20th National Information Systems Security Conference

7-10 October 1997, Baltimore, MD, USA.

The Extended Commercially Oriented Functionality Class for Network-based IT Systems

Alexander Herrigel[1]	Roger French[2]	Herrmann Siebert[3]	Helmut Stiegler[4]	Haruki Tabuchi[5]

ECMA: Standardizing Information and Communication Systems, TC 36, http://www.ecma.ch

Abstract

This paper presents a new approach for security evaluation criteria of network-based IT systems. The Extended Commercially Oriented Functionality Class (E-COFC) addresses a minimum set of security functionalities for the commercial market to reduce technical complexity and to allow timely and cost-effective application. The standard addresses today's commercial requirements and its various legal concerns. In contrast to state-of-the art-approaches, such as the Common Criteria, the standard addresses the contractual relationships upon which business processes are based on. The E-COFC is considered as a baseline standard commercial enterprises can measure against.

1. Introduction

Critical business processes within an enterprise are directly dependent upon network-based IT systems. These network-based systems require complex management and auditing, since they typically involve several different platforms, each with a specific operating system and client/server technology. The enterprise systems and the information they process are subject to a number of threats from different sources. Effective protection of enterprise systems and information databases requires a structured management approach to security, which affects different domains of the enterprise, such as people, IT systems, communication networks, buildings, business, and facility planning. The IT security of an enterprise requires effective protection of business processes, especially mission critical ones, which in turn rely on risk assessment and audit of the network-based infrastructure. The selection and implementation of an adequate protection starts with the selection of the right evaluation criteria.

2. State-of-the-art Approaches

A number of standards or quasi standards [1-6] are available which can be applied to evaluate a specific assurance level of security for a hardware and operating system combination. The latest developed standard is the Common Criteria (CC) [6], an effort by different governments to provide a harmonized criteria for the United States, Canada, and the European Union. From a commercial perspective, the standards have several limitations. The standards do not address different legal parties that might be involved in business process actions. A great number of business processes, however, are based on the Internet architecture which is supporting an IT environment for different business partners. With respect to the contractual relation-

[1]r3 security engineering ag , Zurichstrasse 151, CH - 8607 Aathal, Switzerland, Email: herrigel@r3.ch .

[2]Digital Equipment Corporation, U.S., Email: french@zeke.ENET.dec.com .

[3]EDP Consulting, Germany, Email: 100041.3255@compuServe.com .

[4]STI Consulting, Germany, Email: helmut.stiegler@muenchen.org .

[5]Fujitsu Ltd, Japan, Email: Tabuchi@Saint.NM.Fujitsu.co.jp .

ships between different business partners, special requirements have to be satisfied to address the audit of legal contract issues during the execution of the business processes. Unfortunately, this important commercial and legal aspect has not been taken into account by these standards [1-6]. A number of standards were created based on government requirements and do not reflect commercial needs. Some of these, such as the CC, are technically complex, but not concise[6], and this makes them in many cases impractical and not applicable.

3. The Extended Commercially Oriented Functionality Class

3.1. Introduction

The Extended Commercially Oriented Functionality Class (E-COFC) ECMA 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 minimum security requirements for typical business applications on interconnected systems. The E-COFC is based on an IT Security Policy of a commercial enterprise and takes environmental and organizational constraints into account. The identified minimal security requirements of this standard have to be supported by the system being evaluated, but not necessarily by each individual component system.

3.2. 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 networks[7] and the additionally installed business applications or hardware devices constitute the TOE. The communication network is considered a priori as not secure. The identified minimal security requirements of the E-COFC have to be supported by the TOE but not necessarily by each individual system. The supported 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.

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 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

[6]The following security functionalities are missing in some of the above mentioned standards: Expiration of unused user identifiers, disable users temporarily, date of modification to objects, survive of accountability control information at restarts of TOE, alarm if unable to record audit trail, dynamic control for events recorded during normal operation, and TOE software integrity.

