ECMA Technical Report TR/78
December 1999

ECMA

Standardizing Information and Communication Systems

ECMA Protection Profile E-COFC Public Business Class

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

ECMA Technical Report TR/78
December 1999

ECMA

Standardizing Information and Communication Systems

ECMA Protection Profile E-COFC Public Business Class

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

Brief History

After the ECMA Technical Committee TC36 "IT Security" had completed the development of the Standard ECMA-271 "Extended Commercially Oriented Functionality Class for Security Evaluation (E - COFC)" it was quite natural to continue with the development of a Protection Profile, i.e. a Profile that combines the functional criteria of the E - COFC with a set of assurance criteria. It was decided to use the Common Criteria for this purpose, since these criteria were in the process of being standardized by ISO/IEC JTC1/SC27.

Due to the active support of the US National Institute of Standardization and Technology (NIST) in TC36 it was possible to build this profile, based on the Public Business Class of E - COFC. Starting point and basis of the E - COFC PP development was the NIST PP Version 0.31 by Gary Stoneburner (NIST), 23 July 1998. Kristina C. Rogers (Cygnacom Solutions) was then given the task to convert the E - COFC Public Business Class into a Protection Profile. This work was then adopted by TC36 and updated to include those changes which meanwhile were made to the E - COFC in its second edition.

The purpose of developing a Protection Profile was to demonstrate how the E - COFC criteria can be applied for IT system evaluations.

This Technical Report ECMA TR/78 gives the **technical** details. Another Technical Report will explain the application of the Profile and discuss its limitations. This report is under preparation.

Adopted as ECMA Technical Report TR/78 by the General Assembly of 16 December 1999.

Table of Contents

1 Introduction

1.1 Identification

Title: ECMA Protection Profile, E - COFC Public Business Class, Version 2.02

Assurance level: EAL2 Augmented

Registration: <To be filled in upon registration>

Keywords: electronic commerce, commercial functionality, operating systems, networks, distributed systems, ECMA, E - COFC.

1.2 Protection Profile overview

The Extended Commercially Oriented Functionality Class (E - COFC) Public Business (PB) Class Protection Profile (PP) is based on the requirements for the Public Business Class contained in ECMA-271. The E - COFC PP is Part 2 extended with respect to its functional requirements and EAL2 augmented with respect to its assurance requirements. The E - COFC PP 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 IT Security Policy is based on a Confidentiality Policy, an Integrity Policy, an Accountability Policy and an Availability Policy. 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).

The Protection Profile Rationale is provided in annex A.

2 TOE description

2.1 E - COFC overview

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.

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. 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.

2.2 The TOE environment

The Target of Evaluation (TOE) environment 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.

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:
  - 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).
  - Asynchronous client server communication: Client and server processes communicate on the basis of message passing.
  - 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.
  - 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. The TOE may be connected to the internet under the surveillance of flow control mechanisms which exclude irregular interference with measures to counter the threats to the commercial environment.

2.3 Hierarchical classes

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

- The Enterprise Business class (EB-class) – (includes COFC, ECMA-205, 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).

Each subclass specifies the imposed commercial environment security requirements, the resulting threats and the identified security functionalities. In practice, the subclasses may overlap each other. A minimal set of security functionalities is derived to counter these threats with appropriate countermeasures for the commercial environment.

The ECMA-205 COFC requirements apply to a non-networked environment and are the lowest level of the hierarchy. They are included in the requirements for the Enterprise Business Class. This Protection Profile is for the Public Business Class, the highest level in the hierarchy. The Public Business Class includes the requirements for the Enterprise Business Class and the Contract Business Class.

3 Security environment

This clause identifies the following:

- Secure usage assumptions,
- Organizational security policies, and
- Threats to Security.

3.1 Secure usage assumptions

The specific conditions listed below are assumed to exist in an E - COFC Public Business Class environment.

Table 1 – Security assumptions

Type	Name	Assumption
Physical	A.PHYSICAL	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.
Personnel	A.USER-TRUST	Authorized users are trusted to protect their authentication information and to follow their organizational security policies with respect to the protection of sensitive information.
	A.ADMIN	The security features of the TOE are competently administered.

3.2 Organizational security policies

The E - COFC Public Business Class Protection Profile is intended to reflect the requirements contained in ECMA-271, *Extended Commercially Oriented Functionality Class for Security Evaluation (E - COFC)*, for the Public Business (PB) Class.

3.3 Threats to security

The threats in this clause are based on the threats identified in ECMA-205 and ECMA-271. For a mapping from the threats identified here to the threats in the ECMA documents, please see the accompanying Rationale document.

Table 2 – Threats

	Threat name	Threat description
1	**T.Actions_Traced**	Unauthorized tracing of customer business actions may occur.
2	**T.Blockage**	Two systems may not be able to exchange data due to a communications channel being blocked.
3	**T.Change_Data**	Information may be changed either while it being stored or processed within the TOE or during transmission. The changes may be accidental or intentional. Changes include insertions, replacements, modifications, and deletions. The type of information that can be changed includes user information, system information, business data, and commitment.
4	**T.Comm_Failure**	It may not be possible to set up a connection or transmit data between two systems.
5	**T.Data_Theft**	Business process input data may be stolen.
6	**T.Deny_Data**	An entity may deny ownership of business or commitment data.
7	**T.Deny_Receipt**	An entity may deny that it has received business or commitment data.
8	**T.Deny_Submit**	An entity may deny that it has submitted business or commitment data.
9	**T.Disaster**	Natural disasters may cause TOE or system failure.
10	**T.Disclose_Data**	Information may be disclosed in to unauthorized users. This includes both user information, system information and business data. Information may be disclosed while being stored or processed in the TOE or during transmission. Disclosure of authentication data during transmission would allow someone to logon and assume the identity of an authorized user.
11	**T.False_Routing**	Information may be routed to a false address enabling unauthorized access.
12	**T.History_Untraceable**	It may not be possible to trace the sequence of events during a system failure, malfunction, or betrayal.
13	**T.Impersonate**	Someone may obtain unauthorized access by impersonating an authorized user.
14	**T.Indeterminate_Seq**	It may be impossible to determine the sequence of events in a dispute due to missing time information and business related data.
15	**T.Insider**	An authorized user of the TOE may gain unauthorized access.
16	**T.Intercept**	Commitment data or certificates may be intercepted.
17	**T.Invalid_Certificate**	The TOE may accept invalid commitment data or certificates.
18	**T.Logon_Attack**	A program that tries a large number of passwords successfully guesses the password of an authorized user. This allows an unauthorized individual to logon as an authorized user and to assume the identity of that user.

Table 2 – Threats (concluded)

	Threat name	Threat description
19	**T.Outsider**	An individual who is not an authorized user of the system may gain access to the TOE.
20	**T.Physical**	A component of the system may be accidentally or intentionally damaged.
21	**T.Privacy_Violated**	Unauthorized access to privacy data of system users may occur without detection.
22	**T.Refusal_Undetected**	Unauthorized refusal of valid commitment data or certificates may not be detected.
23	**T.Replace_TOE**	The TOE may be replaced by an untrusted system.
24	**T.Replay**	Someone may obtain unauthorized access by replaying authentication or commitment data.
25	**T.Secret_Disclose**	Authentication information may be disclosed allowing someone to logon and assume the identity of an authorized user.
26	**T.Service_Denied**	Application and network services may not be available for use.
27	**T.TOE_Fail**	TOE or system failure may cause the TOE to enter an insecure state or data to be disclosed or changed.
28	**T.Traffic**	A system may experience degraded performance due to increased communications traffic.
29	**T.Unique_Copied**	Unlawful copies may be made of unique originals.

4 Security objectives

4.1 TOE security objectives

Table 3 – TOE security objectives

	Objective name	Objective description
1	**O.Access_Control**	The TOE must enforce an access control policy to protect information from unauthorized access.
2	**O.Alt_Channel**	The TOE must provide alternate channels for the transmission of data.
3	**O.Anon**	The TOE must provide for anonymity and pseudonymity.
4	**O.Assoc_User_Action**	The TOE shall associate all security relevant actions with a unique user identity.
5	**O.Attest**	The TOE must provide for attestation of submission, delivery and receipt.
6	**O.Audit**	All security relevant actions must be auditable.
7	**O.Authen**	Users must be uniquely identified and authenticated prior to performing any actions to be mediated by the TOE.
8	**O.Authen_Address**	The TOE must be able to authenticate sender and receiver addresses. This includes a priori business qualification of Originator and Destination.
9	**O.Authen_Age**	The TOE must provide for the expiration of authentication information (except for biometric information). This includes cryptographic keys, certificates and commitment data.

Table 3 – TOE security objectives (concluded)

	Objective name	Objective description
10	**O.Authen_Indep**	A user may share the same authentication information as another user, but the TOE must not reveal this fact.
11	**O.Authen_Protect**	The TOE must protect authentication information.
12	**O.Backup**	The TOE must provide data backup and restoration.
13	**O.Trans**	The TOE must be able to protect transmitted information from unauthorized disclosure.
14	**O.Consistency**	The TOE must be able to maintain consistency between TSF data stored on different systems such as user identity, user attributes, and timing information.
15	**O.Dynamic**	The TOE must provide for the selection of auditable events and management of the audit trail during normal operations so that suspected unauthorized activity can be monitored as it occurs without alerting a perpetrator.
16	**O.Filter**	The TOE must provide for the filtering of communications with respect to resource utilization.
16.1	**O.Flow_Control**	The TOE must enforce an information flow control policy at specified boundaries.
17	**O.Integrity**	The TOE must be able to protect and verify the integrity of stored or transmitted data. This includes user and TSF data such as commitment data, business data, business data with commitment data, or certificates.
18	**O.Key_Indep_Gen**	The TOE must generate new keys independently of broken keys.
19	**O.Key_Indep_Distrib**	The TOE must distribute new keys independently of broken keys.
20	**O.Logon_Limit**	The TOE must limit the number of logon attempts.
21	**O.Nonrep_Dest**	The TOE must protect against repudiation by the Destination.
22	**O.Nonrep_Orig**	The TOE must protect against repudiation by the Originator.
23	**O.Recover**	The TOE must be able to recover the TOE to a secure state.
24	**O.Replay**	The TOE must protect against replay attacks.
25	**O.Resid_Prot**	Information stored within the TOE must not be made available to other users upon release.
25.1	**O.Resource**	The TOE must protect against loss of availability through resource exhaustion.
26	**O.Revoke_Cert**	The TOE must provide for the revocation of certificates.
27	**O.Sequence**	The TOE must ensure that it is possible to determine the correct sequence of events. All audit trails within a TOE must include reliable time stamps that can be correlated each other to determine the sequence of events. Similarly, the TOE must support the sequencing of communication data so that the insertion or deletion of network packets can be detected.
28	**O.Status**	It shall be possible to determine the status of security relevant TOE parameters.
29	**O.System_Integrity**	The TOE must provide procedures to verify the integrity of the TOE.
30	**O.Unique**	The TOE must enforce the uniqueness of an original.

4.2 Environmental security objectives

Some policies and threats are beyond the capability of E - COFC compliant components to adequately mitigate without support from the TOE operational environment.

NOTE
Copied from [CS2 PPG] with „authenticated user“ changed to „authorized user“.

Table 4 – Environmental security objectives

Objective name	Objective description
O.Operate	Those responsible for the TOE (in conjunction with mechanisms provided by the TOE) must ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.
O.Manage	Those responsible for the TOE (in conjunction with mechanisms provided by the TOE) must ensure that it is managed and administered in a manner that maintains IT security.
O.Physical	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security.
O.Access_Malicious	The TOE environment must sufficiently mitigate the threat of malicious actions by authorized users.
O.Entry_Sophisticated	The TOE environment must sufficiently mitigate the threat of an individual (other than an authorized user) gaining unauthorized access via sophisticated, technical attack.
O.Access_Non_Technical	The TOE environment must provide sufficient protection against non-technical attacks by authorized users for non-malicious purposes.
O.Entry_Non_Technical	The TOE environment must provide sufficient protection against non-technical attacks by other than authorized users.
O.Detect_Sophisticated	The TOE environment must provide the ability to detect sophisticated attacks and the results of such attacks (e.g., corrupted system state).
O.Denial_Sophisticated	The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks.
O.Comply	The TOE environment, in conjunction with controls implemented by the TOE, must support full compliance with applicable laws, regulations, and contractual agreements.
O.Due_Care	The TOE environment, in conjunction with the TOE itself, must be implemented and operated in a manner that clearly demonstrates due-care and diligence with respect to IT-related risks to the organization.

