envelopes, registration, courier services, etc., there is a need for confidentiality in the situation of electronic interchange and storage of data. Even more so because electronic data can much more easily be copied or disclosed in its usual form, eg only channel coding and formatting as the "envelope", than its physical counterpart.

At present certain unclassified but sensitive information on physical media such as paper, microfilm, or photograph, of business enterprises or medical centres are protected against unauthorised disclosure by physical and procedural methods.

Today the trend is towards more electronic communication and storage of data and hence there is a need for appropriate confidentiality services in an agreed or standardised form to be readily available for all users of electronic information systems.

#### *Service provision*

The extent to which confidentiality services are provided for a specific business or citizen could depend on a system of licenses or certificates.

A particular business might qualify for a confidentiality license depending on its internal procedures and activities. A general (minimum) level of confidentiality could be provided to all users.

It should be possible for certain user groups or businesses to use other confidential services (eg proprietary) than the standard ones provided.

There are strong indications of emerging "bottom up" solutions for these needs (eg the Pretty Good Privacy offering on Internet, beginning 1993).

Other initiatives (eg the announcement of the "Clipper Chip", 16 April 1993) illustrate the growing awareness of governments of the needs of their citizens for confidentiality services.

#### *Awareness*

In general users of electronic data processing systems are not aware of the threats involved in using those systems. Only after they have noticed (the consequences of) an unwanted or unauthorised disclosure of their information will they start to think of the inherent vulnerability of the system they are using. In view of this one should try to create more

security awareness. Users, service providers, operators and authorities should achieve a certain minimum level of awareness of the issues involved in using confidentiality services before embarking on their use.

### *Granularity (meeting differentiated needs)*

Confidentiality services at different granularity and for different types of telecommunication services are needed. Based on his risk analysis the user can then decide which level of confidentiality he needs and then use the services which provides this required level.

Some users may want a range of services of different assurance levels (analogy of courier services, registered mail, ordinary mail). Some users may want visibility of assurances to different extents.

### *Impact of loss of information and Impact of theft of information*

By its nature, actual risks and impacts of disclosure are hard to quantify. But the absence of a baseline of protection of confidentiality will undoubtedly have a negative impact on commercial (and other) usage of international electronic communications in a wide range of business processes.

### *Actors and roles*

Individuals may have a number of roles in more than one organisation - these need defining or clarifying. Their "role" as a private citizen is an important case. The organisations that act as custodians of roles need to be classified also. These are essential ingredients for domain management.

### *Mutual confidence and TTPs*

Users and mechanisms to ensure that they get assurance of compliance to agreed "rules of procedure" from their trading partners, or other private citizens, with whom they are interacting using confidentiality services. TTPs are one mechanism for achieving this, but other lower assurance, lower cost solutions may also need to be considered.

## **Requirements**

- Frameworks and architectures which are accepted as well by the business users as by the national security agencies and the service providers
- standards for services and service provision
- compatibility of confidentiality services with existing communication standards and practices where possible
- verification of practicability of proposed solutions through suitable pilot projects
- model contracts for confidentiality services
- awareness improvement of sector actors of the potential losses due to the absence of confidentiality services.

#### **4.2.5.2. The Case for the Provision of Public Confidentiality Services**

##### **Issue**

The provision of public confidentiality services have to reconcile the needs of the business sector and general public with the obligation of public authorities to provide adequate protection while at the same time maintaining its capability to fight organised crime, maintain public order and national security.

A well developed public confidentiality service would provide for the obligations in a transparent manner.

##### **Discussion**

Business operates increasingly in an international and open environment. The communications take place via private and public networks. Modern network management techniques use alternative routing depending on traffic conditions. This implies that the physical communication is under the control of a variety of intermediaries working under different regulatory and legal conditions for data protection and privacy, and therefore one must consider the network as inherently vulnerable. This means that end-to-end protection is required. This applies also to the general public using international public telephone networks.

It is a fact that business and the general public have been addressing their needs with public domain solutions (published algorithms and freely available software). However, the approach is awkward and its utility therefore limited, since, for example, there is no public directory and he has to manage the keys himself. A public solutions open to all users requiring electronic signature and confidentiality would remove the need for the use of ad hoc solutions. It would also provide for a transparent solution to the need for legally authorised intercepts.

If a public confidentiality scheme is offered, organised crime could also subscribe to such a scheme, but as it would include provisions for legal intercept, it would hardly be attractive. One would expect that such users would continue to find their own solutions as will the classified domain.

An open and public service offering a credible level of confidentiality would therefore provide for the honest user, while not worsening the situation with respect to public order or national security.

The combination of international communication and national security regulations require a common framework for confidentiality services, which on the one hand interoperate within all Community Member States as well as with countries outside the Community which themselves may establish their confidentiality services. This requires either an overlay approach or gateways which link the different national or regional services. These gateways are only required where multinational agreements for co-operation on national security concerns is not yet established. In this case these gateways may provide at least an interim solution.

In order to fulfil its function and eliminate the need for "home-made" solutions, the public confidentiality service must be open to world-wide use and provide its service in a non-discriminatory way.

Confidentiality services should ensure that

- Users are protected and obtain assurance against non authorised interception and disclosure.



- The confidentiality service is of high (technical, procedural) quality and evaluated as such by all Member States.
- Authorised disclosure of the protected user information (under the confidentiality service) is under certain well-defined circumstances possible, eg by secret-sharing.

With this approach, confidentiality mechanisms details (description) do not need to be published or disclosed to the public in general.

While the use must be largely unrestricted, the systems and sub-systems or equipment for the independent implementation of aforementioned confidentiality services can be made subject of export controls, eg export is possible if :

- The users comply with the rules of the exporting nation (end-user declaration) with respect to the disclosure mechanism.
- Multinational business users from EC countries communicate with "central" organisations.
- Other countries on a bilateral agreement liaise with EC if they comply with the rules.

Export restrictions are, inter alia, based on the concern that cryptography may be used by hostile governments or other organisations for the concealment of subversive information. The same concern does not apply to the use of cryptography for integrity and authenticity enhancing service.

There are technical solutions to provide only integrity, integrity plus signature, and integrity, signature and confidentiality. Confidentiality enhancement is de facto only meaningful in communications with also the two other functions being provided.

The problem remains that organised crime and hostile governments are not restrained from adopting public domain solutions or from developing "home-made" mechanisms. Furthermore they are able to exploit legitimate users of systems and solutions to their own ends by use of "traditional" criminal mechanisms of bribery, blackmail or threats to personal safety. Legislation could discourage non-authorised use, but cannot be expected to prevent it, particularly in the case of organised crime. Restrictive legislation impacts the "law-abiding user" much stronger than others.

#### *Choice versus interoperability*

The users and service providers may feel the need to choose solutions to achieve the assurance levels they require. But interoperability will dictate a limited set of possible choices being available, and costs of service provision will also focus debate onto efficient solutions.

#### *Advice and instruction versus prohibition*

This may vary from country to country, however certain minimum-rules will need to be adhered to between parties offering interworking public schemes which includes beyond simply usage also systems and sub-systems or equipment for the independent implementation of such confidentiality services

The confidentiality that users enjoy will depend upon the robustness of the service that is offered. This in turn will depend upon the robustness of the architectures available to perceived threats: key theft, masquerade, deliberate denial of service, inadequate disaster recovery are examples of threats the vulnerability to which may be different for alternate architectures.

Mechanisms are needed that provide for a defined way to pass from one domain to another. This will require collective or multilateral agreements for interoperation.

## Requirements

- Architecture that minimises service vulnerability
- framework for the provision of trans-domain confidentiality services
- guidelines for pan-European confidentiality service providers (including accountability)
- model contract for relationship between service providers across national boundaries
- assurance criteria for service providers and operators
- accreditation process for mutual recognition.

### 4.2.6. Use of Names and Certification of Credentials

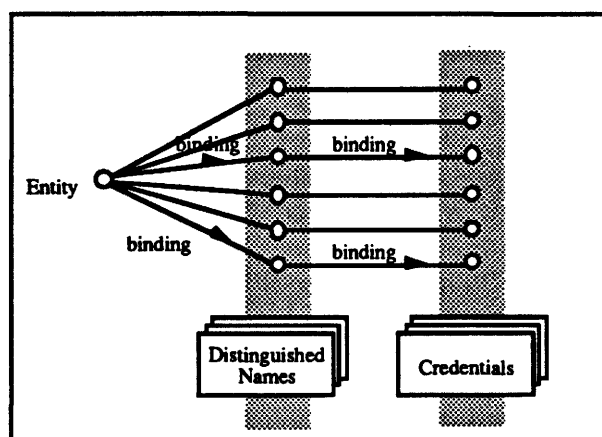
#### Issue

Use of names and of credentials (eg the public key) in international communications.

#### Discussion

Name Assignment and Certifications Authorities are Trusted Third Parties. Their purpose is to allow for individual and authentic addressing of communication system users by means of their authenticated Distinguished Names. A user may ask a Naming Assignment Authority for a Distinguished Name. The Naming Authority will give him a Relative Distinguished Name and supplement it by its own Distinguished Name to the user's Distinguished Name. Thus, although a person may ask several Naming Authorities for the same Relative Distinguished Name, each of his Distinguished Names will be unique, because the Distinguished Names of the Naming Authorities, by definition, will be unique. The concept of an agent that handles the interfaces between the end-user and the naming authorities is important in providing a user friendly interface to this process.

The two functions of name assignment (or identification) and certification are “binding” operations. Name assignment binds a particular name to an entity (a person or device), and certification binds certain credentials to a name. The diagram below shows the double binding process.



A Distinguished Name and a unique cryptographic Public Key are made part of the user's Credentials. The Public Key can be used to verify a (ciphertext) signature which has been effected by the user's complementary Secret Key (not contained in the Credentials). Credentials are signed/certified by the Certification Authority. Thus the user's Certificate consists of the Credentials, their signature by the Certification Authority and, if necessary, the Certification Authority's own Certificate. The user is given his certificate, preferably in a tamper resistant chipcard.

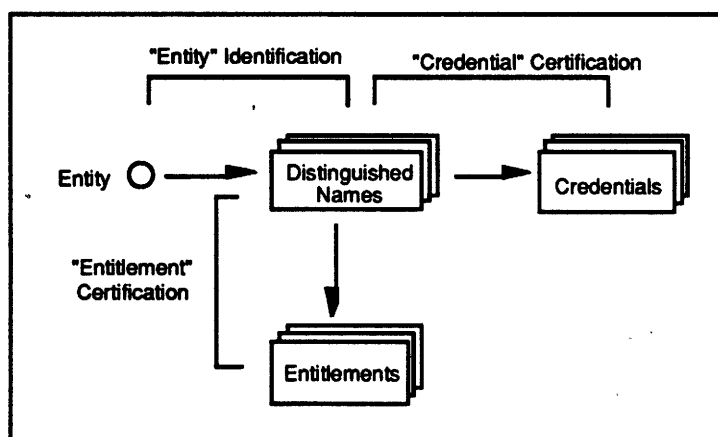
After signing a message with his Secret Key the user concatenates his Certificate to the message and its signature. The receiver of the signed message can use the Certification Authority's widely available Public Key to verify the signer's Certificate and Public Key. With the latter the authenticity and integrity of the message can be verified.

The security services related to name assignment and certification need further standardisation as well as legal recognition, both preferably on an international level.

The United States have already begun to apply relevant US national standards. Therefore, corresponding standardisation action should be started on a European level. Its results should be made the basis for a European contribution to international standardisation. At the same time an interface toward a legal usage of naming and certification services should be defined to ease the adaptation to and to provide for the compatibility of the various EC legal systems.

Other related issues are pseudonyms and anonymity, for which a business requirement has been identified. Different degrees of anonymity should be provided for according to the specific needs in digital cash, tele-shopping, registration in data bases for statistical purpose etc.

As described above, the ability to sign a piece of data is to be distinguished from the entitlement an entity possesses. This relationship is depicted below:



It is necessary to identify requirements and to develop guidelines for the use of names, in relation to:

- > requirements to meet by naming authorities
- > requirements to meet by the user
- > naming principles
- > format of Distinguished Name/Relative Distinguished Name
- > handling protocol between naming authorities, user and certification authority
- > change of names
- > recording of information pertinent to de-referencing of names (by the Directory).

It is further necessary to develop guidelines covering the creation and use of certificates, in relation to:

- > certificate semantics and format
- > certificate handling (production, issuance)
- > signature and its certification (method, process)
- > authentication of certificate owner (method, process)
- > expiry dates
- > renewal of certificates (periodical)
- > renewal of TTP public key (periodical)
- > handling compromises of secret information (secret keys, PIN etc.)
- > revocation of certificates and notification
- > black listing and execution of certificates
- > security standards to be met by certification authorities.

### **Requirements**

- Guidelines covering the use of names
- guidelines covering the use of certificates.

### **4.2.7. Security of Electronically Stored Information**

#### **Issue**

As legally and commercially significant information is transferred and stored electronically, the implications of this on long-term (10's of years) secure storage and retrieval must be properly understood.

#### **Discussion**

Industry is moving increasingly towards electronic trading in all its aspects. Governments are encouraging the use of electronic communication of commercially and legally significant information. As a result, there is a need both to establish irrefutably the origin of, and the delivery of, such information and, particularly, that the information has been signed and stored in an unforgeable way. This unforgeable electronic signature must be trusted for at least 10's of years for some information, and the associated information must be retained in a secure manner that is capable of human interpretation at any time during that period. Any system proposed for electronic signature storage must be as secure and robust as that currently used for hand-written signatures.

Any such system must allow for not just technical evolution, but also social change and other factors (eg the continued existence of trusted public key directory centres, or the way businesses merge, change or collapse). It is not currently clear that the way this can be achieved is yet accepted legally, or the full implications are even properly understood

#### **Requirements**

- Common approach to the security of electronically stored information
- unforgeable secure storage.

## 4.3. Requirements for the Safety of Communication Systems

### Issue

Safety requirements for communication systems must be expressed in ways that capture users expectations, reflect the engineering viewpoints of vendors and service providers and are appropriate for regulators.

Safety requirements have to be integrated with other types of requirement, eg reliability and security.

### Discussion

End user requirements for safety of products or services are often implicit or stated in very "soft" terms or in terms that assume regulation and certification is looking after their needs. These user requirements can be contrasted with the engineering specifications needed by vendors and service providers to build systems and provide for their assurance.

In addition, safety is just one attribute that has to be integrated with all the other types of requirements and potential conflicts identified and resolved. For example, the requirement for visibility of evidence for safety assurance may conflict with security considerations, the need to make access impossible for security reasons may conflict with the need for emergency procedures. (eg evacuation). However users main concerns are ones of cost and choice and these have to be addressed in the dialogue between service providers, vendors and regulators.

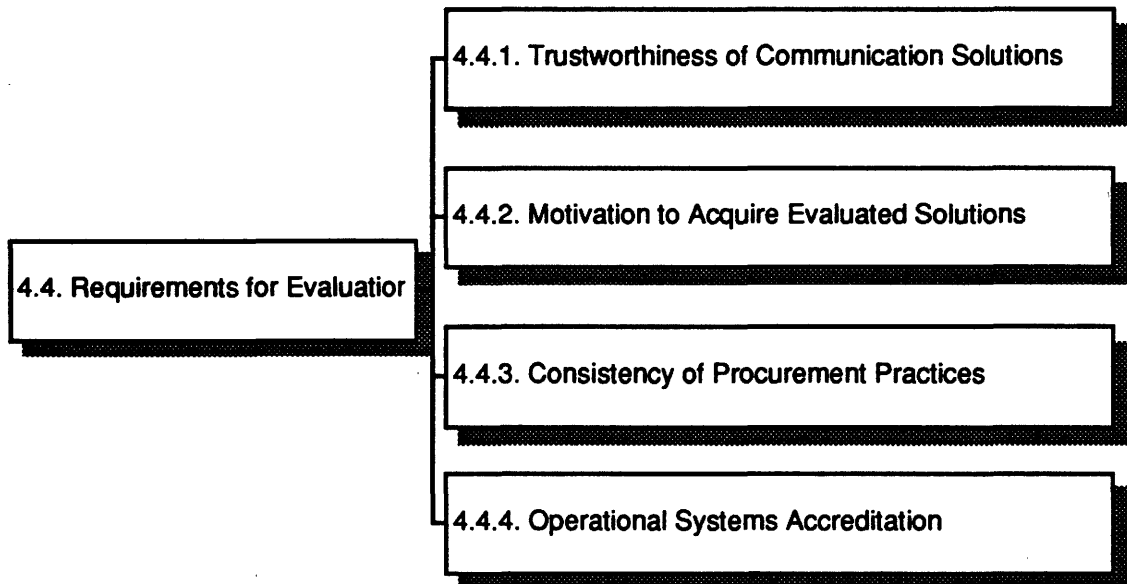
In the safety field, the notion of the tolerability of risk and the use of both qualitative and quantitative risk assessments, provides a lingua franca between regulators and service providers as well as, in a modified form, for users and those with professional interests. This discussion needs to be broadened and integrated with security requirements particularly for domains (eg medical informatics) where open, heterogeneous computer systems have significant IT security and safety components.

In addition to the risks from products or services that the user is willingly engaging in or purchasing there are the risks from indirect accidents (eg major chemical or nuclear accident) and normally in discussions of policies towards the acceptability of risk a distinction is made between these two types of risk with the requirements for indirect risk being more onerous than those entered into voluntary. Again, there is the need to integrate the discussion of these risks with those from security breaches.

### Requirements

- Platform for a dialogue on risk including users, regulators, vendors and service providers
- policy on risk management on a societal level based on objective risk assessment methods
- techniques that permit an integrated approach to the different types of risk (safety, security, commercial, direct, indirect).

## 4.4. Requirements for Evaluations



### 4.4.1. *Trustworthiness of Communication Solutions*

#### **Issue**

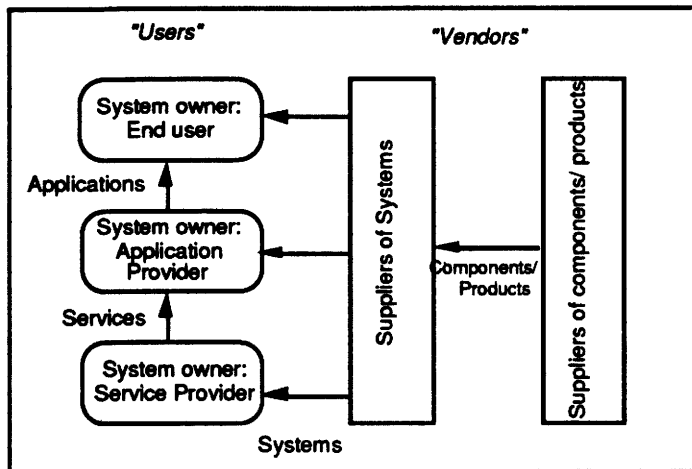
Establishment of trust in components, products, systems, services and applications .

#### **Discussion**

The trustworthiness of a given communication solution and its use imply that the system owners and especially the users need confidence in its security and safety. They also need to be able to compare different solutions with regard to the security and safety capabilities, cost, functionality, performance, availability and reliability.

The diagram below shows schematically the major roles of the actors involved. The end-user normally runs an application, eg a particular banking application. The application is provided by the application provider, who, in turn, may use various services, offered by service providers, eg communication services.

To run and provide applications and services, systems are required, supplied by, normally, several system suppliers. System suppliers purchase components and products from sub-suppliers.



In the end, the trustworthiness of the application must be established. This overall trustworthiness is a function of the trustworthiness of the application provider, the service providers, and the systems, products and components.

Depending on the needs of the user, vendor declarations, self evaluations or formal evaluations may be required at the various stages. The choice of either of these mechanisms will depend on the costs and delays involved in formal certification processes, the level of assurance required and national constraints.

Another major factor is the recognition of certificates in other markets and their utility, eg in protecting the user or vendor against liability claims, where it is possible to do so.

The qualifications, experience and motivation of project managers, evaluators, certifiers, accreditors and system administration staff also affect the resultant level of trust achievable in the operational system.

Users continually need to upgrade their hardware platforms and change or add to software systems to remain commercially competitive and to follow trends, etc. Thus the ease with which systems and products can be re-evaluated or the portability of evaluation results are important issues when deciding on the needs of the user. For example, portability of products and systems across different hardware platforms. For how long will a vendor support the evaluated hardware and software configuration? Will a vendor re-evaluate all upgrades of their product in a timely manner?

### Requirements

- International agreement on criteria and evaluation methods, and mutual recognition of test results
- clarification of the commercial value of “certified products”, eg in terms of liability limitation
- clarification of the status and implied liability of vendor declarations
- international agreement on the methods for evaluating security and safety critical system development processes, and the qualifications and experience needed for individuals that are involved in these processes.

#### **4.4.2. Motivation to Acquire Evaluated Solutions**

##### **Issue**

The advantage of the use of evaluated/certified solutions is not generally accepted for commercial applications.

##### **Discussion**

Formal security evaluations have been carried out at a national level by a comprehensive, costly and time consuming process. The investment in the evaluation process by the vendor has resulted in higher prices for the resulting secure IT product. The duration of the evaluation process, has resulted in many secure products falling behind the technical state of the art.

Up to now, this has often detracted from their broader relevance in the commercial market. Users have often preferred lower cost, more functionality rich products unless forced to purchase evaluated and certified products through some public procurement policy.

Vendors, historically, had products evaluated separately by each national market and their supporting criteria. The resulting limited revenue opportunity did not justify the high cost of getting products evaluated.

It is necessary to change this view by convincing users of the advantages of purchasing evaluated/certified solutions. Rapid adoption of Common evaluation and certification criteria is essential to reduce cost and speed-up mutual recognition of the resulting certificates.

##### **Requirements**

- Rapid adoption of Common Criteria
- agreement on common evaluation method
- portability of test results and mutual recognition
- work sharing between vendors, test centres and users to speed up the evaluation process
- establishment of the "value-added" for the use by administrations and business, eg in terms of liability protection and in relation to insurance costs

#### **4.4.3. Consistency of Procurement Practices**

##### **Issue**

National procurement guidelines for the purchase of evaluated/non-evaluated products are not consistent throughout the EC, nor is there a general agreement on when there is an obligation to use evaluated products, and when it is recommended but discretionary.

##### **Discussion**

Some security evaluated IT and communications products are purchased as a result of a risk analysis where it is determined that the evaluated communications product better suits the organisation's security needs than a non-evaluated product.

However, a survey conducted of over 200 organisations indicated that, to a large extent, evaluated products are purchased today by organisations in the EC because of the expectation



they will be required by law to use certified products. This type of legislated market is occurring especially in those Member States that were involved in the development of ITSEC.

Unless the procurement policies in the EC are harmonised, the public sector use of IT products will become a patchwork of evaluated and unevaluated products. This may create new barriers to the efficient flow of information.

Ways should be found to assist those member states not involved in the early stages of ITSEC to develop and test procurement policies that are based on evaluated communications products.

### **Requirements**

- Identification of categories of applications requiring evaluated solutions
- alignment of national procurement policies concerning evaluated products
- development of guidelines on applicability of evaluation levels.

#### **4.4.4. Operational Systems Accreditation**

##### **Issue**

Procedures for accreditation of operational systems in many (non-military) environments are not standardised or well-managed.

##### **Discussion**

Management needs assurance that their total operational system meets their security needs. The use of off-the-shelf (including evaluated) products does not remove this requirement for a whole system approach.

This assurance can be provided by establishing methods for operational systems accreditation, which is the formal acceptance by management of the residual risk associated with the use of a system, and hence its approval to operate.

This accreditation needs to be based on an assessment of the:

- threats and vulnerabilities (risks) associated with the system
- legal obligations
- impact of the realisation of the risks, and any resultant consequences or costs
- existing protection measures within the organisation
- measures provided by the system itself (e.g. by evaluated products)
- additional countermeasures typically in the following categories: technical, physical, personnel, and procedural.

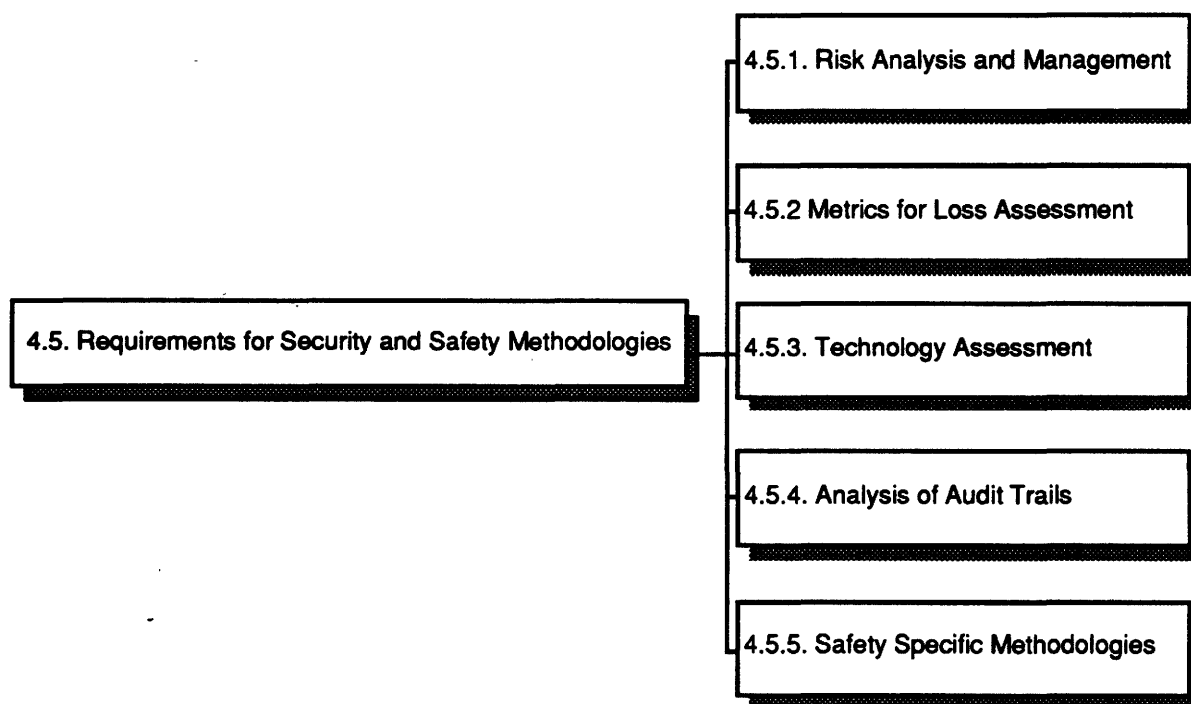
Accreditation needs to be formal, both in order to focus responsibility within one organisation, and because there is a need for organisations to trust partners' accreditation methods and to demonstrate their own security to others. This would provide potential for mutual recognition of accreditation within a community of organisations. External bodies (for example banking organisations or regulatory authorities) may wish to set minimum standards

to be achieved for recognition. Insurance companies could require compliance with these standards.

