Standard ECMA-271
2nd Edition - December 1999

ECMA

Standardizing Information and Communication Systems

Extended Commercially Oriented Functionality Class for Security Evaluation (E - COFC)

Phone: +41 22 849.60.00 - **Fax:** +41 22 849.60.01 - **URL:** http://www.ecma.ch - **Internet:** helpdesk@ecma.ch

Standard ECMA-271
December 1999

ECMA

Standardizing Information and Communication Systems

Extended Commercially Oriented Functionality Class for Security Evaluation (E - COFC)

Phone: +41 22 849.60.00 - **Fax:** +41 22 849.60.01 - **URL:** http://www.ecma.ch - **Internet:** helpdesk@ecma.ch

LL ECMA-271.DOC 25-01-00 09,30

Brief History

ECMA published Standard ECMA-205 “Commercially Oriented Functionality Class for Security Evaluation (COFC)“ in December 1993. This standard was a contribution to the ongoing harmonization process for internationally accepted security evaluation criteria, called Common Criteria.

Standard ECMA-205 provided a set of functional criteria, which was based on commercial requirements with the additional intention in mind to make security evaluation easier and therefore more economical. Many world wide operating computer manufacturers supported this approach.

After completion of Standard ECMA-205, ECMA TC36 (IT Security) continued its work to extend the Standard into the area of interconnected systems. This work had to consider network security as well as commercial requirements for secure electronic business and secure electronic shopping and services.

This new standard is based on the COFC and provides additional functionalities for an enterprise internal network of interconnected systems, for secure electronic business within a closed user group, and for secure electronic shopping and services via a communication line or network. The standard takes aspects of protection against misuse, espionage, fraud etc. into account, but also legal aspects to secure business operations against denial of actually performed business actions.

Standard ECMA-271 is called “Extended Commercially Oriented Functionality Class for Security Evaluation (E - COFC)“. The standard is based on ECMA-205 (COFC) and then hierarchically built up with the Enterprise Business class as first layer, the Contract Business Class as second layer and the Public Business Class as third layer.

After completion of Standard ECMA-271 (E-COFC) ECMA TC36 improved the E-COFC Standard to an E-COFC Version 2 (Standard ECMA-271 Second Edition). This new version addresses the usage of the INTERNET in all three sub-classes and incorporates a number of corrections and improvements. The changes were mostly a result of the development of a Protection Profile for the E-COFC Standard. The E-COFC Protection Profile allows the binding of the E-COFC Functional Criteria to the Assurance Criteria of the ISO/IEC/SC27 Common Criteria Standard. The motivation to develop the E-COFC Protection Profile was based on the fact that international mutual acceptance agreements are presently being negotiated. Once these agreements are made, evaluations on the basis of E-COFC and the Common Criteria can be made **and** the results will be accepted in all countries.

The E-COFC Protection Profile for the Public Business Class is published as an ECMA Technical Report (ECMA TR/78).

This second edition of Standard ECMA-271 has been adopted by the ECMA General Assembly of December 1999.

Table of contents

1 Scope

The Extended Commercially Oriented Functionality Class (E - COFC) extends the application of ECMA's class of commercial security functions (Standard ECMA-205), to an environment of network based systems. The identified security requirements specify a minimal set of security functions for interconnected IT systems.

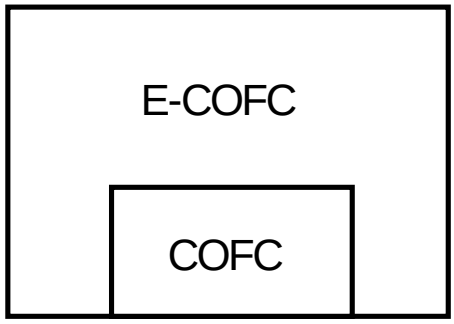

Figure 1 - The ECMA security functionality classes

2 Conformance

A TOE conforms to the requirements of this Standard if it conforms to Standard ECMA-205 **and** to the security functionalities of at least one of the identified classes of this Standard (EB-Class, CB-Class, or PB-Class).

3 References

- ECMA-205:1993 - Commercially Oriented Functionality Class for Security Evaluation (COFC)
- "Trusted Computer Systems Evaluation Criteria", DoD 5200.28-STD, Department of Defense, United States of America, December 1985
- "Information Technology Security Evaluation Criteria (ITSEC) - Harmonized Criteria of France, Germany, the Netherlands, and the United Kingdom", Version 1.2, June 1991
- "Information Technology Security Evaluation Manual (ITSEM)", Provisional Harmonized Methodology, European Commission, Directorate-General XIII, telecommunications, Information Market and Exploitation of Research, September 1993
- "The Canadian Trusted Computer Product Evaluation Criteria", Canadian System Security Center, Communications Security Establishment, Government of Canada, Version 3.0e, January 1993
- "Federal Criteria for Information Technology Security", Volume 1 and Volume 2, National Institute of Standards and Technology & National Security Agency, December 1992
- "Common Criteria for Information Technology Security Evaluation", Version 1.0, CCEB, 1996
- "Requirements for Security during Electronic Information Exchange", R. Barzel, AFNOR, 1995
- "SET, Secure Electronic Transactions Specification by Visa/Mastercard" V. 1.0, 1997
- "rfc2196 Network Working Group", B. Fraser, September 1997

4 Definitions

For the purpose of this document the following definitions apply.

4.1 Terms defined in this Standard

4.1.1 EB-class

Enterprise business class, a class of security requirements for network based electronic business relevant to an enterprise (one legal entity).

4.1.2 CB-class

Contract business class, a class of security requirements for network based electronic business relevant to a defined number of enterprises (closed user group) who operate under a contract.

4.1.3 PB-class

Public business class, a class of security requirements for public electronic business.

4.1.4 Regulatory Board

An impartial notary in a closed user group, which mediates or intervenes in conflict situations between the business partners.

4.1.5 Business action

The sending or receiving of information for performing a business (e.g. sending of an order).

4.1.6 Originator

A person sending business information.

4.1.7 Destination

A person receiving business information.

4.1.8 Qualification of Originator and Destination

The company authorization of a person for specific business actions.

4.1.9 Attestation of submission

A notification that business information was submitted.

4.1.10 Attestation of delivery

A notification that business information was delivered.

4.1.11 Attestation of reception by Destination

A notification that the Destination had received the business information.

4.1.12 Commitment of Originator

The Originator’s company authority for specific business actions.

4.1.13 Customer

A business partner buying goods or services.

4.1.14 Provider

A merchant selling goods or services.

4.2 Terms defined in Standard ECMA-205 (COFC)

The following terms are used with the meanings defined in Standard ECMA-205. The definitions are repeated for convenience.

4.2.1 Access right

The ability of a user to access an object.

4.2.2 Administration

The process of controlling security relevant objects. This process is based on the relevant access rights and guided by one or several users.

NOTE:
These users are sometimes called administrators.

4.2.3 Customer-specifiable

A characteristic set of relevant parameters for which a customer can specify different values.

4.2.4 Identification

The process of recognizing a user by the TOE. The user provides specific credentials to the TOE that is known by the TOE and associated with the user. [Ref.: ITSEC]

4.2.5 User identifier, user ID

A string of characters that uniquely identifies a user.

4.3 Terms defined in other documents

Annex C lists applied terms defined in other standardization documents.

5 Acronyms

The following acronyms are used in this document:

CA	Certification Authority
CB-class	Contract Business class
CCO	Credit Card Organization
COFC	Commercially Oriented Functionality Class
E - COFC	Extended - Commercially Oriented Functionality Class
EB-class	Enterprise Business class
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
PB-class	Public Business class
RA	Registration Authority
RB	Regulatory Board
SET	Secure Electronic Transactions Specification
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation [ITSEC]

6 E - COFC

The Extended Commercially Oriented Functionality Class (E - COFC) is an ECMA standard, which specifies security evaluation criteria for interconnected IT systems. The systems are interconnected through a communication network, which is considered à priori not trusted. The systems may be located at different sites, cities or countries, and are connected through leased lines, public networks or private networks.

6.1 Overview

The E - COFC Standard applies to the security of data processing in a commercial business environment, independent of hardware and software platforms of the participating systems. Its functions are selected to satisfy the minimal set of security requirements for typical business applications of interconnected systems.

The E - COFC is based on an IT Security Policy of a commercial enterprise taking typical environmental and organizational constraints into account. As in reality the IT Security Policy is based on a Confidentiality Policy, an Integrity Policy, an Accountability Policy and an Availability Policy (see figure 2). These dedicated policies are enforced by an appropriate IT security architecture which is decomposed into different domains, such as network security, systems security and application security. This IT security architecture provides a specific set of security services and the associated security management. The security services and the security management are based on a specific set of protocols and mechanisms (security enforcing functions) which may be realized by non-cryptographic (access control) and cryptographic means (symmetric methods, public key methods). For consistency and ease of operation, a specific key management may be an integral part of the security management, supporting specific security services and security mechanisms. With respect to the various system services applied, the security management system activates the adequate security enforcing functions. If cryptographic means are applied, the associated keys and parameters are protected, distributed, and revocated such that unauthorized persons can't have access to them.