5 Security requirements

This clause contains the functional requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, in some cases with modifications.

This Protection Profile (PP) expresses broadly applicable policy in accordance with that specified in ECMA-271. It is anticipated that security targets written against this PP may add policy refinements to capture organizational-specific policy details.

5.1 TOE security functional requirements

Table 5 lists the IT functional requirements and the security objectives each requirement helps to address.

Table 5 – Functional components

	Component	Component name	Refined
1	FAU_GEN.1	Audit data generation	
2	FAU_GEN.2	User identity generation	
3	FAU_SAR.1	Audit review	
4	FAU_SAR.2	Restricted audit review	
5	FAU_SAR.3	Selectable audit review	
6	FAU_SEL.1	Selective audit	
7	FAU_STG.2	Guarantees of audit trail availability	Yes
8	FAU_STG.3	Action in case of possible audit data loss	
9	FCO_NRO.2	Enforced proof origin	
10	FCO_NRR.2	Enforced proof of receipt	Yes
11	FCS_CKM.1	Cryptographic key generation	Yes
12	FCS_CKM.2	Cryptographic key distribution	Yes
13	FCS_CKM.3	Cryptographic key access	Yes
14	FCS_CKM.4	Cryptographic key destruction	Yes
15	FDP_ACC.1	Subset access control	
16	FDP_ACF.1	Security attribute based access control	Yes
17	FDP_DAU.1	Basic data authentication	
17.1	FDP_IFC.1	Subset information flow control	
17.2	FDP_IFF.1	Simple security attributes	
18	FDP_ITT.1	Basic internal transfer protection	
19	FDP_RIP.1	Subset residual information	
20	FDP_SDI.1	Stored data integrity monitoring	
21	FDP_UCT.1	Basic data exchange confidentiality	
22	FDP_UIT.1	Data exchange integrity	
23	FIA_AFL.1	Basic authentication failure handling	
24	FIA_ATD.1	User attribute definition	
25	FIA_SOS.1	Selection of secrets	
26	FIA_UAU.1	Timing of authentication	
27	FIA_UAU.3	Unforgeable authentication	
28	FIA_UAU.5	Multiple authentication mechanisms	
29	FIA_UAU.6	Re-authenticating	

Table 5 – Functional components (concluded)

	Component	Component name	Refined
30	FIA_UAU.7	Protected authentication feedback	
31	FIA_UID.1	Timing of identification	
32	FIA_USB.1	User-subject binding	
33	FMT_MOF.1	Management of security functions behavior	
34	FMT_MSA.1	Management of security attributes	
35	FMT_MSA.2	Secure security attributes	
36	FMT_MSA.3	Static attribute initialization	
37	FMT_MTD.1	Management of TSF data	
38	FMT_SAE.1	Time-limited authorization	
39	FMT_SMR.2	Restrictions on security roles	
40	FPR_ANO.1	Anonymity	
41	FPR_PSE.1	Pseudonymity	
42	FPR_UNO.1	Unobservability	
43	FPT_AMT.1	Abstract machine testing	
44	FPT_FLS.1	Failure with preservation of secure state	
45	FPT_ITC.1	Inter-TSF confidentiality during transmission	
46	FPT_ITI.1	Inter-TSF detection of modification	
47	FPT_ITT.1	Inter-TSF detection of modification	
48	FPT_RCV.1	Manual recovery	
49	FPT_RPL.1	Replay detection	
50	FPT_RVM.1	Non-bypassability of the TSP	
51	FPT_SEP.1	TSF domain separation	
52	FPT_STM.1	Reliable time stamps	
53	FPT_TDC.1	Inter-TSF basic TSF data consistency	
54	FPT_TST.1	TSF testing	
55	FRU_FLT.1	Degraded fault tolerance	
56	FRU_RSA.1	Maximum quotas	
57	FTA_SSL.1	TSF-initiated session locking	
58	FTA_TAB.1	Default TOE access banners	
59	FTA_TAH.1	TOE access history	
60	FTA_TSE.1	TOE session establishment	
61	FTP_ITC.1	Inter-TSF trusted channel	
62	PBC_DYN.1	Dynamic control of audit	
63	PBC_NND.1	Notification of non-delivery	
64	PBC_BKP.1	Backup	
65	PBC_SYN.1	Synchronization	

The functional requirements are described below. Throughout these descriptions the following nomenclature is followed:

- [operation-type: *italics text*] indicates an incomplete operation of the type specified
- [normal text] indicates a completed operation, with the operation type omitted to improve the readability of the resulting requirement.

5.1.1 Class FAU: Security audit

5.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions,

b) All auditable events for the *basic* level of audit, and

c) Events concerning

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)

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [name of object and type of access event for attempts to perform an operation on an object covered by the SFP (FDP_ACF.1 basic auditable events), assignment: *other audit relevant information*]

Dependencies: FPT_STM.1 Reliable time stamps

5.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

5.1.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.4 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

5.1.1.5 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: *searches, sorting, ordering*] of audit data based on [assignment: *criteria with logical relations*].

Dependencies: FAU_SAR.1 Audit review

5.1.1.6 FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [user identity, selection: *object identity, subject identity, host identity, event type*]

b) [assignment: list of additional attributes *that audit selectivity is based upon*].

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

5.1.1.7 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: No other components.

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] audit records will be maintained when the following conditions occur: [refinement: restart of the TOE], [selection: *audit storage exhaustion, failure, attack*].

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.8 FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

FAU_STG.3.1 The TSF shall [assignment: generate an alarm to the authorized administrator] if the audit trail exceeds [assignment: *pre-defined limit*].

5.1.2 Class FCO: Communication

5.1.2.1 FCO_NRO.2 Enforced proof of origin

Hierarchical to: FCO_NRO.1.

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [assignment: *list of information types*] at all times.

FCO_NRO.2.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the Originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of origin*].

5.1.2.2 FCO_NRR.2 Enforced proof of receipt

Hierarchical to: FCO_NRR.1.

FCO_NRR.2.1 The TSF shall enforce the generation of evidence of receipt for received [assignment: *list of information types*].

FCO_NRR.2.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the recipient of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of receipt*].

Refinement:

The TSF shall provide the capability to send an attestation of reception when information was received under the agreed upon conditions of integrity and confidentiality.

Dependencies: FIA_UID.1 Timing of identification

Additional dependencies due to refinement:

FDP_UCT.1 Basic Data Exchange Confidentiality
FDP_UIT.1 Data Exchange Integrity

5.1.3 Class FCS: Cryptographic support

5.1.3.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Refinements:

The cryptographic key generation algorithm selected shall meet the following requirements:

a) The method shall ensure the unpredictable generation of truly random and prime numbers.

b) If a user's key has been broken, the new key shall be generated independently from the broken keys.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.3.2 FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].

Refinement:

The cryptographic key distribution method selected shall meet the following requirements:

a) The lifetime of keys shall be definable, depending on the privacy policy of the user or the IT Security Policy of the enterprise.

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

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

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

e) 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 certificate content shall be verified.

f) The transmission of key exchange information shall be independent from the broken keys.

g) 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.

h) 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.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.3.3 FCS_CKM.3 Cryptographic key access

Hierarchical to: No other components.

FCS_CKM.3.1 The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].

Refinement

The cryptographic key access method specified shall meet the following requirements:

a) The TSF 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.

b) The TSF shall provide adequate means to ensure the authenticity and integrity of the stored registration data.

c) The TSF shall provide adequate means to ensure the authenticity and integrity of the stored certification data.

d) The TSF shall provide adequate means for the authenticity and integrity of the stored certification data.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.3.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Refinement:

The cryptographic key destruction method specified shall meet the following requirement:

a) 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.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

5.1.4 Class FDP: User data protection

5.1.4.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.4.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on [assignment: *security* attributes, named groups of security attributes].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Refinement:

The access control SFP shall support the following requirements:

a) It shall be possible to grant rights down to the granularity of an individual user.

b) It shall be possible to grant the access rights down to the granularity of an individual group.

c) The TSF 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.

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

e) 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.

f) 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.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

5.1.4.3 FDP_DAU.1 Basic data authentication

Hierarchical to: No other components.

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [unique objects].

FDP_DAU.1.2 The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information.

Dependencies: No dependencies.

5.1.4.4 FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to prevent the [disclosure and modification] of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

5.1.4.5 FDP_RIP.2 Full residual information protection

Hierarchical to: FDP_RIP.1.

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] all objects.

Dependencies: No dependencies

5.1.4.6 FDP_SDI.1 Stored data integrity monitoring

Hierarchical to: No other components.

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

Dependencies: No dependencies.

5.1.4.7 FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [transmit and receive] objects in a manner protected from unauthorized disclosure.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

5.1.4.8 FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [selection: *transmit, receive*] user data in a manner protected from [modification, deletion, and insertion] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [modification, deletion, and insertion] has occurred.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

5.1.5 Class FIA: Identification and authentication

5.1.5.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall

[1. Cause the logon procedure to exit and end the session.

2. Provide a mechanism to immediately notify administration when the threshold is exceeded.

3. Ensure that a customer-specifiable interval of time shall elapses before the logon procedure can be restarted on that I/O port.

4. Not suspend the user upon exceeding the above threshold.]

Dependencies: FIA_UAU.1 Timing of authentication

5.1.5.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*] [refinement: and customer-defined information].

Dependencies: No dependencies.

5.1.5.3 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

Dependencies: No dependencies.

5.1.5.4 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

5.1.5.5 FIA_UAU.3 Unforgeable authentication

Hierarchical to: No other components.

FIA_UAU.3.1 The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall [selection: *detect, prevent*] use of authentication data that has been copied from any other user of the TSF.

Dependencies: No dependencies.

5.1.5.6 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following rules:]

[a) assignment: Identification and authentication over many stages a chain of trust has to be established. The system shall be able to verify this chain to the roots.]

[b) assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

Dependencies: No dependencies.

5.1.5.7 FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [of session lock and assignment: *list of conditions under which re-authentication is required*].

Dependencies: No dependencies.

5.1.5.8 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only [feedback that not indicate the presence or absence of such duplicated authentication information.] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

5.1.5.9 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user**.**

Dependencies: No dependencies.

5.1.5.10 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: FIA_ATD.1 User attribute definition

5.1.6 Class FMT: Security management

5.1.6.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behavior of, disable, enable, modify the behavior of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

Iteration of FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [enable and disable] the functions of [auditing auditable events] to [assignment: *the authorized identified roles*].

Dependencies: FMT_SMR.1 Security roles

5.1.6.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

5.1.6.3 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE Security Policy model
[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.1.6.4 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [restrictive, permissive, other property] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.1.6.5 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].

Iteration of FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [modify] the [logon message] to [assignment: *the authorized identified roles*].

Iteration of FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [query] the [status of any user] to [assignment: *the authorized identified roles*].

Iteration of FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [copy to a specifiable storage medium] the [audit trail files] to [assignment: *the authorized identified roles*].

Iteration of FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [generate a status report of] the [values of settable security parameters] to [assignment: *the authorized identified roles*].

Dependencies: FMT_SMR.1 Security roles

5.1.6.6 FMT_SAE.1 Time-limited authorization

Hierarchical to: No other components.

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [unused user IDs, assignment: *list of security attributes for which expiration is to be supported*] to [assignment: *the authorized identified roles*].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.

Iteration of FMT_SAE.1 Time-limited authorization

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [authentication information] to [assignment: *the authorized identified roles*].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [enforce periodic changes] after the expiration time for the indicated security attribute has passed.

Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

5.1.6.7 FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1

FMT_SMR.2.1 The TSF shall maintain the roles: [assignment: *the authorized identified roles*].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [assignment: *conditions for the different roles*] are satisfied.

Dependencies: FIA_UID.1 Timing of identification.