### Requirements

- Definition of the inputs, process and outputs involved in operational systems accreditation and their agreement by relevant communities
- guidelines for the establishment of schemes for operational systems accreditation within different communities.
- guidelines for organisations to determine the appropriate individual or body to perform the accreditation including the skills and training required by operational systems accreditors

## 4.5. Requirements for Security and Safety Methodologies



### 4.5.1. Risk Analysis and Management

#### Issue

A number of Risk Analysis and Management methods are available within the market place. However, potential purchasers have no recognised method to establish which method is the most effective for their purposes.

#### Discussion

It is a fundamental requirement that each enterprise should manage the security of its Information Systems. The strategy to manage information security must be based on, and compatible with, overall Corporate Security Policy, which, in turn, must reflect and support the key business objectives of the enterprise. However, in addition, any security implemented must be commensurate with the levels of risks to which the enterprise is subject, so as to ensure that adequate, but not excessive, investment is made to protect corporate assets.

The Information Security Strategy will help to ensure the most effective use of resources, and will, where appropriate, ensure a consistent approach to security across a range of different systems. How the Information Security Strategy is to be implemented should be described in detail in a Corporate Information Security Policy. Strategic objectives should be produced. These are general security objectives which may be defined, for instance, in terms of the levels of confidentiality, integrity and availability that the enterprise wishes to attain. The application of baseline security standards has a place within an Information Security Strategy, but not as a substitute for Risk Analysis and Management.

The implementation of the Corporate Information Security Policy is thus based upon the process of Risk Analysis and Management: that is the assessment of the levels of risks to which corporate assets are subject and the implementation of appropriate security safeguards. Risk Analysis and Management is therefore the key process for the effective protection of information.

Risk Analysis and Management is relevant to, and should be applied over, the complete life cycle of each information system. It can be applied at differing degrees of detail and rigor depending on the size of the organisation and the complexity of the information system.

To enable successful Risk Analysis and Management requires a set of security methods, tools, evaluation criteria, and, of course, products, standards and guidelines.

There are a number of Risk Analysis and Management methods, supported by appropriate tools, available in the market place and some organisations will have developed their own in-house methods. Enterprises need a means by which they can establish which method is the most effective for their purposes. It is appropriate that such a means is agreed, implemented and fully supported within the EC.

As a result of previous CEC sponsored projects, Risk Analysis and Management models have been developed and encompassed in the supporting "Claims Structure". This "Claims Structure" will allow the evaluation of Risk Analysis and Management methods to be achieved. Currently it is being actively considered by the ISO SC27 Working Group 1 for inclusion in international standards. This is a good example where European expertise, backed and supported by the CEC, is influencing the establishment of International Standards.

Related to these issues are:

- the proposed standards for security incident reporting schemes, the output from which can improve Risk Analysis and Management reviews;
- the availability of methods and tools for contingency planning/disaster recovery, which need to be aligned to the "Claims Structure" and Risk Analysis and Management methods;
- evaluation criteria within ITSEC, the Federal Criteria (Draft criteria produced by NIST in the US) and a EC/US Government Editorial Board to produce a "Common Information Technology Security Criteria".

### **Requirements**

- Consideration of the "Claims Structure" as a standard mechanism for specification of requirements, evaluation and the selection of Risk Analysis and Management methods
- evaluation of the "Claims Structure" for applicability in the safety domain
- support for the "Claims Structure" as an international standard

- further evaluation of methods using the "Claims Structure"
- accreditation of organisations to conduct Risk Analysis and Management method evaluations.

#### **4.5.2. Metrics for Loss Assessment**

##### **Issues**

There is a fundamental need for guidance of any kind on how to assess the loss and damages an organisation might face and how much of this might be addressed by evaluation and certification. Such metrics would increase the perception of the value of a formal evaluation scheme.

##### **Discussion**

Action is necessary to ensure the effective international exploitation of the security product evaluation and certification scheme. There must be a competitive business advantage of developing, implementing and using certified security products, and there must be a well understood correlation between a certified security product and the problems that it can solve.

Progress is hindered by lack of independent measures of the business relevance of the certified product.

Measures can be obtained by:

- vendor/user studies (from actual risk assessment)
- product comparisons (using loss reduction models)
- insurance contracts (both direct and consequential damage assessment)
- vendor cost/benefit profiles (market penetration, Software engineering costs, etc.).

Such studies would prove invaluable to the SMEs who cannot justify extensive Security controls yet are probably the most vulnerable to the consequences of information abuse.

The ITSEC actions should reflect a balance between the product based concepts of security objectives (codes of good practice) and quantitative risk/loss assessment.

This should result in measured, affordable controls as a prerequisite to developing a European and international security market.

##### **Requirements.**

- Mapping of certified product features to specific security incidents
- common, product independent risk analysis processes.

#### **4.5.3. Technology Assessment**

##### **Issue**

The solution of many IT security issues requires anticipation of complex future scenarios. Technology Assessment (TA) provides a framework in which the use of new and future

technology can be investigated to provide security safeguards for a particular application under consideration.

## **Discussion**

When considering new applications, especially those that are likely to have a substantial life cycle, new or developing technology may be of use in providing effective security safeguards.

Technology Assessment is designed to involve relevant factors from different areas and to consider all pertinent perspectives (technical, economical, psychological, political, etc.). Technology Assessment aims at preparing options for political action based on the results of a multidisciplinary approach. Technology Assessment is well established in the US. There is a pilot Technology Assessment project in the field of IT security in Germany funded by BSI.

## **Requirements**

- Identification of the information security issues that may be solved within the Technology Assessment process
- Technology Assessment pilot in Europe in the field of information security to assess the consequences for future information security applications and provide options for political and legal actions.

### **4.5.4. Analysis of Audit Trails**

#### **Issue**

The lack of efficient tools and associated framework prevents the efficient management and analysis of audit trails.

#### **Discussion**

The analysis of audit trails is the last recourse solution to facilitate detection of misuse of information systems. However several drawbacks prevent their efficient analysis in large and distributed information systems:

- Even though the nature of audit information is often well-defined by existing security standards, there are no standards for the storage and distribution of such information.
- The hierarchical ordering and merging of information coming from numerous security services of various nature and location is not possible, thus preventing an efficient synthetic analysis thereof.
- The enormous volume of audit information requires specialised analysis tools. Existing tools are often based on statistical or relational search techniques. They usually leave the Security Officer with fastidious and boring scrutinising tasks and often significant combinations of events remain unnoticed. Artificial Intelligence (AI) based techniques could be of help in this domain. Of course, such tools cannot provide absolute and exhaustive scrutiny.

The acquisition and exploitation of audit information may infringe on the right to privacy of individuals, eg in teleworking systems where such information could be exploited to oversee workers' performance on the job. Similarly, the analysis of credit card payment records provides insight on holder's private habits, even though it is necessary to detect security-critical behaviour. These concerns may warrant the recourse to TTP services to prevent abusive analysis of audit trails.

## **Requirements**

- Rules and regulations for the design, handling and exploitation of audit trail information, in conformance with privacy laws and practices
- prevention of audit data base compromise (eg techniques of separation of information)
- services for the independent acquisition, management, and/or analysis of audit trails
- development of innovative technologies (AI-based) for the exploitation of large audit trails.

### **4.5.5. Safety Specific Methodologies**

#### **Issues**

To establish the processes, techniques and methodologies for achieving safety.

#### **Discussion**

Despite the large resource devoted to research and development in software and systems engineering there is still little data on the effectiveness and costs of different methods and techniques for building dependable systems. The best consensus that can be achieved is reflected in emerging generic international safety standards which either decline to provide guidance or do so in very vague terms. There is a need to define what software engineering processes should be put in place to build systems, how these should be applied and how the results from them can be demonstrated to meet the requirements.

There is also a need to establish variation of requirements throughout the system lifecycle and to understand the role of process maturity and models and their interaction with technologies for development. The tendency in safety (and other) applications, to require a bureaucratic documentation based process, needs review and its cost/benefits established. The relative importance of process based approaches, the competency of those involved and analytical techniques need to be addressed.

Safety is of course just one aspect of dependability and many of the problems in achieving safety are general problems. In order to facilitate the exploitation of generic work on dependable systems and to focus this work on the needs of safe and secure systems there is a need to understand in what ways the engineering of safety systems are different. For example, we need to understand how safety analysis techniques (Hazops, fault tree analysis etc.) fit into requirements capture, the need for special fail-safe architectures and design, the special requirements for hardware fault detection, tolerance and management.

The approaches to achieving safety should also recognise not just the software issue but also the problems of designing trusted hardware and the increasing blurring between hardware engineering and software arising from the use programmable ROMs.

#### **Requirements**

- Assessment of areas of common interest between safety critical and security information practitioners
- software engineering processes and techniques for safety applications including their application and evaluation
- understand the special needs for engineering safe systems.

## **4.6. Requirements for Audits**

### **Issue**

Identification of security and control weaknesses and the identification of corrective actions.

### **Discussion**

Audit and auditability are becoming increasingly important and should be an independent part of an organisations approach to security administration, or brought in on a contract basis. The purpose of an audit function is to identify security and control weaknesses and/or failures in enterprises so that corrective action can be recommended to management. An independent audit review ensures that all authorities are not under the same management.

It is necessary to confirm compliance with standards, check system records and activity, and to ensure that organisation policies are being carried out.

Management is responsible for reviewing audit reports and taking corrective action where necessary.

An increasingly important area of information security auditing activity is the involvement of auditors (internal or external) at the initial stages of system development, both to ensure that adequate controls are built in to the system and also to assess whether the development process itself is adequately controlled. This applies not only to in-house developments, but also third-party developers where bespoke work is being undertaken. The latter situation may need a legal or contractual requirement for audit access to the development staff and environment. Such a requirement (to audit development stages and methods) should be included in public codes of practice and relevant professional standards.

### **Requirements**

- Guidelines for audit review of information security activities
- audit tools to enable reviews of security implementations and identify weaknesses (eg using artificial intelligence)
- guidelines on reviewing any or all security changes
- suitable and consistent level of competence for security auditors and organisations to be accepted throughout the Community
- greater commonality of formats for audit trails, so that they can be used between systems.
- mechanisms to enable qualified auditors to be involved in system development.

## **4.7. Information Valuation**

### **Issue:**

A recognised and common means is required to value information for a range of information security purposes, including insurance, tort law cases, risk analysis and management.

## **Discussion:**

Within the information security arena Information Valuation is required for a number of purposes. These include:

- insurance purposes, where, essentially, a financial cost is required for an insurable asset against an insurable event
- tort law cases, where again a financial cost is required to assess corporate or individual loss, and therefore compensation, for a failure or action involving the provision of or use of information systems
- risk analysis and management activities, in which Information requires to be valued not only on a financially quantifiable basis but also on non-financial impacts, such as failure to meet legal responsibilities and obligations, personal safety, corporate embarrassment; infringement of personal privacy, etc. Some Risk Analysis and Management methods do this already, but not in any standard form.

In addition should Green Paper information security activities be extended to cover safety critical systems, further valuations associated with loss of life or injury will become relevant.

To value the cost of re inputting lost information is relatively easy. However, to value the impact of, for instance, the disclosure of highly confidential information which causes the resignation of the Managing Director is less straightforward.

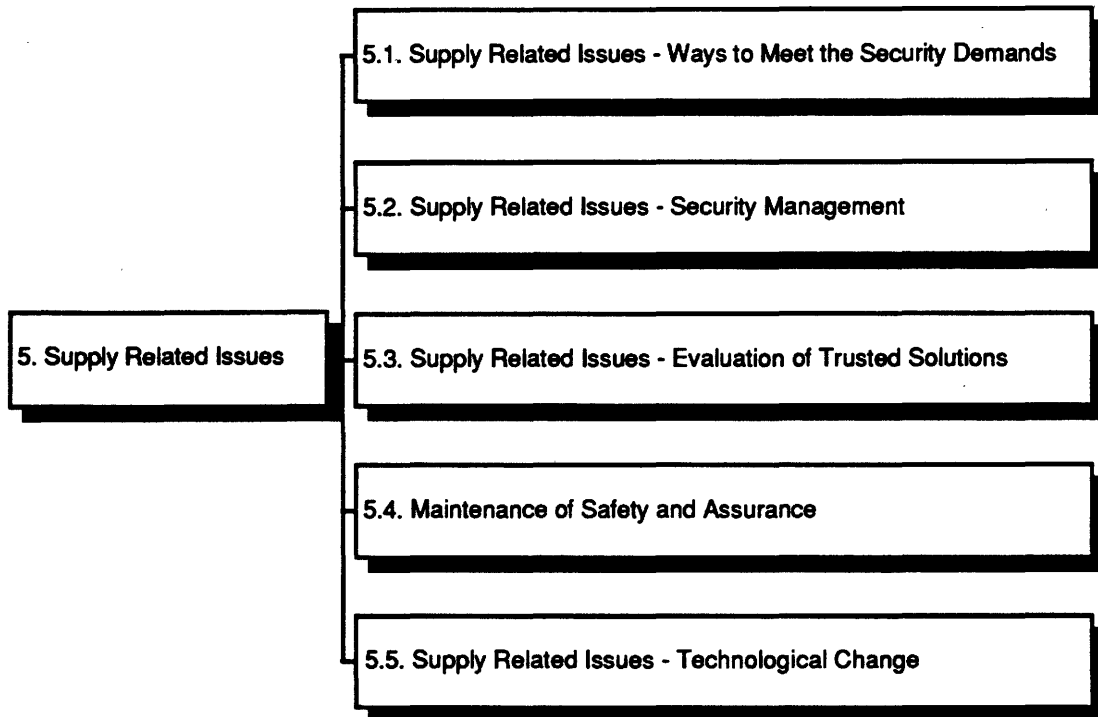
Thus there is a need for a common approach that will allow information to be valued in a way that will allow relative comparisons between financial loss and non-financial impacts, through unavailability of information, unauthorised disclosure of information or unauthorised modification of information or software.

## **Requirements**

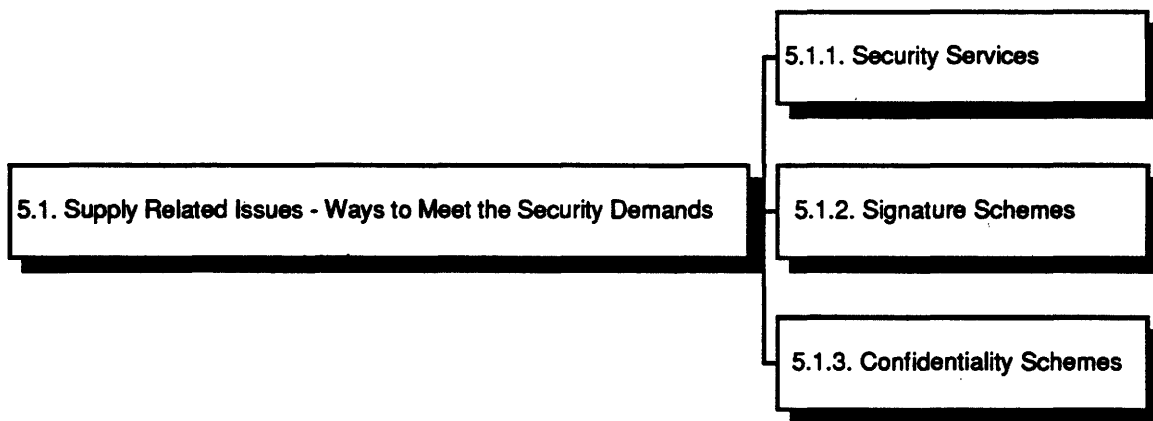
- Development of common practices for information valuation
- assessment of current methods for information valuation
- definition of the rights and duties of information ownership



## 5. SUPPLY RELATED ISSUES



### 5.1. Supply Related Issues - Ways to Meet the Security Demands



#### 5.1.1. Security Services

##### Issue

Agreement on the provision of particular security services is needed to meet the needs of business, administrations and the individual.

Security services are offered mainly to prevent disputes, or resolve them in a way that is structured, efficient, accepted by all parties involved and non-controversial.

## Discussion

Prevention of disputes arises essentially from the very ability of security services to assign responsibility and fault, should one occur.

- Thus, security services must essentially be able to verify the application or non-application of rules and the evidence pertaining to them.
- Security services may or may not generate the evidence itself. In other words the question is whether a third party offering a trusted service also arbitrates litigations pertaining to its principal service. For example, does a signature generation service also provide signature-verification services ?

Two issues arise in this topic :

- What is the legal status of evidence generated by security services ? Does it imply liability ? What is the legal status of decisions made par security service providers when they are not judicial but private (and corollary, what are the rules of appeal) ?
- If evidence is not generated by the arbiter, how is the evidence acquired and authenticated and how is responsibility assigned ? One is faced with the general problems of TTPs : operating rules and legislation, standardisation, inter-operability and accreditation.

Possible solutions to the following service categories have been identified:

### *Non-Repudiation Services*

These can be achieved through straightforward application of the digital signature mechanism.

In an open environment, this would imply the use of public key techniques. Each entity (user) possesses a public key pair, consisting of a public key P, which can be made known to everybody, and a matching secret key, S. The secret key is used to create a digital signature on a message, and the corresponding public key is used to verify the digital signature as been created by means of the secret key. If the public key scheme is an encryption scheme, like RSA, the public key may alternatively be used by anybody to encrypt a confidential message to the owner of the secret key, as this is the only key which can recover the original message.

### *Claim of Origin*

It is possible to prove that claim of origin can only be achieved by using a trusted center, where the electronic documents are registered or authenticated. The point is that in order to establish the origin, we need a digital signature. Of course, anybody can apply his own digital signature to the document, but this will not imply origin or ownership. Hence the only solution is some kind of registration or notary service. In particular, cryptographic techniques have nothing useful to offer in any other way than to apply nonrepudiation services to prove that a document was registered, or by using encryption to protect the content of a document.

### *Claim of Ownership in electronic negotiable documents*

By the use of digital signatures and TTPs electronic negotiable documents can be provided in different ways. Three schemes are presented here.

1. Negotiable documents can be stored by a TTP in that the TTP at any time on request can provide a copy of the document and the name of the document owner. The TTP guarantees that the document is unaltered and that the correct owner is registered. Document transaction is performed on request from the document owner, which could even be authenticated by a digital signature, which also secure against repudiation.

In this scheme the users have to have unconditional trust in the TTP. If the TTP is corrupted it might alter the documents or the owners identity. Several systems exist today that use this approach.

2. If digital signatures are used in the scheme presented in (1) in that the negotiable documents and the "sales contract" proving document transaction are digitally signed, the TTP has only to be trusted to keep the documents securely stored. The owner of a document can be identified by anyone by verifying the signatures of the document and all the "sales contracts" (the identity given in the last "sales contract" in the chain will be the document owner).

In this scheme only functional trust in the TTP is established to keep the digitally signed documents and "sales contracts" securely stored and presented in copy to anyone (or at least to potential document buyers) upon request.

3. By the use of chipcards the negotiable documents can be securely stored and protected against copying or multiple selling by an owner.

The only other way to provide uniqueness is to physically prohibit free copying. This would involve tamper resistance to realise a protected communication with restricted functionality. A message encrypted under a key known to only one entity (eg, the entity's public key) is unique, as long as it is encrypted, and establishes indisputable ownership by the mere fact that it will only be useful to the owner of the key. Only the person in possession of the right key can make any use of the document, which in effect is the property of uniqueness.

A negotiable document is transferred from one chipcard to another, through a public network, in such a way that

- a) It can only be transferred to one particular chipcard only.
- b) Recovery is possible, if the transfer is unsuccessful
- c) the protocol cannot be simulated by any other device than an authorised chipcard.

This solution would require a functionally trusted centre to register the chipcards by their public key.

Also for non-negotiable documents a limit to proliferation may be useful. Consider eg contracts. Generally each party to a written contract holds one original document which cannot be proliferated. When the contract is superseded by a new version, the old version can be located and devalidated. This cannot be paralleled with the usual electronic means. Unless the number of original electronic documents can be limited, devalidation is of little use.

The Document originality can be provided by the use of chipcards. A chipcard can store a secret and protect it. The secret is essential to authenticate the signature of the document. As the chipcard cannot be explored, the secret cannot be transacted into another chipcard. Thus it is practically impossible to duplicate the original chipcard. Such a chipcard can be made a substitute of the negotiable paper document.

In order to produce and to transact chipcard documents via telecommunication trusted equipment is needed. It should be operated by trusted third parties, eg by public notaries.

They may be bestowed with the responsibility to produce chipcard documents and to transact and receive them by means of their trusted equipment. Transaction may be performed by depleting the original chipcard at the sending end, securely transmitting its information and feeding it into another chipcard at the receiving end. This process must be protected for its integrity and confidentiality. Not even the "public notary" must be in a position to alter the information.

Beside issuing negotiable documents there are other ways of securing correct title to property. Instead of a person proving his claim by the presence of a token, the claim may be addressed to a distinct person who then is expected to prove his identity.

This - continuing with the above example - is the case with the freight bill, which is another way to deliver a cargo to the authentic receiver. However, the freight bill cannot be traded as effectively as the bill of lading, although, by omission of additional chipcards and other trusted equipment, it makes it easier to design the electronic substitute process.

One should expect that, unless proper electronic documents will be available, the use of paper for negotiable documents will be continued at the expense of effectiveness and more paper.

### *Fair Exchange of Values*

It is possible to exchange electronic documents of value, such as unique documents or commitments with digital signatures in an interactive protocol, which will not allow any participating party to cheat. The framework for this could be the forthcoming UN/EDIFACT recommendation for Interactive EDI, which is sufficiently flexible to integrate the communication required for fair exchange of values.

### *Untraceability*

Methods have been developed in cryptography, which would allow the implementation of central data base systems, based on individuals in say the EEC, which at the same time would provide complete anonymity to the individual, yet be open to extract any reasonable statistical information. The impact would be quite important. It would be possible at the same time to have all data available for statistical evidence, say for AIDS infected persons, who volunteer to register, yet guarantee the protection of the individual, not based on unconditional trust, but on logical protection, which can only be penetrated if some of the hardest known mathematical problems can be solved.

### *Time-Stamping*

The third party must be trusted by both parties, or at least the dispute resolution mechanism, for the correctness of the date and time supplied, but also for the confidentiality with which they handle the contents of the correspondence.

### **Requirements**

- Harmonisation of legislation on the legal status of evidence generated by any TTP and especially on the intra- and extra- community recognition thereof
- litigation services based on existing international bodies such as the International Chamber of Commerce
- techniques for the establishment, handling and recording of electronic negotiable documents
- date and time stamping for time-critical transactions and applications, including a range of granularities of timing

- international harmonisation of rules and services for time stamping, with the objective of achieving general recognition and acceptance of time stamps and their provision by suitably accredited service providers.

### **5.1.2. Signature Schemes**

#### **Issue**

Introduction of an international digital signature and of identification schemes.

#### **Discussion**

Open communication requires standardised publicly available algorithms. It is possible, however, to develop a scheme for digital signatures, to get laws, regulations or directives in place, to develop supporting profile standards and to develop fully implementable models for TTPs, without specifying in detail the underlying algorithms.

The characteristics required of a digital signature mechanism include that it

- is practically unbreakable
- has a sufficiently large key space, performance (time and space requirements for signing and verification), reasonable size of key, etc.
- includes key generation.

In order to allow for world-wide, unrestricted use of a digital signature scheme, the mechanism should not be usable for the concealment of message content.

The minimum requirement should include

- an estimate of error probability if probabilistic methods are used
- an estimate of probability of occurrence of weak keys (perhaps completely improbable)
- a guarantee of sufficiently high degree of uniform distribution.

In so-called identification schemes (for access control), which do require public key techniques rather than conventional schemes, practical zero-knowledge protocols must be developed and standardised that fit a corresponding digital signature standard.

#### **Requirements**

- Specifications and standards for an international signature scheme
- specifications and standards for the integration of the signature schemes into practical applications
- general application programming interface (API) for the integration of signature schemes into applications. This should include codes which explain the purpose of the applied signature
- development of transaction-oriented multiple signature schemes
- licensing of cryptographic algorithms.

### **5.1.3. Confidentiality Schemes**

#### **Issue**

Agreements on the confidentiality schemes to be used, taking into account the needs of individuals, business, administrations and the duties of law enforcement.

#### **Discussion**

Confidentiality of message contents can be achieved in many different ways and, historically, many ingenious methods have been proposed and applied.

Different requirements exist because of different levels of sensitivity and of different media, eg for data, audio and video communications.

Symmetric encryption, where the sender and the receiver share a common key, is the classically preferred method, because of the speed that can be achieved. The common key must be exchanged via a secure channel before communication can take place. Examples of widely used symmetric mechanisms are the Data Encryption Standard (DES) and the proprietary mechanisms used in mobile communications.

Asymmetric methods, where the sender and receiver use different, but related, keys are simpler to use, because key exchange via a secure channel is not required. These methods are also called "public key cryptology", because the encryption key can be made public. However, it is not possible to use asymmetric encryption in high speed applications (the fastest hardware implementations work in the area of several tenth of kilobytes per second). An example of an asymmetric mechanism is Rivest, Shamir, Adleman (RSA).