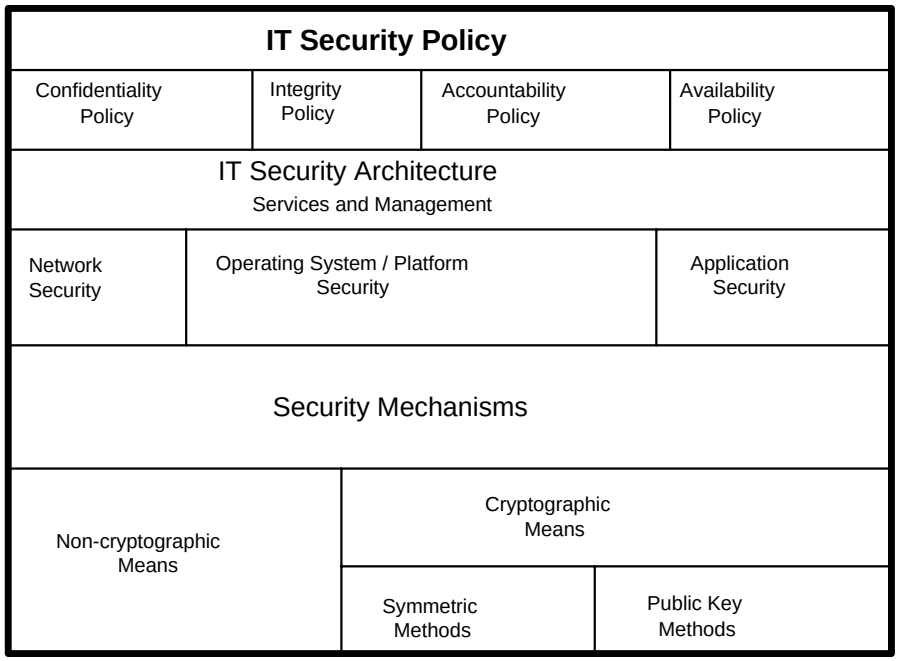

Figure 2 - The different levels of the IT security policy

6.2 The TOE environment

The TOE (Target of Evaluation) is a commercial environment, which consists of several interconnected IT systems. These systems provide on the basis of the installed operating systems different applications and communication facilities for the users and the applications respectively. The installed systems, the communication network and the additionally installed business applications or hardware devices constitute the TOE. The communication network is considered à priori as not secure. The identified minimal security requirements of this standard shall be supported by the TOE but not necessarily by each individual system. The support of the security enforcing functions within a system may be based on the Operating System (OS) or on the combination of the OS and secure hardware or software products.

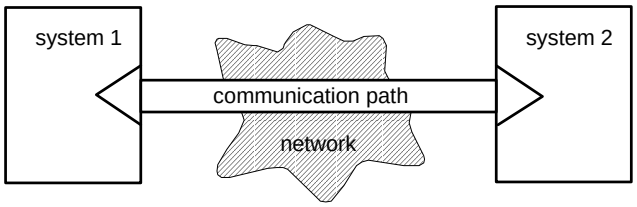

Figure 3 - The TOE model

The TOE environment addresses the following technical constraints:

- A single system is a TOE component consisting of the underlying hardware H and the operating system OS. The ID of the OS is defined by its name (domain name) and its network address. The hardware H is identified by a factory assigned identification number.
- The TOE supports different types of entities such as users and processes. The users execute specific tasks in the system with respect to their different roles in the system environment. The users are accountable for all system activities. A user is registered under the TOE. The TOE generates processes that act on behalf of users. A process requests and consumes resources on behalf of its unique associated user. A process may invoke another process on a different system which is interconnected by the network.

- The TOE may support a network management partitioned into several components, such as the configuration management, the fault management, the performance management and the security management. Although every component contributes to the maintenance of the IT infrastructure, only the security management influences the specified security functionalities. The protocols applied between the network management node and the agent node (retrieving and updating of configuration files) are considered as a special case of a inter-process communication.
- The TOE may support different types of inter-process communication, such as:
  a) Synchronous client server communication: To satisfy a client process, a server process may act as a client to a third process, communicating on the basis of Remote Procedure Calls (RPC).
  b) Asynchronous client server communication: Client and server processes communicate on the basis of message passing.
  c) Dedicated network services: Examples include the File Transfer Protocol Service, the Remote Login or Remote Execute Service, the Network File System, and the Network Information Services.
  d) Different network management protocols, such as Simple Network-Management Protocol (SNMP) or Common Management Information Protocol (CMIP).
- Several users may execute at a given time specific tasks on the same system.
- A user may have remote access to systems of the TOE via a terminal, personal computer, workstation, or laptop.
- The TOE must execute the access control policy of the imposed IT security policy.
- The TOE may support resource sharing such as printer and mass storage on a network.

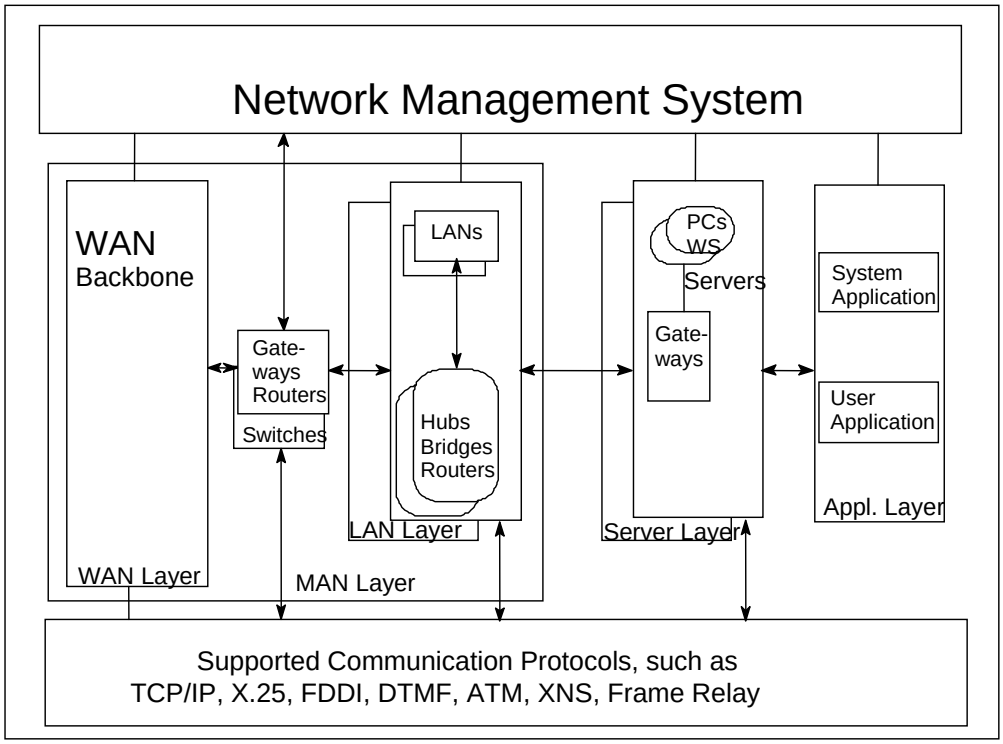

Figure 4 - The TOE environment

6.3 Hierarchical subclasses

With respect to the commercial requirements, the E - COFC is partitioned into the following three hierarchical subclasses of commercial security requirements:

- **The Enterprise Business class (EB-class)** (includes COFC requirements).
- **The Contract Business class (CB-class)** (includes the EB-class and COFC requirements).
- **The Public Business class (PB-class)** (includes the CB-class, EB-class and COFC requirements).

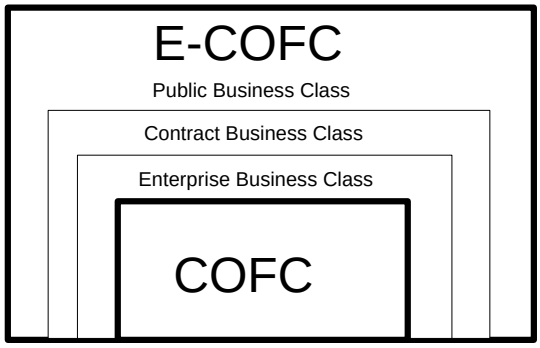

Figure 5 - The hierarchical classes

Each subclass specifies the imposed commercial environment security requirements, the resulting threats and the identified security functionalities. The user of E-COFC has to decide, depending on his actual system and business set up, which of the subclasses meets his requirements. In practice, the subclasses may overlap each other. A minimal set of security functionalities is derived for each subclass to counter the threats. Appropriate countermeasures for each subclass are provided.

Depending to which class the TOE is associated, a baseline set of security requirements for the particular subclass shall be supported by the TOE. If a TOE is associated to two classes the requirements of both classes shall be met. In practice, electronic business actions between business partners are not only based on secure data communication, but also on the provision of legal proof. For example, if a business partner issues an order, the supplier will start actions, which often include major investments, to be able to deliver the ordered goods. The supplier must be able to rely on the electronic data that he received. Since he has no longer a hand-signed paper-document, he must be sure that the received data are authentic and correct. He must have equivalent electronic proof to a hand-signed document to demonstrate to a judge or regulatory board, in case of problems, that a business contract took place. The issuer of the order should not be able to deny that he has sent the order. On the other hand, a supplier who has sent an invoice shall get confirmation that the invoice was received and accepted by the customer. He should have sufficient electronic proof that the customer can not deny the reception of the bill.

Those commercial requirements are the foundation for the CB- and the PB-class, while the EB-class provides the necessary network communication security.

6.4 Usage of the INTERNET

The usage of the INTERNET is allowed in all three subclasses, however, the usage creates vulnerabilities which need special considerations. It is usually necessary to separate the INTERNET access from other business applications, for example by using Virtual Private Networks for the business applications. Alternatively, well configured firewalls and Virus Detection Programs need to be installed to counter the threats. If acceptable to the commercial environment it should be considered to restrict the INTERNET usage to information retrieval and e-mail usage only. Execution of e-mail attached files should be restricted to prevent virus infections. The restrictions shall avoid virus infections, as well as Trojan Horses (e.g. malicious Java applets, malicious Java scripts, malicious Active X). This can be achieved by organizational measures (policies, procedures) and technical measures (Ref.: "rfc 2169 Network Working Group").