[7]If the evaluation sponsor is not the owner of the communication networks the communication paths through the networks have to be evaluated on the basis of the established contract with the network - and communication service provider. In the other case, the sponsor can decide, whether he wants a partial (communication paths only) or full evaluation of the communication networks.

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 SNMP or 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.

3.3. Identified hierarchical classes

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

1. The **Enterprise Business Class** (EB-class) (includes COFC [7, 8] requirements).
2. The **Contract Business Class** (CB-class) (includes the EB-class and COFC requirements).
3. The **Public Business Class** (PB-class) (includes the CB-class, EB-class and COFC requirements).

Each subclass specifies for the imposed commercial environment the commercial requirements, the threats, the resulting security requirements, and the security functionalities. In practice, electronic business actions between business partners are not only based on secure data processing and communication, but also on the provision of legal proof. Those commercial requirements are the foundation for the CB-and the PB-class, while the EB-class provides the necessary network communication security. It is beyond the scope of the paper to present a detailed description of the standard. The reader is referred to [9] for more detailed information.

4. The Enterprise Business Class

4.1. Introduction

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.

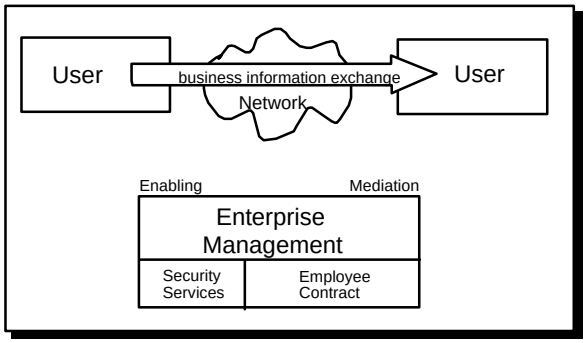

Figure. 1: The Enterprise Business Model.

The model describing the enterprise business is shown in Figure 1. 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 the management

of the enterprise. Conflict mediation is provided by the management actions on the basis of the employee contracts. No specific business actions between different legal parties have to be investigated for this class.

4.2. Threat analysis

Different threat classes such as communication compromise, system compromise, and user compromise have been identified. The specific threats and countermeasures are listed in Table 1.

Table 1: *Identified Threats and Countermeasures of the EB-Class*

Threat	Countermeasure
Undetected modification of transmitted data (accidental, incidental)	Content integrity checking of transmitted data
Undetected deletion of transmitted data (accidental, incidental)	Content integrity checking of transmitted data
Undetected insertion of transmitted data (accidental, incidental)	Content integrity checking of transmitted data Sequence integrity checking of transmitted data
Impersonation of an entity (sender/receiver) involved in a communication process	Authentication of sender and receiver address
Unauthorized disclosure of information during transmission (this may result also in a penetration of a trusted path between a user and a login schema)	Confidentiality
Replay of transmitted data	Sequence integrity checking of transmitted data
Blockage of data exchanged between two systems	Usage of alternative channels
Rising communication traffic to decrease the system performance	Filtering
Connection setup or transmission failure	Authentication of sender and receiver address Physical protection of communication devices Recovery procedures Alternate routes
Undetected modification of stored or processed data (accidental, incidental)	Authentication Access control Recovery
Undetected deletion of stored or processed data (accidental, incidental)	Authentication Access control Recovery
Undetected insertion of stored or processed data (accidental, incidental)	Authentication Access control Recovery
Unauthorized disclosure of information (user information, system information)	Confidentiality
System failure	Recovery Backup
Physical damage (accidental, incidental)	Recovery Backup Physical protection
Outsider attack: Unauthorized access to the TOE to penetrate system information	Authentication Access control
Denial of service (application, network services)	Physical protection Authentication Access control
Bootstrap compromise or unauthorized replacement of privileged subsystems (installation of a spoofing operating system)	Physical protection System verification
Unauthorized access by impersonation	Content integrity checking of exchanged authentication data Sequence integrity checking of exchanged authentication data Replay attack detection mechanism

	Authentication Accountability
Unauthorized access by authorized user	Accountability Access control.

4.3. Derived security functionalities

We list in this section only these security functionalities which have been additionally identified on the basis of the COFC.