For practical applications, a combination of symmetric and asymmetric methods is often used. In these cases, the (session) key is exchanged via an asymmetric mechanism and the actual data to be protected is encrypted at high speed with a symmetric algorithm. Other key exchange schemes are also possible, eg the Diffie-Hellman method, where each partner in a (two-way) communication contributes part of the session key.

The confidentiality level that can be achieved depends on many factors. Besides the quality of the algorithm itself, these factors include its mode of operation, the key length and the key generation method.

Key management is an important factor in confidential communications. In asymmetric encryption, in addition to key pairs being generated, the public key is certified and included in a directory.

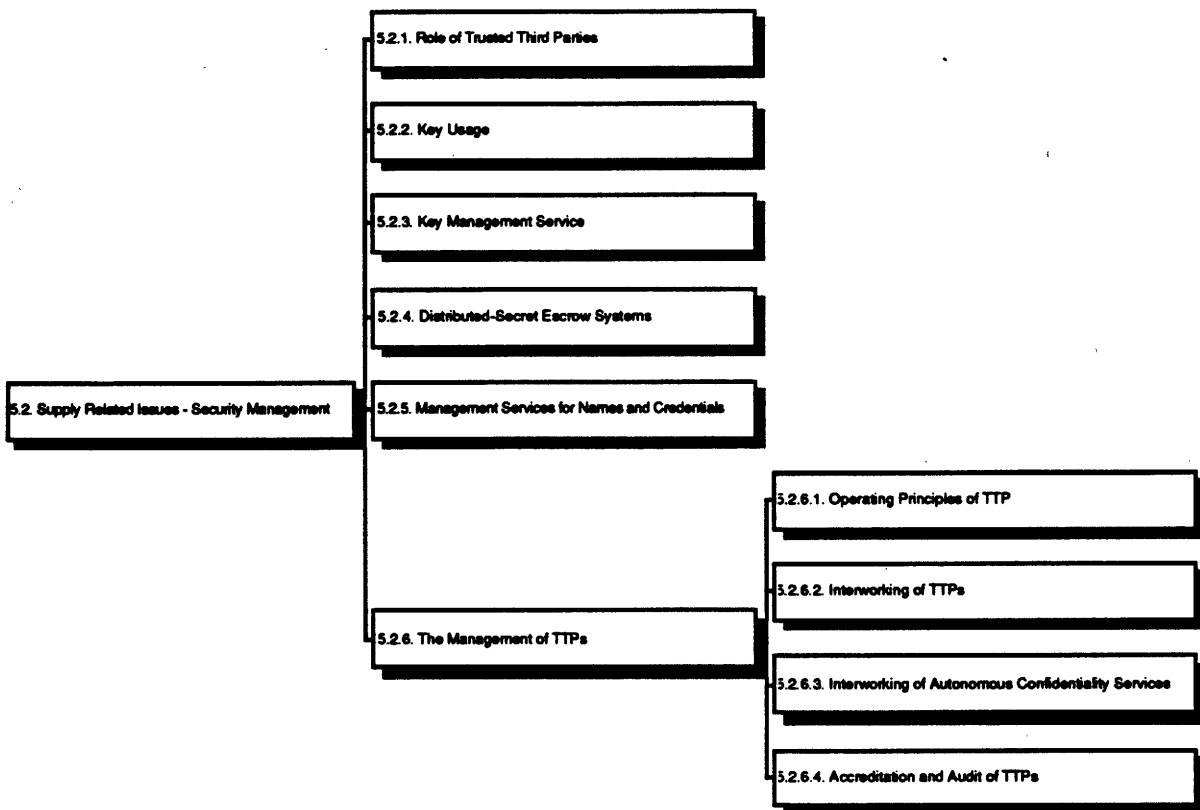
For confidential communications to take place, the sender and the receivers require agreement on the method and protocol used. If confidential communication between different domains using different methods is required, security gateways may perform the necessary translations. These gateways must be secure and trusted.

Although not required for normal business use, it is possible today to produce hardware and even software solutions that produce practically unbreakable cryptograms. This fact potentially represents a threat to public order and may hinder law enforcement in their duties.

#### **Requirements**

- Consensus on the principles of confidentiality services for use by individuals, enterprises and administrations
- trustworthy confidentiality scheme and its supporting administration.

## 5.2. Supply Related Issues - Security Management



### 5.2.1. Role of Trusted Third Parties (TTPs)

#### Issue

Some of the security services necessarily require involvement of a third party. Any such party is trusted in some way. These trusted third parties (TTP) can also be involved in the provision of administrative services. This may satisfy business as well as law enforcement needs.

#### Discussion

When a group of users wants to communicate securely using cryptographic methods, some measures must be taken to distribute and update the keys that are needed. Typically, each user must obtain a key coming from every other user he wants to communicate with, no matter which service is required. For a small, constant user group, this may be a fairly straightforward problem, which can be solved without involving any other parties than the users themselves. For larger and more open user groups, the problem quickly becomes difficult, however, and one needs to involve a so called Trusted Third Party (TTP).

Although several variants exist, there is a main distinction usually made between two types of TTPs: functionally Trusted Third Parties and unconditionally Trusted Third Parties.

The first type arises from the obvious need for reliable registration of users of the system. If public key methods are used, this will usually include certification of public keys as belonging to certain users. A TTP trusted to perform this function is called functionally trusted. It is clear that if the registration is not done in a reliable manner, users cannot even be sure with whom they are communicating. So functional trust represents a minimal amount of trust that must be placed in a TTP. Note that this type of TTP does not need to know the secret key of any user, nor does it need to know any conventional keys used for data

communication between users. The functionality required in this instance is comparable to the functionality of a phone book. It provides a reliable connection between people, or their residence, rather, and their phone numbers.

The second type of TTP is typically needed in systems that use conventional cryptography only. In addition to the registration function mentioned above, such an unconditionally trusted TTP will generate keys for data communication and then communicate them securely to the users who need them. This means that the TTP knows and in principle could make use of all the secret information in the system. Thus measures must be taken to prevent such misuse. This usually involves the use of tamper resistant hardware, ensuring that no key will appear in the clear outside of the trusted environment.

In any case, whichever approach is chosen, Trusted Third Parties must be introduced to handle a number of administrative functions related to the management of users, in particular registration, and the distribution of all relevant information on keys. However, a number of other functions, such as time stamping, are relevant, and all these requirements must be clearly understood to reach the objectives.

One single TTP world-wide is clearly impractical. So there will be one or more networks of TTPs. Some network may only support closed user groups. International networks for an open environment need some framework.

Trusted Third Party services can be considered as value-added communication services available to users wishing to enhance the trust of the services he uses. Therefore TTPs have to be able to offer value added with regard to availability, integrity, confidentiality and assurance. Although TTPs may be set up on a national basis within national law, they must be trusted by the international community.

There are different types of functions which may all or in part be fulfilled by TTPs. The exact nature and extend to which these functions are provided by TTPs will be dictated by practical considerations and may vary considerably.

In general the TTPs operate on the basis of information provided by the user. Certification of information is carried out on the basis of evidence of correctness provided by the user or generated by the TTP itself, eg the keys.

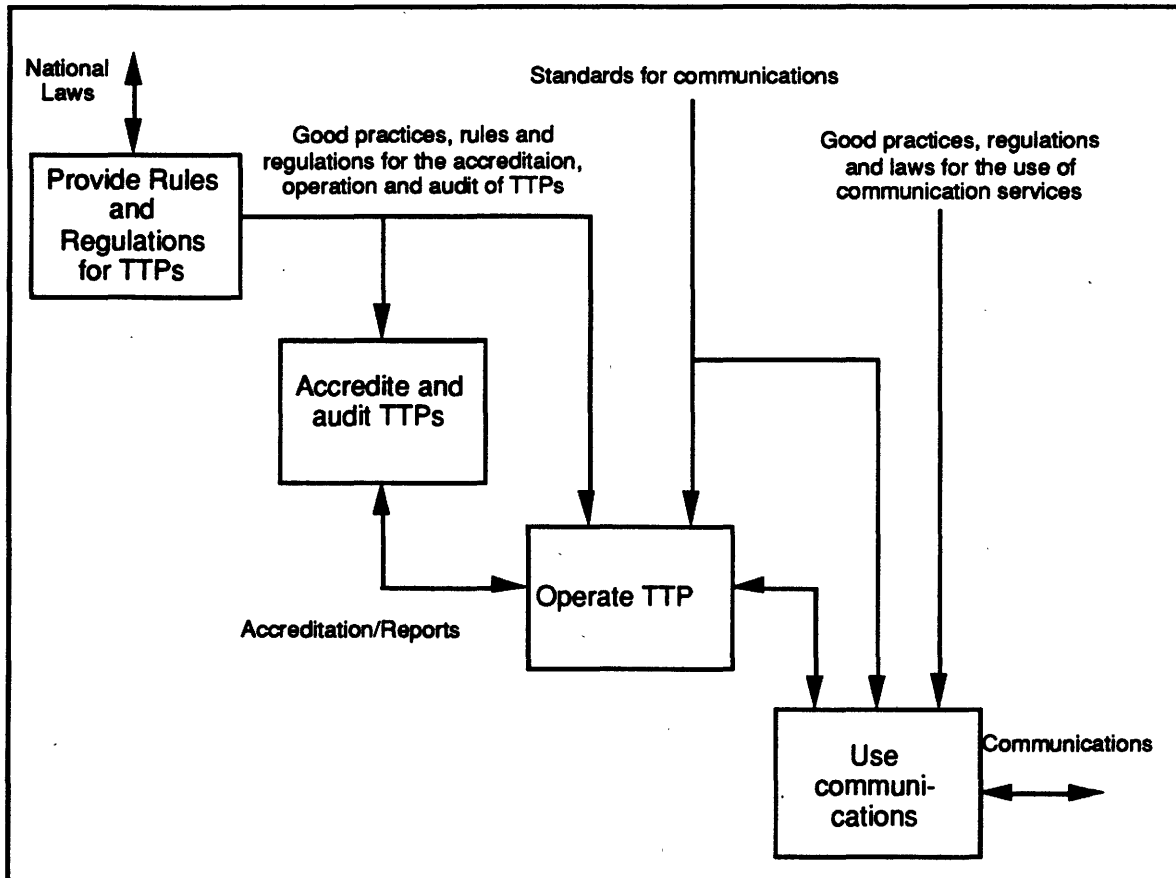
The major services a TTP may offer include some or all of the following:

- Name assignment, ie the function of assigning individuals' and enterprises' unique names and addresses. Individuals may possess several different distinguished names, according to their role, eg as private citizen and as employee of a corporation.
- Certification, ie the function to validate that a name and address has certain credentials, eg a public key for signature.
- Key Management for signature, ie the generation, distribution, establishment, and administration of public and private keys.
- Key Management for confidentiality, ie the function to generate, distribute and administer keys used for confidential communications.
- Management Services for Names and Credentials, ie the function to establish, administer and make available registers with the names of individuals and their certified credentials.
- Security services, ie functions usually performed by the legal profession, mostly concerned with non-repudiation. These include:



- Non-Repudiation services
- Claim of origin
- Claim of ownership
- Fair exchange of values
- Untraceability
- Time stamping.

Common to Trusted Third Party service providers is that they have to be accredited and audited, and that they have to operate under the law of the country using common guidelines. The figure below provides an analysis of the different functions involved in the establishment and operation of TTPs.



The diagram identifies four functions in this process. The functions are:

- the provision of the required good practices, rules and regulations for the accreditation and operation of TTPs
- the accreditation, re-accreditation and audit of TTPs
- the TTP functions themselves
- the use of communications and of the TTP.

This diagram does not imply any particular allocation of responsibility for the functions indicated.

The information flow contains the following major elements:

- National Laws. The operation of TTPs will take place within the laws of the country in which they are located. It is conceivable that some legislation has to be updated to allow TTPs to operate in an international environment.
- Good practices, rules and regulations for the accreditation, operation and audit of TTPs.
- Standards for communications.
- Good practices, regulations and laws for the use of communication services.

### **Requirements**

- Establishment of international framework for the operation of TTPs
- Setting up of conditions for the operation of TTPs in the EC adapted to the needs of national and international users.

### **5.2.2. Key Usage**

#### **Issue**

Digital signatures imply the specification of a full set of procedures dealing with the three phases of key management - user enrolment, key and certification distribution, and operational maintenance (revocation, blacklist, destruction), which must be agreed and accepted.

#### **Discussion**

To apply security to any message or process, four logical layers are relevant:

- Legal intentions and implications (including social requirements)
- The definition and identification of the relevant security service to be applied.
- The underlying mechanisms.
- The algorithm and protocols.

Without standardising or agreeing on the 4th layer, it will not be possible to communicate.

In order to adopt electronic versions of negotiable and quasi-negotiable documents, such as bills of lading, new security services have been identified to meet business requirements, in particular claim of ownership for exchange of values. This needs to go through a standardisation process.

But also for more "classical" services, the current standards do not reflect the granularity of eg non-repudiation needed by business requirements. ISO 7498-2 only addresses non-repudiation of origin and delivery (sometimes called receipt). However, one needs at least origin, submission, delivery and receipt, where submission and delivery would correspond to the services required when a registered letter is mailed.

For hand-written signatures, a person typically knows what he is signing, which is important for legal implications. This is not so easy to achieve with electronic data. In particular it must be clarified to what extent the system must indicate to the user what he is actually signing.

#### **Requirements**

- Standards and profiles in particular to support and improve CCITT X.509.

### **5.2.3. Key Management Service**

#### **Issue**

Key management services for signed and privacy enhanced communications between organisations and individuals.

#### **Discussion**

##### *General*

- Definition of responsibilities and obligations for services that provide trust in the integrity of communications and those that provide confidentiality.
- Development of codes of practice for the generation, distribution and storage and destruction of keys for both purposes (integrity and confidentiality) in environments that have varying levels of assurance.
- Definition of escrow services. Some of the secrets may be of paramount importance and may have to be distributed among trusted parties (distributed-secret-escrow agents) so that none of the parties know the complete secret and not less than a defined minimum of those trusted parties must contribute their part of the secret in order to produce the complete secret.
- Mechanisms and criteria for assessing applicants suitability for the use of TTP services. Not all potential users of TTPs may have the necessary attributes (eg legal status, financial viability, etc.). This essentially applies to TTP services for closed user groups.

##### *Integrity and digital signatures*

- Relationship between the key management functions, directory management and certification needs to be clarified.
- Timeliness of issuing signatures when an application is made - verification of "signature worthiness" of applicant - periodic review of "worthiness" of existing constituency of signature holders.
- Removal of signatures from "active list" and initiation of "attempted illegal use" audit. This is a "certificate management" - "key management" interface management issue.

##### *Privacy Enhancement*

- Management of the domain within which the confidentiality keys are valid. The identity of authorised subjects within the domain: Key distribution to those authorised subjects (people and automated processes.).
- Should the TTP define the domain as well as manage it: if not, should another TTP hold the definition of the domain (ie table of authorised subjects).
- Assessment of the assurance level of the domain within which the confidentiality keys are to be used, ranging from vetted, cleared people with physical and logical access controls to un-cleared people in open environments.

Domains are an important concept in confidentiality provision. The following questions require an answer:

1. What is the scope of validity of a domain for certification and the scope of validity for a confidentiality mechanism ? Who manages the domains ? Who manages inter-domain issues ? Does each domain need a different TTP ?
2. Who determines the scope of a domain ? Who is authorised to change it ? (for both certification and confidentiality.) Is a domain a "contract", and under which circumstances ?
3. What are the assurance criteria for domain management ? Who audits a domain manager ? Who maintains the principles of domain management as technology changes ?
4. Should domains for certification and confidentiality be different in view of the fact that a confidentiality domain will be transitory and that therefore key management principles are different ?
5. When should the use of escrow services be mandated to ensure domain integrity.

### **Requirements**

- Single digital signature mechanism and specifications preferably consistent with other leading countries
- adoption of a confidentiality algorithm standard and specification, and a key distribution mechanism based on an asymmetric public key algorithm
- establishment of "domain assurance" levels and criteria for TTPs to use for confidentiality key management purposes
- codes of practice for TTPs engaged in key management activities, and the provision of escrow services and the methods by which those codes of practice would be audited
- set of criteria for mutual recognition between TTPs acting on behalf of organisations who wish to communicate securely. Merging of signature directories and secure inter-domain communications are fundamental issues.

### **5.2.4. Distributed-Secret Escrow Systems**

#### **Issue**

Some secrets (eg the secret key of a user) may be of paramount importance and may have to be distributed among trusted parties (escrow agents) so that none of the parties knows the complete secret and not less than a defined minimum of those trusted parties must contribute their part of the secret in order to produce the complete secret.

#### **Discussion**

Such schemes are intended to protect the secret against corruption or destruction of the secret holder. Escrow agents are jointly more trustworthy than any of its members.

Normally escrow agents, like information brokers, will use communication services to provide added value services.

A US Presidential Initiative of April 16, 1993, announced a "key-escrow system" Which is to protect both confidentiality of (basic) telephone communication as well as the society's interests against misuse of legal encryption for illegal purposes.

Telephone users are to hold trusted "Clipper Chips" which they can use to encrypt their conversations. Each such device will have two unique keys, numbers that will be needed by authorised government agencies to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" data bases that will be established by the Attorney General. Access to these keys will be limited to government officials with legal authorisation to conduct a wire tap.

There are many possible ways of using distributed-secret escrow systems. The system proposed in the US provides improved protection against corruption of a single secret holder; however, it increases the threat of destruction, because loss of either of the two key-escrow data bases will render the system unavailable. This threat can be met by distributing the secret over a larger number of escrows, so that a subset can reproduce it (eg 2 out of 5).

In view of the international character of communications, the consequences of the US Presidential Initiative and possible improvements should be studied. The US development should be closely observed and should be influenced towards a better compatibility with European regulations.

### **Requirements**

- Investigation and configuration of an escrow systems adapted to European needs.

## **5.2.5. Management Services for Names and Credentials**

### **Issues**

Whenever parties engage in bi- or multi-lateral electronic transactions, they need beforehand some non-transient information on their partners (such as identity, legal representatives or any other kind of credentials eg public keys). This does not imply permanent recording of such information.

### **Discussion**

Management Services for Names and Credentials are established to facilitate access to this type of information, whereby service subscribers are provided with up-to-date data pertaining to the parties listed in there. Because partners may conclude the transactions on the basis of the information (at the minimum, the authenticated identity of their partners) they are provided with, and because some of the information stored by such a service may be protected by privacy legislation, the service itself must be trustworthy and the data it provides correct.

Management Services for Names and Credentials keep objects which are referred to by "Distinguished Names". A Distinguished Name is unique to a communication subject. A subject may have a number of (unique in the above sense) "Alias Names". It is required that the service can reference Alias Names to their subject's natural names. An Alias Name may be a pseudonym. Whether or not the service is allowed to reference a pseudonym and let inquirer know the result will depend on the subject's data privacy rights.

If, as is likely going to be the case, there is more than one provider and certifier of information, the Management Services for Names and Credentials must be part of a network of information suppliers. Network can be organised according to either geographical distribution or business sector or information taxonomy or all three of them. Users may have to subscribe to more than one such service or service type (eg "Public Key directory for the banking sector"). Users may have a number of different roles in an enterprise, each of which needs access to a set of different services. In the case of a multiple service and network of providers, one can speak of a system of Management Services for Names and Credentials.

Because of the damages that could be caused by the distribution of false information, the Management Services for Names and Credentials must apply due care in its operations. In the case of proven negligence the service could be held liable if inaccurate information were provided. The creation, update and destruction (eg in the case of certificate revocation) of information is either mandatory or forbidden. In critical cases (eg; certificate revocation), the update may have to be notified to subscribers without request.

The management of the Management Services for Names and Credentials must thus be accountable. There must be legislation, rules and regulations governing it.

Obviously, the service must cover and be available on an international level.

Obviously there is the issue of standardisation of the service at the user end (external interface) and between service providers (internal interface).

Since international Management Services for Names and Credentials are akin to internationally distributed data bases, they face the same legal questions: who is legally responsible for the information (between the creator, the storer, the distributor) ?

Market pressures are bound to promote the advent of sectorial Management Services for Names and Credentials, and possibly their subsequent interconnection or integration into larger network. In order to avoid fragmentation among proprietary services, there may be a need to lay down base rules for naming, binding, certificates and the associated IPR rules.

## **Requirements**

- Provision of Management Services for Names and Credentials, to include identity, name information, and credentials such as public keys or any signature-verification data
- interoperability specifications and standards for names and credentials
- international harmonisation of legislation, rules and regulations for Management Services for Names and Credentials.

## **5.2.6. The Management of TTPs**

### **5.2.6.1. Operating Principles of TTPs**

#### **Issue**

The need for common operating principles for TTPs.

#### **Discussion**

To be effective, TTPs must :

- operate within a consistent legal framework across the Community
- offer a range of services, with a defined minimum
- conform to European or international standards, where available
- follow accepted good practice
- allow for independent arbitration, without compromising security

- be independent in its operation within accreditation rules
- have a public policy on service refusals, if applicable
- assume responsibility of liability within defined limits for availability and quality of service.

The key questions include :

- Has the TTP a contractual obligation of results in terms of availability, integrity and confidentiality?
- How and by whom are the loss and penalty determined in cases of fraud, negligence or failure of the TTP?
- What assurance to the final user is offered by the accreditation of the TTP?

### **Requirements**

- Harmonised legislation to provide an appropriate framework for arbitration, supervision and litigation
- model for TTPs meeting the requirements of users and authorities.
- baseline for accepted good practice including a study of the level of availability, privacy and security required for the TTP by the final users and how much they are ready to pay for it
- definition of quality of service, including availability, confidentiality, response-time, rules of disclosure to law enforcement agencies
- operational guidelines, including descriptions of minimum set of services and standards to conform to
- standard clauses for the contract between the TTP and the user, concerning the liability of the TTP.

### **5.2.6.2. Interworking of TTPs**

#### **Issue**

Openness and protection.

#### **Discussion**

In practice, the level of information security is dynamically adapted to a given situation. This leads to the concept of Dynamic IS Management and the need to be able to define domains, in which information security is applied homogeneously.

#### *Security Domain Concept*

Domains are user groupings sharing some of their functions and support. For some activities they operate as virtually closed user groups, but have the possibility to interwork with other domains as long as certain minimum requirements ensure no loss of trust or a transparent downgrading.

The notion of a security domain is therefore important for two reasons. Namely,

- It can be used to describe how security is managed and administered, and
- It can be used as a building block in modelling security relevant activities that involve elements under distinct security authorities.

Examples of domain activities are:

- accesses to elements (eg a database for network management)
- a communications link
- operations relating to a specific management function
- non-repudiation operations involving a notary.

### *Security Policy*

The organisation of security within enterprises in terms of business control structures or in the case of some user environment (eg legal, accounting, audit etc.) and functions (eg IT, human resources, insurance) needs to be supported by a set of security policies, standards (both public and in-house), laws and regulations (eg computer crime manual), guidelines and codes of practice etc.

The security policy defines what is meant by security within the domain, the rules by which security may be obtained to the satisfaction of the security authority, and the activities to which it applies. The security policy may also define which rules apply in relations with other security domains in general, and in relations with particular other security domains.

The management of inter-domain openness and protection may be different depending on similarities in purpose, and agreements will be needed to achieve appropriate levels of assurance. Mechanisms by which TTPs achieve efficient, coherent management of policies, procedures and controls between domains need development.

### **Requirements**

- Guidelines for domain creation, management and control
- common framework for domain interworking
- agreement on management, TTPs, accreditation, auditing and relations with law enforcement agencies.

### **5.2.6.3. Interworking of Autonomous Confidentiality Services**

#### **Issue**

Till such time that a universal service is being offered, interworking between autonomous confidentiality services is likely to be the normal situation because of the differentiated requirements. This implies the need for generally accepted rules for the relationship between these services.

#### **Discussion**

For quite a time the conflict between national security issues and the business need for international communications has blocked significant progress in the area of confidentiality services in telecommunications. With the recent US initiatives, pressure from European companies will grow to have access to equivalent services. But within Europe we have the



situation that neither the legal situation in the different EC countries nor their national security policies are harmonised enough to have a single confidentiality service scheme with a single algorithm established within the foreseeable future. Therefore it is necessary to have a framework, which enables user-transparent interoperability between different national or regional schemes and which do not block the way for a single scheme which may be established in the far future. Interoperability is also required with non-European schemes like the US. scheme. To provide this interoperability the way information is passed from one national security domain to another has to be specified and the national schemes have to be compatible with this specified way. The establishment of such a framework for interoperability is therefore a subject which needs international harmonisation. Aspects related to this are requirements for the cryptographic algorithms and for key management issues.

## **Requirements**

- Minimum requirements to ensure interoperability, including standards, specifications, rules of procedure and operating practices
- demonstration of trans-European confidentiality services using a suitable application, eg the realisation of administrative telematics applications.

### **5.2.6.4. Accreditation and Audit of TTPs**

#### **Issue**

The need for harmonised procedures for the accreditation and audit of TTPs.

#### **Discussion**

Although the accreditation and audit of TTPs may be a local or national responsibility, the procedures to be followed must be harmonised and have a common basis in order to ensure mutual trust.

It is assumed that national governments will be responsible for approving accrediting bodies. This may require to create new national laws or to adapt existing laws.

From the TTP point of view, timely and fair responses to requests for accreditation will be important.

From the user point of view, the agreed terms of the accreditation need to be properly documented and inspectable.

To maintain public trust in TTPs, an audit process must be put in place.

Other issues are related to the

- requests for accreditation from service providers in other EC and non-EC countries
- certification of certificates
- signature of authority and accreditor.

Existing Community rules for accreditation (eg of test centers) should be used as a basis for this work.

## Requirements

- Development of international guidelines for the accreditation and audit of TTPs
- adaptation of applicable legislation or regulations to provide an appropriate legal framework for use throughout the Community and in the relations with third countries.