5.1.7 Class FPR: Privacy

5.1.7.1 FPR_ANO.1 Anonymity

Hierarchical to: No other components.

FPR_ANO.1.1 The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*].

Dependencies: No dependencies.

5.1.7.2 FPR_PSE.1 Pseudonymity

Hierarchical to: No other components.

FPR_PSE.1.1 The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*].

FPR_PSE.1.2 The TSF shall be able to provide [assignment: *number of aliases*] aliases of the real user name to [assignment: *list of subjects*].

FPR_PSE.1.3 The TSF shall [selection: *determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [assignment: *alias metric*].

Dependencies: No dependencies.

5.1.7.3 FPR_UNO.1 Unobservability

Hierarchical to: No other components.

FPR_UNO.1.1 The TSF shall ensure that [assignment: *list of users and/or subjects*] are unable to observe the operation [assignment: *list of operations*] on [assignment: *list of objects*] by [assignment: *list of protected users and/or subjects*].

Dependencies: No dependencies.

5.1.8 Class FPT: Protection of the TOE security functions

5.1.8.1 FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components.

FPT_AMT.1.1 The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorized user, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies: No dependencies.

5.1.8.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].

Dependencies: ADV_SPM.1 Informal TOE Security Policy model

5.1.8.3 FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Dependencies: No dependencies.

5.1.8.4 FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to: No other components.

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment: a defined modification metric].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

Dependencies: No dependencies.

5.1.8.5 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure and modification] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies.

5.1.8.6 FPT_RCV.1 Manual recovery

Hierarchical to: No other components.

FPT_RCV.1.1 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

Dependencies: FPT_TST.1 TSF testing
AGD_ADM.1 Administrator guidance
ADV_SPM.1 Informal TOE Security Policy model

5.1.8.7 FPT_RPL.1 Replay detection

Hierarchical to: No other components.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [authentication data, commitment data, certificates, assignment: *list of identified entities*].

FPT_RPL.1.2 The TSF shall perform [assignment: *list of specific actions*] when replay is detected.

Dependencies: No dependencies.

5.1.8.8 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

5.1.8.9 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.1.8.10 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

5.1.8.11 FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [access control parameters for business transactions, logs of business transactions, assignment: *list of TSF data types*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

Dependencies: No dependencies.

5.1.8.12 FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Dependencies: FPT_AMT.1 Abstract machine testing

5.1.9 Class FRU: Resource utilization

5.1.9.1 FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

FRU_FLT.1.1 The TSF shall ensure the operation of [alternate communication channels] when the following failures occur: [transmission blockage].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

5.1.9.2 FRU_RSA.1 Maximum quotas

Hierarchical to: No other components.

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [communication resources] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].

Dependencies: No dependencies.

5.1.10 Class FTA: TOE access

5.1.10.1 FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: *time interval of user inactivity*] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].

Dependencies: FIA_UAU.1 Timing of authentication

5.1.10.2 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Dependencies: No dependencies.

5.1.10.3 FTA_TAH.1 TOE access history

Hierarchical to: No other components.

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [date, time, method, and location] of the last successful session establishment to the user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [date, time, method, and location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

Dependencies: No dependencies.

5.1.10.4 FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [an administrator temporarily disabling a user's access to the TOE].

Dependencies: No dependencies.

5.1.11 Class FTP: Trusted path channels

5.1.11.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Dependencies: No dependencies.

5.1.12 New components

Several E - COFC requirements did not have corresponding CC Part 2 components. These components have been added to the E - COFC Protection Profile as extensions to Part 2.

5.1.12.1 PBC_DYN.1 Dynamic control of audit

Hierarchical to: No other components.

PBC_DYN.1.1 The TSF shall provide a [selection: *authorized users*] with the capability to perform the following actions at any time during normal TOE operation:

a) enable or disable auditable events

b) change the selection of attributes to be audited,

c) manage the audit trail.

Dependencies: No dependencies.

5.1.12.2 PBC_NDD.1 Notification of non-delivery

Hierarchical to: No other components.

PBC_NDD.1 If delivery was not accomplished, the Originator or Destination shall be notified by the transport service for the reasons of failed delivery.

Dependencies: No dependencies.

5.1.12.3 PBC_BKP.1 Backup

Hierarchical to: No other components.

FTP_BKP.1.1 The TSF shall provide procedures for software and data backup and restoration.

Dependencies: No dependencies.

5.1.12.4 PBC_SYN.1 Synchronization

Hierarchical to: No other components.

PBC_SYN.1.1 The TSF shall be able to provide the capability to determine the order in which security relevant events occurred.

Dependencies: FPT_STM.1 Trusted Time Stamp.

5.2 TOE assurance requirements

This clause is copied from [CS2 PPG] because it is believed that the assurance requirements for the CS2 and E - COFC Protection Profiles are equivalent.

The assurance requirements for the E - COFC PB-Class are the EAL2 assurance components augmented by additional assurance components from the Common Criteria.

Table 6 – Assurance components

Assurance class	Component ID	Component title
Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: High-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - Sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.2.1 Class ACM: Configuration management

5.2.1.1 ACM_CAP.3 Authorization controls

Dependencies: CM_SCP.1, ALC_DVS.1

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the TOE configuration items.

ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 ACM_SCP.2 Problem tracking CM coverage

Dependencies: ACM_CAP.3

Developer action elements:

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Class ADO: Delivery and operation

5.2.2.1 ADO_DEL.1 Delivery procedures

Dependencies: None

Developer action elements:

ADO_DEL.1.1D The developer shall document the procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe the procedures which are necessary to maintain security when distributing versions of the TOE to a user site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies: AGD_ADM.1

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures to be used for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall confirm that the installation procedures result in a secure configuration.

5.2.3 Class ADV: Development (ADV)

5.2.3.1 ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 ADV_HLD.1 Descriptive high-level design

Dependencies: ADV_FSP.1, ADV_RCR.1

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify the interfaces of the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate an complete instantiation of the TOE security functional requirements.

5.2.3.3 ADV_RCR.1 Informal correspondence demonstration

Dependencies: None

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.4 ADV_SPM.1 Informal TOE Security Policy model

Dependencies: ADV_FSP.1

Developer action elements:

ADV_SPM.1.1D The developer shall provide an TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that there are no security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Class AGD: Guidance documents

5.2.4.1 AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all security parameters under the control of the administrator indicating safe values as appropriate.

AGD_ADM.1.5C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.6C The administrator guidance shall be consistent with all other documents supplied for evaluation.

AGD_ADM.1.7C The administrator guidance shall describe all security requirements on the IT environment which are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 AGD_USR.1 User guidance

Dependencies: ADV_FSP.1

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including all assumptions about user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation delivered for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements on the IT environment which are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Class ALC: Life cycle support

5.2.5.1 ALC_DVS.1 Identification of security measures

Dependencies: None

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall check whether the security measures are being applied.

5.2.5.2 ALC_FLR.2 Flaw reporting procedures

Dependencies: None

Developer action elements:

ALC_FLR.2.1D The developer shall document the flaw remediation procedures.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

Content and presentation of evidence elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.2.6C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

Evaluator action elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6 Class ATE: Tests

5.2.6.1 ATE_COV.2 – Analysis of coverage

Dependencies: ADV_FSP.1, ATE_FUN.1

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator Actions:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.2 ATE_DPT.1 Testing: High level design

Dependencies: ADV_HLD.1, ATE_FUN.1

Developer action elements:

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TOE operates in accordance with the high level design.

Evaluator action elements:

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.3 ATE_FUN.1 Functional testing

Dependencies: None

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The test results in the test documentation shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each security function operates as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.4 ATE_IND.2 Independent Testing - Sample

Dependencies: ADV_FSP.1, AGD_USR.1, AGD_ADM.1, ATE_FUN.1

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test the TSF to confirm that the TSF operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.7 Class AVA: Vulnerability assessment

5.2.7.1 AVA_MSU.2 Validation of analysis

Dependencies: ADO_IGS.1, AGD_ADM.1, AGD_USR.1, ADV_FSP.1

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, consistent and reasonable.

AVA_MSU.2.3.C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to check that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.2.7.2 AVA_SOF.1 Strength of TOE security function evaluation

Dependencies: ADV_FSP.1, ADV_HLD.1

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each identified mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.2.7.3 AVA_VLA.1 Developer vulnerability analysis

Dependencies: ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

Developer action elements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C The evidence shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, based on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.2.8 Class AMA: Maintenance of assurance

None.

5.3 Security requirements for the IT environment

The environment is required to satisfy the secure usage assumptions in 3.1 and to meet all of the environmental security objectives outlined in 4.2.

Annex A

PP Rationale

A.1 Introduction to PP Rationale

This annex provides the Rationale for the E - COFC Public Business Class Protection Profile (PP) under separate cover. This PP Rationale document has two goals: first, to show that the E - COFC Protection Profile is internally consistent and technically correct and secondly, to show that the E - COFC PP is a faithful instantiation of Standard ECMA-271, *Extended Commercially Oriented Functionality Class*.

Clauses A.2 through A.5 address the internally consistency and technical correctness of the E - COFC PP. Clause A.2 shows that the identified threats have been addressed, and that are no objectives that do not address any identified threats. In the functional requirements clause, it shows that there are functional components to address all of the identified objectives. It also shows that there are no functional components that do not address objectives. The dependencies clause shows that all of the dependencies have been satisfied. The assurance rationale clause provides the rationale for the selection of EAL2 and the augmented assurance components.

Since the E - COFC Public Business Class Protection Profile is intended to implement ECMA-271, clauses have been provided to map the ECMA-271 material to the E - COFC Protection Profile. Clause A.6 demonstrates how the PP threats were derived from the threats contained in ECMA-205 and ECMA-271. Clause A.7 shows how the PP objectives were derived from material in ECMA-205 and ECMA-271. Clause A.8 maps the ECMA-271 security functionalities to the functional components included in the E - COFC PP. Clause A.9 maps the E - COFC PP functional components to the ECMA–271 security functionalities.

A.2 Security objectives rationale

This clause shows that the identified threats have been addressed and that there are no objectives that do not address any identified threats or policies.

A.2.1 All identified threats addressed

This clause shows that all the identified threats have been addressed.

Table A.1 – All threats met by objectives

No	PP threat name	PP threat description	PP objectives
1	T.Actions_Traced	Unauthorized tracing of customer business actions may occur without detection.	O.Access_Control O.Anon
2	T.Blockage	Two systems may not be able to exchange data due to a communications channel being blocked.	O.Alt_Channel
3	T.Change_Data	Information may be changed either while it being stored or processed within the TOE or during transmission. The changes may be accidental or intentional. Changes include insertions, replacements, modifications, and deletions. The type of information that can be changed includes user information, system information, business data, and commitment.	O.Access_Control O.Authen O.Integrity O.Recover O.Sequence O.Status O.System_Integrity
4	T.Comm_Failure	It may not be possible to set up a connection or transmit data between two systems.	O.Alt_Channel O.Audit
5	T.Data_Theft	Business process data may be stolen.	O.Access_Control O.Authen
5.1	T.Deny_Service	Application and network services may not be available for use.	O.Authen O.Access_Control O.Resources
6	T.Deny_Data	An entity may deny ownership of business or commitment data.	O.Nonrep_Orig O.Attest O.Assoc_User_Action
7	T.Deny_Receipt	An entity may deny that it has received business or commitment data.	O.Attest O.Nonrep_Dest
8	T.Deny_Submit	An entity may deny that it has submitted business or commitment data.	O.Attest O.Nonrep_Orig
9	T.Disaster	Natural disasters may cause TOE or system failure.	O.Backup O.Recover
10	T.Disclose_Data	Information may be disclosed in to unauthorized users. This includes both user information, system information and business data. Information may be disclosed while being stored or processed in the TOE or during transmission. Disclosure of authentication data during transmission would allow someone to logon and assume the identity of an authorized user.	O.Access_Control O.Authen O-Flow_Control O.Resid_Prot O.Authen_Protect
11	T.False_Routing	Information may be routed to a false address enabling unauthorized access.	O.Authen_Address
12	T.History_Untraceable	It may not be possible to trace the sequence of events during a system failure, malfunction, or betrayal.	O.Consistency O.Sequence