7 The Enterprise Business class (EB-class)

7.1 The model

The following characteristics have been identified for the EB-class:

All users are employees of a single enterprise (legal entity). The usage of the IT systems which are part of the TOE is regulated by the employee contract. Only one legal party is responsible for all business actions. In case of outsourcing, the responsibility can be partly delegated to other legal parties on the basis of special contracts. The model describing the enterprise business is shown in the following figure:

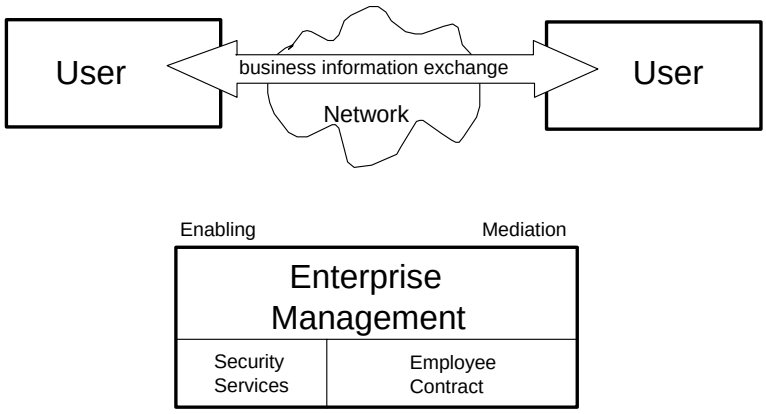

Figure 6 - The enterprise business model

The exchange of business information is done on behalf of the involved system users. The security of the exchange is enabled by the security services provided by management. Conflict mediation is provided by management actions on the basis of the employee contracts.

7.2 Commercial security requirements

The following paragraphs list the required capabilities the TOE shall provide to meet the IT security policy for the exchange of business information. These requirements are in addition to the requirements of ECMA-205 (COFC).

7.2.1 Secure user authentication

Secure authentication is required for the information exchanged between the user and the target system.

7.2.2 Secure client/server communication

Secure data exchange over the network shall be maintained throughout the communication. This includes the authenticity, integrity, and confidentiality of the exchanged information to prevent unauthorized disclosure.

7.2.3 Software integrity

Software integrity on all involved systems shall be maintained throughout the operation.

7.2.4 Availability and reliability

Availability and reliability shall meet the specified customer requirements to ensure that system- and business data can be restored in acceptable time to maintain the business processes.

7.2.5 Accountability and audit

Accountability mechanisms shall be in place to enable holding users accountable for their actions with respect to contract relations and legal issues. In particular, timing information shall be collected in such a way that actions on different systems can be related.

7.3 Threat analysis

The following types of threats have been identified for the Enterprise business class:

Table 1 - Identified threats and countermeasures

	Threat	Countermeasure
1	Unauthorized modification of transmitted data (accidental, intentional)	• Content integrity checking of transmitted data
2	Unauthorized deletion of transmitted data (accidental, intentional)	• Content integrity checking of transmitted data
3	Unauthorized insertion of transmitted data (accidental, intentional)	• Content integrity checking of transmitted data • Sequence integrity checking of transmitted data

Table 1 - Identified threats and countermeasures (continued)

4	Impersonation of an entity (sender/receiver) involved in a communication process	• Authentication of sender and receiver address
5	Unauthorized disclosure of information during transmission (this may result also in a penetration of a trusted path between a user and a login schema)	• Transmission confidentiality
6	Replay of transmitted data	• Sequence integrity checking of transmitted data
7	Blockage of data exchanged between two systems	• Usage of alternative channels
8	Rising communication traffic to decrease the system performance	• Filtering
9	Connection setup or transmission failure	• Authentication of sender and receiver address • Physical protection of communication devices • Recovery procedures • Alternate routes
10	Unauthorized modification of stored or processed data (accidental, intentional)	• Authentication • Access control • Recovery • Integrity checking
11	Unauthorized deletion of stored or processed data (accidental, intentional)	• Authentication • Access control • Recovery • Integrity checking
12	Unauthorized insertion of stored or processed data (accidental, intentional)	• Authentication • Access control • Recovery • Integrity checking
13	Unauthorized disclosure of information (user information, system information)	• Authentication • Access control • Object Reuse • Accountability
14	System failure	• Recovery • Backup
15	Physical damage (accidental, intentional)	• Recovery • Backup • Physical protection
16	Outsider attack: Unauthorized access to the TOE to penetrate system information	• Accountability • Authentication • Access control • Virus checking • Flow Control (Firewall)
17	Denial of service (application, network services, malicious code import (trojan horse)	• Accountability • Physical protection • Authentication • Access control • Virus checking • Flow Control (Firewall) • Resource usage control

Table 1 - Identified threats and countermeasures (continued)

18	Bootstrap compromise or unauthorized replacement of privileged subsystems (installation of a spoofing operating system)	• Physical protection • System verification
19	Unauthorized access by impersonation	• Content integrity checking of exchanged authentication data • Sequence integrity checking of exchanged authentication data • Replay attack detection mechanism • Authentication • Accountability
20	Insider attack: Unauthorized access by authorized user	• Accountability • Access control

7.4 Security functionalities

7.4.1 Identification and authentication

7.4.1.1 Unique identification and authentication (ECMA-205, 6.1.1)

The TOE shall uniquely identify and authenticate users except in the case of anonymous users whose interactions shall be restrictable to a customer defined set of tasks.

7.4.1.2 Identification and authentication prior to all other interactions (ECMA-205, 6.1.2)

Identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication.

7.4.1.3 Secure authentication protocol

The TOE shall support a secure authentication protocol. The applied protocol shall verify the content integrity of the sender and receiver address. In addition the applied protocol shall prevent replay attacks and protect against interception.

If the networks are under full physical control of the enterprise, non-cryptographic techniques may be applied. Otherwise cryptographic techniques shall be applied.

7.4.1.4 Associate Information to users (ECMA-205, 6.1.3)

A mechanism shall be available for administration to associate customer-defined information, e.g. user name and affiliation with each user.

7.4.1.5 Logon message (ECMA-205, 6.1.4)

The TOE shall provide an advisory warning message upon TOE entry regarding unauthorized use, and the possible consequences of failure to meet those requirements. The message shall be customer-specifiable to meet their own requirements and state laws.

Upon successful session establishment, the TOE shall display the date, time, method, location of the last successful session establishment to the user. Upon successful session establishment, the TOE shall display the date, time, method, location of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

7.4.1.6 Number of logon trials (ECMA-205, 6.1.5)

1. The TOE logon procedure shall exit and end the session if the user authentication procedure is incorrectly performed a customer-specifiable number of times within a logon session.
2. The TOE shall provide a mechanism to immediately notify administration when the threshold is exceeded.
3. When the above threshold is exceeded, a customer-specifiable interval of time shall elapse before the logon procedure can be restarted on that I/O port.
4. The TOE shall not suspend the user upon exceeding the above threshold.

7.4.1.7 Expiration of unused user IDs (ECMA-205, 6.1.6)

The TOE shall allow the customer to specify an action which is taken by the TOE after a period of time during which the user was not logged on. The time-period shall be customer-specifiable. As an example, the following actions may be provided:

- disabling the access of the user to the TOE,
- alerting administration.

7.4.1.8 Session lock or terminate

The TOE shall support a session lock. The TOE shall provide an idle process monitor for each front-end which inhibits after a customer defined amount of time user interactions except user authentication.

7.4.1.9 Disable users temporarily (ECMA-205, 6.1.7)

The TOE shall allow administration to temporarily disable a user accessing the TOE.

7.4.1.10 User status information (ECMA-205, 6.1.8)

A mechanism shall be available for administration to provide the status, e.g. active, inactive etc. of any user.

7.4.1.11 Authentication information protection (ECMA-205, 6.1.9)

The TOE shall protect the integrity of the stored authentication information and the confidentiality of any associated secrets.

7.4.1.12 Authentication information sharing (ECMA-205, 6.1.10)

User-provided authentication information need not be unique. For example: two users may provide the same password, however the TOE shall not indicate the presence or absence of such duplicated authentication information.

7.4.1.13 Authentication information aging (ECMA-205, 6.1.11)

If the authentication information is not biometric, the TOE shall provide a mechanism which enforces periodic changes. The time-period shall be customer-specifiable..

7.4.2 Access Control

7.4.2.1 Authenticated user identification (ECMA-205, 6.2.1)

Control of access to objects shall only be granted to authenticated users, e.g. through an authenticated user identifier.

7.4.2.2 Individual user (ECMA-205, 6.2.2)

The TOE shall be able to distinguish and administer access rights between each user and the objects which are subject to the administration of access rights. It shall be possible to grant the access rights down to the granularity of an individual user.

7.4.2.3 User groups (ECMA-205, 6.2.3)

The TOE shall be able to distinguish and administer access rights between each user group and the objects which are subject to the administration of access rights on the basis of membership to a group of users. It shall be possible to grant the access rights down to the granularity of an individual group.

7.4.2.4 Objects (ECMA-205, 6.2.4)

Distinct security relevant objects shall be subject to the administration of access rights:

- The objects of one user to protect them from any other user and their objects.
- The objects of the TOE (security relevant objects) to protect them from any user and their objects.

To allow functional separation of administrative users it shall be possible to grant access rights to individual security relevant objects to different users.