## 5.3. Supply Related Issues - Evaluation of Trusted Solutions

### 5.3. Supply Related Issues - Evaluation of Trusted Solutions

5.3.1. Evaluation of Products, Systems, Services and Applications

5.3.2. International Harmonisation and Mutual Recognition

5.3.3. Suppliers' Declarations

5.3.4. Self-evaluation

5.3.5. Evaluation of Application

5.3.6. Evaluation of Communication Services

5.3.7. Trusted Network Management

5.3.8. Evaluation of Methods and Tools

5.3.9. Physical and Procedural Issues

5.3.10. Modifications to Evaluated Products and Re-evaluation

5.3.11. Performance Reporting for Trusted Products

5.3.12. Rationalisation of Evaluation

### **5.3.1. Evaluation of Products, Systems, Services and Applications**

#### **Issue**

Need for evaluations in support of communication requirements in both the public and private sectors.

#### **Discussion**

There is a whole spectrum of possible evaluation methods in use today. These range from:

- supplier declarations (the most common practice at the moment is that the vendor's product information states the intended functionality and quality of the product but not the level of assurance)
- acceptance testing by the purchaser (also common, where the purchaser trials the product before committing to it)
- indirect evaluation (where a supplier has a product range with a common product architecture, and the top-of-the-range product has been put through a formal evaluation. Though the other products in the range have not been evaluated directly, assurances can be inferred from the fact that one product has been successfully evaluated)
- acceptance testing by a third party (also known as a Security Qualification, where a third party performs specific security testing on behalf of the purchaser, but without the formality of a formal evaluation)
- formal evaluation by an accredited test laboratory (this can be a third party test facility or a manufacturer's test laboratory).

Obviously, mutual recognition and acceptance of standards, criteria and evaluation processes are necessary to achieve fully cost effective solutions from all perspectives, ie user, supplier and service provider.

#### **Requirements**

- Commitment of management to the security function within enterprises
- establishment of common definitions for the different evaluation options
- Community and international standards for criteria and methodology
- choice in the access to independent evaluation capabilities.

### **5.3.2. International Harmonisation and Mutual Recognition**

#### **Issue**

At the moment different evaluation criteria and evaluation schemes are in use. These are especially the US, TCSEC, the European ITSEC and the Canadian CTCPEC. Other countries like Japan have first drafts of criteria. This situation is not acceptable to international manufacturers who would have to perform different evaluations against different criteria and schemes for a single product. This will unnecessarily increase the cost of the product without enhancing the security features.

## **Discussion**

Various activities are currently under way to harmonise evaluation criteria and evaluation schemes. The ITSEC and ITSEM is the result of such a harmonisation process within Europe. The United Kingdom, France, Germany and the Netherlands are discussing the mutual recognition of each other's certificates based on ITSEC and ITSEM, with the intention of achieving agreement in 1994.

In North America, the US and Canada co-operated in the production of the first draft of the Federal Criteria. Following publication of the Federal Criteria in early 1993, it has been decided to make all effort to align the ITSEC and the Federal Criteria to produce a joint European/North American set of Criteria compatible with existing practices in both North America and Europe in 1994. This is the first step towards international harmonisation between the two groups and would be a major step forward. ISO/IEC JTC1/SC27, Working Group 3 is also working on an ISO standard for evaluation criteria, based on the ITSEC and the Federal Criteria.

Harmonisation of evaluation criteria is only the first step to reaching mutual recognition of evaluation results. It will need to be accompanied by agreement on evaluation methodology, evaluation schemes, certification and accreditation practices. Only then will mutual recognition between North America and Europe be possible. Even within the European Community mutual recognition has turned out to be an arduous task and mutual recognition of certificates is not yet achieved, mainly for legal reasons. This indicates that world-wide mutual recognition of certificates requires many, yet unknown, problems to be solved.

Looking into the international arena, the only evaluation process and certification scheme in the area of communications security (ie computer networks) which has been in place for a significant time is the US TCSEC evaluation scheme. The focus of this scheme is mainly to evaluate and certify commercial operating system products suitable for government applications. Currently the US are trying to widen this scope with the Federal Criteria and the accompanying trust technology programme of NIST whose main goal is to establish a more commercially oriented evaluation and certification scheme with industrial evaluation facilities like the IT Security Evaluation Facilities (ITSEFs) in Europe.

Both the Federal Criteria as well as the trust technology program look like a much better basis for international harmonisation but nevertheless a considerable amount of work is necessary to achieve this goal. Also, since both the new US criteria and commercial evaluation process are not yet well established there is an opportunity to influence this process. The fact that the US have sponsored two parallel ITSEC evaluation of their TMach operating system show clearly that the US side watches the European activities in this area very carefully and tries to get as much information as possible (both positive and negative!) about the European evaluation process.

Thus there is a will for co-operation which is clearly based on the fact that US manufacturers sell large quantities of products in Europe. Other countries like Sweden, Australia and Japan are watching this process very carefully.

## **Requirements**

- Establishment of conditions and procedures for mutual recognition of evaluations
- establishment of conditions and procedures for EC-wide/international evaluations
- international and EC standardisation of evaluation criteria and methods.

### **5.3.3. Supplier Declarations**

#### **Issue**

For solutions that need security, but not the kind requiring formal evaluations, supplier declarations are used. Currently, these are not defined in terms of what they cover, what assurance they offer compared to formal evaluation or who is liable if such products or systems fail.

#### **Discussion**

Between the requirements for formally evaluated solutions and no evaluation at all, there is a market for security products used by business and the general public. Vendors do incorporate security features in their products and provide some level of assurance, by virtue of the normal quality standards used to develop and maintain the product and the specific claims made by the supplier about the product.

Currently, end-users are not able to reliably compare such products from different manufacturers because there are no guidelines which specify the minimum content of supplier declaration documentation. Users have to rely on supplier sales literature.

Supplier declarations need to address the issue of assurance and liability, if a fault in the product causes loss, injury or death to users. This would then enable the user to calculate what the risks are in using products covered by vendor declarations rather than products that have been formally evaluated.

It may be possible to extend the formal evaluation scheme to include vendor declarations as a sub-E1 methodology. The scope of vendor declarations could be specified, together with the documentation required (for example, the claims on security features could use the same format as the ITSEC security target), quality procedures needed and auditing of vendors (perhaps by EDP auditors). This method would also allow users to see how vendor declarations compared with formal evaluation, in terms of security features and assurance requirements and keep a single, coherent evaluation scheme.

It may also be necessary to ascertain exactly where vendor declarations could be used, or more importantly, where they should not be used. For example, it may not be applicable for use in safety-critical systems.

#### **Requirements**

Agreed definition of scope and liabilities of supplier declarations

incorporation of supplier declarations in the ITSEC/ITSEM evaluation scheme

specification of the types of systems which should not rely on products covered by supplier declarations.

### **5.3.4. Self-evaluation**

#### **Issue**

To reduce the time and cost of formal evaluations, and to facilitate re-evaluation, there is an opportunity for vendors and service providers to both develop and formally evaluate systems, products and services.

## **Discussion**

Currently there are two methods used by users to assess the technical security measures provided by a product or service and their assurance:

- supplier declarations, and
- assessment by an organisation licensed to undertake formal evaluations; using an evaluation scheme.

In general, vendors and service suppliers have a quality assurance department which monitors and audits the development of products and the use of services, ensuring that this is all done to the company quality standards. This provides support for supplier declarations.

Vendors and service suppliers could set up a department which would be an in-house evaluation facility and would undertake formal evaluations in the same manner as current independent ITSEFs. Such in-house ITSEFs would be monitored and controlled in the same way as third party ITSEFs. The only difference would be that the in-house ITSEFs would be a part of the vendors organisation.

Self-evaluation may speed up evaluations, reduce their costs, and help with re-evaluation as the evaluations could be done as an integrated part of the development planned and executed by the same company, but different departments.

There are certain types of systems for which self-evaluation would be deemed not appropriate due to them requiring high-levels of assurance. End-users may also wish to have independent formal evaluation rather than self-evaluation to ensure that there is no conflict of interest.

End-users must be made aware of the advantages and disadvantages of supplier declarations, self-evaluation and third party evaluation so that they can procure a product/system with full knowledge of the security features and assurance they are getting.

Self-evaluation compliments independent formal evaluation. The ITSEC/ITSEM evaluation criteria should be extended to incorporate self-evaluation and specify how it fits in between supplier declarations and third party evaluation.

## **Requirements**

- Specification of accreditation for in-house evaluation facilities
- extension of the ITSEC/ITSEM evaluation criteria to include self-evaluation.

### **5.3.5. Evaluation of Applications**

#### **Issue**

The user interest is finally with the security of his application. The use of secure products, systems and services is a necessary but not a sufficient condition to meet the user requirements for the protection of the application.

#### **Discussion**

At present, evaluations and certification schemes address primarily products and systems. Communication services are only partially addressed and applications running on the products and via networks (in particular public networks) are left to the user to address. However with the restrictive handling of confidentiality mechanisms and opposition against end-to-end encryption, the user is left exposed.

## **Requirements**

- Methods for evaluations to cover services and applications.

### **5.3.6. Evaluation of Communication Services**

#### **Issue**

With the ITSEC and ITSEM Europe has already a scheme for the independent security evaluation of IT-products and (to some extent) IT-systems. At the moment this scheme does not fully cover the aspect of the evaluation of communication services, but extensions to this scheme seem possible which are able to address the items not yet covered by the current ITSEC/ITSEM scheme.

#### **Discussion**

The main item where communications security is considered in the public is in the area of telecommunication services. Especially when people send sensitive information to others using telecommunication services they are interested that this information

- gets to the intended recipient(s) in time
- is not altered by the service
- it not received by anyone else than to the intended recipient(s).

Not all these aspects are of the same importance for each kind of communication. The level of importance is highly dependent on the kind of information one wants to transfer.

The use of telecommunication services grows rapidly as more powerful equipment and services become available. A lot of companies and especially administrations have policies which forbid the use of specific telecommunication services for highly sensitive information since they do not trust the communication services providers that some of the above mentioned security issues are enforced adequately. They use conventional techniques for the exchange of sensitive information with conventional security measures (eg sending sealed letters by registered mail or by courier).

In a time where industrial success depends on the fast exchange of all types of information these conventional techniques become more and more unacceptable. So the service providers will incorporate security provisions within their services. But nevertheless a lot of companies (and the national governments) will continue to use the conventional techniques since they do not trust those security services unless they are under their own control or being verified by independent experts.

Providing a security service as part of a telecommunication service will normally result in all entities involved in the provision of the telecommunication service being involved in providing the security service. Additional entities may even be necessary (like eg a trusted third party for key management issues or authentication services). These entities use systems and products to provide their part of telecommunication (and security) service. The total service is therefore provided by an interaction of all the entities.

The current ITSEC/ITSEM scheme is aimed at the technical evaluation of security measures within products and systems. It does not cover organisational, personnel, administrative or non-IT related physical security measures. Still many security services for telecommunication will heavily rely not only on IT-security measures but also on the above mentioned other security controls. For example a trusted third party will surely need extensive organisational, personnel and non-IT physical control. So it is clear that an extension to the ITSEC/ITSEM

evaluation scheme is necessary to cover these aspects. The following section tries to identify how this can be done and which areas are not yet covered.

Looking at communication services one can easily identify several different types of communications-products and systems which have to co-operate to provide the service. This includes for example

- the end user equipment (telephone, modem or even his computer)
- digital dialling switches
- data concentrators
- conventional computer systems with databases for eg user profiles, directory information
- conventional computer systems providing mailbox services
- the communication media
- gateways etc.

For a specific telecommunication service one can identify the task each of these products or systems has to fulfil to provide this service. The same is true for security services. Each component involved contributes for one aspect of the security objectives or functions. These will then differ significantly in the functionality as well as in the assurance level required. Various topics regarding this may lead to problems, for instance: assumptions on the security provisions to be taken in the environment of the product or system. Some of the security measures will heavily depend on hardware features. Evaluation of non-IT security features, like effectiveness of personnel and administrative security measures has to be established. The integration of all security measures has to be checked for consistency, completeness and effectiveness. For the evaluation of a communication service, therefore, different evaluations of systems involved in providing the service are necessary before the whole service can be evaluated.

## **Requirements**

- Evaluation of communications hardware and infrastructure security features
- formal accreditation scheme for secure communication services
- accreditation guidelines for the telecommunication sector
- trial service evaluations for existing telecommunication services
- articulation of the requirements of service evaluation.

### **5.3.7. Trusted Network Management**

#### **Issue**

Trusted Network Management systems need to maintain a given assurance level while optimising the use of communication assets to achieve good economics and quality of service.

#### **Discussion**

There is a growing dependence in the security of network management systems for managing and controlling the provision of telecommunications. This is due to an increased reliance on distributed systems, the provision of new value added services and operations, and on the increased sophistication and richness of network and service functionality. Such dependency is placing greater demands on performance and quality of service. Tomorrow's electronic highways should be managed networks that should ideally interoperate in a seamless way to



ensure efficient "self-healing" network operations and flexible creation and provision of a broad range of services, including those supplied by third party suppliers. The management of telecommunications systems security is thus growing in complexity commensurate with the growth in communications systems and the associated services and business use.

The major network management issues involve the protection of electronic information in storage, in transmission and being processed. Information used and applied to the controlling and maintenance of networks and services. Information that is used as input to the process of decision making and operational support, and which is also used as input to the emerging new wave of intelligent systems and communications. The provision of appropriate and effective network management solutions is fundamental to the success of the future telecommunications infrastructure for Europe.

Given the complex telecommunication systems that are evolving, the interrelationships that are needed for multi-domain working, grade of service requirements against a future European framework for legislation and regulation needed to maintain multi-domain working, the provision and maintenance of network management security the question of security evaluation is a key issue. What is the alternative if evaluation of network management security is not carried out ?

There are a number of constraints imposed by end users, service providers and network operators on the provision of security for network management eg concerning the employment of intelligence in networks and the idea of securing shared resources, dealing with different threat analysis and the responsibility for service liability.

### **Requirements**

- Methods for network management evaluation
- definition of Functionality Classes (or Protection Profiles) suitable for systems, products and services used in network management systems
- accreditation guidelines for the trusted network management
- trial evaluations for existing network management systems.

### **5.3.8. Evaluation of Methods and Tools**

#### **Issue**

The methods and tools used to design, develop and maintain trusted products and systems need to be trustworthy.

#### **Discussion**

Methods and tools used to develop trusted products and systems must be trusted to function correctly. For example, a compiler and linker must be trusted not to include malicious code in the resulting executable image. Such malicious code may only be visible if the executable image or object code is directly investigated (ie decompiled).

There is a need for trusted compilers, linkers, semi-formal tools (CASE tools) and formal methods tools (eg 'Z' and LOTOS tool, etc.), configuration management tools, etc.

The evaluation may take the form of a straight forward assessment of tools or the production of rules for how each specific tool should be used to develop trusted products.

A register could be produced and maintained of methods and tools which are suitable (or not suitable) for the development of trusted products and systems. When a new tool is developed, the vendor will have to ensure that the tool is added to the list, if he wishes to use it (or sell it to a third party to use) on developing trusted software. The register may also be able to say which tools can be used for which assurance level.

### **Requirements**

- Guidelines for the evaluation of methods and tools used to develop trusted products, systems and services
- register of methods and tools which can be used to develop trusted solutions.

### **5.3.9. Physical and Procedural Issues**

#### **Issue**

Need to produce a common standard for the physical and procedural issues required to maintain the security of evaluated products and systems.

#### **Discussion**

There is no point for two organisations in two different countries in buying the same ITSEC E3 product, configuring them in the same way only to find that their physical and procedural security measures (eg personnel, system administration, system operation, end-user organisation, building security, system maintenance etc.) are incompatible with the security of the system. Each country would have a product with a security level that included the same environmental assumptions, but these may be interpreted differently and the different interpretations may be accepted by the system accreditors in each country.

As well as having international harmonisation on the evaluation criteria, effort should also be made to produce guidelines for the physical and procedural measures required to maintain trusted systems which apply internationally. Thus as well as having mutual certification, it would also be possible to have mutual accreditation.

### **Requirements**

- Guidelines for physical and procedural measures required to maintain trusted systems.

### **5.3.10. Modifications to Evaluated Products and Re-evaluation**

#### **Issue**

The shortening life cycle of products and the rapid evolution of services and applications due to competitive pressures implies the need for frequent adaptations and therefore re-evaluation.

#### **Discussion**

The impact of Open System, with its emphasis on portability and interoperability, has resulted in many new products being incremental releases of existing products, for new operational platforms, applications, etc. There may be multiple releases or versions of a hardware or software solution in a short period of time. The evaluation and certification of the product may take longer than the period between releases or updates to the solution. A certificate currently applies to a specific release or version. Changes may invalidate the certificate.

There is a need to devise a method to cope with these product or system changes so that the certified status of a product may be maintained.

Particular concerns include:

- **Scope of the evaluation** - Is an evaluation necessary for every single platform-dependent configuration of a product already certified ?
- **Assurance** - Is it necessary to have an entire new release evaluated again in which only a small modification occurred (eg a spelling mistake in the user interface) ?
- **Re-use of previous evaluation work and results** - Must the evaluation of sensitive and relevant but unmodified components of a product be repeated ? ITSEC and ITSEM have created a good basis on which to identify the key issues of re-evaluation and subsequent re-certification.

Practical experience of re-evaluation is limited but the problem may be mitigated by identifying key requirements. One approach is to categorise code in the security Target of Evaluation (ITSEC-TOE).

This "Traffic Light" approach includes:

- a) **GREEN** code that has no bearing on the security functionality of the product or system and that may be modified in future releases without impact on the security of the product or system.
- b) **YELLOW** code that might impact the security of the product or system and that must be inspected by an independent party (such as an ITSEF) before re-certification can be considered.
- c) **RED** code that is critical to the security functionality of the product or system for which any modifications may require re-evaluation of the whole product or system.

This approach will assist developers, evaluators and certifiers in containing the level of necessary re-evaluation commitment following any modifications. Feedback on how well this approach works is required.

Experience is available on the parallel field of quality evaluation of software products. A framework for re-evaluation is outlined in ISO9126 and associated processes. It is likely that the impact of software quality on "operational" correctness of security products will force alignment of the various processes.

### **Requirements**

- Definition of rules and procedures for re-evaluation based on methods currently used
- alignment of the design process with the principles of re-evaluation, "design-for-change".

### **5.3.11. Performance Reporting for Trusted Products**

#### **Issue**

Obligation to take corrective action in the case of faults found in evaluated products.

## **Discussion**

Despite the successful evaluation and certification of a product or system, there is a small chance, smaller with the higher assurance levels, that a security related fault will be detected. The Developer or Vendor is likely to have this fault reported to him and ought to take steps to correct this fault as quickly as possible and issue a new release of the software or hardware.

The Certification Body needs to be informed of the occurrence of such a fault and the steps the Developer intends to take to correct the fault. The Certification Body and the Developer need to discuss the need for any re-evaluation work and agree a timescale for this.

Where a Developer is unwilling to correct the fault, the Certification Body needs to decide whether to withdraw the certified status and publish the fact that a fault exists (although not necessarily the details of the fault) or, perhaps, change the conditions upon which the certificate was granted.

When a fault does occur, perhaps due to the way a system has been configured, or due to a specific fault with the product, end-users should be obliged to report the fault to the Developer and to their Certification Body. If this product is in wide spread use throughout the World, it may be necessary to inform all end-users who could be affected that a fault exists, detailing the security implications. In-order to be able to this, it would be necessary to set up an international register of evaluated product users (or an equivalent system).

## **Requirements**

- Incident reporting system for Certification Bodies
- user and supplier obligations to report incidents
- supplier obligations to take corrective actions, and to initiate re-evaluation
- register of evaluated product and their owners.

### **5.3.12. Rationalisation of Evaluations**

#### **Issue**

Speeding up and lowering cost of evaluation and thereby improve attractiveness of security evaluations.

#### **Discussion**

Two key factors to the success of a security market enhancement are that evaluations are approachable and that the products or systems are developed in a way that is meant to meet the ITSEC requirements beforehand. It must also be understood that in many industrial cases, security, while indeed an important feature of a product or service, is only one aspect of an even larger target which is product quality or the quality of service.

Considerable work has been carried on in the broad field of software quality and its engineering which might be valuable to the security community. Several standards address quality through an evaluation and certification approach, eg ISO 9000 and ISO 9126, at the organisation level, at the process and at the product level.

Those standards are well established and the demand for certificates based on them is growing rapidly. There is an urgent need to consider the harmonisation of the ITSEC and ITSEM contents, to take into account to a much larger and clearer extent the benefits brought by these standards to security and to help reduce costs and needs of several, disconnected or

even conflicting evaluation and certification processes. The ITSEC approach seems to be sufficiently well accepted today to consider its integration into a broader context. A closer technical look at quality standards and ITSEC/ITSEM taken together shows that, although they are all based on the same fundamental ideas and principles, there are residual conflicts when evaluations are to be carried out, either due to different requirements or to different evaluation approaches.

The following steps seem relevant:

- While preserving the current technical principles and requirements, a better distinction between specifically security related requirements and more quality related requirements should be made so that it becomes clearer, if not explicit, what the various other evaluation systems and associated requirements can cover and/or contribute to.
- As all standards evolve, the ITSEC and ITSEM will have to be updated, at the level of the actually required documentation, for instance, to be directly compatible with what the other domains require, while still remaining specific.
- Parts of the current ITSEC requirements might eventually be replaced by requirements for relevant quality certificates, and hopefully vice versa.

### **Requirements**

- Alignment of security evaluation criteria and methods with those for quality and safety, where sensible
- portability of results between quality, safety and security evaluations.

## **5.4. Maintenance of Safety and Assurance**

### **Issues**

To maintain safety and assurance in operation for systems in changing environments, with changing system elements over long periods of time (30 years)

### **Discussion**

There is a need to maintain the safety and assurance of systems during operation and after decommissioning. These problems are exacerbated by the emergence of large, distributed systems with safety implications and the changing nature of the organisations in which they are embedded. There is the danger that key safety or security properties are established by properties of the organisation that are not made explicit and are undermined as the organisation changes. This could include the move to contract out work to contractors with a different mindset to the service provider; the slow undermining of safety culture (this is especially important in some Eastern European countries) and the consequential problems of relying on procedures and drills; ; the changing technical and linguistic skills rate of the workforce.

There are also the technical issues associated with the evaluation and development of systems and the need for methods and techniques that recognise the impact of these changes and allow for appropriate design and engineering measures to be implemented. Coupled to these changes to the system is the problem posed by the relatively rapidly changing technology and the likely obsolescence of the systems being used. The need to plan for obsolescence should be recognised from the outset and consideration given to the extent of information required for re-engineering. This covers the capture of expertise, design rationale, development documentation and the access to tools used in developing the system that themselves may be

obsolete and may involve IPR issues as well. Organisations need to know how to plan for obsolescence, how to determine the best approach to re-engineering (complete re-development, translation of software, emulation of old hardware etc.), when it should be done and the risk, costs and benefits.

Many systems are already obsolete and do not possess the documentation necessary for re-engineering. Strategies for dealing with these systems in a cost effective manner that preserves safety need to be developed and associated reverse engineering techniques developed for the system (hardware, software, people, organisation).

There is also a need to address the reuse of old systems in new applications and the implications for safety assurance and certification.

### **Requirements**

- Approach for tracking the evolution of systems and identifying when significant changes to safety and security requirements are taking place
- strategies and techniques for re engineering of obsolete systems.

## **5.5. Technological Change**

### **5.5.1. Evolving technology**

#### **Issue**

Changes in the way in which technology is used throughout society will result in demands for new technological approaches to information security.

#### **Discussion**

Over the next decades it is to be expected that the macro economic climate will change dramatically. This is mainly driven by the shift in geographic location of the generation of the world's GDP from North America and Europe to a more even spread, with the Pacific rim countries producing a larger share. The health and nutrition problems that will face the developing world will become more acute as a greater fraction of their population enters adulthood. Information underpins these processes in a number of ways.

The financial aspects of global businesses will become vital to their survival and the timely, accurate and where appropriate private communication of financial information on a global and adaptable scale will be critical. Health care information will need to be routinely available as health carers deal with the health problems of an increasing number of mobile people. Transportation of food to areas in need will require logistic information to be available in remote and underdeveloped parts of the world quickly and accurately. As computer related products become more complex and are developed to go faster and to provide more functionality, new approaches to solving the security and safety-critical aspects of these products will have to be developed.

The developed world will make increasing use of their less structured employment patterns to earn money in a variety of ways and in performing a range of tasks, less and less to do with manufacturing. Success will only be possible by the exploitation of mobility and wide bandwidth telecommunications services. It has the potential to provide quality of life together with high productivity. The effectiveness of this approach, in providing a method of revenue generation, will depend on the performance, reliability and security of the information and transportation infrastructures.

There is also a need to educate the technology providers to consider the security and safety-critical aspects of products and systems whilst they are being developed on the drawing board, rather than as later add-ons, when it may be too costly or even impossible to provide a satisfactory level of security.

Ultimate goals for technological change are that individuals:

- can communicate with each other using global personal communicators which are wire-free and fibre-less
- will have instant access to all types of information (eg multimedia), through databases and high-speed links from wherever they are located
- be present anywhere anytime through virtual presence and reality (e.g. teleconferencing).
- travel faster and more safely
- work in a paperless office
- never carry cash, using instead an electronic purse or wallet.

Driving technologies within these scenario include:

**Telecommunications:** Bandwidth will become a commodity on telecommunication systems. The added value in using it comes from the quality of service provided. One aspect of such quality is that of security. To provide security on wide band public switched networks, investment is needed that is focused on those aspects of security that are required by the telecoms service provider for his own purposes and by the end user to support his application. Community wide and international specifications on security in Asynchronous Transfer mode (ATM), Synchronous Digital Hierarchy (SDH) and associated signalling structures will be necessary.