Table A.1 – All threats met by objectives (continued)

No	PP threat name	PP threat description	PP objectives
13	T.Impersonate	Someone may obtain unauthorized access by impersonating an unauthorized user, for example by hijacking a communications session.	O.Assoc_User_Action O.Authen O.Authen_Address O.Integrity O.Replay O.Sequence
14	T.Indeterminate_Seq	It may be impossible to determine the sequence of events in a dispute due to missing time information and business related data.	O.Audit O.Sequence
15	T.Insider	An authorized user of the TOE may gain unauthorized access.	O.Access_Control O.Assoc_User_Action O.Audit O.Authen O.Dynamic
16	T.Intercept	Commitment data or certificates may be intercepted.	O.Authen_Age O.Key_Indep_Gen O.Key_Indep_Trans
17	T.Invalid_Certificate	The TOE may accept invalid commitment data or certificates.	O.Access_Control O.Authen_Age O.Integrity O.Revoke_Cert
18	T.Logon_Attack	A program that tries a large number of passwords successfully guesses the password of an authorized user. This allows an unauthorized individual to logon as an authorized user and to assume the identity of that user.	O.Logon_Limit
19	T.Outsider	An individual who is not an authorized user of the system may gain access to the TOE.	O.Access_Control O.Authen O.Dynamic O.Flow_Control
20	T.Physical	A component of the system may be accidentally or intentionally damaged.	O.Backup O.Recover
21	T.Privacy_Violated	Unauthorized access to privacy data of system users may occur.	O.Access_Control O.Anon O.Authen
22	T.Refusal	Unauthorized refusal of valid commitment data or certificates may occur.	O.Access_Control O.Integrity O.Revoke_Cert
23	T.Replace_TOE	The TOE may be replaced by an untrusted system.	O.System_Integrity
24	T.Replay	Someone may obtain unauthorized access by replaying authentication or commitment data.	O.Sequence O.Replay O.Authen_Address

Table A.1 – All threats met by objectives (concluded)

No	PP threat name	PP threat description	PP objectives
25	T.Secret_Disclose	Authentication information may be disclosed allowing someone to logon and assume the identity of an authorized user.	O.Authen_Age O.Authen_Indep O.Authen_Protect
26	T.Service_Denied	Application and network services may not be available for use.	O.Authen O.Access_Control O.Flow_Control O.Denial_Sophisticated O.Dynamic O.Alt_Channel
27	T.TOE_Fail	TOE or system failure may cause the TOE to enter an insecure state or data to be disclosed or changed.	O.Backup O.Recover
28	T.Traffic	A system may experience degraded performance due to increased communications traffic.	O.Filter
29	T.Unique_Copied	Unlawful copies may be made of unique originals.	O.Unique

A.2.2 No unnecessary objectives

This clause shows that every objective addresses at least one threat.

Table A.2 – All objectives necessary

Objective name	Objective description	Threat addressed
O.Access_Control	The TOE must enforce an access control policy protects information from unauthorized access.	T.Disclose_Data T.Change_Data T.Outsider T.Denial T.Insider T.Invalid_Certificate T. Refusal T.Data_Theft T.Privacy_Violated T.Actions_Traced T.Replace_TOE
O.Alt_Channel	The TOE must provide alternate channels for the transmission of data.	T.Blockage T.Comm_Failure T.Service_Denied
O.Anon	The TOE must provide for anonymity and pseudonymity.	T.Privacy_Violated T.Actions_Traced
O.Assoc_User_Action	The TOE shall associate all security relevant actions with a unique user identity.	T.Insider T.Impersonate T.Insider

Table A.2 – All objectives necessary (continued)

Objective name	Objective description	Threat addressed
O.Attest	The TOE must provide for attestation of submission, delivery and receipt.	T.Deny_Receipt T.Deny_Submit T.Deny_Data
O.Audit	All security relevant actions must be auditable.	T.Insider T.History_Untraceable T.Comm_Failure
O.Authen	Users will be uniquely identified and authenticated prior to performing any actions to be mediated by the TOE.	T.Outsider T.Insider T.Change_Data T.Denial T.Impersonate T.Data_Theft T.Disclose_Data T.Privacy_Violated
O.Authen_Address	The TOE must be able to authenticate sender and receiver addresses. This includes a priori business qualification of Originator and Destination.	T.Impersonate T.Comm_Failure T.False Routing
O.Authen_Age	The TOE must provide for the expiration of authentication information (except for biometric information).	T.Secret_Disclose T.Invalid_Certificate
O.Authen_Indep	A user may share the same authentication information as another user, but the TOE must not reveal this fact.	T.Secret_Disclose
O.Authen_Protect	The TOE must protect authentication information.	T.Secret_Protect T.Disclose_Data
O.Backup	The TOE must provide data backup and restoration.	T.TOE_Fail T.Disaster T.Comm_Failure T.Physical
O.Confidentiality _Trans	The TOE must be able to protect transmitted information from unauthorized disclosure.	T.Disclose_Data
O.Consistency	The TOE must be able to maintain consistency between TSF data stored on different systems such as user identity, user attributes, and timing information.	T.History_Untraceable
O.Dynamic	The TOE must provide for the selection of auditable events and management of the audit trail during normal operations so that suspected unauthorized activity can be monitored as it occurs without alerting a perpetrator.	T.Insider T.Outsider T.False_Routing T.Blockage T.Service_Denied
O.Filter	The TOE must provide for the filtering of communications with respect to resource utilisation.	T.Traffic

Table A.2 – All objectives necessary (concluded)

Objective name	Objective description	Threat addressed
O_Flow_Control	The TOE must enforce an information flow policy at specefied boundaries.	T.Outsider T.Service_Denied T.Disclose_Data
O.Integrity	The TOE must be able to protect and verify the integrity of stored or transmitted data. This includes user and TSF data such as commitment data, business data, business data with commitment data, or certificates.	T.Modif_Data T.Delete_Data T.Insert_Data T.Impersonate T.Change_Data T.Invalid_Certificate T.Refusal
O.Key_Indep_Gen	The TOE must generate new keys independently of broken keys.	T.Intercept
O.Key_Indep_Distrib	The TOE must distribute new keys independently of broken keys.	T.Intercept
O.Logon_Limit	The TOE must limit the number of logon attempts.	T.Log_Attack
O.Nonrep_Dest	The TOE must protect against repudiation by the Destination.	T.Deny_Receipt
O.Nonrep_Orig	The TOE must protect against repudiation by the Originator.	T.Deny_Submit T.Deny_Data
O.Recover	The TOE must be able to recover the TOE to a secure state.	T.TOE_Fail T.Disaster T.Comm_Failure T.Change_Data T.Physical
O.Replay	The TOE must protect against replay attacks.	T.Impersonate T.Replay
O.Resid_Prot	Information stored within the TOE must not be made available to other users upon release.	T.Disclose_Data
O.Revoke_Cert	The TOE must provide for the revocation of certificates.	T.Invalid_Certificate T.Refusal
O.Resource	The TOE must protect against loss of availability through resource exhaustion.	T.Service_Denied
O.Sequence	The TOE must ensure that it is possible to determine the correct sequence of events. All audit trails within a TOE must include reliable time stamps that can be correlated each other to determine the sequence of events. Similarly, the TOE must support the sequencing of communication data so that the insertion or deletion of network packets can be detected.	T.Insert_Trans_Data T.Replay T.Impersonate T.Indeterminate_Seq T.History_Untraceable
O.Status	It must be possible to determine the status of security relevant TOE parameters.	T.Change_Data
O.System_Integrity	The TOE must provide for procedures shall be provided to verify the software integrity of the TOE.	T.Change_Data T.Replace_TOE
O.Unique	The TOE must enforce the uniqueness of an original.	T.Unique_Copied

A.3 Functional requirements rationale

This clause shows that all the objectives are addressed by functional components and that all functional components address at least one objective.

A.3.1 All objectives addressed

This clauses shows that all the objectives have been addressed by functional components.

Table A.3 – All objectives met by CC functional components

Objective name	Objective description	E - COFC Req. No.	E - COFC Req. title	Functional component(s)
O.Access_Control	The TOE must enforce an access control policy protects information from unauthorized access.	6.2, 7.4.2	Access control	FDP_ACC.1
		7.4.2.2	Individual user	FDP_ACF.1
		7.4.2.3	User groups	
		7.4.2.5	Types of access rights	
		7.4.2.6	Default access rights	
		7.4.2.7	Precedence of access rights	
		7.4.7.5	Denial of service	
		7.4.2.10	Application controlled access rights	
		7.4.2.4	Objects	FPT_SEP.1
				FMT_SMR.2
				FAU_SAR.2
		7.4.2.6	Default access rights	FMT_MSA.3
		7.4.2.9	Verification of rights	FPT_RVM.1
		9.4.2	Access control	FPR_UNO.1
O.Alt_Channel	The TOE must provide alternate channels for the transmission of data.	7.4.7.4	Transmission blockage	FRU_FLT.1
O.Anon	The TOE must provide for anonymity and pseudonymity.	9.4.2.1	Protection against unlawful disclosure	FPR_ANO.1 FPR_PSE.1
O.Assoc_User_ Action	The TOE shall associate all security relevant actions with a unique user identity.	6.3.1, 7.4.4.1	Associate actions and users	FAU_GEN.2 FIA_USB.1
O.Attest	The TOE must provide for attestation of submission, delivery, and receipt.	8.4.2.3	Attestation of submission, delivery, receipt	FCO_NRO.1 FCO_NRR.1 FCO_NND.1
			(under agreed upon conditions of confidentiality and integrity)	FPT_ITC.1 FPT_ITI.1

Table A.3 – All objectives met by CC functional components (continued)

Objective name	Objective description	E - COFC Req. No.	E - COFC Req. title	Functional component(s)
O.Audit	All security relevant actions must be auditable.	6.3, 7.4.4	Accountability and audit	FAU_GEN.1 FAU_SEL.1
		7.4.4.3	Enable and disable events	FMT_MOF.1 R
		7.4.4.8	TOE restart	FAU_STG.2
		7.4.4.9	Copy audit trails	FMT_MTD.1
		7.4.4.10	Alarm if unable to record	FAU_STG.3
		7.4.4.12	Dynamic control	New
		7.4.4.13	Audit tools	FAU_SAR.1
				FAU_SAR.3
		7.4.7.5	Denial of service	FAU_GEN.1
		8.4.2.5	Requirements for the tracing of data	FAU_STG.1
		9.4.3.1	Inter-related accountability	FAU_STG.1
O.Authen	Users will be uniquely identified and authenticated prior to performing any actions to be mediated by the TOE.	6.1, 7.4.1	Identification and authentication	FIA_UID.1 FIA_UAU.1
		7.4.1.1	Unique I & A	
		7.4.1.2	I & A prior to all other interactions	
		7.4.7.5	Denial of service	FAU_GEN.1
		7.4.1.3	Secure authentication protocol	FIA_UAU.3
		7.4.1.4	Associate information to users	FIA_ATD.1 FMT_MSA.1
		7.4.1.5	Logon message	FTA_TAB.1 FMT_MTD.1 FTA_TAH.1
		7.4.1.8	Session lock or terminate	FTA_SSL.1 FTA_SSL.3 FIA_UAU.6
		7.4.1.9	Disable users temporarily	FTA_TSE.1
		9.4.1	Identification and authentication	FIA_UAU.5 FCS_CKM.2
O.Authen_ Address	The TOE must be able to authenticate sender and receiver addresses. This includes a priori business qualification of Originator and Destination.	7.4.1.3	Identification and authentication of users	FCO_NRO.2 FCO_NRR.2
		7.4.3.2	Address integrity of exchanged information	FCO_NRO.2 FCO_NRR.2
		8.4.1.1	Qualification	FDP_ACF.1 FCS_CKM.2

Table A.3 – All objectives met by CC functional components (continued)