As an example the following security relevant objects may be subject to the administration of access rights:

- The identification and authentication mechanisms objects.
- The access control mechanisms objects.
- The accountability mechanisms objects for non-administrative tasks.

- The accountability mechanisms objects for administrative tasks.
- The audit mechanisms objects.

7.4.2.5 Types of access rights (ECMA-205, 6.2.5)

The TOE shall support at least these access right types:

- Read: Allows to read but not to modify a protected object.
- Modify: Allows to read and to modify a protected object.

7.4.2.6 Default access rights (ECMA-205, 6.2.6)

The TOE shall provide a mechanism to specify default access rights for users not otherwise specified either explicitly or implicitly by group membership.

7.4.2.7 Precedence of access rights (ECMA-205, 6.2.7)

The precedence rules shall be clear and unambiguous.

As an example the following rules are provided:

- The access rights associated with an individual user take precedence over the access rights associated with any group of which that user is a member.
- The access rights associated with any group of which a user is a member take precedence over any default access rights for that user.

For TOE's where a user can be member of multiple groups simultaneously, if any group entry allows an access right for that user, then the user is allowed that right.

7.4.2.8 Date of modification (ECMA-205, 6.2.8)

The TOE shall be able to provide the date and the time of the last modification to objects which are subject to the administration of rights.

7.4.2.9 Verification of rights (ECMA-205, 6.2.9)

With each attempt of users or user groups to access objects which are subject to administration of rights, the TOE shall verify the validity of the request. Unauthorized access attempts shall be rejected.

7.4.2.10 Application controlled access rights (ECMA-205, 6.2.10)

The TOE shall provide the capability to allow access to the TOE via specific customer-defined applications, such that the application's access control security policies take precedence over the access rights of the invoking user.

7.4.3 Client / server communication

7.4.3.1 Content integrity of exchanged information

When two systems are exchanging information the integrity of the information content shall be verified.

7.4.3.2 Address integrity of exchanged information

When two systems are exchanging information the integrity of the sender and receiver address shall be verified. The applied protocol shall prevent replay attacks.

7.4.3.3 Confidentiality of exchanged information

When two systems are exchanging information the TOE shall support the confidentiality of the exchanged information against unauthorized disclosure.

7.4.4 Accountability and audit

7.4.4.1 Associate actions and users (ECMA-205, 6.3.1)

For every interaction the TOE shall be able to establish the identity of the user.

7.4.4.2 Logging (ECMA-205, 6.3.2)

The TOE shall contain an accountability component which enables the system administration to log each of the events specified in ECMA-205, 6.3.2.1 to 6.3.2.4 with the required data to provide sufficient information

for a posterior investigation. Note: The logging of accountability data may be done on the system where the action takes place, but may also be under central control.

7.4.4.3 Use of identification and authentication mechanism (ECMA-205, 6.3.2.1)

The TOE shall log at least logons and security-related activities of administration.

Administration shall have the capability to enable or disable the logging of other events which include at a minimum:

1. Valid and invalid user authentication attempts.

7.4.4.4 Attempts to exercise access rights (ECMA-205, 6.3.2.2)

The TOE shall log at least each of the following events:

1. Unsuccessful data or transaction access attempts.

Administration shall have the capability to enable or disable the logging of other events which include at a minimum:

1. Disk file access.
2. Tape volume or tape file access.
3. Program execution.
4. On-line execution of commands which are security relevant.

7.4.4.5 Creation or deletion of an object which is subject to the administration of rights (ECMA-205, 6.3.2.3)

Administration shall have the capability to enable or disable the logging of other events which include at a minimum:

1. Creation and deletion of an object.

7.4.4.6 Actions by authorized users affecting the security of the TOE (ECMA-205, 6.3.2.4)

The TOE shall log at least each of the following events:

1. Introduction or deletion (suspension) of users.
2. Introduction or removal of storage data.
3. Start up or shut down of the TOE.
4. Changes to user's security profiles, administration or attributes.
5. Changes to system security parameters (not listed in COFC)

7.4.4.7 Logged information (ECMA-205, 6.3.2.5)

For each of the events specified in ECMA-205, 6.3.2.1 to 6.3.2.4 the TOE shall log the following information:

1. Date.
2. Time.
3. User identifier.
4. Type of event.
5. Name of object.
6. Type of access attempt.
7. Success or failure of the attempt.

7.4.4.8 TOE restart (ECMA-205, 6.3.3)

Accountability control information shall survive restart of the TOE.

7.4.4.9 Copy audit trails (ECMA-205, 6.3.4)

The TOE shall provide a mechanism for automatic copying of audit trail files to a customer-specifiable storage medium after a customer-specifiable period of time.

7.4.4.10 Alarm if unable to record (ECMA-205, 6.3.5)

The TOE shall generate an alarm to the authorized administrator if the size of the audit data in the audit trail exceed a pre-defined limit. The TOE shall provide the authorized administrator with the ability to manage the audit trail at any time during the operation of the TOE.

7.4.4.11 Select users (ECMA-205, 6.3.6)

It shall be possible to selectively account for the actions of one or more users.

7.4.4.12 Dynamic control (ECMA-205, 6.3.7)

Administration should be able to dynamically display and modify the types of events recorded during normal TOE operation. This control shall include selective disabling of the recording of default audit events and the enabling and disabling of other optional events.

7.4.4.13 Audit tools (ECMA-205, 6.3.8)

Tools to examine the audit trail for the purpose of audit shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

7.4.4.14 Synchronization

Specific synchronization features for the audit data shall be supported. At a minimum the relation of local clocks shall be recorded such that causal relations between events on different systems become traceable.

7.4.5 Object reuse

7.4.5.1 Object reuse (ECMA-205, 6.4)

The TOE shall be able to treat all returned storage objects before reuse by other users, in such a way that no conclusion can be drawn regarding the preceding content.

7.4.6 Accuracy

7.4.6.1 TOE software integrity (ECMA-205, 6.5.1)

Procedures, e.g. use of modification dates, checksums etc., shall exist that make it possible to verify that the currently installed TOE has remained consistent with the delivered and installed software.

7.4.6.2 Data integrity (ECMA-205, 6.5.2)

The TOE shall make available a mechanism to verify the integrity of data, e.g. checksum.

7.4.6.3 Security parameters status report (ECMA-205, 6.5.3)

The TOE shall provide a mechanism for administration to generate a status report detailing the values of all customer-specifiable security parameters.

7.4.6.4 Flow Control at the boundaries of the network

The TOE shall provide mechanisms for controlling the boundaries of its network against potentially harmful interactions with partners or intruders from the internet. The control must be able to exclude irregular interference with the commercial environment. Flow control may be based on packet filtering, inbound/outbound restrictions with respect to applications, connection rules, additional authentication requirements, etc.

7.4.7 Availability and reliability of service

7.4.7.1 Recovery (ECMA-205, 6.6.1)

Procedures or mechanisms shall be provided to allow recovery after a TOE failure or other discontinuity.

7.4.7.2 Data Backup (ECMA-205, 6.6.2)

Procedures shall be provided for software and data backup and restoration.

7.4.7.3 Filtering

Filtering procedures shall be provided to prevent performance degradation due to rising communication traffic to an unacceptable level.

7.4.7.4 Transmission blockage

Alternate communication channels shall be provided to recover from transmission blockage.

7.4.7.5 Denial of service

Mechanisms shall be present to mitigate the possibility of intentional denial of service.

7.4.8 Key management (if cryptographic means are applied by the TOE)

7.4.8.1 Key generation

The key generation shall be based on state-of-the-art cryptographic techniques to ensure the unpredictable generation of strong keys.

7.4.8.2 Sufficient key length

The length of the keys shall meet the customers security requirements, e.g. preferable user defined. On the basis of the selection, dedicated cryptographic techniques shall be applied.

7.4.8.3 Key confirmation

The security management shall support a key distribution technique addressing the integrity and confidentiality of the keying information as required.

7.4.8.4 Key validation

On the basis of specific organizational or technical means, the security management shall verify that the keying information has been successfully distributed (Distributed Key Validation Process).

7.4.8.5 Key revocation

The security management shall support the revocation of distributed keys by technical or organizational means (Key Revocation Process).

7.4.8.6 Key backup and archiving

The security management shall support dedicated procedures for the backup and archiving of the keys. These procedures shall ensure that unauthorized persons can’t have access to the keys.

7.4.8.7 Restricted lifetime of keys

The lifetime of keys shall be user definable, depending on the privacy policy of the user or the IT security policy of the enterprise.