**Multi-media:** Multi media applications will integrate all known representations of information into files, documents, messages and displays. Representations such as voice, audio, still image, text, video and graphics will become interchangeably available from a range of equipment that users interact with, including mobile telephones, personal computers, television sets and personal communicators. All aspects of security must be incorporated for potential implementation in all of these systems in order that a user may implement a level of security service appropriate to the application and the environment.

**Global teleconferencing:** Teleconferencing is becoming the substitute for travel. In order to make it really cost effective applications such as multimedia, mobility, access to mass data and if necessary access to one or more parties who are travelling in private vehicles need to be incorporated within the teleconferencing application. True geographic independence will come only if such an application works on a global scale and provides all the security services that are needed by the community of users. Such an application will demand the integration of the security services provided for each of the sub-applications alone. Specifications to allow such integration should be defined and the technology to provide the security functionality developed.

**Data access:** Access to huge amounts of data from a mobile terminal will be essential. Such data needs to be communicated securely, whether it be held in volatile memory, in the form of mechanically read ROM or transmitted over a network. Specifications for securing such data need to be developed as do the necessary bulk encryption services for huge data volumes. The technology components of such services will be a major challenge and need to be defined now.

**Transportation:** Human involvement in controlling mass transportation mechanisms is already decreasing as technology becomes more reliable. If human involvement or individual transportation is to shrink in the same way then mass production of cost effective safety assured technologies will be essential. Collision avoidance, guidance and navigation systems will be essential parts of every domestic vehicle and the requirements for the information safety and security critical elements of such systems need to be defined, standardised and developed. This applies to the further evolution of all current forms of transport, personal (e.g. car, motor bike), aeroplanes, helicopters, ships etc., and future methods of public transportation possibly involving space flight.

**Health-related technology:** Much progress has been made on developing a variety of innovative products that diagnose and treat health problems. This includes robotics, micro and laser surgery and sophisticated computerised life support equipment. There are also many supporting technologies including the authenticity of medical records and the authorisation of clinical events which currently require individuals to 'sign' (in one form or another) in order to provide authenticity and authorisation within a local health institution, nationally and internationally (throughout Europe and the World). All these evolving technologies have security and safety-critical implications which need to be resolved. Development of electronic signature and trusted third party technology will be very important in resolving current authenticity and authorisation needs in the health domain.

Technologically this represents a major challenge going well beyond present day techniques.

### **Requirements**

- Incorporation of information security requirements into R&D and engineering of new systems, services and applications
- information security technology for multi-media and other advanced services and applications.

### **5.5.2. Technology for trusted products**

#### **Issue**

Need of new technologies for the design, development, testing and evaluation of trusted products and systems based on future technological changes.

#### **Discussion**

As new technologies are developed, there is always a need for trusted variants. In order to be able to develop trusted variants, the required 'trusted developers tool-kit' must also be improved so that the development and evaluation of trusted products is made easier for all levels of assurance. This will also encourage the development of trusted products and improve their cost-effectiveness.

Areas where improvement in tools technology is most needed include:

- Tools for development and verification of trusted software and hardware: Currently, there is no clearly accepted catalogue of tools for trusted software and hardware development. This makes it increasingly difficult to decide whether new development techniques, such as new languages and compilers are suitable for the development of trusted products. Current tool technology needs to be assessed to see what is suitable and what isn't suitable for trusted development. Tools need to be developed for areas where there are no acceptable commercially available offerings.



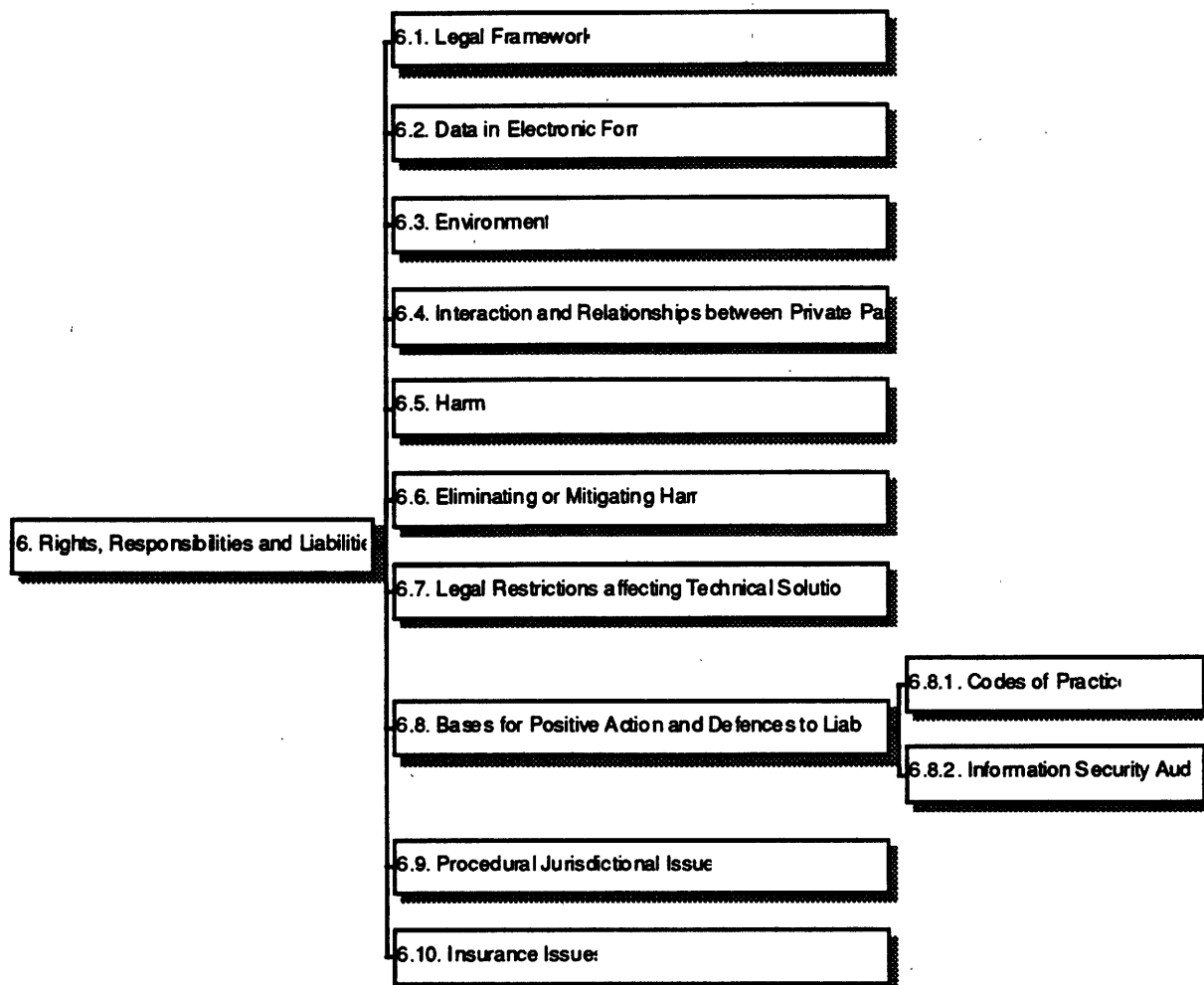
- Formal methods are not widely used to develop trusted systems, mainly due to lack of maturity of the methods, the intellectual difficulties inherent in the use of such methods, the lack of automated support tools and the substantial increase in costs for the development process. All of these issues need to be addressed in order for the use of formal methods to be more widely used and thus to enable high assurance products to be developed.
- Improvement in safety-critical and security evaluation tools (see above).

### **Requirements**

development of tools for the development and verification of trusted software and hardware, where there are no acceptable commercially available offerings

investigation into the current use and available automated support for formal methods to find out where the improvements in formal methods technologies need to be made.

## 6. RIGHTS, RESPONSIBILITIES AND LIABILITIES



### 6.1. Legal Framework

#### Issue

A differentiated approach needs to be taken to the establishment of a legal framework for information security.

#### Discussion

To formulate such an approach, one must look first at the special problems that electronic data presents, why electronic data is or may be (legally) different from data in paper form, and what needs to be done about it. The issues identified as crucial to the establishment of a legal model for the security of electronic data include:

- meshing European Community rules, regulations and guidelines about the security of electronic data with those already in force on the international, supranational, and national levels;
- ascertaining the best legal measures for dealing with the legally relevant features of electronic data that are different from those of data on paper;

- dealing with the expectations and awareness of suppliers, users and third parties vis-a-vis their own interaction with and response to the law of the security and the evidence of electronic data;
- establishing a framework for the validity of asserting defences such as certification, information security audits ;
- establishing a framework for the adoption of an appropriate duty of care
- addressing substantive and procedural issues relating to information security law and law of evidence; and
- ensuring that the model which is created supports and is consistent with public policy.

In addition, any model which is developed must be valid for not only computer processed electronic data, but also for electronic data which is transmitted over telecommunications networks via satellites or via other communications facilities, especially as the distinctions between the technologies blur.

It is against this backdrop that the following approach to the rights, responsibilities and liabilities relating to the security of information systems was developed.

In this, a glossary of concepts and terms must be developed so that the ideas, recommendations and conclusions discussed in this chapter can be understood and applied and so that there can be a guarantee, to the extent possible, of consistency in the analysis of the subject matter.

A report consisting of preliminary recommendations for the necessity and (realistic) potential for the evolution of a new model for the protection of and economic rights deriving from electronic data and information should be prepared.

### **Requirements**

- Glossary of concepts and terms
- model for the evolution of protection of and economic rights deriving from electronic data and information.

## **6.2. Data held in Electronic Form**

### **Issue**

A distinction must be made of data held in electronic form and data held in material form.

## Discussion<sup>8</sup>

Adopting the widest possible definition of information security is fundamental to creating a model for information security legislation. For example, a substantial body of current legislation relating to information security is based on the protection of intellectual property rights or (personal) data, and not necessarily on physical intrusions to systems. As such, new rights and liabilities may have to be created, and these run to the protection of economic as well as to intellectual property interests. Also, as much attention needs to be devoted to the data (and information) which systems generate as to the systems themselves. Thus, consideration must be given to such issues as how data are:

- valued (as an asset)
- perceived (by users, owners, individuals and organisations who are subject to this information)
- generated (by systems)
- potentially a threat.

A paper document normally consists of three aspects:

- the carrier (the sheet of paper)
- text and pictures (the physical representation of the information)
- information about the originator to verify the authenticity (usually a written signature)

The connections among carrier, text and signature are self-evident. Therefore normally only the carrier (the paper) is mentioned. It gives delimitation and structure to one finalised representation of the content. These aspects are physically "locked" via the paper that carries the information in one "unchangeable" and durable combination. Paper documents are normally given the necessary signs of authenticity by a written signature: the reader has confidence in the information about the originator and in that the text is not altered. A signature also gives a warning before a judicial act and conforms the final content in a contract, etc. Paper documents are in principle unique physical examples; originals. The stored state and readable state are identical. The paper document is immediately readable and the storing is normally in a language that the user will understand without special training. A manipulation of a paper document has to be a material attack, traceable upon the physical object. An individual makes - often unconsciously - a visual authenticity control when he is reading an important paper document. The information within a paper document is directly transcribed from a human thought process.

Electronic documents confer new dimensions. The carrier, the text and the "signature" are not related to each other in the same "locked" and durable form as in a paper document.

---

8 The following definitions are used in the text of this section:

"data" means a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or automatic means;

"information" is the meaning assigned to data by means of conventions applied to that data;

"information systems" means computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance.

Descriptions of electronic documents will normally make immaterial wordings, not physical objects, the starting point. It could on occasion be difficult to obtain information about how the user intended to process stored text-data and computer programs. Without certain technical authentication procedures there is no "lock" for the information in an electronic document and such objects are not immediately readable. Manipulation of a digital record consists of untraceable alterations of a bit pattern. The visual authenticity control of a paper document has no correspondence in the area of electronic information services. Computerised materials often are the result of automatic processing that at times may not be directly connected to a human thought.

The following may be considered factors which differentiate electronic from material (ie non-electronic) data:

### *Evidence*

Special rules apply in certain jurisdictions relating to the production and admissibility of computer generated information and data and the burden of proof regarding computer-generated information submitted to court.

### *Form*

In certain jurisdictions the law insists upon the adoption of a certain form (embodiment) in order for a document or other instrument to be legally valid, eg in the UK, a will must be a paper document. There may also exist procedural and organisational requirements. In the medical sector, for example, eligibility for reimbursement of a digital imaging examination will be granted by some social security authorities only if the medical file can be presented in material form.

### *Processing Facility*

Automated processing, which characterises electronically held data, means that electronic data can be processed in a way which is far faster, more efficient and more accurate than processing of data in paper-based systems. In some cases, processing can only practically be carried out electronically. For example, census data can be processed in a meaningful timescale only in an automated environment; such processing would be virtually impossible if this data were manipulated only on paper. It is normally impossible to show that electronic processing is perfectly correct. At best a reasonable belief of correctness can be achieved.

### *Preservation*

Some jurisdictions require that documents be available for consultation and review for up to 150 years. The preservation and storage of documents in material form is increasingly a problem while the preservation and long-term storage of non-material (ie electronic) documents is currently uncertain, especially as to their integrity. It is likely that the technology used to store data today will be out of date at some time in the future, and that archives can no longer be read.

### *Accessibility*

Data in electronic form are, by definition, not in a form in which a human being can, without other aids, inspect, review, supervise, read or understand. In all cases, specific technical methods are needed so as to represent electronic data in human processable form, and these methods may not be readily subject to verification.

### *Data Compression*

Data are more and more accessible, both in terms of cost and physical convenience, as data compression techniques make it possible to reduce vast quantities of data to, for example, a single CD-ROMs, thus increasing the size and scale of potential harm.

### *Aggregation*

Aggregation involves reorganising (ie sorting, merging, appending and deleting) the data contained in disparate databases - a fundamental and commercial reason for implementing automated data processing systems. New information (whether properly or fraudulently generated) can be derived through aggregation, thus creating output which was neither intended nor understood to be potentially available at the time or point of collection. The amount of such new information and, indeed, the number of documents that may be generated by aggregation, is indeterminate and potentially infinite.

### *Quasi-material form*

Electronic data are non-material, but stored on a material medium. It is therefore difficult to ascertain which legal principles should apply.

### *Dissemination*

Once data is made publicly available in an electronic form it is for all practical purposes impossible to prevent the further dissemination of that material, even if it is inaccurate, incomplete or invalid.

### *Persistence*

Related to dissemination is persistence. Persistence characterises the condition where inaccurate, invalid or incomplete data may persist on multiple computers and databases, and may even be erroneously reinstated on computers and databases on which corrections or deletions were thought to have been properly made.

### *Originality*

It is already often difficult (and sometimes impossible) to differentiate between originals and copies of electronic data or output from electronic data processing. It will become increasingly difficult. The same applies to photocopied data. Legal and practical requirements for original documents become impossible to enforce.

### *Ownership (s.a. intellectual property rights)*

Information cannot be 'owned' in most jurisdictions. Often, this status derives from public policy which mandates that information must be in free circulation and available to all or from a strand of legal analysis which renders it impossible to exert sole domain over information, or permanently deprive its 'owner' of use. It also reflects common sense, which suggests that if something is the case, it can be known by anyone and, once known cannot subsequently become unknown. It is possible, however, to own the intellectual property rights *in* such information: rights such as copyright, confidentiality and trade secret protection. The models for information derived from electronic data and that for information held in material form are similar, but the nature of electronic information (which allows it to be cut, sliced, transmitted, transformed, etc.) may require new rights and protections to be developed (see reference to economic rights, above).

### *Durability*

Documents in material form generally continue to retain their legal status even though they may suffer minor damage such as, for example, bent corners, small tears or moisture spots. However, minor damage to data in electronic form may severely affect the durability of such data and its legal status, unless special processes and techniques have been introduced to resist such damage.

### *Expectations*

Non-specialists in electronic information and data processing and storage are largely ignorant and often frightened of computer processing and computer-generated information and documents. One consequence of these perceptions is that non-specialists have unreal expectations of the confidential nature and the exclusivity of the data being collected, stored and processed.

### *Data exchange*

Data and information have historically been exchanged in material form, thereby maximising the (perceived) control over dissemination and monitoring which people had of the data and information being exchanged. None of these "comfort" factors operate in the electronic exchange of data unless they have been made explicitly available. People may not know enough to put them in place, or to complain about their absence. In particular, in a face-to-face conversation the exchange is specifically not fixed in a material form, and is limited to 'processing' by the parties present. On the other hand, an electronic conversation may be fixed, may persist and may unwittingly convert slander (spoken) into libel (embodied in electronic form and then generated into material form).

### *Standardisation of the use of electronic data*

Conventional paper based systems are based on methods and interpretations which are assumed to be well understood by all individuals involved. Data in electronic form must closely follow complete sets of standards (codes, formats, etc) and instructions for equipment use to be as intelligible as recorded conventional information. To some degree such standards and instructions must still be developed.

### **Requirements**

- Identification, categorisation and analysis of existing (current) rules and laws dealing with data held in electronic form
- definition of the dependent and consequent legal relationships, obligations and liabilities for each of the characteristics (differences) in the context of information systems security.

## **6.3. Environment**

### **Issue**

The legal, commercial and political environment which gives rise to the requirement for information security has changed more in the last five years than in the previous two thousand. It is likely that this change will become even more rapid, and will develop in ways which cannot be readily foreseen at present.

## **Discussion**

### *Legislative environment*

It is within this environment that legislators, and government officials must write legislation that is not only effective today, but will endure for some time, and not be overtaken by technological change as it occurs. This means that information security legislation cannot be drafted on a reactive basis (ie it cannot be written to correct problems which have occurred in the past), but rather on a proactive basis, ie it must anticipate the effect of technology on society.

To achieve a proactive approach to information security legislation, legislators and their advisers must have detailed knowledge of information and information security. If this knowledge - and control - does not exist, real dangers can emerge. For example, legislation based on incomplete or skewed research can result in:

- threats to the democratic processing of data
- the evasion of weak legislative controls by such means as siting businesses in data havens.

New thinking about information security law also requires:

- a reconsideration of the legislative balance between privacy and the free circulation of data
- the management of technology vis-a-vis data protection responsibilities
- a complete re-examination of the existing framework of commercial, company and other regulatory legislation so that the new law of information security can be incorporated systematically.

### *Commercial environment*

The rate of technological change mentioned in the previous section has an especially critical effect on organisations: the rate of day-to-day changes in technology currently exceeds the rate at which organisations can change in order to adopt and implement these changes. It is unlikely that this situation will change in the near future or the medium term. Attempts at implementing rapidly changing technology require substantial investment and introduce a reliance upon third parties to provide essential technical infrastructure and support which was never necessary when information could only be processed in a material form. In some instances, organisations may be specifically forbidden from providing some elements of infrastructure themselves, for example, telecommunications. This shift in expertise from inside organisations to third parties means that vulnerability and dependency is significantly increased. To some extent, organisations may be at the mercy of their service providers.

Similarly, organisations find technology change difficult to manage because the requisite expertise is not always present at the right level, and indeed it may never be cost effective for any but the largest organisations to develop and retain such expertise in-house.

### *Political environment*

Tension exists between a government's vested interest in maximising the development and exploitation of technology as a way of guaranteeing its country's commercial success, and its duty to preserve the privacy and rights of individuals. Consequently, there is a danger that government policy in promoting economic growth may result in the distortion of the decision-making process for selecting save technology and vice-versa.



It is essential that an informed public debate take place as to whether a special regime is required for the management and regulation of electronic data handling and processing in the political environment. This debate must take place in the light of existing legal frameworks but the conclusions must be sufficiently flexible as to withstand the constantly changing technological and political environment.

### **Requirements**

- Re-examination in the context of information security rights, responsibilities and liabilities of the management of information systems security within organisations and organisations' relationships with third party providers of information security (and related) services
- models to introduce certainty and consistency with respect to legal obligations for owners, directors, managers, employees, consultants, contractors, Trusted Third Parties, auditors and lawyers
- model clauses relating to information security which can be included in contracts or other agreements in place between parties
- an understanding of the rights, responsibilities and obligations which underpin and define the relationship between information security and the political environment requires:
  - examination of the context in which governments collect and process data.
  - review of the role of information in investigatory activities and in ensuring the public order
  - resolution of the conflict between supra-national government objectives and national governmental objectives with respect to data collection, processing, transmission and storage, etc.

## **6.4. Interaction and Relationships between Private Parties**

### **Issue**

Central to the environment in which information security exists are the relationships which are formed between private parties.

### **Discussion**

Such relationships include:

- mere communication between them (by electronic means)
- contracts and other agreements forged between them
- regulation of their society, ie by the laws which govern their interaction.

### **Requirements**

- Identification of the interests which need to be protected and regulated, and harm which needs to be redressed if and when security goes wrong, whether the relevant law is civil or criminal.

## **6.5. Harm**

### **Issue**

The harm that can be caused by the reliance on electronic communication systems.

### **Discussion**

Harm is the negative by-product of reliance on electronic data systems without being able to develop a reliable trust in them either purposely (ie where the user or beneficiary of the data processing is otherwise in a position to take appropriate security measures) or passively (ie where the user or beneficiary is otherwise not in a position to take appropriate security measures). This is in direct contrast with the trust which has evolved in (as well as the controls over and the management of) paper-based systems throughout their history. As a result, there is a great deal of work which needs to be done to close the gap between the methods of inculcating trust in and controlling and managing electronic systems as opposed to paper-based systems. It is also important to ensure that, to the greatest extent possible, relevant mechanisms are no more burdensome than those applicable to paper-based systems.

A comprehensive list of the common and extraordinary threats which endanger electronic communication must be constructed so that the boundaries of harm can be established. It is likely that most threats will fall under the following headings:

- theft and fraud
- mis- and dis-information
- invasion of privacy
- harm due to inadequate technology

Listings of some of these threats may be obtained from work published by standards bodies or carried out for national and supra-national administrative bodies. It may be that additional work may be needed in order to avoid legislative delay.

### **Requirements**

- Comprehensive list of the common and extraordinary threats which endanger electronic communication.

## **6.6. Eliminating or Mitigating Harm**

### **Issue**

Legal possibilities to eliminate or mitigate harm caused directly or indirectly through the use of electronic communication.

### **Discussion**

Options for eliminating or mitigating harm already exist in the form of treaties, laws and rules ("legislation") which address to some extent the harms which threaten electronic data and processing. However, in many cases, this legislation has been drafted:

- in the context of paper-based systems and as such is applied by analogy; or

- by attempting to adapt existing and often ill-suited legislation to electronic data and processing; or
- by bolting on to existing legislation provisions which relate specifically to electronic data and processing but which are not followed through in the main body of the legislation (and thus creating ineffective, incomplete or confusing rights, obligations or liabilities); or
- by interpreting existing legislation so that it encompasses electronic data and processing (eg "record-keeping" provisions)

Existing legislation which follows one or more of these four patterns exists as or in the form of:

- Supra-national and international treaties and guidelines, eg the European Convention of Human Rights
- Constitutional rights
- Consumer protection
- Criminal acts, eg theft and the deprivation of ownership, forgery, fraud, counterfeiting, destruction to property
- Civil acts, eg libel and slander, trespassing, unauthorised disclosure, laws granting judicial immunity
- Company and organisational law
- Provisions related to professional confidentiality, mostly embodied in penal law, eg medical confidentiality.

Legislation created specifically to address the harms relating to electronic data and processing also exists but often does not go far enough in protecting the underlying rationale (usually economic) or take into account the complete matrix of rights, responsibilities and liabilities on the one hand, and technical obligations on the other (eg in the form of physical and organisational measures):

- Data protection laws and principles
- Computer crime laws
- Law protecting intellectual property rights,.

There is, however, one instrument which can be distinguished and which constitutes a strong foundation from which future legislation can be built, and that is the OECD Principles.

Any action must:

- take into account the potential threats to the rights and responsibilities associated with electronic information systems
- consider the possibility that greater liabilities will attach in the absence of appropriate remedies.

## **Requirements**

- Threat analysis so as to be able to identify, develop and implement new legal remedies to deflect harm
- re-examination of the applicability and suitability of existing legislation to the mitigation of harm.

## **6.7. Legal Restrictions affecting Technical Solutions**

### **Issue**

Legal restrictions to the use of technically feasible solutions often exist.

### **Discussion**

It is essential to recognise that technology and custom and practice must be considered in the context of and balanced with law and legal solutions. A process must be undertaken to ensure that technical solutions are legal ones, and that technical custom and practice adhere to the laws, codes of practice, guidelines and other regulatory instruments in force. For example, a technological breakthrough in speeding up the production of multiple copies of copyrighted works may be technically valuable, but illegal when used in all but a narrow range of circumstances.

Technical countermeasures to different kinds of attacks, such as cryptography, exist for communication system security which are both economically and operationally effective. However, legal restrictions to their use often exist, usually because of fears over national security and their use to hide criminal acts.

Political debate involving governments, law enforcement agencies, commercial enterprises and individuals needs to take place.

### **Requirements**

- Identification of any real dangers which could exist where confidentiality measures are used
- balance illegal against valid use and extract those uses for and conditions under which the balance militates in favour of valid use.

## **6.8. Limitations to Liability**

### **6.8.1. Recommendations for Liability Limiting Measures**

#### **Issue**

In case of a security incident, liability need to be properly apportioned.

#### **Discussion**

Codes of practice comprise an essential element in the development of information systems security regulation. They may provide both a basis for regulation (by setting out principles and guidelines to be followed) and for a possible defence (against claims of negligence).

Points to be addressed include:

- Definition of the role, function and effect of codes of practice
- Identification of the concerned parties, eg the beneficiaries, those addressed by the code, eg suppliers of goods and services, integrators and facilitators, suppliers of raw products
- Coverage, eg physical security devices, practices, services
- Legislative/regulatory aspects, eg
  - individual or body empowered to issue the code (eg secretary of state, professional body)
  - scope of the issuer's authority
  - intended effect (eg binding or merely persuasive)
- Standards to be adopted, eg
  - "in a good and workmanlike manner"
  - "using materials of good quality and fit for their several purposes"
  - effect of standards of care, eg "due regard"
- Types of liability
- Accountability and directors (compliance statements)
- Adjudication of claims under a code
- Structure of codes
- Drafting of baseline requirements.