Objective name	Objective description	E - COFC Req. No.	E - COFC Req. title	Functional component(s)
O.Authen_Age	The TOE must provide for the expiration of authentication information (except for biometric information). This includes cryptographic keys, certificates and commitment data.	6.1.11, 7.4.1.13	Authentication information aging	FMT_SAE.1
		7.4.1.7	Expiration of unused user IDs	FMT_SAE.1
O.Authen_Indep	A user may share the same authentication information as another user, but the TOE must not reveal this fact.	6.1.10, 7.4.12	Authentication information independence	FIA_UAU.7
O.Authen_Protect	The TOE must protect authentication information.	6.1.9, 7.4.1.11	Authentication information protection	FPT_SEP.1
				FCS_CKM.3
				FIA_SOS.1
O.Backup	The TOE must provide data backup and restoration.	6.6.2, 7.4.7.2	Data backup	PBC_BKP.1
O.Confidentiality	The TOE must be able to protect information from unauthorized disclosure. This includes TSF data and user data during transmission. (User data internal to a system is protected by internal access control.)	7.4.3.3	Confidentiality of exchanged information	FDP_UCT.1 FPT_ITC.1 FPT_ITI.1
O.Consistency	The TOE must be able to maintain consistency between TSF data stored on different systems such as user identity, user attributes, and timing information.	8.4.1.2	Consistency	FPT_TDC.1
		9.4.3.1	Inter-related accountability	
O.Dynamic	The TOE must provide for the selection of auditable events and management of the audit trail during normal operations so that suspected unauthorized activity can be monitored as it occurs without alerting a perpetrator.	7.4.4.10	Alarm if unable to record	PBC_DYN.1
		7.4.4.12	Dynamic control	
O.Filter	The TOE must provide for the filtering of communications with respect to resource utilisation	7.4.7.3	Filtering	FRU_RSA.1
O.Integrity	The TOE must be able to protect and verify the integrity of stored or transmitted data. This includes user and TSF data such as commitment data, business data, business data with commitment data, or certificates.	6.5.1, 7.4.6.2	Data integrity	FDP_SDI.1
		7.4.7.5	Denial of service	FDP_SDI.1
		7.4.3.1	Content integrity of exchanged information	FDP_UIT.1 FDP_ITT.1 FPT_ITI.1 FPT_ITT.1
		9.4.4.1	Content integrity and content validation of exchanged commitment data or certificates	FCS_CKM.2
O.Key_Indep_Gen	The TOE must be able to generate new keys independently of broken keys.	9.4.5.1	Registration	FCS_CKM.1

Table A.3 – All objectives met by CC functional components (concluded)

Objective name	Objective description	E - COFC Req. No.	E - COFC Req. title	Functional component(s)
O.Key_Indep_ Distrib	The TOE must distribute new keys independently of broken keys.	9.4.5.3	Distribution	FCS_CKM.2
O.Logon_Limit	The TOE must limit the number of logon attempts.	6.1.5, 7.4.1.6	Number of logon trials	FIA_AFL.1
O.Nonrep_Dest	The TOE must protect against repudiation by the Destination.	8.4.2.2	Non-repudiation of the Destination	FCO_NRR.1
		8.4.2.3		FCO_NND.1
O.Nonrep_Orig	The TOE must protect against repudiation by the Originator.	8.4.2.1	Non-repudiation of the Originator	FCO_NRO.1
O.Recover	The TOE must be able to recover the TOE to a secure state.	6.6.1, 7.4.7.1	Recovery	FPT_RCV.1
O.Flow_Control	The TOE must enforce an information flow control policy at specified boundaries.	7.3.16 7.3.17 7.4.7.5	Outsider attack: Unauthorized access to the TOE to penetrate system information. Denial of service (application, network services, malicious code input (Trojan Horse)) Denial of service	FDP_IFC.1 FDP_IFF.1 FDP_IFC.1
O.Replay	The TOE must protect against replay attacks.	7.4.1.3	Secure authentication protocol	FIA_UAU.3 FPT_RPL.1
		9.4.4.2	Address integrity of exchanged commitment data or certificates	FCO_NRO.2 FCO_NRR.2
O.Resid_Prot	Information stored within the TOE must not be made available to other users upon release.	6.4, 7.4.5	Object reuse	FDP_RIP.2
O.Revoke_Cert	The TOE must provide for the revocation of certificates.	9.4.5.4	Revocation	FCS_CKM.4
O.Sequence	The TOE must ensure that it is possible to determine the correct sequence of events. All audit trails within a TOE must include reliable time stamps that can be correlated each other to determine the sequence of events. Similarly, the TOE must support the sequencing of communication data so that the insertion or deletion of network packets can be detected.	7.4.4.14	Synchronization	PBC_SYN
		8.4.2.4	Timing information of audit data	FPT_STM.1
		9.4.3.1	Inter-related accountability	PBC_SYN
O.Status	It must be possible to determine the status of security relevant TOE parameters.	6.5.3, 7.4.6.3	Security parameters status report	FMT_MTD.1
		7.4.1.10	User status information	FMT_MTD.1
O.System_ Integrity	The TOE must provide procedures shall be provided to verify the software integrity of the TOE.	6.5.1, 7.4.6.1	TOE software integrity	FPT_TST.1
O.Unique	The TOE must enforce the uniqueness of an original.	9.4.3.4	Uniqueness of original	FDP_DAU.1 R
O.Resource	The TOE must protect against loss of availability through resource exhaustion.	7.3.17	Denial of service (application, network services, malicious code input (Trojan Horse))	FRU_RSA.1

A.3.2 All functional components necessary

This clauses shows that each functional components addresses at least one objective.

Table A.4 – All functional components necessary

No	Component	Name	Objectives
1	FAU_GEN.1	Audit data generation	O.Audit
2	FAU_GEN.2	User identity generation	O.Assoc_User_Action
3	FAU_SAR.1	Audit review	O.Audit
4	FAU_SAR.2	Restricted audit review	O.Access_Control
5	FAU_SAR.3	Selectable audit review	O.Audit
6	FAU_SEL.1	Selective audit	O.Audit
7	FAU_STG.2	Guarantees of audit trail availability	O.Audit
8	FAU_STG.3	Action in case of possible audit data loss	O.Audit
9	FCO_NRO.2	Enforced proof of origin	O.Attest O.Authen_Address O.Nonrep_Orig O.Replay
10	FCO_NRR.2	Enforced proof of receipt	O.Attest O.Authen_Address O.Nonrep_Dest O.Replay
11	FCS_CKM.1	Cryptographic key generation	O.Key_Indep_Gen
12	FCS_CKM.2	Cryptographic key distribution	O.Authen O.Authen_Address O.Integrity O.Key_Indep_Distrib
13	FCS_CKM.3	Cryptographic key access	O.Authen_Protect
14	FCS_CKM.4	Cryptographic key destruction	O.Revoke_Cert
15	FDP_ACC.1	Subset access control	O.Access_Control
16	FDP_ACF.1	Security attribute based access control	O.Access_Control O.Authen_Address
17	FDP_DAU.1	Basic data authentication	O.Unique
17.1	FDP_IFC.1	Subset information flow control	O.T_Outsider
17.2	FDP_IFF.1	Simple security attributes	O.Flow_Control
18	FDP_ITT.1	Basic internal transfer protection	O.Integrity
19	FDP_RIP.2	Full residual information protection	O.Resid_Prot
20	FDP_SDI.1	Stored data integrity monitoring	O.Integrity
21	FDP_UCT.1	Basic data exchange confidentiality	O.Attest O.Confidentiality

Table A.4 – All functional components necessary (continued)

No	Component	Name	Objectives
22	FDP_UIT.1	Data exchange integrity	O.Attest O.Integrity
23	FIA_AFL.1	Basic authentication failure handling	O.Logon_Limit
24	FIA_ATD.1	User attribute definition	O.Authen
25	FIA_SOS.1	Selection of secrets	O.Authen_Protect
26	FIA_UAU.1	Timing of authentication	O.Authen
27	FIA_UAU.3	Unforgeable authentication	O.Authen O.Replay
28	FIA_UAU.5	Multiple authentication mechanisms	O.Authen
29	FIA_UAU.6	Re-authenticating	O.Authen
30	FIA_UAU.7	Protected authentication feedback	O.Authen_Indep
31	FIA_UID.1	Timing of identification	O.Authen
32	FIA_USB.1	User-subject binding	O.Assoc_User_Action
33	FMT_MOF.1	Management of security functions behavior	O.Audit
34	FMT_MSA.1	Management of security attributes	O.Authen
35	FMT_MSA.2	Secure security attributes	Dependency (FCS_CKM.2)
36	FMT_MSA.3	Static attribute initialization	O.Access_Control
37	FMT_MTD.1	Management of TSF data	O.Authen O.Status
38	FMT_SAE.1	Time-limited authorization	O.Authen_Age
39	FMT_SMR.2	Restricted security roles	O.Access_Control
40	FPR_ANO.1	Anonymity	O.Anon
41	FPR_PSE.1	Pseudonymity	O.Anon
42	FPR_UNO.1	Unobservability	O.Access_Control
43	FPT_AMT.1	Abstract machine testing	Dependency (FPT_TST)
44	FPT_FLS.1	Failure with preservation of secure state	Dependency (FRU_FLT)
45	FPT_ITC.1	Inter-TSF confidentiality during transmission	O.Confidentiality
46	FPT_ITI.1	Inter-TSF detection of modification	O.Integrity
47	FPT_ITT.1	Basic internal TSF data transfer protection	O.Confidentiality O.Integrity
48	FPT_RCV.1	Manual recovery	O.Backup O.Recover
49	FPT_RPL.1	Replay detection	O.Replay
50	FPT_RVM.1	Non-bypassability of the TSP	O.Access_Control
51	FPT_SEP.1	TSF domain separation	O.Access_Control O.Authen_Protect
52	FPT_STM1	Reliable time stamps	O.Sequence

Table A.4 – All functional components necessary (concluded)

No	Component	Name	Objectives
53	FPT_TDC.1	Inter-TSF basic TSF data consistency	O.Consistency O.Sequence
54	FPT_TST.1	TSF testing	O.System_Integrity
55	FRU_FLT.1	Degraded fault tolerance	O.Alt_Channel
56	FRU_RSA.1	Maximum quotas	O.Filter O.Resources
57	FTA_SSL.1	TSF-initiated session locking	O.Authen
58	FTA_TAB.1	Default TOE access banners	O.Authen
59	FTA_TAH.1	TOE access history	O.Authen
60	FTA_TSE.1	TOE session establishment	O.Authen
61	FTP_ITC.1	Inter-TSF trusted channel	Dependencies (FDP_UCT.1 and FDP_UIT.1)
62	PBC_DYN.1	Dynamic control of audit	O.Dynamic
63	FCO_NND.1	Notification of non-delivery	O.Attest O.Nonrep_Dest
64	PBC_BKP.1	Backup	O.Backup
65	PBC_SYN.1	Synchronization	O.Sequence

A.3.3 Explicitly stated requirements

The following requirements are explicitly stated in this PP because these E - COFC requirements have no corresponding CC components:

PBC_DYN.1 Dynamic Control of Audit

PBC_NDD.1 Notification of Non-Delivery

PBC_BKP.1 Backup

PBC_SYN.1 Synchronisation

A.4 Functional requirements dependencies

Functional components possess dependencies that are stated requirements for the PP to include further components in support of the primary requirements. To meet the evaluation requirements, it is necessary either for all dependencies to be satisfied or for a rationale to be provided as to why any dependencies are not satisfied. Table A.5 demonstrates how the dependencies of each included component have been satisfied. All of the components of this PP are listed with a numeric line number. The dependencies of each component, if any, are listed alongside that component with a reference to the line number of the component which satisfies them. In the case of assurance component dependencies, AGD_AGD.1 is satisfied hierarchically by assurance level EAL2 and ADV_SPM.1 has been added as an assurance component. Component reference line numbers followed by `(H)' indicate that the dependency is satisfied by a hierarchical component to that referenced. This table demonstrates that there are no unsatisfied dependencies.