8 The Contract Business class (CB-class)

8.1 The model

The CB-class is built on top of the EB-class. It adds to the network security requirements of the EB-class those requirements identified for business information exchange between independent enterprises which constitute a closed user group. The enterprises agree in a contract on a defined mode of operation, the business conditions and the security rules, which are the foundations of their business information exchange. They establish a "Regulatory Board" (RB) which acts as impartial judge to mediate conflicts within the user group and acts also as a "Trust Center" to handle security matters such as key management. All business partners who sign the contract constitute a closed user group. Users shall only get access to the systems if they belong to a business partner that has signed the contract. The business information exchange within the closed user group is described with the following model:

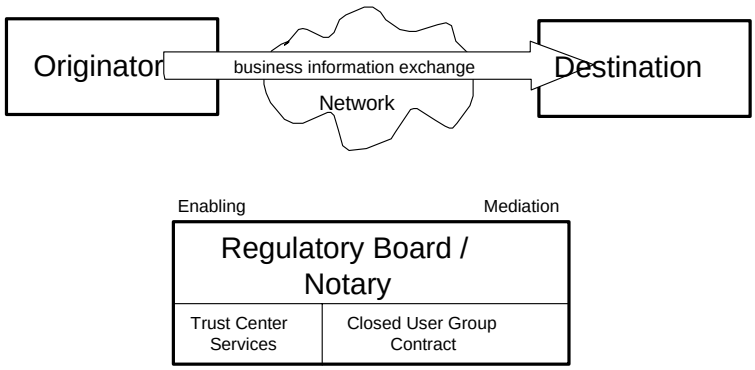

Figure 7 - The contract business model

8.1.1 Exchange of information

The business information is exchanged between the Originator and the Destination. These terms describe functional roles in the business process. The Originator is a user or a process on behalf of a user that sends business information such as a document, order, etc. to a Destination. The Destination is a user or process on behalf of a user that receives the business information and acts on it (e.g. processes an order). If the business information flow is reversed then the Originator becomes the Destination and the Destination becomes the Originator (e.g. for confirmation, invoice, etc.). The Originator and the Destination shall be authorized according to the closed user group contract to perform the business actions. If the information is confidential, the Originator and Destination are users (processes) that are authorized to process the exchanged information. The secure exchange of business information is enabled by Trust Center Services like key generation, key distribution, key revocation, key certification and security logging. The Trust Center Services are under control of the RB. The TOE has to establish a secure basis for various kinds of business. On the basis of the security functions provided by the underlying TOE it has to be accredited that the security requirements of all the business actions stated in the contract of the cooperating enterprises can be fulfilled by the enterprises. The business information may be exchanged using an independent communication service or using a service that belongs to one or more members of the closed user group.

8.1.2 Regulatory Board

The Regulatory Board or Notary is an impartial element in the closed user group. The members of the RB mediate or intervene in conflict situations between the business partners of the closed user group. The RB works on the basis of a contract signed by all legal parties of the closed user group. Organization, independence, limitations and authority of the Regulation Board shall be clearly stated in the contract. The RB acts as an independent organization or office imposing the legal rules on all participating parties. The acceptance of the Regulatory Board is a contractual pre-requisite for all legal parties of the closed user group. Only persons registered by the Regulatory Board may become system users. The Regulatory Board may delegate the administration to the different enterprises but shall keep the overall control.

8.1.3 Closed User Group Contract

The Closed User Group Contract is the legal foundation for the closed user group on which business actions are based. The contract sets the ground rules and business conditions for the organization, the mode of operation, the security policy, the conflict management, the control- and audit-power, as well as duties and responsibilities of the Regulatory Board. It defines the legal (contractual) relations to other partners (e.g. communication service). It specifies the conditions for joining the closed user group, the business actions under its control, and the relevant services. If cryptographic services are required, the appropriate services and algorithms shall be specified to ensure that no breach of confidentiality can take place during the information exchange. The processes and mechanisms to be used and the conditions under which they operate shall be specified in the contract. The contract shall at least address the following areas:

- Organization of the Regulatory Board
- Liability regulations of installed systems
- Definition of business actions and their security requirements

- IT security policy, including:
  - Confidentiality
  - Accountability and audit
  - Availability and reliability
  - Integrity
- Change management
- Elaboration of proof

8.1.3.1 Organization of the Regulatory Board

The Regulatory Board has to be established by the members of the closed user group. The closed user group contract shall define the constitution of the Regulatory Board, its legal position and the membership conditions.

8.1.3.2 Definition of business actions and their security requirements

The contract shall specify the controlled business actions and their relevant security requirements.

8.1.3.3 IT security policy

The contract shall specify the IT security policy addressing the business and legal requirements. It shall provide procedures for the case that the security of the TOE becomes compromised. The selection, protection, management and the replacement or neutralization of lost or expired security elements constitute a critical aspect and shall be fully specified.

8.1.3.4 Accountability and audit

The contract shall define all elements needed for the after-the-fact reconstruction of a business action and the identification of individual accountability. It shall be specified how these elements will be generated, stored and maintained. The contract shall also define the mechanisms to be implemented to order and to correlate events (time stamping) across physical separated systems.

8.1.3.5 Availability and reliability

Availability and reliability mechanisms shall be specified in the contract. Targets and measures to ensure the availability of service, especially back up measures, recovery plans and the storing of business information shall be addressed.

Information exchange reliability has a direct influence on the operational security and consequently on the level of security for the business. Targets and measures to ensure the reliability of service, especially backup measures, recovery plans and the storing of business information shall be addressed.

8.1.3.6 Elaboration of proof

With respect to the identified legal and business requirements the contract shall specify the elements of proof which the TOE shall support. Audit, backup, archiving and replacement issues have to be addressed. It is important to take into account the fact that the elements of proof can become compromised.

8.1.3.7 Change management

System changes shall be done only through a change management process. The change management shall contain organizational and technical procedures indicating areas where security may be effected.

8.2 Commercial security requirements

The following paragraphs list the required capabilities the TOE shall provide for the exchange of business information. These requirements are in addition to the requirements of the EB-class.

8.2.1 Authorization of Originator and Destination

For many business actions the Originator needs à priori assurance of the authorization of the Destination. For example, the Originator of an order assumes, that it can only be received by someone who is authorized to receive and process orders (e.g. the order department). A user is authorized by his company for defined business actions. In addition the authorization of the Originator is required for other business cases.

8.2.2 Attestation of submission

In many cases the Originator needs an attestation of the transport service that the processed business information was successfully submitted. The Originator can then transfer the responsibility for the information transport to the electronic transport service if an attestation of submission is generated.

8.2.3 Attestation of delivery

The attestation of delivery is needed in business actions. It confirms the delivery of information to the transport service of the Destination under the agreed upon conditions such as integrity or confidentiality.

8.2.4 Attestation of reception by Destination

Many business actions require an attestation that the Destination received the business information (for example an invoice) from its transport service.

8.2.5 Commitment of Originator and Destination

A Destination (Originator) may require assurance that the Originator (Destination) is committed regarding the submission and the content of the received information. Such an assurance is often needed before action is taken on the contents. It means that the Originator (Destination) shall not be able to deny the submission or back out on the content of the information.

8.2.6 Chronology of events

Trusted timing information shall be provided with submission of information, attestation of submission, attestation of delivery and attestation of receipt.

8.2.7 Accountability and audit

Audit information shall be stored such that relevant actions with respect to contract relations and legal issues on all involved systems can be analyzed. Stored timing information shall relate actions on different systems.

8.2.8 Document integrity

The document integrity requirements are covered by the EB-class and by ECMA-205 (COFC).

8.2.9 Document confidentiality

The document confidentiality requirements are covered by the EB-class and by ECMA-205 (COFC).

8.3 Threat analysis

The following table lists the threats and countermeasures in addition to those of the EB-class:

Table 2 - Identified threats and countermeasures

	Threat	Countermeasure
1	Denial of submission of business information	• Non-repudiation of Originator
2	Denial of reception of business information	• Attestation of submission • Attestation of reception by Destination • Non-repudiation of Destination
3	Denial of business information content ownership	• Non-repudiation of Originator
4	False routing of business information enabling unauthorized access	• Authentic business role qualification of Originator and Destination (business role authorization)

Table 2 - Identified threats and countermeasures (continued)

5	Inability to mediate disputes between two different parties of the closed user group because of missing timing information and business process related data.	• Logging of relevant requests on behalf of system users for associated business actions such that they can be analyzed with respect to contract relations and legal issues on all involved systems. • Storing of timing information to enable the tracing of business process actions on different systems.

8.4 Security functionalities

The following security requirements have been defined for the CB class which have to be applied in addition to those defined in the COFC and in the E - COFC EB-class. If the TOE only supports a subset of the business actions as shown in Table 4, only the corresponding subset of security requirements shall be fulfilled.

8.4.1 Access control (user authorization)

8.4.1.1 Qualification

Only qualified users shall be able to access the business action services (see also ECMA-205). The business role qualification data of the Originator or Destination shall be automatically distributed.

8.4.1.2 Consistency

Consistency of related access control parameters for business actions shall be provided over all systems.

8.4.2 Accountability and audit

8.4.2.1 Non-repudiation of the Originator

The TOE shall support dedicated mechanisms for the non-repudiation of the Originator.

8.4.2.2 Non-repudiation of the Destination

The TOE shall support dedicated mechanisms for the non-repudiation of the Destination.

8.4.2.3 Attestation of submission, delivery and reception

The transport service shall establish an attestation when information was submitted and an attestation when the information was successfully delivered. The Destination shall send an attestation of reception when information was received under the agreed upon conditions such as integrity or confidentiality. If delivery was not accomplished, the Originator or Destination shall be notified by the transport service for the reasons of failed delivery.

8.4.2.4 Timing information of audit data

Trusted timing information shall be logged for the attestation of submission, attestation of delivery and attestation of reception by Destination.

8.4.2.5 Requirements for the tracing of audit data

Audit information shall be authentically stored such that relevant actions with respect to contract relations and legal issues on all involved systems can be analyzed. The stored timing information shall enable the tracing of business process actions on different systems.