Identification and authentication

Identification and authentication of users:

The TOE shall support a secure authentication protocol. The applied protocol shall verify the content integrity of the authentication data and the integrity of the sender or receiver address. In addition, the 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.

Session lock or terminate:

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

Client/server communication

Content integrity of exchanged information:

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

Address integrity of exchanged information:

If two systems are exchanging information, the integrity of the sender- and receiver addresses must be verified. The applied protocol shall prevent replay attacks.

Confidentiality of exchanged information:

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

Accountability and Audit

Synchronization:

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

Reliability

Filtering:

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

Transmission blockage:

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

Key management[8]

Key generation:

The key generation shall be based on state-of-the-art cryptographic techniques which ensure the unpredictable generation of truly random and prime numbers.

Sufficient key length:

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

Key confirmation:

The security management shall support a key distribution technique which addresses the authenticity (asymmetric techniques) or confidentiality (symmetric techniques) of the keying information.

[8] if cryptographic means are applied by the TOE.

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).

Key revocation:

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

Key backup and archiving:

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

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.

5. The Contract Business Class

5.1. Introduction

The CB-class is built on top of the EB-class. It adds to the network security requirements of the EB-class those requirements which are typical for business actions (business information exchange) between independent enterprises which belong to 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 actions. They establish a "Regulatory Board" (RB) which acts as impartial judge to mediate conflicts within the user group and acts also as "Trusted Center" to handle security matters (for example key management). All business partners who sign the contract form 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 within the closed user group can be described with the following model: The business information is exchanged between the "Originator" and the "Destination". These terms describe functional roles in the business process.

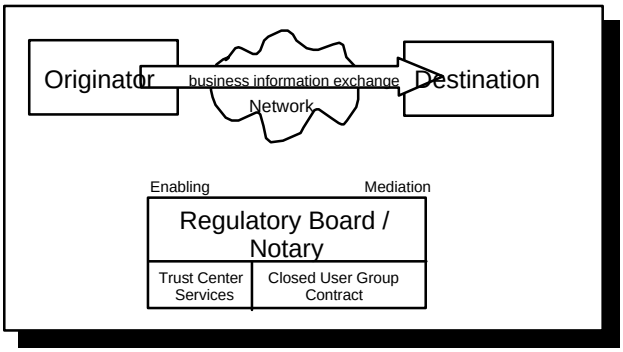

Figure 2: The Contract Business Model.

The Originator is a user or a process on behalf of a user that sends business information (document, order, invoice 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. The Originator and the Destination must be authorized according to the closed user group contract to perform the business actions. If the information is confidential, the Originator and Destination are persons (processes) that are authorized to read or use 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.

The Regulatory Board

The RB is an impartial element in the closed user group. The members of the RB mediate or intervene

in conflict situations between different business partners of the closed user group. The board works on the basis of a contract which is signed by all legal parties of the closed user group. Organization, independence, constraints, and authority of the RB must be clearly stated in the contract. The RB acts as an independent organization or office which imposes the legal rules on all participating parties. The acceptance of the RB is a contractual prerequisite for all legal parties of the closed user group. Only persons which are registered by the RB may become system users. The RB may delegate the administration to the different enterprises but keeps the overall control.

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 RB. It defines the legal (contractual) relations to other partners (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 must 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 must be specified in the contract. The contract must address at least the following areas: Organization of the RB, definition of business actions and their security requirements, and the IT security policy (including confidentiality, accountability and audit, availability, reliability, elaboration of proof, access control, change management).

Example of business actions

The TOE has to establish a secure basis for various kinds of business. In order to understand and motivate the derived security functionalities on the level of the TOE, an example of typical business actions with the associated security requirements is presented (see Table 4).

This top-down approach for deriving requirements on the TOE-level, which manufacturers have to fulfill, has to be reversed in case of accreditation of installed cooperating systems. 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.