Table A.5 – Dependencies

	Component	Dependencies	Ref
1	FAU_GEN.1	FPT_STM.1	52
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	1 31
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SAR.3	FAU_SAR.1	3
6	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	1 37
7	FAU_STG.2	FAU_GEN.1	1
8	FAU_STG.3	FAU_STG.1	7(H)
9	FCO_NRO.2	FIA_UID.1	31
10	FCO_NRR.1	FIA_UID.1	31
11	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2 (added)	12 14 35
12	FCS_CKM.2	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2 (added)	11 14 35
13	FCS_CKM.3	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2 (added)	11 14 35
14	FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1 FMT_MSA.2 (added)	11 35
15	FDP_ACC.1	FDP_ACF.1	16
16	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	15 36
17	FDP_DAU.1	No dependencies	-
17.1	FDP_IFC.1	FDP_IFF.1	17.2
17.2	FDP_IFF.1	No dependencies	-
18	FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	15
19	FDP_RIP.1	No dependencies	-
20	FDP_SDI.1	No dependencies	-
21	FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or FDP_IFC.1	61 15
22	FDP_UIT.1	FTP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or FDP_IFC.1	61 15
23	FIA_AFL.1	FIA_UAU.1	26
24	FIA_ATD.1	No dependencies	-
25	FIA_SOS.1	No dependencies	-
26	FIA_UAU.1	FIA_UID.1	31

Table A.5 – Dependencies (continued)

	Component	Dependencies	Ref
27	FIA_UAU.3	No dependencies	-
28	FIA_UAU.5	No dependencies	-
29	FIA_UAU.6	No dependencies	-
30	FIA_UAU.7	FIA_UAU.1	26
31	FIA_UID.1	No dependencies	-
32	FIA_USB.1	FIA_ATD.1	24
33	FMT_MOF.1	FMT_SMR.1	39 (H)
34	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1	15 39 (H)
35	FMT_MSA.2	ADV_SPM.1 FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	Added 15 34 39 (H)
36	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	34 39 (H)
37	FMT_MTD.1	FMT_SMR.1	39 (H)
38	FMT_SAE.1	FMT_SMR.1 FPT_STM.1	39 (H) 52
39	FMT_SMR.2	FIA_UID.1	31
40	FPR_ANO.1	No dependencies	-
41	FPR_PSE.1	No dependencies	-
42	FPR_UNO.1	No dependencies	-
43	FPT_AMT.1	No dependencies	-
44	FPT_FLS.1	ADV_SPM.1	Added
45	FPT_ITC.1	No dependencies	-
46	FPT_ITI.1	No dependencies	-
47	FPT_ITT.1	No dependencies	-
48	FPT_RCV.1	FPT_TST.1 AGD_ADM.1 ADV_SPM.1	54 EAL1 Added
49	FPT_RPL.1	No dependencies	-
50	FPT_RVM.1	No dependencies	-
51	FPT_SEP.1	No dependencies	-
52	FPT_STM.1	No dependencies	-
53	FPT_TDC.1	No dependencies	-
54	FPT_TST.1	FPT_AMT.1 (added)	43
55	FRU_FLT.1	FPT_FLS.1 (added)	44
56	FRU_RSA.1	No dependencies	-
57	FTA_SSL.1	FIA_UAU.1	26
58	FTA_TAB.1	No dependencies	-

Table A.5 – Dependencies (concluded)

	Component	Dependencies	Ref
59	FTA_TAH.1	No dependencies	-
60	FTA_TSE.1	No dependencies	-
61	FTP_ITC.1	No dependencies	-
62	PBC_DYN.1	No dependencies	-
63	PBC_NDD.1	No dependencies	-
63	PBC_BKP.1	No dependencies	-
64	PBC_SYN.1	FPT_STM.1	52

A.5 Assurance requirements rationale

The E - COFC Public Business Class Protection Profile currently calls for the assurance components of Evaluation Assurance Level 2 (as shown in table A.6) augmented with the additional Common Criteria components as shown in table A.7. These are the same assurance components selected for [CS2 PPG]. The assurance components were selected, because they were felt to represent the state of the art for Commercial-of-the-Shelf (COTS) software.

The EAL2 functional components have been augmented with additional components for testing, configuration management, and flaw remediation which are considered within the state of the art. Since they are frequently not available for COTS products, requirements such as detailed design documentation were not included. Also, ADV_SPM.1 was added, because it is a dependency of some of the functional components.

Table A.6 – EAL2 components

Assurance class	Component ID	Component title
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - Sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table A.7 – Augmented components

Assurance class	Component ID	Component title
Configuration management	ACM_CAP.3	Authorization controls
	ACM_SCP.2	Problem tracking CM coverage
Development	ADV_SPM.1	Informal security policy model
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing - high-level design
Vulnerability assessment	AVA_MSU.2	Validation of analysis

A.6 Mapping of E - COFC threats to PP threats

This clause shows how the threats included in the E - COFC Protection Profile were derived from the threats listed in the ECMA-271 (E - COFC) and ECMA–205 (COFC) standards. The purpose of this clause is to show that the threats identified in the E - COFC PP are consistent with the threats identified in the E - COFC ECMA-271 standard.

The first three columns are the PP threat number, the name of the threat in the PP, and the PP threat description. The fourth column is a reference to the E - COFC or COFC documents. CO refers to threats addressed in ECMA-205, Commercially Oriented Functionality Class. This is lowest class hierarchically and all of the COFC functionalities are included in ECMA-271. ECMA-271 has three hierarchical classes: Enterprise Business (EB), Contract Business (CB), and Public Business(PB). The fourth column contains CO, EB, CB, or PB, depending on where in the document the threat was found. The last column lists the description of the threat from ECMA-271 or ECMA-205.

Table A.8 – E - COFC to PP threat mapping

No	PP threat name	PP threat description	E - COFC Ref	E - COFC threat description
1	T.Actions_Traced	Unauthorized tracing of customer business actions may occur.	PB15	Unauthorized tracing of customer business actions (tracing of cookies)
2	T.Blockage	Two systems may not be able to exchange data due to a communications channel being blocked.	EB7	Blockage of data exchanged between two systems
3	T.Change_Data	Information may be changed either while it being stored or processed within the TOE or during transmission. The changes may be accidental or intentional. Changes include insertions, replacements, modifications, and deletions. The type of information that can be changed includes user information, system information, business data, and commitment.	CO6	Manipulation of information (accidental or intentional)
			EB1	Unauthorized modification of transmitted data (accidental, incidental)
			EB2	Unauthorized deletion of transmitted data (accidental, incidental)
			EB3	Unauthorized insertion of transmitted data (accidental, incidental)
			EB10	Unauthorized modification of stored or processed data (accidental, incidental)
			EB11	Unauthorized deletion of stored or processed data (accidental, incidental)
			EB12	Unauthorized insertion of stored or processed data (accidental, incidental)
			PB1	Unauthorized modification or replacement of commitment data
			PB2	Unauthorized deletion or insertion of commitment data
4	T.Comm_Failure	It may not be possible to set up a connection or transmit data between two systems.	EB9	Connection setup or transmission failure
5	T.Data_Theft	Business process input data may be stolen.	PB10	Theft of business process input data
6	T.Deny_Data	An entity may deny ownership of business or commitment data.	CB 3	Denial of business information content ownership
			PB4	Denial of commitment data ownership
7	T.Deny_Receipt	An entity may deny that it has received business or commitment data.	CB2	Denial of reception of business information
			PB6	Denial of commitment data reception
8	T.Deny_Submit	An entity may deny that it has submitted business or commitment data.	CB1	Denial of submission of business information
			PB 5	Denial of commitment data submission
9	T.Disaster	Natural disasters may cause TOE or system failure.	CO8	Natural disasters

Table A.8 – E - COFC to PP threat mapping (continued)

No	PP threat name	PP threat description	E - COFC Ref	E - COFC threat description
10	T.Disclose_Data	Information may be disclosed in to unauthorized users. This includes both user information, system information and business data. Information may be disclosed while being stored or processed in the TOE or during transmission. Disclosure of authentication data during transmission would allow someone to logon and assume the identity of an authorized user.	CO5	Disclosure of information
			EB5	Unauthorized disclosure of information during transmission (this may result also in a penetration of a trusted path between a user and a login schema)
			EB13	Unauthorized disclosure of information (user information, system information)
			PB11	Disclosure of business data to unauthorized persons
11	T.False_Routing	Information may be routed to a false address enabling unauthorized access.	CB 4	False routing of business information enabling unauthorized access
12	T.History_Untraceable	It may not be possible to trace the sequence of events during a system failure, malfunction, or betrayal.	PB14	Untraceable history in case of failures, malfunctioning, or betrayal
13	T.Impersonate	Someone may obtain unauthorized access by impersonating an unauthorized user, for example by hijacking a communications session.	EB4	Impersonation of an entity (sender/receiver) involved in a communication process
			EB19	Unauthorized access by impersonation
14	T.Indeterminate_Seq	It may be impossible to determine the sequence of events in a dispute due to missing time information and business related data.	CB5	Unability to mediate disputes between two different parties of the closed user group because of missing timing information and business process related data.
15	T.Insider	An authorized user of the TOE may gain unauthorized access.	CO2	Insider attack – Individual responsibility
			EB20	Insider attack: Unauthorized access by authorized user
16	T.Intercept	Commitment data or certificates may be intercepted.	PB9	Interception of commitment data or certificates
17	T.Invalid_Certificate	The TOE may accept invalid commitment data or certificates.	PB7	Unauthorized acceptance of invalid/ invalidated commitment data or certificates
18	T.Logon_Attack	A program that tries a large number of passwords successfully guesses the password of an authorized user. This allows an unauthorized individual to logon as an authorized user and to assume the identity of that user.	CO3	Automatic logon attacks
19	T.Outsider	An individual who is not an authorized user of the system may gain access to the TOE.	CO1	Outsider attack – Unauthorized access to the TOE
			6.4	Usage of the INTERNET
			EB16	Outsider attack: Unauthorized access to the TOE to penetrate system information
			EB17	Denial of service (application, network services)

Table A.8 – E - COFC to PP threat mapping (concluded)

No	PP threat name	PP threat description	E - COFC Ref	E - COFC threat description
20	T.Physical	A component of the system may be accidentally or intentionally damaged.	EB15	Physical damage (accidental, incidental)
21	T.Privacy_Violated	Unauthorized access to privacy data of system users may occur.	PB12	Unauthorized access on linked privacy data of system users
22	T.Refusal	Unauthorized refusal of valid commitment data or certificates may occur.	PB8	Unauthorized refusal of valid/validated commitment data or certificates
23	T.Replace_TOE	The TOE may be replaced by an untrusted system.	EB18	Bootstrap compromise or unauthorized replacement of privileged subsystems (installation of a spoofing operating system)
24	T.Replay	Someone may obtain unauthorized access by replaying authentication or commitment data.	EB6	Replay of transmitted data
			PB 3	Unauthorized replay of commitment data
25	T.Secret_Disclose	Authentication information may be disclosed allowing someone to logon and assume the identity of an authorized user.	CO4	Disclosure of authentication information
26	T.Service_Denied	Application and network services may not be available for use.	EB17	Denial of service (application, network services)
27	T.TOE_Fail	TOE or system failure may cause the TOE to enter an insecure state or data to be disclosed or changed.	CO7	TOE failure
			EB14	System failure
28	T.Traffic	A system may experience degraded performance due to increased communications traffic.	EB8	Rising communication traffic to decrease the system performance
29	T.Unique_Copied	Unlawful copies may be made of unique originals.	PB13	Unlawful multiple use (e.g. by copying) of unique data

A.7 Mapping of E - COFC threats and Countermeasures to Protection Profile objectives

The tables are organized by the E - COFC hierarchical levels:

- Commercially Oriented Functionality Class
- Enterprise Business Class
- Contract Business Class
- Public Business Class

The purpose of this clause is to show how the objectives included in the E - COFC Protection Profile were derived from the material in ECMA-205 (COFC) and ECMA-271 (E - COFC). ECMA-205 contains a table that maps security enforcing functions to its identified threats. ECMA-271 contains threats tables for each of the three classes – enterprise business, contract business, and public business. These three classes are hierarchical to each other with the Public Business class being the highest level. The ECMA-271 threats are addressed by counter-measures. The material in these tables was used as the basis for objectives in the E - COFC Protection Profile as well as the need to provide a justification for each of the functional components.