#### **Requirements**

- Recommendations for liability limiting measures.

### **6.8.2. Information Security Audit**

#### **Issue**

Ensurance of adequate compliance to security measures, Codes of Practice, laws and regulation.

#### **Discussion**

Many organisations currently undertake an information security (or computer) audit on a regular basis. It is a tool for ensuring that the appropriate and relevant security measures are in place, and it can be a defence against claims of fraud or negligence in the operation of the organisation's electronic data processing systems or the data which those systems process.

The following are key issues to be examined with respect to the information security audit:

- What should be covered by such audits
- Compliance and disclosure

- Requirement for audit through company law or other administrative law
  - Responsibility for failure to protect, eg
    - civil penalties for non-compliance
    - shareholder suits
    - automatic disqualification and loss of position
    - restitution of losses
  - Who should be authorised to carry out such audits and the nature and extent of their training, and the extent of their responsibilities and liabilities
- Creation of the defences to liability
    - Identification of existing
      - minimum standards for security
      - legislation and regulation
    - Creation of
      - the proper balance between compliance and protection
      - appropriate security measures
  - Recommendations for the coverage and timing of audits.

### **Requirements**

- Framework for the monitoring of compliance to regulations, recommendations and good practices.

## **6.9. Procedural Jurisdictional Issues**

### **Issue**

The creation of any rights or responsibilities and the identification of liabilities must be done within the framework of jurisprudentially acceptable procedures and mechanisms.

### **Discussion**

Within the framework of international law are concepts and definitions of procedural issues relating to jurisdiction which are recognised by all legal systems found within the European Union.

The procedural issues and mechanisms to be addressed with respect to breaches of contract and of torts (specific ones relating to information security may/will have to be created) and the commission of crimes relating to information security include:

- The jurisdiction of national courts, administrative bodies, tribunals, etc, in co-operation, where appropriate, with the Court of Justice, to hear and rule on actions and disputes arising from and charges relating to information security
- The formulation of rules relating to:
  - the collection, presentation and authentication of evidence (in any form)
  - procedure (eg service and form of writs, drafting of pleadings, statutes of limitations, etc)
- Mutual Assistance.

These issues are compounded by different positions in national law with regard to:

- insider trading (using computerised trading and computerised information systems)
- pornography (using computers for definition, dissemination and access)
- transborder data flow (using communication networks)
- interception (generally, as found in the telecommunications sphere but which involves computerised components of telecommunications systems)
- encryption (used illegally and therefore used in contravention of the criminal law)
- computer crime.

The procedural issues raised by these differences should be examined further with the involvement of all interested parties with a view to identify their exact nature and the most appropriate way to overcome these or at least limit their impact.

### **Requirements**

- Development of suitable conventions
- agreement on electronic evidence
- agreement on civil procedures relating to information security and electronic evidence
- code on the commercial procedures relating to the use of electronic records.

## **6.10. Insurance Issues**

### **Issue**

When electronic documents and information replace traditional documents, the insurance industry will need objective measures to assess the security mechanisms available or in use to determine what cover, if any, they should provide for customers using such things.

### **Discussion**

Insurance is something which is used by commerce and industry to provide relief in the event that a disaster occurs to them for which insurance is available. Insurance does not, of itself prevent the occurrence of disasters. It provides financial payments to the insured, and may sue those who cause a disaster if there is malice or negligence involved.

Insurance can be provided in a number of ways; a bilateral contract between an insurer and an insured, a mutual contract between a group of parties who are self-insuring, relief of last resort - usually provided by a national administration.

Where there are insurance contracts the insurer may impose conditions upon the insured to conduct themselves in accordance with 'rules of behaviour' contained in the insurance contract, or may vary the cost of the insurance or the extent of the indemnity provided according to the 'standards' observed by the insured.

Most of the documents that we use today for the purposes of administration or the carrying out of commercial transactions are supported by an underlying basis of insurance. Cheques and bearer bonds are printed by special 'fraud resisting' techniques, and as a result, insurance cover is available to the issuer or user in the event that a document is misused. Commonly, authorised copies of documents are often issued where originals are not readily available, and

the validity of these copies is underwritten by insurance policies. Letters handled by the postal service may have an implied minimum value for insurance purposes.

Insurance rates are built up on the basis of a claims history for the risk that is being underwritten. This may present a number of problems where there is no claims history available, or where the potential risk may be difficult to quantify. Further, insurance companies may not be in a position to know what standards ought to be followed by insurers to minimise risks. This may cause over-reaction by the insurance market once the first claims for failure come in.

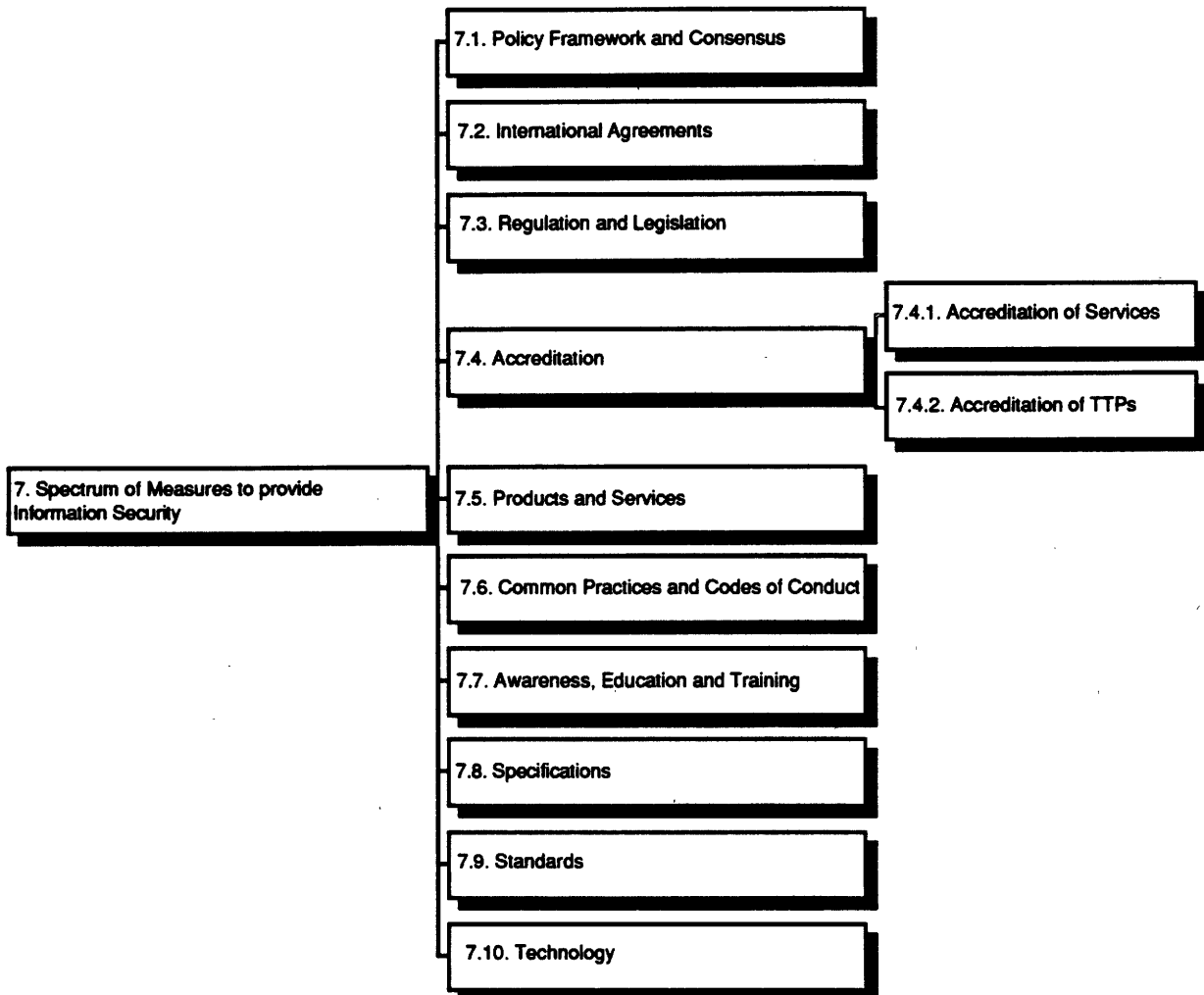
To provide for a balanced approach to the introduction and general use of electronic documents and methods, a broader educational programme should be considered for the insurance sector to clarify the issues involved and methods available. Such a programme could build upon the work carried out in the preparation of this document, work on baseline security standards by both BSI/DISC and IBAG.

### **Requirements.**

- Criteria and procedures for the assessment of insurance risks
- identification of situations which may need to be covered by an insurance obligation as a pre-condition of service provision, operation or usage.



## 7. SPECTRUM OF MEASURES TO PROVIDE INFORMATION SECURITY



### 7.1. Policy Framework and Consensus

#### Purpose

To provide a minimum framework for trusted information and communications services on an international scale and to establish a multi actor consensus on essential requirements and options for the provision of information security and related issues.

#### Background

Information and its exchange via global networks is inextricably associated with all public and private activities involving the citizen, service providers, operators, vendors, administrations and authorities in numerous ways for all kind of purposes. With the increasing globalisation of the economies an agreed framework for the protection of information either associated with intellectual property, privacy, internal security and other legitimate reasons is needed. While there are several conventions and recommendations, the rapid evolution of technology and services implies the need to reflect on a common framework which could assist countries and regions to maintain interworking and avoid

technical barriers to trade and communications without compromising their priorities in the protection of information assets.

Solutions for open communications between a variety of parties on a global scale do exist. They differ in detail and convenience in usage. However, the ability to use them depends critically on a broad consensus on the use of one or the other option. Nationally constrained solutions, such as DES, RSA in the USA are of little utility if they can not be used by US business in the pursuit of their global business interests and vice versa if others can not make use of these techniques for their communications with US partners.

To achieve agreement and reasonably general acceptance by the users concerned is as important as the technical performance of the solution in question.

## **7.2. Agreements**

### **Purpose**

International agreements on a minimum set of features and operational concepts as required for trusted and open service provision.

### **Background**

While a common framework and general consensus may go a long way, there is the need to get formal agreement on certain aspects. These may, for example, relate to issues surrounding liability, accreditation and certification and the fighting of organised crime..

## **7.3. Regulation and Legislation**

### **Purpose**

Adjustment of national regulations and legislation to permit seamless interworking of trusted services.

### **Background**

The provision of information security is seen to be related in some areas closely to public order and defence issues. The related national regulations and legislations vary considerably. In order to avoid the creation of technical barriers to trade and communications outside the domains of internal order and national security, adjustments of legislation and regulations may be required in some countries.

## **7.4. Accreditation**

### **7.4.1. Accreditation of Services**

#### **Purpose**

Evaluation of communication services.

#### **Background**

Common criteria for security evaluation are mainly focused on IT products and IT systems. However, there is a perceived need for criteria to support the evaluation of communication

services. This later criteria may be considered as an extension to the current criteria or there may be a need to develop separate criteria.

The evaluation of a service and its subsequent accreditation will be a critical requirement in many user applications, in particular those that need to use trans-European communication services. The consistency, completeness and effectiveness of the security enhancements of communication services needs to be checked for an overall fitness for purpose. Hence there is a need for a framework for accreditation of communications services.

#### **7.4.2. Accreditation of TTPs**

##### **Purpose**

Procedures for the accreditation and audit of TTPs.

##### **Background**

TTPs will need to interwork and communicate internationally to provide a service infrastructure to support a range of security services such as digital signature and confidentiality. TTPs will thus need to process, store and distribute a range of security-related information for the use and management of such services. This implies the need for a set of harmonised procedures for the accreditation and audit of TTPs in order to ensure mutual trust by the public in TTPs and the services they provide.

### **7.5. Products and Services**

##### **Purpose**

In order to facilitate a harmonious development of the provision of security of information systems in the Community for the protection of the public and of business interests, it will be necessary to develop a consistent approach as to its provision of security. Where independent organisations will have to be mandated, their functions and conditions will need to be defined and agreed and, where required, embedded into the regulatory framework. The objective would be to come to a clearly defined and agreed sharing of responsibilities between the different actors on a Community level as a prerequisite for mutual recognition.

##### **Background**

At present, the provision of security of information systems is well organised only for specific areas and limited to addressing their specific needs. The organisation on a European level is mostly informal, and mutual recognition of verification and certification is not yet established outside closed groups. With the growing importance of the security of information systems, the need for defining a consistent approach to the provision of security for information systems in Europe and internationally is becoming urgent. The most urgent needs identified relate to digital signatures and confidentiality services.

### **7.6. Common Practices and Codes of Conduct**

##### **Objectives**

Development of Codes of Practice to

- support the development and harmonisation of sectorial practices

- support the development of a standardised approach to the development of baseline controls
- support the development and harmonisation of baseline controls.

## **Background**

Codes of practice are found in many industries and disciplines. They encapsulate the collective wisdom and experience of the practitioners of a trade or profession or of an industry. For example codes of practice for the building trade. To the practitioners of a trade or profession, the need for codes of practice is self evident.

Codes of practice are not always obvious because they are often given other names. In some situations they may be called standards manuals in others requirements specifications. The property that sets them apart and makes them recognisable as codes of practice is the encapsulation of collective wisdom. The collective wisdom represents the means by which all parties to a transaction are protected from harm. In legal or business management terms this may be called a "standard of due care."

Any professional discipline needs to have a vehicle to encapsulate the collective wisdom of its practitioners. They help to ensure consistency across the wide spectrum of practitioners. That has to be true of something as important as information processing.

We have mentioned elsewhere the move towards empowerment and distributed systems. Empowerment means that the person responsible for an operating unit of an enterprise is free to obtain its services and resources anywhere. Where once information processing was done in-house, it is now just as likely to be out-sourced.

When information was once processed centrally the computer centre was well protected, both physically and logically. Indeed the protection of computer centres was the trigger for the development of corporate information security programmes. With information processing spread throughout the enterprise, the need for a central site vanishes. With it goes the ease of justifying the costs of high levels of security.

These two factors taken together mean that responsibility for information security is fragmented and put in the hands of people who have other responsibilities. Their mind set does not contain the same awareness of the need for security. Neither do they understand the interdependence of security and control measures.

The growth of legal, regulatory and contractual requirements for security create the need for a generally accepted set of controls and security measures. Words like due diligence and compliance with best practice can be satisfied by compliance with codes of practice. They provide the baseline needed for any comparison of actual with best practice.

Looking to the future we can see that information processing will become a basic skill for any skilled worker or manager. Where industries have their own codes of practice governing the way they operate, information security should become a sub-set.

Codes of practice must be formulated in such a way that audits can be performed to establish compliance.

## **7.7. Awareness, Education and Training**

### **Purpose**

Improved awareness of the issues of information security by specific actions and a greater emphasis in the education and training of related professions.

### **Background**

In the end it is the human factor which decides the level of information security, irrespective of the technical and operational measures one may wish to deploy. In this sense awareness and the teaching of appropriate skills in the context of the information professions, is an important measure to be considered. This may entail the creation of special training schemes and curricula, but most of all the appropriate inclusion of information security related issues in the teaching of information professions in general. This is in many cases essential, since information security is very closely related to the way information is used in a given context, ie often it has to be embedded in the application and management procedure and can not be added on as an external procedure.

## **7.8. Specifications**

### **Objectives**

To develop specifications for the application of security, in order to ensure interworking, interoperation and mutual recognition.

### **Background**

Functional specifications for products or services are documents that are to be used as parts of purchase specifications. They specify the functions of a solution and the required performance characteristics. Implementation aspects are only dealt with if they are particularly important for the fulfilment of a specific function. Specifications call up standards and profiles, as far as available. Options in the standards are resolved in specifications.

Common specifications for methodologies, eg evaluation, serve as a basis for mutual recognition.

## **7.9. Standards**

### **Purpose**

Development of standards for information security.

### **Background**

European security standards developed over the next decade will have a decisive influence on the technological structure of the entire European market and will change the conditions of trade in export markets and national markets.

The standards making infrastructure for the development of IT and telecommunication standards has become increasingly complex. The number of groups, the range of work items and the overall process at different levels of international, regional and national standardisation is a complex maze. Security standardisation is no exception to this situation. In general there is a reoccurring problem which is that of coordination between groups

developing standards similar in nature and scope. Such coordination is necessary to avoid duplication of work and the unnecessary waste of resource, and to ensure that the standards that are developed are consistent and they form a coherent set.

At the European level the establishment of the Advisory Expert Group ITAEGV has provided an ideal mechanism for the coordination of security standards work within Europe. In addition, ITAEGV is in the process of developing a European Memorandum, M-IT-06, which is a Taxonomy and Directory of European Standardisation Requirements for Information Systems Security based on market driven requirements. This memorandum also contains a future work programme for security standardisation.

Traditionally the principal contributors to standards making have been suppliers, designers and professionals. The end user of products and services has only been peripherally interested or involved. The end user has been concerned that standards have been used in relation to the products he buys but not greatly interested in what they are.

There is a need for a more effective mechanism and framework through which user interest is able to collectively express their requirements and priorities so that they can contribute to the standardisation process in a way which will balance the very strong interest of the supply industry.

The long-term benefits of security standardisation requires investment by companies and users and as such they must be prepared to organise themselves more effectively to participate in the standards making process.

## **7.10. Technology**

### **Purpose**

Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future requirements for the security of information systems.

### **Background**

Work on security of information systems would need to address development and implementation strategies, technologies, and integration and verification.

The strategic R&D work would have to cover conceptual models for secure systems (secure against compromise, unauthorised modifications and denial of service), functional requirements models, risk models and architectures for security.

Verification and validation of the security of the technical system and its applicability would be investigated through integration and verification projects.

In addition to the consolidation and development of security technology, a number of accompanying measures are required concerned with the creation, maintenance and consistent application of standards, and the validation and certification of IT and telecommunication products with respect to their security properties, including validation and certification of methods to design and implement systems.

The fourth RD&T Community Framework Programme might be one of the tools to foster co-operative projects at precompetitive and prenormative levels.

## **8. CROSS IMPACT ANALYSIS**

**Sect. Issues / Requirement**

3.	GENERAL ISSUES																			
3.1.	Globalisation of the economy and mobility																			
	Revision of the scope and approach to information security to reflect the new conditions, challenges and requirements brought about by globalisation	Δ		Δ																
	Adaptation of the respective policies and regulations			Δ	Δ															
	Clearly defined conventions on the expectations, responsibilities, duties and liabilities, related to levels of security, harm, and good practices.			Δ	Δ					Δ										
3.2.	Internal market ("four freedoms")																			
	Adaptation of the existing provisions with respect to their conformance to the internal market policy of the EC implying the removal of existing internal barriers and the avoidance of the formation of new technical barriers due to divergent application of security and safety rules, regulations and legislation	Δ		Δ																
	Provision to business and the public of solutions available throughout the community and preferably at the international level respecting the "one stop" and "pay-per-use" principles									Δ										
	Consistent deployment of standards and certification where critical for the working of the internal market									Δ							Δ	Δ		
	Certification and standards that reflect the needs of the different market segments																		Δ	
3.3.	Human rights and the protection of communications																			
	Common approach defining rights, responsibilities and duties of individuals, business and of the authorities.	Δ	Δ	Δ						Δ										
3.4.	Social acceptance of identification and authentication methods																			
	Clarification of the ownership and privacy issues related to the use of biometric data	Δ	Δ	Δ						Δ										
	Agreed classification of biometric data and conditions requiring secure handling of such data				Δ					Δ										
	Definition of the rights and responsibilities of individuals, business users, corporations and administrations using biometric techniques.			Δ	Δ															
3.5.	Human rights and the safety of systems																			
	Community wide standard for design practices and codes of conduct																		Δ	Δ
	Harmonised legal environment for vendors and users of safety critical systems	Δ	Δ	Δ																



**Sect. Issues / Requirement**

3.6.	Confidence in communication systems and services																			
	Real-time indication for the user of the trustworthiness of a service or system			Δ		Δ														Δ
	Feedback mechanisms for security and safety related incidents involving communications			Δ				Δ												Δ
	Independent assessment of the levels of trustworthiness being achieved					Δ														
	Investigation of the reasons why the security and safety of systems are compromised							Δ												Δ
	Understanding of the relative importance of the different system components and the components of the wider system and usage context							Δ												Δ
	Methods/frameworks for evidence reporting					Δ														Δ
	Role (costs, benefits) of certification in providing confidence and communicating this in the market place																			Δ
	Establishment of agreed claim limits to establish assurability					Δ														Δ
3.7.	Management of openness and protection																			
	Generic framework for the management of open and protected communications in a user/business oriented environment:	Δ				Δ	Δ	Δ	Δ	Δ										Δ
	Definition of agreed security domains																			Δ
	User interface for the management of openness/protection																			Δ
	Objective records and procedures for the accounting of open/protected transactions																			Δ
3.8.	Common concerns of commercial and national security																			
	Common requirements of business, citizens and authorities to adequately protect commercial and personal information and its communication	Δ	Δ	Δ	Δ	Δ														Δ
3.9.	Security and law enforcement on international scale																			
	Effective, internationally agreed, economic, ethical and usable solutions to meet business, administration and personal needs	Δ	Δ	Δ																
	Mechanisms for authorised interception for law enforcement	Δ	Δ	Δ																Δ
	Reporting of incidents and crimes adjusted to the conditions of the internal market																			Δ
	Equipment, software and an infrastructure of trusted third parties.																			Δ

**Sect. Issues / Requirement**

3.10.	Economics of the security of information systems														
	“IS-to-cost” techniques for business and private users.							△	△	△					△
	Incorporation of good information security design practice in the development of products and services						△	△							△
	Definition of information security as business and marketing factor							△	△						
	Identification of acceptance levels for insurers, regulators and the commercial courts	△	△	△			△				△				
	Specification of duties and responsibilities of parties to the use of information systems and their security requirements	△	△	△				△							
	Security architecture and “building blocks” specifications and standards, with a view to minimising the cost of providing commonly needed levels of security.										△				△
3.11.	Social recognition of information crime														
	Education and training on the information security requirements and concepts needed to operate in a secure manner in the information age										△				
	Clarification of “info-ethics” for the professional and individual user in its relationship to information security	△	△	△				△	△						
	Clarification of responsibilities of the sector actors in general and in their relations within each other, with particular reference to open and distributed applications.	△	△	△			△	△	△						
3.12.	Human factors														
•	Adjustment of personnel management practices and organisational procedures to reduce the vulnerability by the actions of staff and other people			△				△	△						
	Greater use of non-technical management controls							△	△						

**Sect. Issues / Requirement**

3.13.	Safety critical environments																		
	Common approach to the handling of security and safety critical requirements			Δ				Δ	Δ										
	Methodologies for threat, vulnerability and hazard analysis for the protection of information systems used in safety-critical environments					Δ	Δ	Δ			Δ								Δ
	Methodologies for the design, development and procurement of safety critical systems, covering project management, development environment, auditing of process, configuration management and change control			Δ		Δ	Δ	Δ											Δ
	Common approach to security evaluation of information systems in safety-critical environments.						Δ	Δ			Δ								
	Common approach to information systems recovery in safety critical environments						Δ	Δ			Δ								
3.14.	Embedding systems																		
	Methods of testing that enable standards of reliability to be ensured, including tests to destruction where appropriate			Δ				Δ										Δ	Δ
	Approach for the certification of safe products																		Δ
	Definition of requirements for fail-safe system architectures and implementations										Δ			Δ					Δ
	Anti-tampering and protection specifications and standards.										Δ			Δ					
	Quality label, that indicates the quality level of the embedded system					Δ					Δ								Δ
	Awareness of designers of the potential impact of innovation in the validity of test technology.									Δ									Δ
4.	DEMAND RELATED ISSUES																		
4.1.	Requirements for enterprises and individuals																		
4.1.1.	Agreement on security requirements for enterprises																		
	Taxonomy and directory of business user requirements and security objectives derived from experience with practical applications.									Δ	Δ								

**Sect. Issues / Requirement**

4.1.2.	Security administration																			
	Guidelines for establishment of security administration function.									Δ	Δ									
	Recommendation on moving towards commonality of laws on data privacy and protection, particularly relating to individuals.	Δ	Δ	Δ						Δ										
	Means to provide increased awareness and relevant education and training.																			Δ
	Guidelines for consideration of balanced security, taking account of level of risk in different areas (physical, personnel, hardware, software, data, etc.)										Δ									
4.1.3.	Security objectives for enterprises																			
	Standard techniques for drawing-up security policies for typical situations										Δ									Δ
	Methods and techniques for agreeing levels of security and security objectives.										Δ									Δ
4.1.4.	Exploiting innovation																			
	Assessment methods for the impact of changes on systems											Δ								Δ
	Procedural and regulatory framework needs to address convergence of safety and security etc. (implications for standards)	Δ	Δ	Δ																
	Methods for identifying early on where innovations are likely to be unacceptable from a safety perspective or will result in such economic penalties that they are not viable commercially.								Δ											Δ
4.1.5.	Sectoral specifics																			
	Consolidation and development of a set of codes of practice and baseline controls addressing specific business sector requirements.											Δ								Δ
4.1.6.	Security domains																			
	Mechanisms for management of policies, procedures and controls between domains for TTPs											Δ	Δ							Δ
	Generation of guidelines for domain creation, management and control											Δ	Δ					Δ	Δ	
	Development of a common framework for domain interworking											Δ							Δ	Δ
	Agreement on management, TTPs, accreditation, auditing and relations with law enforcement agencies.	Δ	Δ	Δ								Δ	Δ	Δ						

**Sect. Issues / Requirement**

4.1.7.	Security labelling											
	Guidelines for security labelling.								△			△
	Standard on how to express labels and on the meanings of a basic set of information labels.											△
	Codes of practice and accreditation methods for domains claiming to support standard labels, and their mutual recognition.								△			
4.1.8.	Administration of access to security related data											
	Easy to use tools for access right management and key management.								△			△
	Secure solutions for remote administration.								△			
	Awareness for control issues concerning security related data; and implications of non-action.						△		△			
4.1.9.	Security requirements for individual users											
	User profiles identifying standard types of users together with typical requirements.										△	
4.2.	Requirements for security functions											
4.2.1.	Access control											
	Group access control scenarios and schemes based on levels of commonality								△	△	△	△
	Techniques, products, specifications and standards addressing access control matched to the scenarios identified										△	△
	Parameters common to most or all of the above techniques, products, specifications and standards and the feasibility of establishing common formats for them										△	
	Identification of the key features for coherence in the supporting infrastructure								△			
	Basic access control mechanisms for pilot implementation.									△	△	
	Develop delegation scenarios.									△	△	△
	Identification of techniques, products, specifications and standards addressing delegation and their association with the identified scenarios.								△	△	△	
4.2.2.	Requirements for electronic cash											
	Agreement on the concepts underlying electronic cash										△	△
	International standards.											△

**Sect. Issues / Requirement**

4.2.3.	Requirements for security services																			
	Scenarios for the use of electronic security services																			
	User specifications for electronic security services																			
	Establishment of international application rules that can operate under the different legal frameworks and that ensure international communicability																			
	Identification of different scenarios where it is appropriate for the public interest to mask or hide the identity of the end user, taking into account the balance between full anonymity and audit.																			
4.2.4.	Digital signature																			
4.2.4.1.	The individual Right to signature																			
	Clarification of the right to signature and the attached entitlement.																			
4.2.4.2.	Consistency of Legal principles for digital signatures																			
	EC-wide/international agreement on the legal functions of signatures																			
	Clarification of the conditions of acceptance of the authority of an digital signature, e.g. For legally binding purposes, i.e.. As substitute for hand-written original signatures.																			
	Recommendation for the implementation for a public digital signature scheme for use by business, administrations and the general public.																			
	Legislative rules and, where appropriate, liabilities, for keys, certificates and TTPs to cover revocation of any or all the entities involved in the "chain of proof" needed in the signature technique.																			
4.2.4.3.	Universal acceptance of digital signatures																			
	Development, together with the legal profession, of recommendations for the practical use of digital signatures as a full equivalent to hand-written signatures in legal transactions including the conditions required for evidence																			
	Demonstration, through pilot projects, that digital signatures can be used as equivalent to hand-written signatures																			
	Inclusion in the curriculum of relevant educational institutes (eg engineering, law and business schools) the use of digital signature.																			