Business actions can generally be seen as the transmission of a "document" 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 document. The requirements to the TOE may be different for different business actions. For example, an order involves a financial commitment of the Originator. The TOE shall ensure that only qualified users should be able to send or receive orders (this improves the reliability of the business action). The Destination (receiver of the order) must be able to securely identify the Originator, because his acting on the order will result in financial 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 timely processed. Business conditions may require that the document is handled confidentially (for example to counter industrial espionage). In this case the TOE shall support encryption techniques, such that only the Destination can decrypt the file. 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 also requirements to the transport system which are:

- Attestation of submission
- Attestation of delivery
- Attestation of reception by Destination
- Return if undeliverable

Table 4: Typical Security Requirements for Business Actions (Examples)

Business Action (send / receive)	Qualification of Originator	Qualification of Destination	Commitment of Originator	Secured Identity of Originator	Non-repudiation of Originator	Non-repudiation of Destination	Document Integrity	Document Confidentiality
Contract	x	x	x	x	x	x	x	optional
Order/Invoice/ Response to Call for Tender	x	x	x	x	x	x	x	optional
Offer	x		x	x	x		x	optional
Private Call for Tender/Order-Confirmation	x	x	x	x	x		x	optional
Public Call for Tender	x		x	x	x		x	optional
Financial Order	x	x	x	x	x	x	x	x

- Time-stamping

The transport system shall provide evidence that the information was timely transmitted. The attestation of submission and delivery gives the Originator of a business action assurance and proof that the document was timely transmitted. In case a document can not be delivered, it shall be returned to the sender. Time stamping is required on all attestations and shall include time, date, and place of the event. The protection of transmitted information by encryption techniques (to counter unauthorized disclosure) shall be specified in the contract taking legal regulations into account.

5.2. Threat analysis

Table 3 lists the threats and countermeasures which have to be identified in addition to those of the EB-class:

Table 3: Identified Threats and Countermeasures of the CB-Class

Threat	Countermeasure
Denial of submission	Attestation of submission Non-repudiation of Originator
Denial of reception	Attestation of delivery Non-repudiation of Destination
Denial of document ownership	Non-repudiation of Originator
False routing of information enabling unauthorized access	Authentic business role qualification of Originator and Destination.
A dispute between two different legal parties of the closed user group has to be mediated by the RB. Because of missing timing information and business process related data, the RB can't resolve the dispute.	Relevant requests on behalf of system users for associated business actions shall be logged such that they can be analyzed with respect to contract relations and legal issues on all involved systems. The stored timing information shall enable the tracing of business process actions on different systems.

5.3. Derived security functionalities

The following security functionalities 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 supports only a subset of the business actions listed in Table 4, only the corresponding subset of security requirements shall be fulfilled.

Access control

Qualification:

Only qualified users shall be able to access the business action services (see also COFC [7, 8]). The business role qualification data of the Originator or Destination shall be authentically distributed.

Consistency:

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

Accountability and audit:

Non-repudiation of the Originator:

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

Non-repudiation of the Destination:

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

Attestation of submission, delivery, and reception:

The transport service shall establish an attestation when information was submitted, delivered, and received. If delivery was not accomplished, the Originator shall be informed by the transport service giving the reasons why the delivery was not possible.

Timing information of audit data:

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

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.

6. The Public Business Class

6.1. Introduction

The PB-class is built on top of the EB-class and the CB-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 network-based information services. The terms Customer and Provider are used in this class. A Provider system which is offering a specific service supports 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 is described by the following model:

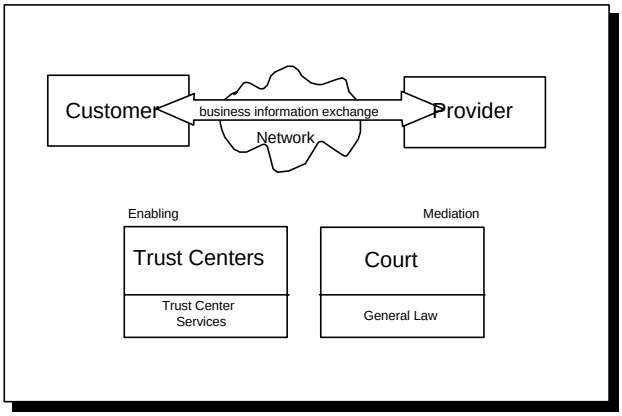

Figure 3: The Public Business Model.