Table A.9 – Commercially Oriented Functionality Class threats and objectives

REF	Threat name	E - COFC threat description	Security enforcing function	Objective name
CO1	T.Outsider	Outsider attack - Unauthorized access to the TOE	Identification and Authentication prior to all other interactions (6.1.2)	O.Authen
CO2	T.Insider	Insider attack - Individual responsibility	Unique Identification and Authentication (6.1.1)	O.Authen
			Accountability (6.3.1)	O.Assoc_User_Action
			Logging (6.3.2)	O.Audit
CO3	T.Log_Attack	Automatic logon attacks	Number of logon trials (6.1.5)	O.Logon_Limit
CO4	T.Secret_Disclose	Disclosure of authentication information	Authentication information protection (6.1.9)	O.Authen_Protect
			Authentication information sharing (6.1.10)	O.Authen_Indep
			Authentication information aging (6.1.11)	O.Authen_Age
CO5	T.Disclose_Data	Disclosure of information	Access Control (6.2)	O.Access_Control
			Object Reuse (6.4)	O.Resid_Prot
CO6	T.Change_Data	Manipulation of information (accidental or intentional)	Access Control (6.2)	O.Access_Control
			Accuracy (6.5)	O.Integrity
				O.Status
				O.System_Integrity
CO7	T.TOE_Fail	TOE failure	Recovery (6.7.1)	O.Recover
			Data Backup (6.7.2)	O.Backup
CO8	T.Disaster	Natural disasters	Data backup (6.7.2)	O.Backup
			Recovery (6.7.1)	O.Recover

Table A.10 – Enterprise Business Class threats and objectives

Ref	Threat name	Threat description	Countermeasure	Objective name
EB1	T.Change_Data	Unauthorized modification of transmitted data (accidental, incidental)	Content integrity checking of transmitted data	O.Integrity
EB2	T.Change_Data	Unauthorized deletion of transmitted data (accidental, incidental)	Content integrity checking of transmitted data	O.Integrity
EB3	T.Change_Data	Unauthorized insertion of transmitted data (accidental, incidental)	Content integrity checking of transmitted data	O.Integrity
			Sequence integrity checking of transmitted data	O.Sequence
EB4	T.Impersonate	Impersonation of an entity (sender/receiver) involved in a communication process	Authentication of sender and receiver address	O.Authen_Address
EB5	T.Disclose_Data	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	O.Confidentiality
EB6	T.Replay	Replay of transmitted data	Sequence integrity checking of transmitted data	O.Sequence
EB7	T.Blockage	Blockage of data exchanged between two systems	Usage of alternative channels	O.Alt_Channel
EB8	T.Traffic	Rising communication traffic to decrease the system performance	Filtering	O.Filter
EB9	T.Comm_Failure	Connection setup or transmission failure	Authentication of sender and receiver address	O.Alt_Channel O.Audit
			Physical protection of communication devices	A.Physical
			Recovery	O.Recover
			Alternate routes	O.Alt_Channel
EB10	T.Change_Data	Unauthorized modification of stored or processed data (accidental, incidental)	Authentication	O.Authen
			Access control	O.Access_Control
			Recovery	O.Recover
			Integrity checking	O.Integrity
EB11	T.Change_Data	Unauthorized deletion of stored or processed data (accidental, incidental)	Authentication	O.Authen
			Access control	O.Access_Control
			Recovery	O.Recover
			Integrity checking	O.Integrity

Table A.10 – Enterprise Business Class threats and objectives (continued)

Ref	Threat name	Threat description	Countermeasure	Objective name
EB12	T.Change_Data	Unauthorized insertion of stored or processed data (accidental, incidental)	Authentication	O.Authen
			Access control	O.Access_Control
			Recovery	O.Recover
			Integrity checking	O.Integrity
EB13	T.Disclose_Data	Unauthorized disclosure of information (user information, system information)	Access control	O.Access_Control
			Authentication	O.Authen
			Object reuse	O.Resid_Prot
			Accountability	O.Audit
EB14	T.TOE_Fail	System failure	Recovery	O.Recover
			Backup	O.Backup
EB15	T.Physical	Physical damage (accidental, incidental)	Recovery	O.Recover
			Backup	O.Backup
			Physical protection	A.Physical
EB16	T.Outsider	Outsider attack: Unauthorized access to the TOE to penetrate system information	Authentication	O.Authen
			Access Control	O.Access_Control
			Virus checking	O.Integrity
			Flow control	O.Flow_Control
			Accountability	O.Audit
EB17	T.Deny_Service	Denial of service (application, network services)	Physical protection	A.Physical
			Authentication	O.Authen
			Access control	O.Access_Control
EB18	T.Replace_TOE	Bootstrap compromise or unauthorized replacement of privileged subsystems (installation of a spoofing operating system)	Physical protection	A.Physical
			System verification	O.System_Integrity

Table A.10 – Enterprise Business Class threats and objectives (concluded)

Ref	Threat name	Threat description	Countermeasure	Objective name
EB19	T.Impersonate	Unauthorized access by impersonation	Content integrity checking of exchanged authentication data	O.Integrity
			Sequence integrity checking of exchanged authentication data.	O.Sequence
			Replay attack detection mechanism	O.Replay
			Authentication	O.Authen
			Accountability	O.Assoc_User_Action
EB20	T.Insider	Insider attack: Unauthorized access by authorized user	Accountability	O.Assoc_User_Action O.Audit
			Access control	O.Access_Control

Table A.11 – Contract Business Class threats and objectives

Ref	Threat name	Threat description	Countermeasure	Objective
CB1	T.Deny_Submit	Denial of submission of business information		
			Non-repudiation of Originator	O.Nonrep_Orig
CB2	T.Deny_Receipt	Denial of reception of business information	Attestation of delivery	O.Attest
			Attestation of reception by Destination	O.Attest
			Non-repudiation of Destination	O.Nonrep_Dest
CB3	T.Deny_Data	Denial of business information content ownership	Non-repudiation of Originator	O.Nonrep_Orig O.Audit O.Attest
CB4	T.False_Routing	False routing of business information enabling unauthorized access	Authentic business role qualification of Originator and Destination (a priori authorization)	O.Authen_Address
CB5	T.Indeterminate_Seq	A dispute between two different 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.	Unability to mediate disputes between two different parties of the closed user group because of missing timing information and business process related data.	O.Audit
			The stored timing information shall enable the tracing of business process actions on different systems.	O.Sequence

Table A.12 – Public Business Class threats and objectives

Ref	Threat name	Threat description	Countermeasure	Objective
PB1	T.Change_Data	Unauthorized modification or replacement of commitment data	Content integrity checking of transmitted commitment data, business data, and business data with commitment data	O.Integrity
PB2	T.Change_Data	Unauthorized deletion or insertion of commitment data	Content integrity checking of transmitted commitment data, business data, and business data with commitment data	O.Integrity
PB3	T.Replay	Unauthorized replay of commitment data	Sequence integrity checking of commitment data, business data, and business data with commitment data	O.Sequence O.Replay O.Authen_Address
PB4	T.Deny_Data	Denial of commitment data ownership	Non-repudiation of Originator	O.Nonrep_Orig
PB5	T.Deny_Submit	Denial of commitment data submission	Non-repudiation of Originator	O.Nonrep_Orig
PB6	T.Deny_Receipt	Denial of commitment data reception	Non-repudiation of Destination	O.Nonrep_Dest
PB7	T.Invalid_Certificate	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	O.Integrity O.Authen_Age
			Up-to-date storage and distribution of digitally signed revocation lists	O.Revoke_Cert
			Access control.	O.Access_Control
PB8	T.Refusal	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	O.Integrity
			Up-to-date storage and distribution of digitally signed revocation lists	O.Revoke_Cert
			Access control	O.Access_Control
PB9	T.Intercept	Interception of commitment data or certificates	Restricted lifetime of cryptographic keys, certificates and commitment data.	O.Key_Age
			Generation of new keys independent from the broken keys.	O.Key_Indep_Gen
			Transmission of key exchange information independent from the broken keys	O.Key_Indep_Trans

Table A.12 – Public Business Class threats and objectives (concluded)

Ref	Threat name	Threat description	Countermeasure	Objective
PB10	T.Data_Theft	Theft of business process input data	Authentication	O.Authen
			Access control	O.Access_Control
			Accountability	O.Audit
PB11	T.Disclose_Data	Disclosure of business data to unauthorized persons	Authentication	O.Authen
			Access control	O.Access_Control
			Accountability	O.Audit
PB12	T.Privacy_Violated	Unauthorized access on linked privacy data of system users	Authentication	O.Authen
			Access control	O.Access_Control
			Accountability	O.Audit
			Anonymity or pseudonymity mechanisms	O.Anon
PB13	T.Unique_Copied	Unlawful multiple use (e.g. by copying) of unique data	Uniqueness enforcing functions and uniqueness violation detection measures	O.Unique
PB14	T.History_Untraceable	Untraceable history in case of failures, malfunctioning, or betrayal	Interrelated accountability	O.Sequence
				O.Consistency
PB15	T.Actions_Traced	Unauthorized tracing of customer business actions (tracing of cookies)	Access control	O.Access_Control
			Anonymity or pseudonymity mechanisms	O.Anon

A.8 Mapping of E - COFC functionalities to CC functional components

This clause shows how the E - COFC security functionalities were mapped to Common Criteria (CC) functional components. Notes have been added where selections, assignments, and refinements were made. There were four cases where it was impossible to map the E - COFC security functionalities to existing CC components and new components were defined. The four new components are PBC_DYN.1, FCO_NND.1, PBC_BKP.1, and PBC_SYN.1.

Table A.13 – Mapping of E - COFC functionalities to CC components

7.4	EB-Class security functionalities	Component	Component text
	Note: There are many ECMA-271 requirements for the management of TSF functions and data. For ease of reference, the applicable CC components are listed here.	**FMT_MOF.1**	**Management of security functions behavior** FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].
		FMT_MSA.1	**Management of security attributes** FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].
		FMT_MTD.1	**Management of TSF data** FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].
7.4.1	Identification and authentication		
7.4.1.1	Unique identification and authentication (Ref.: 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.	**FIA_UID.1**	**Timing of identification** FIA_UID.1.1 The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified. FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
		FIA_UAU.1	**Timing of authentication** FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.4.1.2	Identification and authentication prior to all other interactions (Ref.: 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.	**FIA_UID.1** **FIA_UAU.1**	**Timing of identification** **Timing of authentication** 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.
7.4.1.3	**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.	**FCO_NRO.2**	**Enforced proof of origin** FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [assignment: *list of information types*] at all times. FCO_NRO.2.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the Originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies. FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of origin*].
	If the networks are under full physical control of the enterprise, non-cryptographic techniques may be applied. Otherwise cryptographic techniques shall be applied.	**FCS_CKM.2**	**Cryptographic key distribution** FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*]. Refinement added.
		FCO_NRR.2	**Enforced proof of receipt** FCO_NRR.2.1 The TSF shall enforce the generation of evidence of receipt for received [assignment: *list of information types*]. FCO_NRR.2.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the recipient of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies. FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of receipt*].

	In addition the applied protocol shall prevent replay attacks and protect against interception.	**FIA_UAU.3**	**Unforgeable authentication** FIA_UAU.3.1 The TSF shall prevent use of authentication data that has been forged by any user of the TSF. FIA_UAU.3.2 The TSF shall prevent use of authentication data that has been copied from any other user of the TSF.
		FPT_RPL.1	**Replay detection** FPT_RPL.1.1 The TSF shall detect replay for the following entities: [assignment: *list of identified entities]*. FPT_RPL.1.2 The TSF shall perform [assignment: *list of specific actions*] when replay is detected. Assignment: authentication data.
7.4.1.4	**Associate information to users** (Ref.: 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.	**FIA_ATD.1**	**User attribute definition** FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*]. Customer-defined information added as assignment
		FMT_MSA.1	**Management of security attributes** See 7.4 for text.
7.4.1.5	**Logon message.** The TOE shall provide an advisory warning message upon TOE entry regarding unauthorized use, and the possible consequences of failure to meet those requirements.	**FTA_TAB.1**	**Default TOE access banners** FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.
	The message shall be customer-specifiable to meet their own requirements and state laws. (Ref.: ECMA-205 6.1.4).	**FMT_MTD.1**	**Management of TSF data** See 7.4 for text. Selection: modify. Assignment: logon message.