9 The Public Business class (PB-class)

9.1 The model

The PB-class is built on top of the CB-class, which is built on top of the EB-class. It adds on those requirements, which are typical for public business in an open environment (no closed user group). Public business typically covers areas like selling of goods, tickets and other merchandise, but also home banking, insurance, network based information services and others. The terms Customer and Provider are used in this class. A provider system is offering a dedicated service containing a set of business actions. For each business action the term Originator and Destination can be applied as outlined in the CB-class. The business actions are described by the following model:

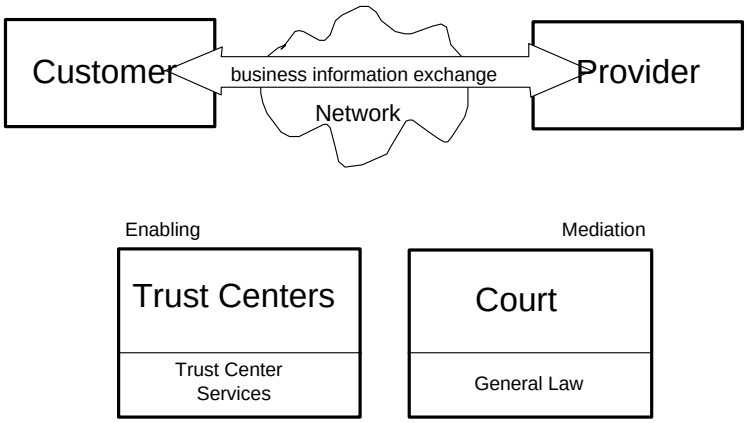

Figure 8 - The public business model

The Public Business class is characterized by business on the basis of pre-existing contracts that legally connect the Provider and the Customer for a set of pre-defined business actions. The Provider or the Customer is a user or a process on behalf of a user that generates, processes, transmits, or receives business information requests. In contrast to the CB-class there is no RB which resolves possible conflicts. Conflicts have to be resolved on the basis of the business or consumer law. Secure business transactions between the Customer and Provider are based on "Trust Centers" (TC) which provide as independent organizations the required key management and distribution services. In contrast to the EB-class and the CB-class the business relationships may be beyond the contractual relationships. Different scenarios of contractual relations are possible. Also in the case of electronic advertising the contracts are provided by business and consumer law. The formal contractual relationship between the Customer and the Provider is either direct or through other business organizations. Annex B shows examples of public business with different contractual relations (see annex B).

9.2 Commercial security requirements

The following paragraphs list the required capabilities the TOE shall provide for different business actions. These requirements are in addition to the requirements of the EB-class and CB-class.

9.2.1 Multistage identification and authentication

The authentication of different legal parties and users depends on the contractual relations and the specific business process actions. At least one of the parties involved in the business process action has to be uniquely identified and authenticated. The multistage identification and authentication process may be executed at different points in time. Timing consistency shall be maintained along the different stages in the verification process for identification and authentication.

9.2.2 Interrelated commitments

The commitment of the Originator to the Destination in a business action is based on interrelated commitments, addressing the contractual relations of the involved legal parties. In most cases the commitment of the Originator is the payment authorization.

9.2.3 Protection against unlawful multiple use of unique data

The uniqueness of data, if required, has to be maintained and preserved along the chain of business actions executed on behalf of the contractual relationships. The unauthorized copying (to produce a falsification) of payment data and receipts shall be prohibited.

9.2.4 Unauthorized building of user profiles from business data

The unauthorized collection of user relevant business data in order to build user profiles shall be prohibited.

9.2.5 Interrelated accountability

The time and causal relation between transactions of a business action shall be recorded and maintained across all involved systems allowing for investigation in case of problems.

9.3 Threat analysis

The following table lists the identified threats in addition to those of the EB-class and the CB-class.

Table 3 - Identified threats and countermeasures

	Threat	Countermeasure
1	Unauthorized modification or replacement of commitment data	• Content integrity checking of transmitted commitment data, business data, and business data with commitment data
2	Unauthorized deletion or insertion of commitment data	• Content integrity checking of transmitted commitment data, business data, and business data with commitment data
3	Unauthorized replay of commitment data	• Sequence integrity checking of commitment data, business data, and business data with commitment data
4	Denial of commitment data ownership	• Non-repudiation of Originator
5	Denial of commitment data submission	• Non-repudiation of Originator
6	Denial of commitment data reception	• Non-repudiation of Destination
7	Unauthorized acceptance of invalid/ invalidated commitment data or certificates	• Content integrity checking and content verification of commitment data, business data, business data with commitment data, or certificates • Up-to-date storage and distribution of digitally signed certificate information • Access Control
8	Unauthorized refusal of valid/validated commitment data or certificates	• Content integrity checking and content verification of commitment data, business data, business data with commitment data, or certificates • Up-to-date storage and distribution of digitally signed certificate information • Access Control
9	Interception of commitment data or certificates	• Restricted lifetime of cryptographic keys, certificates and commitment data • Generation of new keys independent from the broken keys • Transmission of key exchange information independent from the broken keys
10	Theft of business process input data	• Authentication • Access Control • Accountability
11	Disclosure of business data to unauthorized persons	• Authentication • Access Control • Accountability

Table 3 - Identified threats and countermeasures (continued)

12	Unauthorized access on linked privacy data of system users	• Authentication • Access Control • Accountability • Anonymity or pseudonymity mechanisms
13	Unlawful multiple use (e.g. by copying) of unique data	• Uniqueness enforcing functions and uniqueness violation detection measures
14	Untraceable history in case of failures, malfunctioning, or betrayal	• Interrelated accountability
15	Unauthorized tracing of customer business actions (tracing of cookies)	• Access Control • Anonymity or pseudonymity measures

9.4 Security functionalities

9.4.1 Identification and authentication

9.4.1.1 Multistage identification and authentication

For identification and authentication over many stages a chain of trust shall be provided. The system shall be verify this chain to the roots.

9.4.2 Access control

9.4.2.1 Protection against unlawful disclosure

The system shall support state-of-the-art anonymity or pseudonymity measures. Dedicated techniques shall be supported to prevent the unauthorized monitoring of the logged system user's activities.

9.4.3 Accountability and audit

9.4.3.1 Interrelated accountability

The audit data of the interrelated systems shall be authentically stored and shall enable the complete tracing of business transactions between at least two different legal parties.

9.4.3.2 Commitment data ownership and submission

The TOE shall support dedicated mechanisms for the non-repudiation of the Originator (commitment data, business data, commitment data with business data).

9.4.3.3 Commitment data reception

The TOE shall support dedicated mechanisms for the non-repudiation of the Destination (commitment data, business data, commitment data with business data).

9.4.3.4 Uniqueness of original

Security mechanisms, such as watermarking, bill of lading scheme, digital ticketing, etc. shall be provided.

9.4.4 Communication of commitment data

9.4.4.1 Content integrity and content validation of exchanged commitment data or certificates

When two systems are exchanging commitment data or certificates, the integrity and validation of the commitment data, the business data, the commitment data with business data**,** or the certificate content shall be verified.

9.4.4.2 Address integrity of exchanged commitment data or certificates

When two systems are exchanging commitment data or certificates, the integrity of the sender and receiver address shall be verified. The protocol shall prevent replay attacks.

9.4.5 Trust Center security functionalities (key management)

The trust relationship between the different independent business parties is based on notary services which register and manage the associated security information needed. The services of such a notary are based on

cryptographic public key techniques and based on a root for the chain of trust in certificates. The following phases which are based on time stamping services shall be supported:

- Registration,
- Certification,
- Distribution and
- Revocation

9.4.5.1 Registration

The users identity is verified in this process on the basis of reference documents. In addition, a distinguished name for the user and a unique reference number to the user's key, which was authentically transmitted to the registration entity are assigned. The entity responsible for the registration process is called Registration Authority (RA). The RA shall provide adequate means for the authenticity and integrity of the stored registration data. If a user's key has been broken, the new key shall be generated independent from the broken keys. In addition the transmission of key exchange information shall be independent from the broken keys.

9.4.5.2 Certification

The certification process generates the legal binding relation between the business process entity and the credentials used in the business process. The certification process shall at least cover the certification of the user's key and the certification of user's attributes, e.g. this certification can be applied on the basis of the Certification Authority's (CA) digital signature.

Specific security means shall be provided to enable the secure verification of the authentic certificate by an entity, which is part of a business process. The CA shall provide adequate means for the authenticity and integrity of the stored certification data.

9.4.5.3 Distribution

The certificate information shall be authentically distributed. Adequate verification mechanisms shall be provided to ensure that the correct entity has received and verified the distributed certificate.

9.4.5.4 Revocation

The following phases have to be supported for this process: the revocation request, the revocation, and the revocation notification. The revocation request shall process the information of the certificate. Specific security means shall be provided to ensure the authenticity and integrity of a revocation request. After the revocation request has been verified the corresponding CA shall revoke the stored certificate of the entity. A revocation certificate shall be generated containing the original certificate information and additional information such as date of revocation, cause of revocation, entity identification number who has requested the revocation, and the distinguished name of the CA who has executed the revocation. The CA shall provide adequate means for the authenticity and integrity of the stored revocation data.

Annex A

(informative)

Examples for the Contract Business class (CB-class)

Examples of business actions and their security requirements which cover most trade areas are given below. Some areas however, may require additional functions (e.g. health care systems including the exchange of medical data).

Business actions are considered as the transmission of information in a specific digital format from an Originator to a Destination. The transmitted information can fulfill different business purposes. For example, the transmitted document can be a contract, an order, an invoice, a response to call for tender, an offer, a private call for tender, an order-confirmation, a public call for tender, a financial order, or any other business action related information.

The requirements to the TOE may be different for different business information exchange. For example, an order involves a financial commitment of the Originator. The TOE shall ensure that only authorized users shall be able to send or receive orders improving the reliability of the business information exchange. The Destination shall be able to securely identify the Originator, because his acting on the order will involve expenditures. The Destination shall acknowledge the reception of the order (non-repudiation of Destination) since this gives the Originator assurance that the order can be processed in time. Business conditions require the confidential transmission of the information exchanged (for example to counter industrial espionage). Other business actions have less requirements. For example, a public call for tender does not need assurance that only qualified people receive the call, nor does it require the non-repudiation of Destination.