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-and CB -class the business relationships may be beyond the contractual relationships. Different sce-

narios of contractual relations are possible. In the case of electronic advertising the contracts are also provided by business and consumer law. The formal contractual relationship between the Customer and the Provider is either direct or through other business organizations such as credit card organizations as shown in the following example.

Customer/Provider/Credit Card Org. example

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.

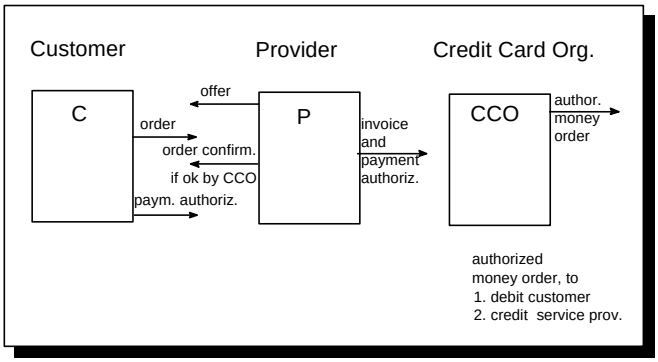

Figure 4: Customer/Provider Business Actions via a Credit Card Organization.

The business sequence may be as follows:

1. The Provider displays his offers.
2. The Customer selects a specific offer and sends the order.
3. The Customer authenticates himself as member of a credit card organization.
4. The Provider 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 a 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.

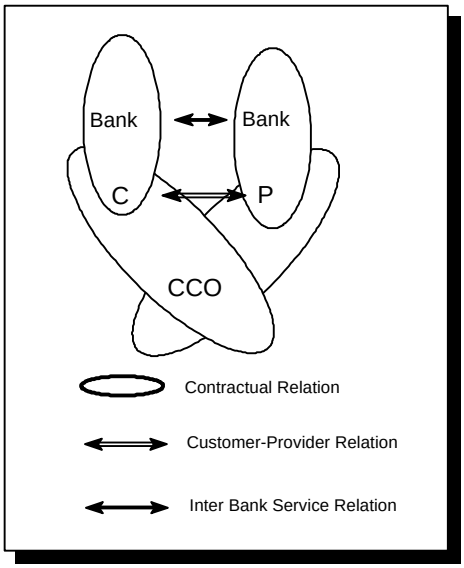

Figure 5: The different relations of the involved business parties.

This example is also valid for debit card transactions. In this case the bank takes the role of the credit card organization[9]. Figure 5 illustrate the dif-

[9]This simplified example may be enhanced with several credit card organizations. In this case the single credit card organization (see Figure 4) has to be replaced by a payment gateway which offers a single interface to the provider and mediates the payment requests with the different credit card organizations. A possible protocol for a practical implementation is the SET specification [10].

ferent contractual, Customer-Provider, and inter bank service relations.

6.2. Threat analysis

Table 5 lists the threats and countermeasures which have been identified in addition to those of the EB-class and the CB-class.

Table 5: Identified Threats and Countermeasures for the PB-class

Threat	Countermeasure
Undetected modification or replacement of commitment data	Content integrity checking of transmitted commitment data
Undetected deletion or insertion of commitment data	Content integrity checking of transmitted commitment data
Undetected replay of commitment data	Sequence integrity checking of commitment data
Denial of commitment data ownership	Non-repudiation of Originator
Denial of commitment data submission	Non-repudiation of Originator
Denial of commitment data reception	Non-repudiation of Destination
Undetected acceptance of invalid/ invalidated commitment data or certificates	Content integrity checking and content verification of commitment data or certificates Authentic distribution of revocation lists Access Control
Undetected refusal of valid/validated commitment data or certificates	Content integrity checking and content verification of commitment data or certificates Authentic distribution of revocation lists Access Control
Interception of commitment data or certificates	Restricted lifetime of cryptographic keys, certificates and commitment data
Theft of business process input data	Authentication Access Control
Disclosure of business data to unauthorized persons	Authentication Access Control
Undetected unauthorized access on linked privacy data of system users	Authentication Access Control Anonymity or pseudonymity measures
Unlawful multiple use (e.g. by copying) of unique data	Uniqueness enforcing functions and uniqueness violation detection measures

6.3. Derived security functionalities

Identification and authentication

Multistage identification and authentication:

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

Access control

Protection against unlawful disclosure**:**

The TOE 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.