**Sect. Issues / Requirement**

4.2.5.	Privacy Enhancement																				
4.2.5.1.	Perception of Requirements for Privacy Enhancement																				
	Frameworks and architectures which are accepted as well by the business users as by the national security agencies and the service providers			Δ				Δ		Δ											
	Standards for services and service provision																			Δ	
	Compatibility of confidentiality services with existing communication standards and practices where possible							Δ		Δ		Δ	Δ	Δ							Δ
	Verification of practicability of proposed solutions through suitable pilot projects							Δ		Δ		Δ									Δ
	Model contracts for confidentiality services			Δ	Δ			Δ													
	Awareness improvement of sector actors of the potential losses due to the absence of confidentiality services.									Δ											
4.2.5.2.	The case for the Provision of public confidentiality services																				
	Architectures that minimises service vulnerability				Δ			Δ	Δ	Δ	Δ										
	Framework for the provision of trans-domain confidentiality services			Δ	Δ			Δ		Δ											
	Guidelines for pan-European confidentiality service providers (including accountability)	Δ	Δ	Δ				Δ	Δ	Δ											
	Model contract for relationship between service providers across national boundaries			Δ				Δ													
	Assurance criteria for service providers and operators							Δ	Δ	Δ											
	Accreditation process for mutual recognition.				Δ																
4.2.6.	Use of names and certification of credentials																				
	Guidelines covering the use of names.			Δ				Δ				Δ									Δ
	Guidelines covering the use of certificates.			Δ	Δ			Δ		Δ		Δ	Δ	Δ							Δ
4.2.7.	Security of electronically stored information																				
	Common approach to the security of electronically stored information		Δ	Δ	Δ			Δ	Δ	Δ	Δ	Δ	Δ								
	Unforgeable secure storage			Δ				Δ		Δ		Δ	Δ	Δ							Δ

**Sect. Issues / Requirement**

4.3.	Requirements for the safety of communication systems																			
	Platform for a dialogue on risk including users, regulators, vendors and service providers																			Δ
	Policy on risk management on a societal level based on objective risk assessment methods	Δ	Δ	Δ																
	Techniques that permit an integrated approach to the different types of risk (safety, security, commercial?, Direct, indirect)																		Δ	Δ
4.4.	Requirements for evaluations																			
4.4.1.	Trustworthiness of communication solutions																			
	International agreement on criteria and evaluation methods, and mutual recognition of test results			Δ		Δ	Δ	Δ	Δ										Δ	Δ
	Clarification of the commercial value of “certified products”, e.g. In terms of liability limitation								Δ	Δ										
	Clarification of the status and implied liability of vendor declarations					Δ			Δ	Δ	Δ									
	International agreement on the methods for evaluating security and safety critical system development processes, and the qualifications and experience needed for individuals that are involved in these processes.			Δ					Δ										Δ	Δ
4.4.2.	Motivation to acquire evaluated solutions																			
	Rapid adoption of common criteria																			Δ
	Agreement on common evaluation method									Δ									Δ	
	Portability of test results and mutual recognition					Δ				Δ									Δ	Δ
	Work-sharing between vendors, test centres and users to speed up the evaluation process									Δ									Δ	Δ
	Establishment of the “value-added” for the use by administrations and business, e.g. In terms of liability protection																		Δ	
4.4.3.	Consistency of procurement practices																			
	Identification of categories of application requiring evaluated solutions					Δ	Δ			Δ									Δ	
	Alignment of national procurement policies concerning evaluated products	Δ				Δ	Δ			Δ										
	Development of guidelines on applicability of evaluation levels									Δ									Δ	Δ



**Sect. Issues / Requirement**

4.4.4.	Operational Systems Accreditation										
	Definition of the inputs, process and outputs involved in operational systems accreditation and their agreement by relevant communities			Δ	Δ		Δ		Δ		
	guidelines for the establishment of schemes for operational systems accreditation within different communities						Δ		Δ	Δ	
	guidelines for organisations to determine the appropriate individual or body to perform the accreditation including the skills and training required by operational systems accreditors						Δ		Δ	Δ	
4.5.	Requirements for security and safety methodologies										
4.5.1.	Risk analysis and management										
	Consideration of the "claims structure" as a standard mechanism for specification of requirements, evaluation and the selection of risk analysis and management methods						Δ	Δ	Δ		
	Evaluation of the "claims structure" for applicability in the safety domain						Δ	Δ	Δ		
	Support for the "claims structure" as an international standard									Δ	
	Further evaluation of methods using the "claims structure"						Δ	Δ	Δ	Δ	
	Accreditation of organisations to conduct risk analysis and management method evaluations.				Δ				Δ		
4.5.2.	Metrics for Loss Assessment										
	Mapping of certified product features to specific security incidents								Δ		Δ
	common, product independent risk analysis processes.						Δ				Δ
4.5.3.	Technology assessment										
	Identification of the information security issues may be solved within the Technology Assessment process						Δ				Δ
	Technology Assessment pilot in Europe in the field of information security to assess the consequences for future information security applications and provide options for political and legal actions.						Δ			Δ	Δ

**Sect. Issues / Requirement**

4.5.4.	Analysis of audit trails																			
	Rules and regulations for the design, handling & exploitation of audit trail information, in conformance with right-of-privacy laws and practices.			Δ				Δ			Δ									Δ
	Prevention of audit data base compromise (e.g. Techniques of separation of information)								Δ			Δ								Δ
	Services for the independent acquisition, management, and/or analysis of audit trails							Δ	Δ											
	Development of innovative technologies (AI-based) for the exploitation of large audit trails).																			Δ
4.5.5.	Safety specific methodologies																			
	Assessment of areas of common interest between safety critical and security information practitioners																			Δ
	Software engineering processes and techniques for safety applications including their application and evaluation																			Δ
	Understand the special needs for engineering safe systems																			Δ
4.6.	Requirements for audits																			
	Guidelines for audit review of information security activities										Δ	Δ							Δ	
	Audit tools to enable reviews of security implementations and identify weaknesses (eg using artificial intelligence)										Δ									Δ
	Guidelines on reviewing any or all security changes										Δ	Δ							Δ	
	Suitable and consistent level of competence for security auditors and organisations to be accepted throughout the Community	Δ		Δ	Δ					Δ										
	Greater commonality of formats for audit trails, so that they can be used between systems.										Δ									
	Mechanisms to enable qualified auditors to be involved in system development										Δ	Δ								
4.7.	Information valuation																			
	Development of common practices for information valuation										Δ	Δ							Δ	Δ
	Assessment of current methods of information valuation										Δ									Δ
	Definition of the rights and duties of information ownership			Δ																

**Sect. Issues / Requirement**

5.	SUPPLY RELATED ISSUES																			
5.1.	Supply related issues- ways to meet the security demands																			
5.1.1.	Security services																			
	Harmonisation of legislation on the legal status of evidence generated by any TTPs and especially on the intra- and extra- community recognition thereof.	Δ		Δ				Δ	Δ											
	Litigation services based on existing international bodies such as the international chamber of commerce	Δ		Δ				Δ	Δ	Δ										
	Techniques for the establishment, handling and recording of electronic negotiable documents.							Δ	Δ	Δ	Δ	Δ	Δ	Δ						
	Date and time stamping for time-critical transactions and applications, including a range of granularities of timing.							Δ	Δ			Δ	Δ	Δ						
	International harmonisation of rules and services for time stamping, with the objective of achieving general recognition and acceptance of time stamps and their provision by suitably accredited service providers.							Δ	Δ			Δ								Δ
5.1.2.	Signature schemes																			
	Specifications and standards for an international signature scheme																			
	Specifications and standards for the integration of the signature schemes into practical applications																			
	General application programming interface (API) for the integration of signature schemes into applications. This should include codes which explain the purpose of the applied signature.																			
	Development of transaction-oriented multiple signature schemes							Δ	Δ		Δ			Δ						Δ
	Licensing of cryptographic algorithms.							Δ	Δ	Δ								Δ	Δ	
5.1.3.	Confidentiality schemes																			
	Consensus on the principles of confidentiality services for use by individuals, enterprises and administrations	Δ	Δ	Δ	Δ	Δ							Δ							Δ
	Trustworthy confidentiality scheme and its supporting administration.							Δ	Δ	Δ										
5.2.	Supply related issues - security management																			
5.2.1.	Role of trusted third parties (TTPs)																			
	Establishment of international framework for the operation of TTPs.	Δ	Δ	Δ	Δ	Δ	Δ													Δ
	Setting up of conditions for the operation of TTPs in the EC adapted to meeting the needs of national and international users.	Δ	Δ	Δ	Δ	Δ	Δ													



**Sect. Issues / Requirement**

5.2.6.	The management of TTPs																						
5.2.6.1.	Operating principles of TTPs																						
	Harmonised legislation to provide an appropriate framework for arbitration, supervision and litigation																						
	Model for TTPs meeting the requirements of users and authorities.																						
	Baseline for accepted good practice including a study of the level of availability, privacy and security required for the TTP by the final users and how much they are ready to pay for it																						
	Definition of quality of service, including availability, confidentiality, response-time, rules of disclosure to law enforcement agencies																						
	Operational guidelines, including descriptions of minimum set of services and standards to conform to																						
	Standard clauses for the contract between the TTP and the user, concerning the liability of the TTP.																						
5.2.6.2.	Interworking of TTPs																						
	Generation of guidelines for domain creation, management and control																						
	Common framework for domain interworking																						
	Agreement on management, TTPs, accreditation, auditing and relations with law enforcement agencies.																						
5.2.6.3.	Interworking of autonomous confidentiality services																						
	Minimum requirements to ensure interoperability, including standards, specifications, rules of procedure and operating practices																						
	Demonstration of trans-European confidentiality services using a suitable application, e.g. the realisation of administrative telematics applications.																						
5.2.6.4.	Accreditation and Audit of TTPs																						
	Development of international guidelines for the accreditation and audit of TTPs																						
	Adaptation of applicable legislation or regulations to provide an appropriate legal framework for use throughout the community and in the relations with third countries.																						

**Sect. Issues / Requirement**

5.3.	Supply related issues - evaluation of trusted solutions																			
5.3.1.	Evaluation of products, systems, services and applications																			
	Commitment of management to the security function within enterprises																			Δ
	Establishment of common definitions for the different evaluation options																			Δ
	Community and international standards for criteria and methodology																			Δ
	Choice in the access to independent evaluation facilities.																			Δ
5.3.2.	International harmonisation and mutual recognition																			
	Establishment of conditions and procedures for mutual recognition of evaluations																			Δ
	Establishment of conditions and procedures for EC-wide/international evaluations																			Δ
	International and EC standardisation of evaluation criteria and methods.																			Δ
5.3.3.	Vendor declarations																			
	Agreed definition of scope and liabilities of vendor declarations																			Δ
	Incorporation of vendor declarations in the ITSEC/ITSEM evaluation scheme																			Δ
	Specification of the types of systems which should not incorporate products covered by vendor declarations.																			Δ
5.3.4.	Self-evaluation																			
	Specification of accreditation for in-house evaluation facilities																			Δ
	Extension of the ITSEC/ITSEM evaluation criteria to include self-evaluation																			Δ
5.3.5.	Evaluation of applications																			
	Methods for evaluations to cover services and applications.																			Δ

**Sect. Issues / Requirement**

5.3.6.	Evaluation of communication services																				
	Evaluation of communications hardware and infrastructure security features																			Δ	Δ
	Formal accreditation scheme for secure communication services																				Δ
	Accreditation guidelines for the telecommunication sector																				Δ
	Trial service evaluations for existing telecommunication services																				Δ
	Articulation of the requirements of service evaluation.																				Δ
5.3.7.	Trusted network management																				
	Methods for network management evaluation																				Δ
	Definition of functionality classes (or protection profiles) suitable for systems, products and services used in network management systems																				
	Accreditation guidelines for the trusted network management																				Δ
	Trial evaluations for existing network management systems.																				Δ
5.3.8.	Evaluation of methods and tools																				
	Guidelines for the evaluation of methods and tools used to develop trusted products, systems and services																				Δ
	Register of methods and tools which can be used to develop trusted solutions.																				Δ
5.3.9.	Physical and procedural issues																				
	Guidelines for physical and procedural measures required to maintain trusted systems.																				Δ
5.3.10.	Modifications to evaluated products and re-evaluation																				
	Definition of rules and procedures for re-evaluation based on methods currently used																				Δ
	Alignment of the design process with the principles of re-evaluation, "design-for-change".																				Δ

**Sect. Issues / Requirement**

5.3.11.	Performance reporting for trusted products																			
	Incident reporting system for certification bodies																			
	User and supplier obligations to report incidents																			
	Supplier obligations to take corrective action and to initiate re-evaluation																			
	Register of evaluated product and their owners.																			
5.3.12.	Rationalisation of evaluations																			
	Alignment of security evaluation criteria and methods with those for quality and safety, where sensible																			
	Portability of results between quality, safety and security evaluations.																			
5.4.	Maintenance of safety and assurance																			
	Approach for tracking the evolution of systems and identifying when significant changes to safety and security requirements are taking place																			
	Strategies and techniques for re engineering of obsolete systems.																			
5.5.	Technological change																			
5.5.1.	Evolving technology																			
	Incorporation of information security requirements into R&D and engineering of new systems, services and applications																			
	Information security technology for multi-media and other advanced services and applications																			
5.5.2.	Technology for trusted products																			
	Development of tools for the development and verification of trusted software and hardware, where there are no acceptable commercially available offerings																			
	Investigation into the current use and available automated support for formal methods to find out where the improvements in formal methods technologies need to be made																			



**Sect. Issues / Requirement**

6.	<b>RIGHTS, RESPONSIBILITIES AND LIABILITIES</b>																			
6.1.	<b>Legal framework</b>																			
	Glossary of concepts and terms																			
	Model for the evolution of protection of and economic rights deriving from electronic data and information																			
6.2.	<b>Data held in electronic form</b>																			
	Identification, categorisation and analysis of existing (current) rules and laws dealing with data held in electronic form																			
	Definition of the dependent and consequent legal relationships, obligations and liabilities for each of the characteristics (differences) in the context of information systems security.																			
6.3.	<b>Environment</b>																			
	Re-examination in the context of information security rights, responsibilities and liabilities of the management of information systems security within organisations and organisations' relationships with third party providers of information security (and related) services																			
	Models to introduce certainty and consistency with respect to legal obligations for owners, directors, managers and employees, consultants, contractors, trusted third parties, auditors and lawyers																			
	Model clauses relating to information security which can be included in contracts or other agreements in place between parties.																			
	An understanding of the rights, responsibilities and obligations which underpin and define the relationship between information security and the political environment requires:																			
	Examination of the context in which governments collect and process data																			
	Review of the role of information in investigatory activities and in ensuring the public order.																			
	Resolution of the conflict between supra-national government objectives and national governmental objectives with respect to data collection, processing, transmission and storage, etc.																			

**Sect. Issues / Requirement**

6.4.	Interaction and relationships between private parties																		
	Identification of the interests which need to be protected and regulated, and harm which needs to be redressed if and when security goes wrong, whether the relevant law is civil or criminal.										Δ	Δ							
6.5.	Harm																		
	Comprehensive list of the common and extraordinary threats which endanger electronic communication.										Δ	Δ							
6.6.	Eliminating harm or mitigating harm																		
	Threat analysis so as to be able to identify, develop and implement new legal remedies to deflect harm										Δ	Δ							
	Ré-examination of the applicability and suitability of existing legislation to the mitigation of harm.		Δ	Δ							Δ								
6.7.	Legal restrictions affecting technical solutions																		
	Identification of any real dangers which could exist where confidentiality measures are used										Δ	Δ	Δ						
	balance illegal against valid use and extract those uses for and conditions under which the balance militates in favour of valid use.	Δ									Δ	Δ	Δ						
6.8.	Limitation of liability																		
6.8.1.	Liability management																		
	Recommendations for liability limiting measures											Δ	Δ						
6.8.2.	Information security audit																		
	Framework for the monitoring of compliance to regulations, recommendations and good practices.										Δ	Δ	Δ	Δ					
6.9.	Procedural jurisdictional issues																		
	Development of suitable conventions																		
	Agreement on electronic evidence											Δ	Δ	Δ	Δ				
	Agreement on civil procedures relating to information security and electronic evidence											Δ	Δ	Δ	Δ				
	Code on the commercial procedures relating to the use of electronic records											Δ	Δ	Δ	Δ				
6.10.	Insurance issues																		
	Criteria and procedures for the assessment of insurance risks																		
	Identification of situations which may need to be covered by an insurance obligation as a pre-condition of service provision, operation or usage.																		

## **ANNEX 1: RECALLING THE ACTION LINES FROM THE COUNCIL MANDATE**

### **Action line I - Development of a strategic framework for the security of information systems**

#### ***Issue***

Security of information systems is recognised as a pervasive quality necessary in modern society. Electronic information services need a secure telecommunications infrastructure, secure hard- and software as well as secure usage and management. An overall strategy, considering all aspects of security of information systems, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world.

#### ***Objective***

A strategically oriented framework has to be established to reconcile social, economic and political objectives with technical, operational and legislative options for the Community in an international context. The sensitive balance between different concerns, objectives and constraints are to be found by sector actors working together in the development of a common perception and agreed strategy framework. These are the prerequisites for reconciling interests and needs both in policy-making and in industrial developments.

#### ***Status and trends***

The situation is characterised by growing awareness of the need to act. However, in the absence of an initiative to co-ordinate efforts, it seems very likely that dispersed efforts various sectors will create a situation which will de facto be contradictory, creating progressively more serious legal, social and economic problems.

#### ***Requirements, options and priorities***

Such a shared framework would need to address and situate risk analysis and risk management concerning the vulnerability of information and related services, the alignment of laws and regulations associated with computer/telecommunications abuse and misuse, administrative infrastructures including security policies, and how these may be effectively implemented by various industries/disciplines, and social and privacy concerns (eg the application of identification, authentication, non-repudiation and possibly authorisation schemes in a democratic environment ).

Clear guidance is to be provided for the development of physical and logical architectures for secure distributed information services, standards, guidelines and definitions for assured security products and services, pilots and prototypes to establish the viability of various administrative structures, architectures and standards related to the needs of specific sectors.

Security awareness must be created in order to influence the attitude of the users towards an increased concern about security in information technology (IT).

## **Action line II - Identification of user and service provider requirements for the security of information systems**

### ***Issues***

Security of information systems is the inherent prerequisite for the integrity and trustworthiness of business applications, intellectual property and confidentiality. This leads inevitably to a difficult balance and sometimes choices, between a commitment to free trade and a commitment to securing privacy and intellectual property. These choices and compromises need to be based on a full appreciation of requirements and the impact of possible options for the security of information systems to respond to them.

User requirements imply the security functionalities of information systems interdependent with technological, operational and regulatory aspects. Therefore, a systematic investigation of security requirements for information systems forms an essential part of the development of appropriate and effective measures.

### ***Objective***

Establishing the nature and characteristics of requirements of users and service providers and their relation to security measures of information systems.

### ***Status and trends***

Hitherto, no concerted effort has been undertaken to identify the rapidly evolving and changing requirements of the major actors for the security of information systems. Member States of the Community have identified the requirements for harmonisation of national activities (especially of the "IT security evaluation criteria"). Uniform evaluation criteria and rules for mutual recognition of evaluation certification are of major importance.

### ***Requirements, options and priorities***

As a basis for a consistent and transparent treatment of the justified needs of the sector actors, it is considered necessary to develop an agreed classification of user requirements and its relation to the provision of security in information systems.

It is also considered important to identify requirements for legislation, regulations and codes of practice in the light of an assessment of trends in service characteristics and technology, to identify alternative strategies for meeting the objectives by administrative, service, operational and technical provisions, and to assess the effectiveness, user friendliness and costs of alternative security options and strategies for information systems for users, service providers and operators.

## **Action Line III - Solutions for immediate and interim needs of users, suppliers and service providers**

### ***Issues***

At present it is possible to protect adequately computers from unauthorised access from the outside world by "isolation", ie by supplying conventional organisational and physical

measures. This applies also to electronic communications within closed user group operating on a dedicated network. The situation is very different if the information is shared between user groups or exchanged via a public, or generally accessible, network. Neither the technology, terminals and services nor the related standards and procedures are generally available to provide comparable security for information systems in these cases.

### ***Objectives***

The objective has to be to provide, at short notice, solutions which can respond to the most urgent needs of users, service providers and manufacturers. This includes the use of common IT-security evaluation criteria. These should be conceived as open towards future requirements and solutions.

### ***Status and trends***

Some user groups have developed techniques and procedures for their specific use responding, in particular, to the need for authentication, integrity and non-repudiation. In general, magnetic cards or smart cards are being used. Some are using more or less sophisticated cryptographic techniques. Often this implied the definition of user-group specific "authorities". However, it is difficult to generalise these techniques and methods to meet the needs of an open environment.

ISO is working on OSI Information System Security (ISO DIS 7498-2) and CCITT in the context of X400. It is also possible to insert security segments into the messages. Authentication, integrity and non-repudiation are being addressed as part of the messages (EDIFACT) as well as part of the X400 MHS.

At present, the Electronic Data Interchange (EDI) legal framework is still at the stage of conception. The International Chamber of Commerce has published uniform rules of conduct for the exchange of commercial data via telecommunications networks.

Several countries (eg Germany, France, the United Kingdom and the United States) have developed, or are developing, criteria to evaluate the trustworthiness of IT and telecommunication products and systems and the corresponding procedures for conducting evaluations. These criteria have been co-ordinated with the national manufacturers and will lead to an increasing number of reliable products and systems starting with simple products. The establishment of national organisations which will conduct evaluations and offer certificates will support this trend.

Confidentiality provision is considered by most users as less immediately important. In the future, however, this situation is likely to change as advanced communication services and, in particular, mobile services will have become all-pervasive.

### ***Requirements, options and priorities***

It is essential to develop as soon as possible the procedures, standards, products and tools suited to assure security both in information systems as such (computers, peripherals) and in public communications networks. A high priority should be given to authentication, integrity and non-repudiation. Pilot projects should be carried out to establish the validity of the proposed solutions. Solutions to priority needs on EDI are looked at in the TEDIS programme within the more general content of this action plan.

## **Action line IV - Development of specifications, standardisation, evaluation and certification in respect of the security of information systems**

### ***Issues***

Requirements for the security of information systems are pervasive and as such common specifications and standards are crucial. The absence of agreed standards and specifications for IT security may present a major barrier to the advance of information-based processes and services throughout the economy and society. Actions are also required to accelerate the development and use of technology and standards in several related communication and computer network areas that are of critical importance to users, industry and administrations.

### ***Objective***

Efforts are required to provide a means of supporting and performing specific security functions in the general areas of OSI, ONP, ISDN/IBC and network management. Inherently related to standardisation and specification are the techniques and approaches required for verification, including certification leading to mutual recognition. Where possible, internationally agreed solutions are to be supported. The development and use of computer systems with security functions should also be encouraged.

### ***Status and trends***

The United States, in particular, has taken major initiatives to address the security of information systems. In Europe the subject is treated in the context of IT and telecommunications standardisation in the context of ETSI and CEN/CENELEC in preparation of CCITT and ISO work in the field.

In view of growing concern, the work in the United States is rapidly intensifying and both vendors and service providers are increasing their efforts in this area. In Europe, France, Germany and the United Kingdom have independently started similar activities, but a common effort corresponding to the United States is evolving only slowly.