All business actions have requirements to the transport system which are:

- Attestation of submission
- Attestation of delivery
- Attestation of reception by destination
- Return if undeliverable
- Trusted time-stamping

The transport system shall provide evidence that the information was transmitted in time. The attestation of submission, delivery, and attestation of reception by destination gives the Originator of a business action assurance and proof that the business information was transmitted in time. In case business information can not be delivered, it shall be returned to the sender. Trusted time stamping is required on all attestations and shall include time, date, and place of the event.

The following examples describe applications, which are typical for the Contract Business class (CB-class). A single business action may result in several information exchanges.

Example 1: Sending a Contract

The Originator submits contract information in a specific digital format. He is committed to the content of the submitted information. This can be authorized with a digital signature. A follow-on business action may be based on the transmitted information. Only authorized users should be able to send or receive documents of a defined type.

The Originator and Destination require:

- Assurance that the Destination is authorized to receive the information
- Proof that the document was sent in time
- Proof that the information was delivered and received by the Destination in time
- Non-repudiation of Destination
- Information content confidentiality
- Information content integrity
- Trusted time stamping of events
- Attestation of submission, delivery, and reception by Destination of the information exchanged
- Authentication of sender address
- Non-Repudiation of Originator
- Originator commitment

In the postal service this business action is comparable to the sending of a hand-signed letter by registered mail to a qualified address; additionally the delivery is confirmed by the transport service.

Example 2: Order placement

The Originator sends an order to a supplier.

In the postal service this business action is comparable to the sending of a hand-signed letter by registered mail to a qualified address; additionally the delivery is confirmed by the transport service.

The Originator and Destination require:

- Assurance that the Destination is authorized to receive the order
- Attestation of submission, delivery, and reception by Destination of the information exchanged
- Trusted time stamping of events
- Non-Repudiation of Destination
- Information content integrity
- Information content confidentiality
- Authentication of sender address
- Assurance that the order comes from an authorized buyer. This allows when appropriate to send an invoice, which will not be contested, on procedural grounds.
- Authentication of sender address
- Commitment of the Originator to the received information. This commitment allows the delivery according to the terms of the order.
- Non-repudiation of Originator

Example 3: Submitting an offer

The Originator sends an offer to a customer.

The Originator and Destination require:

- Attestation of submission, delivery, and reception by destination of the information exchanged
- Trusted time stamping of events
- Information content confidentiality
- Information content integrity
- Assurance that the Originator is authorized to submit the information
- Trusted time stamping of events
- Authentication of sender address
- Originator commitment

Example 4: Public call for tender

The Originator sends a public call for tender

The Originator and Destination require:

- Attestation of submission, delivery, and reception by Destination of the information exchanged
- Authentication of sender address
- Trusted time stamping of events
- Information content integrity
- Commitment of the Originator

Example 5: Financial order

The Originator (for example a bank customer) and the Destination require:

- Assurance that the financial order is only sent to a qualified Destination
- Attestation of submission, delivery, and reception by Destination of the information exchanged
- Information content integrity
- Information content confidentiality
- Trusted time stamping of events
- Non-repudiation of Destination
- Non-repudiation of Originator
- Assurance of the qualification of the Originator
- Secured identity of the Originator
- Commitment of Originator to the received information

Annex B

(informative)

Examples of Customer/Provider based business (PB-class)

Scenario 1: Customer/Provider public business

This scenario is based on a pre-existing contractual relationship between the Customer and the Provider. The service contract regulates trade conditions (delivery, warranty, copyright, etc.) and the mode of payment (deduction from bank account, payment via credit card organization, mailed invoice, etc.). The applied payment is based on inter bank service relations.

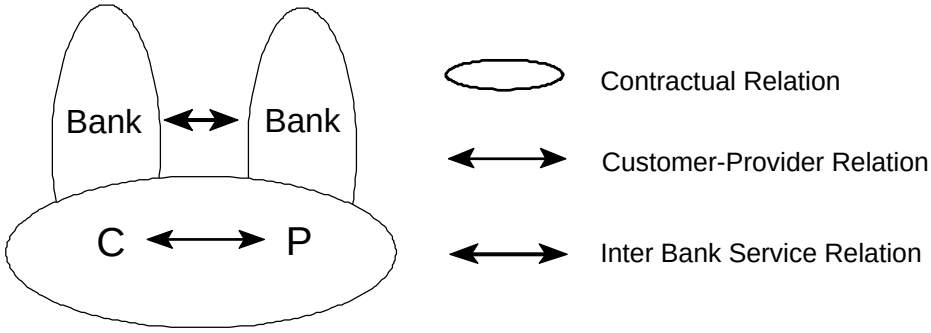

Figure B.1 - Customer/Provider contractual relation for public business

A possible sequence of actions might be:

1) The Provider displays his offer(s).
2) The Customer authenticates himself to the provider's system.
3) The Customer selects an offer and sends the order.
4) The Provider confirms the order with an invoice.
5) The Customer authorizes the Provider to deduct the amount due from his account.
6) The Provider delivers the products or services and deducts the amount due from the customer's account. The deduction is based on the inter bank service relations if a debit card is used.

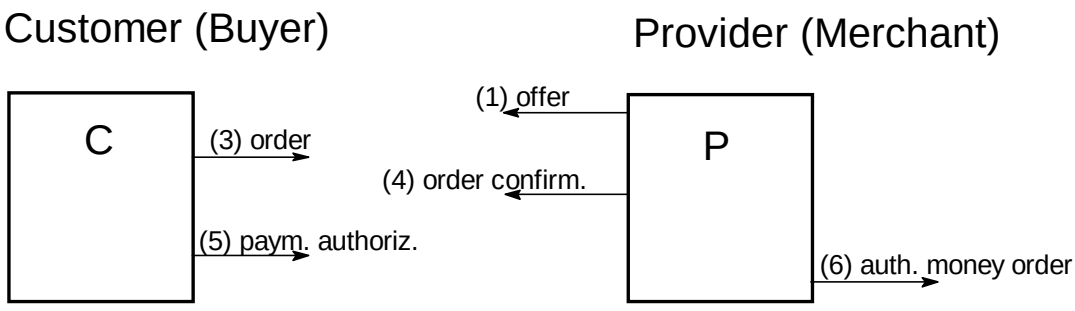

Figure B.2 - Customer/Provider public business

Scenario 2: Customer/Provider public business via a credit card organization (CCO)

In this scenario there exists no contract between the Customer and the Provider. However, the Customer has a contract with a credit card organization that allows the credit card organization to deduct money from the Customer's bank account if an invoice with payment authorization is presented by a Provider. The Provider has a contract with the same credit card organization. It ensures that the organization will pay the amount due if an invoice with Customer's payment authorization is presented. The Provider has the obligation to check prior to confirming the order that the credit card organization accepts the order for this Customer. The applied payment is based on inter bank service relations.

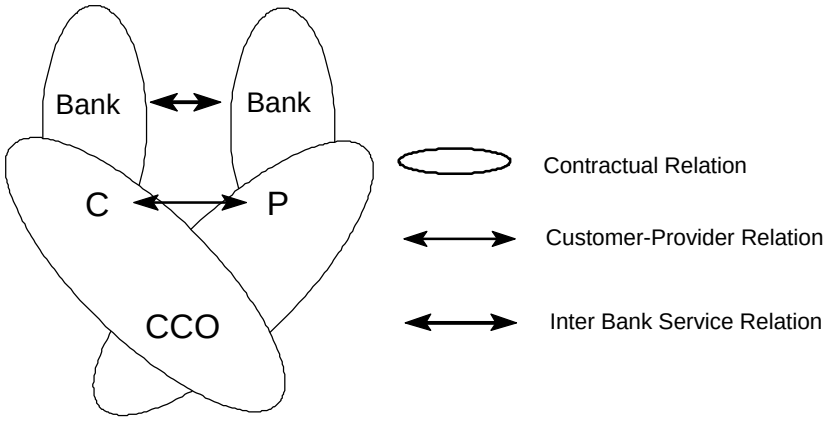

Figure B.3 - Contractual relationship for public business via a credit card organization

The business sequence may be as follows:

1) The Provider displays his offer(s).
2) The Customer authenticates himself as member of a credit card organization.
3) The Customer selects a specific offer and sends the order.
4) The Provider requests and obtains confirmation (authentication code) from the credit card organization to ensure that the invoice for this Customer will be accepted.
5) The Provider confirms the order to the Customer.
6) The Customer sends payment authorization to the Provider.
7) The Provider sends this payment authorization together with the invoice to the credit card organization.
8) The credit card organization debits the Customer's account and credits the Provider's account with the amount due via the inter bank service relation.
9) The Provider delivers the products or services.

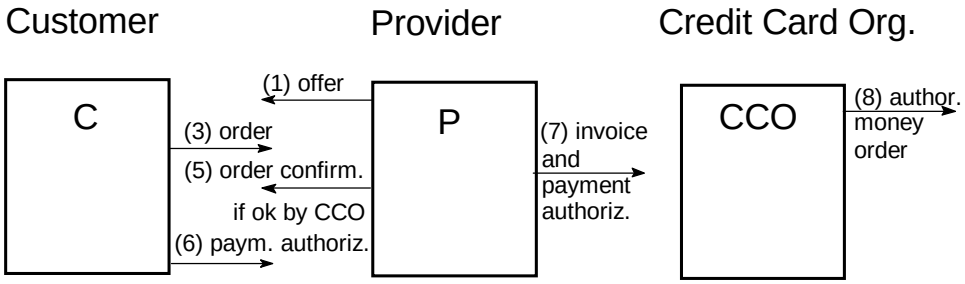

Figure B.4 - Customer/Provider public business via a credit card organization

NOTES

- *The above example is also valid for debit card transactions. In this case the bank takes the role of the credit card organization.*
- *This example is simplified in so far that usually several credit card organizations are involved. In this case the single credit card organization (see figure B.4) has to be replaced by a payment gateway which offers a single interface to the Provider and mediates the communication with the different credit card organizations. A possible protocol for practical implementation is the SET specification, see 3, References.*

Scenario 3: Customer/Provider public business with pay-card

The Customer has a contract with his bank which enables him to load his cash card by deducting a specified money amount from his bank account. The Provider has a contract with his bank to accept the cash card information and pay him the amount due. The Provider's bank will charge the Customer's bank accordingly. Therefore service contracts between the involved banks shall exist. This arrangement allows anonymous payment.