Accountability and audit

Interrelated accountability:

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

Commitment data ownership and submission:

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

Commitment data reception:

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

Uniqueness of original:

If uniqueness of original is required, adequate techniques, such as cryptographic based registration,

watermarking, or bill of lading scheme, ticketing, certificates, etc. shall be provided.

Commitment data communication

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

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

Address integrity of exchanged commitment data or certificates:

If two systems are exchanging commitment data or certificates, the integrity of the sender- and receiver addresses must be verified. The applied protocol shall prevent replay attacks.

Key management

In this class the trust relationship between the different independent business parties is based on notary services which register and manage the associated security information needed for the corresponding business process. 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 have to be supported: Registration, certification, distribution and revocation.

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 public 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.

Certification:

The certification process generates the legal binding between the business process entity and his credentials he will use in the business process. The certification process shall cover two aspects, the certification of the user's public key and the certification of user's attributes. This certification is 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 the business process. The CA shall provide adequate means for the authenticity and integrity of the stored certification data.

Distribution:

The certificate information shall be distributed on an authentic channel to the associated entity. Adequate verification mechanisms shall be provided to ensure that the correct entity has received and verified the distributed certificate.

Revocation:

The following phases shall 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 revokes the stored certificate of the entity. A revocation certificate is 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.

7. Conclusions and Future Work

From our perspective, the E-COFC has the following advantages:

1. The E-COFC standard is easy to understand since the specification of a minimum set of security functionalities reduces the technical complexity. The derived set provides a reasonable protection for commercial multi-user, network-based IT systems.

2. In contrast to other approaches, such as the CC, the E-COFC addresses the security requirements for business processes with different legal parties.

We are currently planning to setup and deploy an ECMA based commercial protection profile registry. One of the first profiles to be registered are the COFC, the E-COFC, and the CC profiles such as CS1 and CS2 in close cooperation with ISO.

References

[1] "Trusted Computer Systems Evaluation Criteria", DoD 5200.28-STD, Department of Defense, United States of America, December 1985.

[2] "Information Technology Security Evaluation Criteria (ITSEC)-Harmonized Criteria of France, Germany, the Netherlands, and the United Kingdom", Version 1.2, June 1991.

[3] "Information Technology Security Evaluation Manual (ITSEM)", Provisional Harmonized Methodology, European Commission, Directorate-General XIII, telecommunications, Information Market and Exploitation of Research, September 1993.

[4] "The Canadian Trusted Computer Product Evaluation Criteria", Canadian System Security Center, Communications Security Establishment, Government of Canada, Version 3.0e, January 1993.

[5] "Federal Criteria for Information Technology Security", Volume 1 and Volume 2, December 1992, National Institute Of Standards and Technology & National Security Agency.

[6] "Common Criteria for Information Technology Security Evaluation", Version 1.0, CCEB.

[7] "Standard ECMA-205, Commercially Oriented Functionality Class for Security Evaluation (COFC) ", ECMA, December 1993.

[8] Alexander Herrigel, Roger French, and Haruki Tabuchi, European Computer Manufactures Association (ECMA), TC36/TG1, "ECMA's Approach for IT Security Evaluations", 18th National Computer Security Conference, Baltimore Convention Center, Baltimore, MD, October 10-13, 1995, USA.

[9] Draft Standard ECMA, "Security Functionalities of the E-COFC", Second draft for review and comments, ECMA TC36, June 1977.

[10] Secure Electronic Transactions Specification by Visa/Mastercard,V. 1.0, 1997.