### ***Requirements, options and priorities***

In the security of information systems there is inherently a very close relationship between regulatory, operational, administrative and technical aspects. Regulations need to be reflected in standards, and provisions for the security of information systems need to comply in a verifiable manner to the standards and regulations. In several aspects, regulations require specifications which go beyond the conventional scope of standardisation, ie include codes of practice. Requirements for standards and codes of practice are present in all areas of security of information systems, and a distinction has to be made between the protection requirements which correspond to the security objectives and some of the technical requirements which can be entrusted to the competent European standards bodies (CEN/CENELEC/ ETSI).

Specifications and standards must cover the subjects of security services of information systems (personal and enterprise authentication, non-repudiation protocols, legally acceptable electronic proof, authorisation control), their communication services (image communication privacy, mobile communications voice and data privacy, data and image data-base protection, integrated services security), their communication and security management (public/private key system for open network operation, network management protection, service provider

protection) and their certification (assurance criteria and levels, security assurance procedures for secure information systems).

## **Action line V - Technological and operational developments in the security of information systems**

### ***Issues***

Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future requirements for the security of information systems is a prerequisite for the development of the services market and the competitiveness of the European economy as a whole.

Any technological developments in the security of information systems will have to include both the aspects of computer security and security of communications as most present-day systems are distributed systems, and access to such systems is through communications services.

### ***Objective***

Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future requirements for the security of information systems.

### ***Requirements, options and priorities***

Work on security of information systems would need to address development and implementation strategies, technologies, and integration and verification.

The strategic R&D work would have to cover conceptual models for secure systems (secure against compromise, unauthorised modifications and denial of service), functional requirements models, risk models and architectures for security.

The technology-oriented R&D work would have to include user and message authentication (eg through voice-analysis and electronic signatures), technical interfaces and protocols for encryption, access control mechanisms and implementation methods for provable secure systems.

Verification and validation of the security of the technical system and its applicability would be investigated through integration and verification projects.

In addition to the consolidation and development of security technology, a number of accompanying measures are required concerned with the creation, maintenance and consistent application of standards, and the validation and certification of IT and telecommunication products with respect to their security properties, including validation and certification of methods to design and implement systems.

The third RD&T Community Framework Programme might be used to foster co-operative projects at precompetitive and prenormative levels.

## **Action line VI - Provision of security of information systems**

### ***Issues***

Depending on the exact nature of the security features of information systems, the required functions will need to be incorporated at different parts of the information system including terminals/computers, services, network management to cryptographic devices, smart cards, public and private keys, etc. Some of these can be expected to be embedded in the hardware or software provided by vendors, while others may be part of distributed systems (eg network management), in the possession of the individual user (eg smart cards) or provided from a specialised organisation (e. g. public/private keys).

Most of the security products and services can be expected to be provided by vendors, service providers or operators. For specific functions, eg the provision of public/private keys, auditing authorisation, there may be the need to identify and mandate appropriate organisations.

The same applies for certification, evaluation and verification of quality of service which are functions which need to be addressed by organisations independent of the interests of vendors, service providers or operators. These organisations could be private, governmental or licensed by government to perform delegated functions.

### ***Objective***

In order to facilitate a harmonious development of the provision of security of information systems in the Community for the protection of the public and of business interests, it will be necessary to develop a consistent approach as to its provision of security. Where independent organisations will have to be mandated, their functions and conditions will need to be defined and agreed and, where required, embedded into the regulatory framework. The objective would be to come to a clearly defined and agreed sharing of responsibilities between the different actors on a Community level as a prerequisite for mutual recognition.

### ***Status and trends***

At present, the provision of security of information systems is well organised only for specific areas and limited to addressing their specific needs. The organisation on a European level is mostly informal, and mutual recognition of verification and certification is not yet established outside closed groups. With the growing importance of the security of information systems, the need for defining a consistent approach to the provision of security for information systems in Europe and internationally is becoming urgent.

### ***Requirements, options and priorities***

Because of the number of different actors concerned and the close relations to regulatory and legislative questions, it is particularly important to pre-agree on the principles which should govern the provision of the security of information systems.

In developing a consistent approach to this question, one will need to address the aspects of identification and specification of functions requiring, by their very nature, the availability of some independent organisations (or interworking organisations). This could include functions such as the administration of a public/private key system.

In addition, it is required to identify and specify, at an early stage, the functions which in the public interest need to be entrusted to independent organisations (or interworking



organisations). This could, for example, include auditing, quality assurance, verification, certification and similar functions.



## **ANNEX 2: RECOMMENDATION OF THE COUNCIL OF THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)**

### **CONCERNING GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS**

26 November 1992

**THE COUNCIL,**

**HAVING REGARD TO:**

the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, articles 1 (b), 1 (c), 3 (a) and 5 (b) thereof;

the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [C(85)139, Annex];

**RECOGNISING:**

the increasing use and value of computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance (all hereinafter referred to collectively as information systems);

the international nature of information systems and their world-wide proliferation;

that the increasingly significant role of information systems and growing dependence on them in national and international economies and trade and in social, cultural and political life call for special efforts to foster confidence in information systems;

that, in the absence of appropriate safeguards, data and information in information systems acquire a distinct sensitivity and vulnerability, as compared with paper documents, due to risks arising from available means of unauthorised access, use, misappropriation, alteration, and destruction;

the need to raise awareness of risks to information systems and of the safeguards available to meet those risks;

that present measures, practices, procedures and institutions may not adequately meet the challenges posed by information systems and the concomitant need for clarity, predictability, certainty, and uniformity of rights and obligations, of enforcement of rights, and of recourse and redress for violation of rights relating to information systems and the security of information systems;

the desirability of greater international co-ordination and co-operation in meeting the challenges posed by information systems, the potential detrimental effects of a lack of co-ordination and co-operation on national and international economies and trade and on participation in social, cultural and political life, and the common interest in promoting the security of information systems;

**AND FURTHER RECOGNISING:**

that the Guidelines do not affect the sovereign rights of national governments in respect of national security and public order (“ordre public”) subject always to the requirements of national law;

that, in the particular case of federal countries, the observance of the Guidelines may be affected by the division of powers in the federation;

**RECOMMENDS THAT MEMBER COUNTRIES:**

1. establish measures, practices and procedures to reflect the principles concerning the security of information systems set forth in the Guidelines contained in the Annex to this Recommendation, which is an integral part hereof;
2. consult, co-ordinate and co-operate in the implementation of the Guidelines, including international collaboration to develop compatible standards, measures, practices and procedures for the security of information systems;
3. agree as expeditiously as possible on specific initiatives for the application of the Guidelines;
4. disseminate extensively the principles contained in the Guidelines;
5. review the Guidelines every five years with a view to improving international co-operation on issues relating to the security of information systems.

Annex to the Recommendation of the Council of 26 November 1992  
GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

26 November 1992

I. AIMS

The Guidelines are intended:

- To raise awareness of risks to information systems and of the safeguards available to meet those risks;
- To create a general framework to assist those responsible, in the public and private sectors, for the development and implementation of coherent measures, practices and procedures for the security of information systems;
- To promote co-operation between the public and private sectors in the development and implementation of such measures, practices and procedures;
- To foster confidence in information systems and the manner in which they are provided and used;
- To facilitate development and use of information systems, nationally and internationally; and
- To promote international co-operation in achieving security of information systems.

II. SCOPE

The Guidelines are addressed to the public and private sectors.

The Guidelines apply to all information systems.

The Guidelines are capable of being supplemented by additional practices and procedures for the provision of the security of information systems.

III. DEFINITIONS

For the purposes of these Guidelines:

- "data" means a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means;
- "information" is the meaning assigned to data by means of conventions applied to that data;
- "information systems" means computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance;
- availability means the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner;

- confidentiality means the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner;
- integrity means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

#### IV. SECURITY OBJECTIVE

The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.

#### V. PRINCIPLES

##### **1. Accountability Principle**

The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

##### **2. Awareness Principle**

In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

##### **3. Ethic Principle**

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

##### **4. Multidisciplinary Principle**

Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.

##### **5. Proportionality Principle**

Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

##### **6. Integration Principle**

Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.

##### **7. Timeliness Principle**

Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security of information systems.

## **8. Reassessment Principle**

The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

## **9. Democracy Principle**

The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

# **VI. IMPLEMENTATION**

Governments, the public sector and the private sector should take steps to protect information systems and to provide for their security in accordance with the Principles of the Guidelines. In achieving the Security Objective and in implementing the Principles, they are urged, as appropriate, to establish and to encourage and support the establishment of legal, administrative, self-regulatory and other measures, practices, procedures and institutions for the security of information systems. Where provision has not already been made, they should, in particular:

### **Policy Development**

- Adopt and encourage the adoption of appropriate policies, laws, decrees, rules, and international agreements, including provision for:
  - harmonised world-wide technical standards, methods and codes of practice;
  - promotion of expertise and best practice in the security of information systems;
  - formation and validity of contracts and other documents created and executed in or by means of information systems;
  - allocation of risks and liability for failures of the security of information systems;
  - penal, administrative or other sanctions for misuse of information systems;
  - jurisdictional competence of courts, including rules on extraterritorial jurisdiction, and administrative competence of other bodies;
  - mutual assistance, extradition and other international co-operation in matters relating to the security of information systems; and
  - means of obtaining evidence in information systems and the admissibility of such evidence in penal and non-penal legal and administrative proceedings.

### **Education and Training**

- Promote awareness of the necessity for and the goals of security of information systems, including:
  - ethical conduct in the use of information systems; and
  - adoption of good security practices.
- Provide and foster education and training of:
  - developers, owners, providers and users of information systems;

- specialists and auditors of information systems;
- specialists and auditors of security of information systems; and
- law enforcement authorities, investigators, attorneys and judges.

### **Enforcement and Redress**

- Provide accessible and adequate means for the exercise and enforcement of rights arising from the implementation of the Guidelines and for recourse and redress for violations of those rights.
- Provide prompt assistance in procedural and investigative matters relating to breaches of security of information systems.

### **Exchange of Information**

- Facilitate the exchange of information relating to the Guidelines and their implementation.
- Publish generally measures, practices and procedures established in observance of the Guidelines and for the security of information systems.

### **Co-operation**

- On national and international levels, consult, co-ordinate and co-operate between and among governments and the private sector to encourage implementation of the Guidelines and to harmonise as completely as possible measures, practices and procedures for the security of information systems.



## APPENDIX A: REFERENCES

- A Code of Practice for Information Security Management BSI/DISC PD0003 (ISDN 0 580 22536 4), September 1993, London, UK.
- EEC Report "Security in Open Networks", SOGITS Document Nr. 303
- CEN/CENELEC Workshop on Security Aspects of OSI Functional Standards, October 1992. ISO/IEC JTC1/SC18 "User Requirements for Security in TOS", Jan 1990.
- CEN/CENELEC/ETSI Memorandum M-IT-06 "Taxonomy and Directory of European Standardisation Requirements for Information Systems Security", Issue 1.1, October 1993
- CEC/DXIII/B The Electronic Signature Series of Publications:
  - The Key to Mobility, A Reflection Note, Brussels, May 1992
  - Results of the Call for Ideas on the Reflection Note, Brussels, October, 1992
  - Electronic Signature Workshop Report, Brussels, December 1992
- CCITT 1990 X.400 Series of Recommendations, "Message Handling System"
- CCITT 1991 X.509 Directory System Authentication Framework
- ISO 7498-2 (CCITT X.800) "OSI Security Architecture"
- ISO/IEC/CCITT Open Systems Security Frameworks, November 1992
  - Frameworks Overview
  - Authentication Framework
  - Access Control Framework
  - Non-repudiation Framework
  - Integrity Framework
  - Confidentiality Framework
  - Security Audit Framework
- ISO/IEC Study Documents
  - "Interdomain Security Labels", ISO/IEC JTC1/SC27/N792
  - "Guidelines for the Use and Management of TTP Services", ISO/IEC JTC1/SC27/N786
- Trusted Computer Systems Evaluation Criteria, DoD 5200,28-STD, Department of Defense, United States of America, December 1990.
- Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1.2, June 1992.
- NIST Special Publication 500-160 "Report of the International Workshop on Integrity Policy in Computer Information Systems", January 1991.
- ETSI/EWOS X.400 Functional Profile A/3311
- Council Decision concerning the Community Programme in the field of telecommunications technologies - Research and Development in Advanced Communications Technologies in Europe (RACE) - 88/28/EC, Dec. 1987
- Council Decision concerning the European Strategic Programme for Research and Development in IT (ESPRIT) - 88/279/EC, Dec. 1987.
- Communication from the Commission to the Council on Trade EDI Systems (TEDIS) COM (86)/662, Dec. 1986.
- Federal Criteria for Information Technology Security, Volume II, Version 1.0, Dec. 1992, NIST.
- Information Security INFOSEC 92 - Security Investigations, CEC/DGXIII/F/GE1190/GI, Jan 1992.
- Information Security INFOSEC 93 - Security Investigations, CEC/DGXIII/F/IN933448, July 1993.
- IT Security Evaluation Manual - ITSEM, CEC/DGXIII/B/243/93-EN., Version 1.0, September 1993.

- **Minimum Security Functionality Requirements for Multi-User Operating Systems, NIST, Computer Security Division, Issue 1, January 1992.**
- **MITRE Public-Key Infrastructure Study, Final Report, Sept 1993**
- **Scope of the Federal Criteria Project, Joint NIST/NSA Statement, January, 1992**
- **Taxonomy of Security Standardisation, Version 2.0, CEN/ITAEGV/N69, April 1992**
- **The Canadian Trusted Computer Product Evaluation Criteria, Canadian System Security Centre, January 1993**

## APPENDIX B: ABBREVIATIONS

ABS	Automated Breaking System	GSE	Global Security Environment
AI	Artificial Intelligence	GSM	Groupe Special Mobile
AMHS	Automated Message Handling System	IBAG	INFOSEC Business Advisory Group
API	Application Programming Interface	IBC	Integrated Broadband Communication
ATM	Asynchronous Transfer Mode	IEC	International Electrotechnical Commission
BSI	Bundesamt für Sicherheit in der Informationstechnik (D)	IEEE	Institute of Electrical and Electronics Engineers
BSI	British Standards Institute (UK)	INTERPOL	International Police
BT	British Telecom	IPR	Intellectual Property Rights
CASE	Computer Aided System Engineering	IS	Information Security
CCITT	Comité Consultative International Télégraphique et Téléphonique	ISDN	Integrated Services Digital Network
CD	Compact Disc	ISO	International Organisation for Standardisation
CEC	Commission of the European Communities	ITAEGV	IT Advisory Expert Group for Information Security
CEN	Comité Européen de Normalisation	ITSEC	Information Technology Security Evaluation Criteria
CENELEC	Comité Européen de Normalisation Electrotechnique	ITSEF	Information Technology Evaluation Facility
CESG	Communication Electronics Security Group	ITSEM	Information Technology Security Evaluation Manual
COMPUSEC	Computer Security	JTC 1	Joint Technical Committee One
COMSEC	Communication Security	LAN	Local Area Network
COTS	Commercial off the Shelf	LSE	Local Security Environment
CPIC	Canadian Police Information Centre	MHS	Message Handling System
CSBM	Confidence and Security-Building Measure	MOD	Ministry of Defence
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria	NCIC	National Crime Information Centre
DES	Data Encryption Standard	NIST	National Institute of Standards and Technology (US)
DIS	Draft International Standard	ODP	Open Distributed Processing
EC	European Community	OECD	Organisation for Economic Cooperation and Development
ECU	European Currency Unit	ONP	Open Network Provision
EDI	Electronic Data Interchange	OSI	Open System Interconnection
EDIFACT	EDI for Administration, Commerce and Transport	PGP	Pretty Good Privacy (Encryption Software)
EDP	Electronic Data Processing	PIN	Personal Identification Number
ESE	Electronic Security Environment	PNC2	Police National Computer 2 (UK)
ETNO	European Telecommunications Network Operators	R&D	Research and Development
ETSI	European Telecommunication Standards Institute	ROM	Read Only Memory
FBI	Federal Bureau of Investigation (US)	RSA	Rivest, Shamir and Adleman (asymmetric encryption algorithm)
FPR	Fichier des Personnes Recherches	SCSSI	Service Central de la Sécurité des Systèmes d'Information (F)
GDP	Gross Domestic Product	SDH	Synchronous Digital Hierarchy
		SME	Small and Medium Enterprise

<b>SOG-IS</b>	<b>Senior Officials Group - Information Systems Security</b>
<b>SRI</b>	<b>Stanford Research Institute</b>
<b>SSPS</b>	<b>System Security Policy Statement</b>
<b>TA</b>	<b>Technological Assessment</b>
<b>TCSEC</b>	<b>Trusted Computer System Evaluation Criteria</b>
<b>TEDIS</b>	<b>Trade EDI System</b>
<b>TOE</b>	<b>Target of Evaluation</b>
<b>TTP</b>	<b>Trusted Third Party</b>
<b>UN</b>	<b>United Nations</b>
<b>WAN</b>	<b>Wide Area Network</b>

## APPENDIX C: INDEX

- acceptance testing, 87
- access control, 41
- access to security related data, 39
- accessibility, 105
- accreditation, 118
- accreditation of services, 118
- accreditation of TTPs, 85, 119, 137
- Action Lines, 1, 143
- Action Plan, 1
- actors and roles, 51
- advice and instruction versus prohibition, 53
- aggregation, 106
- arbitration, 5
- assurance, 95
- asymmetric encryption, 74
- audit of TTPs, 85, 137
- audit trails, 65
- audits, 67
- authentic naming, 41
- authentication, 17
- authorisation mechanisms, 41
- authority of a digital signature, 49
- availability, 24
- awareness, 50, 121
- bio-technology, 18
- biometrics, 17, 18, 41
- CASE, 93
- certification, 4, 6, 76
- certification of credentials, 54
- chipcards, 71
- choice versus interoperability, 53
- civil acts, 111
- claim of origin, 4, 43, 70
- claim of ownership, 4, 44, 70
- codes of conduct, 119
- commercial and national security, 23
- commercial environment, 108
- Commercial Off The Shelf (COTS), 25
- common practices, 119
- communication crime, 5
- company and organisational law, 111
- competitive advantage, 24
- computer crime laws, 111
- confidence in communication, 19
- confidence in services, 19
- confidentiality level, 74
- confidentiality schemes, 74
- confidentiality services, 4
- confidentiality, user needs, 50
- consistency of procurement practices, 60
- constitutional rights, 111
- consumer protection, 111
- cost of detection, 33
- cost of security, 24, 33
- costs, 24
- counterfeiting, 111
- countermeasures, 24
- credentials, 76
- credit cards, 42
- criminal acts, 111
- data access, 99
- data compression, 106
- Data Encryption Standard (DES), 74
- data exchange, 107
- data held in electronic form, 103
- data protection laws, 111
- demand for certificates, 96
- demand for confidentiality, 50
- demand related issues, 12, 30
- demands for new technological approaches, 98
- deprivation of ownership, 111
- destruction to property, 111
- digital signature, 4, 46, 48, 71
- directories, 4
- dissemination, 106
- distinguished name, 55
- distributed-secret escrow systems, 80
- domains, 37
- durability, 107
- duty of care, 23
- economics of the security, 24
- education and training, 121
- electronic cash, 42
- electronic negotiable documents, 70
- electronic trading, 33
- eliminating harm, 110
- embedded systems, 6
- embedded systems security, 28
- escrow services, 80
- ethical principles, 26
- European Convention of Human Rights, 111
- EUROPOL, 24
- evaluation, 6
- evaluation of applications, 90
- evaluation of communication services, 91
- evaluation of methods and tools, 93
- evaluation of trusted solutions, 86
- evidence, 5, 105
- expectations, 107
- faceprints, 17
- fair exchange of values, 4, 45, 72
- fingerprints, 17
- forgery, 111
- form, 105
- formal evaluation, 59, 87
- four freedoms, 15
- FPR, 23
- fraud, 111
- functionality and assurance, 32
- general issues, 12, 14
- globalisation of the economy, 15
- granularity (meeting differentiated needs), 51
- Green Paper, 2
- hazards, 28
- health-related technology, 100
- human factors, 27
- human rights and the protection of communications, 16

human rights and safety, 19  
 identification, 17  
 identification mechanisms, 41  
 ignorance, 26  
 impact of loss of information, 51  
 impact of theft of information, 51  
 incident containment, 6  
 incident reporting, 6  
 indirect evaluation, 87  
 information security audit, 113  
 innovation, 36  
 INPOL, 23  
 insurance, 115  
 integrity and digital signatures, 79  
 intellectual property rights (s.a. ownership), 111  
 interconnected law enforcement/criminal  
 information systems, 23  
 internal market, 4, 15  
 international mutual recognition, 87  
 international agreements, 118  
 international harmonisation, 87  
 international scale, 23  
 interworking of autonomous confidentiality  
 services, 84, 137  
 interworking of TTPs, 83  
 Is-to-Cost, 25  
 issues (of general nature), 14  
 issues (related to demand), 30  
 issues (related to supply), 69  
 judicial immunity, 111  
 jurisdictional issues, 114  
 key generation, 48  
 key length, 48  
 key management, 4, 74, 76  
 key management service, 79  
 key usage, 78  
 keystroke dynamics, 17  
 lack of care, 26  
 legal framework, 102  
 legal functions of signatures, 48  
 legal principles for digital signatures, 47, 130  
 legal restrictions affecting technical solutions, 112  
 legislation, 118  
 legislative environment, 108  
 liability, 5, 102, 104, 107, 109, 111, 112, 141  
 liability limiting measures, 112  
 libel, 111  
 life-cycle costs, 25  
 lip prints, 17  
 loss assessment, 64  
 LOTOS, 93  
 machine phrenology, 17  
 maintenance of safety and assurance, 97  
 management of openness and protection, 21  
 management of TTPs, 82  
 management services for credentials, 81  
 management services for names, 81  
 mandatory assurance, 24  
 measures to provide information security, 117  
 medical confidentiality, 111  
 mitigating harm, 110  
 mobility, 15  
 modifications to evaluated products, 94  
 motivation to acquire evaluated solutions, 60  
 multi-media, 99  
 mutual confidence and TTPs, 51  
 mutual recognition, 6  
 name assignment, 76  
 names, 54  
 NCIC, 23  
 negligence, 26  
 negotiable documents, 71  
 non-repudiation, 4  
 non-repudiation services, 43, 70  
 non-retinal and retinal blood vessel analysis, 17  
 objective records, 22  
 one-stop, 16  
 Open Distributed Processing (ODP), 21  
 Open Network Provision (ONP), 21  
 Open System Interconnection (OSI), 21  
 openness, 21, 37  
 operating principles of TTPs, 82  
 operational systems accreditation, 61  
 organisation of security, 34  
 organised crime, 23  
 originality, 106  
 ownership, 106  
 ownership of biometric data, 19  
 palm prints, 17  
 pay-per-use, 16  
 performance, 24  
 performance reporting for trusted products, 95  
 persistence, 106  
 physical and procedural issues, 94  
 PNC2, 23  
 policy framework, 117  
 political environment, 108  
 preservation, 105  
 privacy enhancement, 49, 79  
 privacy of biometric data, 19  
 procedural issues, 114  
 process signatures, 47  
 processing facility, 105  
 products and services, 119  
 professional confidentiality, 111  
 protection, 21, 37  
 protection of information in safety critical  
 environments, 27  
 protection of workstation, 48  
 provision of public confidentiality services, 52, 131  
 public digital signature scheme, 49  
 public key, 55  
 quality criteria, 6  
 quasi-material form, 106  
 random (unpredictable) components, 41  
 rationale, 3, 11  
 rationalisation of evaluations, 96  
 re-evaluation, 94  
 re-use, 95  
 recklessness, 26  
 regulation, 118  
 relationships between private parties, 109  
 requirements for action, 3  
 requirements for evaluations, 58  
 responsibilities, 102  
 right to signature, 46, 130

rights, 102  
rights, responsibilities and liabilities issues, 13  
risk analysis and management, 62  
Rivest, Shamir, Adleman (RSA), 74  
safety critical systems, 6  
safety of communication systems, 57  
safety specific methodologies, 66  
Schengen information system, 24  
scope of the evaluation, 95  
scope, definition, 12  
secret key, 55  
sectoral specifics, 36  
security administration, 33  
security and innovation, 35  
security and law enforcement, 23  
security and safety methodologies, 62  
security domains, 22, 37  
security functions, 40  
security hazards, 29  
security incident reporting, 63  
security labelling, 38  
security management, 75  
security methodologies, 35  
security objectives, 35  
security objectives for enterprises, 34  
security of electronically stored information, 56  
security of information systems, definition, 11  
security policy, 35  
security requirements for enterprises, 31  
security requirements for individual users, 39  
security services, 43, 69  
self evaluations, 6, 59, 89  
Senior Officials Group on the Security of Information Systems (SOGIS), 1  
service provision, 50  
signature dynamics, 17  
signature schemes, 73  
single market, 11  
slander, 111  
smart cards, 18  
social acceptance, 17  
social recognition of information crime, 26  
software quality, 96  
specifications, 121  
standardisation, 5  
standardisation of the use of electronic data, 107  
standards, 121  
structure of document, 12  
supplier declarations, 89  
supply related issues, 13, 69  
supra-national and international treaties, 111  
symmetric encryption, 74  
technological change, 98  
technology, 122  
technology assessment, 64  
telecommunications, 99  
teleconferencing, 99  
terrorism, 23  
theft, 111  
time-stamping, 4, 45, 72  
transportation, 100  
trespassing, 111  
Trevi information system, 24  
trust services, 3  
trusted network management, 92  
Trusted Third Parties (TTPs), 4, 75  
trustworthiness of communication, 58  
TTPs (accreditation of, audit of), 85, 137  
TTPs (interworking of), 83  
TTPs (management of), 82  
TTPs (mutual confidence of), 51  
TTPs (operating principles of), 82  
unauthorised disclosure, 111  
universal acceptance of digital signatures, 49, 130  
untraceability, 4, 45, 72  
valuation of information, 67  
vendor declarations, 6, 59  
weak information security, 23  
Z, 93