The scenario relies on a process whereby pay-cards are loaded or purchased on the basis of an explicit contract. A special system is needed, to allow a Customer to load his cash card and the Provider to charge the cash card (deduct money from the cash card) and generate the necessary information securely which the bank can accept to initiate the corresponding money transactions (pay the Provider and charge the Customer's bank). This service can be anonymous, since the Customer has not to identify himself. To avoid the risk of „lost money“ (when the pay-card is lost), the system may require PIN authentication. The applied payment is based on inter bank service relations.

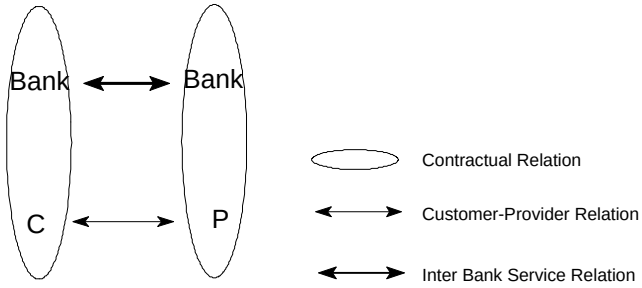

Figure B.5 - Contractual relations for public business with pay-card

The business sequence may be as follows:

1) The Provider displays his offer(s).
2) The Customer selects the offer and sends the order.
3) The Provider verifies the card (card authentication). Optionally, card holder authentication (PIN) is required, depending on the type of card.
4) The Provider deducts the amount due from the pay-card.
5) The Provider delivers the products or services.
6) The Provider charges his bank on the basis of the collected money amounts and Customer’s bank IDs.
7) The provider’s bank credits his account with the amounts and charges the customers’ banks on the basis of the Customer’s bank IDs via the inter bank service relations.

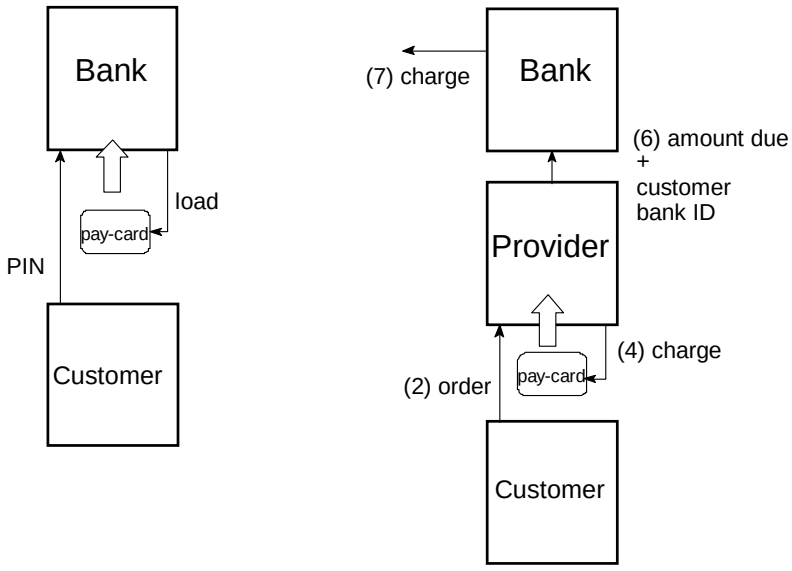

Figure B.6 - Public business between Customer and Provider with pay-card

Scenario 4: Electronic advertising

Electronic advertising is a special case since no money is involved. Consequently a contract is not necessary. The Provider is bound to the general consumer law as any other advertisement. The Customer is normally anonymous. The provider's concern is, that his information is not modified by unauthorized persons for other business actions.

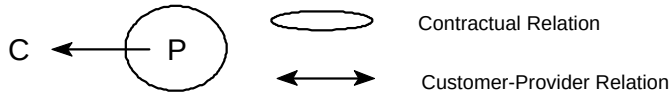

Figure B.7 - Contractual situation for advertising

The business sequence is as follows:

1) The Provider displays his advertisements
2) The Customer retrieves (reads) the information

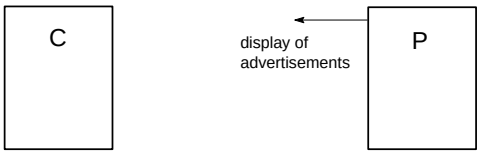

Figure B.8 - Electronic advertising

Annex C

(informative)

Terms defined in other documents

The following terms are used with the meanings defined in the referenced documents. The definitions are repeated here for convenience.

Access: A specific type of interaction between a subject and an object that results in the flow of information from one to the other. [TCSEC]

Access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO 7498-2]

Access control list: A list of entities, together with their access rights, which are authorized to have access to a resource. [ISO 7498-2]

Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO 7498-2]

Audit trail: See Security Audit Trail.

Audit: See Security Audit.

Authentication: To establish the validity of a claimed identity. [ITSEC]

Authentication information: Information used to establish the validity of a claimed identity. [ISO 7498-2]

Authorization: The granting of rights, which includes the granting of access based on access rights. [ISO 7498-2]

Availability: The property of being accessible and useable upon demand by an authorized entity. [ISO 7498-2]

Business action: An action between business partners to perform a commercial business.

Certificate (User): The public keys of a user, together with some other information, rendered unforgettable by encipherment with the secret key of the certification authority which issued it. [ISO/IEC 9594-8 ; CCITT X.509]

Certification authority: An authority trusted by one or more users to create an assign certificates. Optionally the certification authority may create the user's keys. [ISO/IEC 9594-8 ; CCITT X.509]

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO 7498-2]

Cryptographic key: A parameter used with an algorithm to validate, authenticate, encrypt or decrypt a message. [ISO 8732]

Customer: The person or organization that purchases a Target of Evaluation. [ITSEC]

Data integrity: The property that data has not been altered or destroyed in an unauthorized manner. [ISO 7498-2]

Digital signature: Data appended to, or a cryptographic transformation (see Cryptography) of a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO 7498-2]

Impersonation: See Masquerading

Integrity: The prevention of unauthorized modification of information. [ITSEC]. See also Data Integrity.

IT security architecture: See Security architecture

IT security policy: See Security policy

Key generation: The origination of a key or a set of distinct keys. [FIPS PUB 39; AR 380-380]

Key management: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy. [ISO 7498-2]

Key: See cryptographic key

Masquerading: An attempt to gain access to a system by posing as an authorized user. [AR 380-380; NCSC-WA-001-85]

Mechanism: See security mechanism.

Notarization: The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, time and delivery. [ISO 7498-2]

Notary: An organization responsible for notarization. (see Notarization

Object reuse: The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. [TCSEC]

Object: A passive entity that contains or receives information. [TCSEC, ITSEC]

Password: Confidential authentication information usually composed of a string of characters. [ISO 7498-2]

Policy: Administrative decisions, which determine how certain security-related concepts will be interpreted as system requirements. All such policy decisions must eventually be interpreted formally and implemented. [MTR-8201] See also Security Policy.

Privacy: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. [ISO 7498-2]

Procedure: The description of the course of action taken for the solution of a problem. [CBEMA]

Repudiation: The denial by one of the entities involved in a communication of having participated in all or part of the communication. [ISO 7498-2: 1989]

Security architecture: The architecture of parties and entities relevant to security, and the complete set of security procedures and information flows for the realization of security features. [ETSI ETR 232 11/95]

Security audit trail: Data collected and potentially used to facilitate a security audit. [ISO 7498-2]

Security audit: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures. [ISO 7498-2]

Security enforcing: That which directly contributes to satisfying the security objectives of the Target of Evaluation. [ITSEC]

Security mechanism: The logic or algorithm that implements a particular security enforcing or security relevant function in hardware or software. [ITSEC]

Security policy: A plan or course of action adopted for a data processing system, designed to implement and determine computer security. [ISO/IEC 2382-08]

Security service: A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers. [ISO 7498-2]

See also Identity-based and rule-based Security Policy. [ISO 7498-2]

System integrity:	The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. [NCSC-TG-004, Glossary of Computer Security Terms]
Target of evaluation (TOE):	IT system or product which is subject to security evaluation. [ITSEC]
Trusted Third Party:	A security authority, or its agent, trusted by other entities with respect to security related activities. In the context of this standard a claimant and/or a verifier for the purpose of authentication trust a trusted third party. [ITAEGV N99]
User:	Any person who interacts directly with a computer system. [TCSEC]

Free printed copies can be ordered from:
ECMA
114 Rue du Rhône
CH-1204 Geneva
Switzerland

Fax: +41 22 849.60.01
Email: documents@ecma.ch

Files of this Standard can be freely downloaded from the ECMA web site (www.ecma.ch). This site gives full information on ECMA, ECMA activities, ECMA Standards and Technical Reports.

ECMA

114 Rue du Rhône
CH-1204 Geneva
Switzerland

See inside cover page for obtaining further soft or hard copies.