	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.	**FTA_TAH.1**	**TOE access history** FTA_TAH.1.1. Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last successful session establishment to the user. FTA_TAH.1.2. Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment. FTA_TAH.1.3. The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information. Date, time, method, and location selected.
7.4.1.6	**Number of logon trials** (Ref.: 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.	**FIA_AFL.1**	**Basic authentication failure handling** FIA_AFL.1.1 The TSF shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*]. FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*]. E - COFC text added as assignment.
7.4.1.7	**Expiration of unused user IDs** (Ref.: 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, or alerting administration.	**FMT_SAE.1**	**Time-limited authorization** FMT_SAE.1.1 The TSF shall restrict the ability to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*] to [assignment: *the authorized identified roles*]. FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed. Assignment: Unused user IDs.

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. **Note:** It appears that only one of FTA_SSL.1 or FTA_SSL.3 is required. Selected FTA_SSL.1	**FTA_SSL.1**	**TSF-initiated session locking** FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: *time interval of user inactivity]* by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session. FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur]*.
		FIA_UAU.6	**Re-authenticating** FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*]. Assignment: session lock.
7.4.1.9	**Disable users temporarily** (Ref.: ECMA-205 6.1.7). The TOE shall allow administration to temporarily disable a user accessing the TOE.	**FTA_TSE.1**	**TOE session establishment** FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: attributes]. Assignment: An administrator temporarily disabling a user's access to the TOE.
7.4.1.10	**User status information** (Ref.: ECMA-205 6.1.8). A mechanism shall be available for administration to provide the status, e.g. active, inactive etc. of any user.	**FMT_MTD.1**	**Management of TSF data** See 7.4 for text. Selection: query Assignment: status of any user.
7.4.1.11	**Authentication information protection** (Ref.: ECMA-205 6.1.9). The TOE shall protect the integrity of the stored authentication information and the confidentiality of any associated secrets.	**FPT_SEP.1**	**TSF domain separation** FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.
7.4.1.12	**Authentication information sharing** (Ref.: 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.	**FIA_UAU.7**	**Protected authentication feedback** FIA_UAU.7.1 The TSF shall only provide [assignment: *list of feedback*] to the user while the authentication is in progress E - COFC text added as feedback assignment.

7.4.1.13	**Authentication information aging** (Ref.: 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.	**FMT_SAE.1**	**Time-limited authorization** FMT_SAE.1.1 The TSF shall restrict the ability to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*] to [assignment: *the authorized identified roles*]. FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed. Assignment: authentication information. Assignment: enforce periodic changes.
7.4.2	**Access control**		
	Note on access control (7.4.2): The Common Criteria only provides a skeletal framework for expressing access control requirements. It is left up to the developer of a protection profile and/or security target to specify the access control policy with respect to subject and object attributes, modes of access and rules for allowing access. The generic access control components are provided here.	**FDP_ACC.1**	**Subset access control** FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].
		FDP_ACF.1	**Security attribute based access control** FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes, named groups of security attributes*]. FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]. FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]. FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

7.4.2.1	**Authenticated user identification** (Ref.: ECMA-205 6.2.1). Control of access to objects shall only be granted to authenticated users, e.g. through an authenticated user identifier.	**FIA_UAU.1**	**Timing of authentication** 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.
7.4.2.2	**Individual user** (Ref.: 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.	**FDP_ACC.1** **FDP_ACF.1**	**Access control policy** Security attribute based access control See 7.4.2 for text. Refinement added.
7.4.2.3	**User groups** (Ref.: 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.	**FDP_ACF.1**	**Security attribute based access control** See 7.4.2 for text. Refinement added.
7.4.2.4	**Objects** (Ref.: 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.	**FPT_SEP.1**	**TSF domain separation** FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

	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.	**FMT_SMR.2**	**Restrictions on security roles** FMT_SMR.2.1 The TSF shall maintain the roles [assignment: *the authorised identified roles*]. FMT_SMR.2.2 The TSF shall be able to associate users with roles. FMT_SMR.2.3 The TSF shall ensure that [assignment: *conditions for the different roles*] are satisfied.
	The audit mechanisms objects.	**FAU_SAR.2**	**Restricted audit review** FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
7.4.2.5	**Types of access rights** (Ref.: 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.	**FDP_ACF.1**	**Security attribute based access control** See 7.4.2 for text. Refinement added.
7.4.2.6	**Default access rights** (Ref.: 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. Note: This requirement was interpreted to mean that the ability to specify access rights for world or public, or the equivalent shall be provided.	**FDP_ACF.1**	**Security attribute based access control** See 7.4.2 for text. Refinement added.
		FMT_MSA.3	**Static attribute initialization** FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: restrictive, permissive, other property] default values for security attributes that are used to enforce the SFP. FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

7.4.2.7	**Precedence of access rights** (Ref.: 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.	**FDP_ACF.1**	**Security attribute based access control** See 7.4.2 for text. Refinement added.
7.4.2.8	**Date of modification** (Ref.: 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.	**FAU_GEN.1**	**Audit data generation** FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and [selection: success, failure] of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*] Note: Covered by Basic level of auditing.
7.4.2.9	**Verification of rights** (Ref.: 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.	**FPT_RVM.1**	**Non-bypassability of the TSP** FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before assignment operation within the TSC is allowed to proceed.
7.4.2.10	**Application controlled access rights** (Ref.: 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.	**FDP_ACF.1**	**Security attribute based access control** See 7.4.2 for text. Refinement added.
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. Note: Used FDP for user data and FPT for TSF data.	**FDP_UIT.1**	**Data exchange integrity** FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP and/or information flow control SFP*] to be able to [selection*: transmit, receive*] user data in a manner protected from undetectable [selection: *modification, deletion, insertion, replay*] errors. FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [selection: *modification, deletion, insertion, or replay*] has occurred. Modification, deletion, insertion all selected for integrity.
		FDP_ITT.1	**Basic internal data transfer protection** FDP_ITT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to prevent the [selection: *disclosure, modification, loss of use*] of user data when it is transmitted between physically-separated parts of the TOE. Modification selected.
		FPT_ITI.1	**Inter-TSF detection of modification** FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment: a defined modification metric]. FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.
		FPT_ITT.1	**Basic internal TSF data transfer protection** FPT_ITT.1.1 The TSF shall protect TSF data from [selection: *disclosure, modification*] when it is transmitted between separate parts of the TOE. Modification selected.

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.	**FCO_NRO.2**	**Enforced proof of origin** 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.
		FCO_NRR.2	**Enforced proof of receipt** 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.
	The applied protocol shall prevent replay attacks.	**FPT_RPL.1**	**Replay detection** 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.

7.4.3.3	**Confidentiality of exchanged information**. When two systems are exchanging information the TOE shall support the confidentiality of the exchanged information against unauthorized disclosure. Note: Used FDP for user data and FPT for TSF data.	**FDP_UCT.1**	**Basic data exchange confidentiality** FDP_UCT.1.1 The TSF shall enforce the [assignment: *access control SFP and/or information flow control SFP*] to be able to [selection*: transmit, receive*] objects in a manner protected from unauthorized disclosure. Transmit and receive selected.
		FDP_ITT.1	**Basic internal data transfer protection** When two systems are exchanging information the integrity of the information content shall be verified. Disclosure selected.
		FPT_ITC.1	**Inter-TSF confidentiality during transmission** FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.
		FPT_ITT.1	**Basic internal TSF data transfer protection** See 7.4.3.1 for text. Disclosure selected.

7.4.4	**Accountability and audit.** Notes on Audit: The basic audit components are FAU_GEN.1 and FAU_SEL.1. Notes on Audit (continued): Several E - COFC requirements to enable or disable auditable events are not addressed directly, but could be covered under FMT_MOF.1.	**FAU_GEN.1**	**Audit data generation** FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions. b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and c) Other auditable events defined below: The TOE shall log at least each of the following events: Introduction or deletion (suspension) of users. Introduction or removal of storage data. Start up or shut down of the TOE. Changes to user's security profiles, administration or attributes. Changes to system security parameters (not listed in COFC) FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*]
		FAU_SEL.1	**Selective audit** FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [selection: *Object identity, User identity, Subject identity, Host identity, Event Type*] b) [assignment: *list of additional attributes that audit selectivity is based upon.*]
		FMT_MOF.1	**Management of security functions behavior** See 7.4 for text.
7.4.4.1	**Associate actions and users** (Ref.: ECMA-205 6.3.1). For every interaction the TOE shall be able to establish the identity of the user.	**FAU_GEN.2**	**User identity generation** FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the events.
		FIA_USB.1	**User-subject binding** FIA_USB.1.1 The TSF shall associate the appropriate security attributes with subjects acting on behalf of that user.

7.4.4.2	**Logging** (Ref.: 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.	**FAU_GEN.1**	**Audit data generation** See 7.4.4 for text. Note: Basic level of audit selected.
7.4.4.3	**Use of identification and authentication** Mechanism (Ref.: ECMA-205 6.3.2.1). The TOE shall log at least logons and security-related activities of administration.	**FAU_GEN.1** FIA and FMT audit events	**Audit data generation** See 7.4.4 for text.
	Administration shall have the capability to enable or disable the logging of other events which include at a minimum:	**FMT_MOF.1**	**Management of functions in TSF** See 7.4.4 for text.
	1. Valid and invalid user authentication attempts.	**FAU_GEN.1** FIA audit events	**Audit data generation** See 7.4.4 for text.
7.4.4.4	**Attempts to exercise access rights** (Ref.: ECMA-205 6.3.2.2). The TOE shall log at least each of the following events: 1. Unsuccessful data or transaction access attempts.	**FAU_GEN.1** FDP audit events	**Audit data generation** See 7.4.4 for text.
	Administration shall have the capability to enable or disable the logging of other events which include at a minimum:	**FMT_MOF.1**	**Management of functions in TSF** See 7.4 for text.
	1. Disk file access. 2. Tape volume or tape file access	**FAU_GEN.1** FDP or FMT audit events	**Audit data generation** See 7.4.4 for text.
	3. Program execution.	**FAU_GEN.1** FDP audit events	**Audit data generation** See 7.4.4 for text.
	4. On-line execution of commands which are security relevant.	**FAU_GEN.1** FDP audit events	**Audit data generation** See 7.4.4 for text.
7.4.4.5	**Creation or deletion of an object which is subject to the administration of rights** (Ref.: 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.	**FAU_GEN.1** FDP audit events	**Audit data generation** See 7.4.4 for text.

7.4.4.6	**Actions by authorized users affecting the security of the TOE** (Ref.: ECMA-205 6.3.2.4). The TOE shall log at least each of the following events: 1. Introduction or deletion (suspension) of users.	**FAU_GEN.1** FIA, FTA, and/or FMT audit events	**Audit data generation** See 7.4.4 for text.
	2. Introduction or removal of storage data.	**FAU_GEN.1** FMT audit events	**Audit data generation** See 7.4.4 for text.
	3. Start up or shut down of the TOE.	**FAU_GEN.1** FMT audit events	**Audit data generation** See 7.4.4 for text.
	4. Changes to user's security profiles, administration or attributes.	**FAU_GEN.1** FMT audit events	**Audit data generation** See 7.4.4 for text.
	5. Changes to system security parameters.		
7.4.4.7	**Logged information** (Ref.: ECMA-205 6.3.2.5). For each of the events specified in COFC 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.	**FAU_GEN.1**	**Audit data generation** See 7.4.4 for text. Note: Name of object and type of access event added as assignments.
7.4.4.8	**TOE restart** (Ref.: ECMA-205 6.3.3). Accountability control information shall survive restart of the TOE.	**FAU_STG.2**	**Guarantees of audit data availability** FAU_STG.2.1 The TSF shall protect stored audit records from unauthorized deletion. FAU_STG2.2 The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records. FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] audit records will be maintained when the following conditions occur [selection: *audit storage exhaustion, failure, attack*]. Note: Restart of TOE added as refinement.
7.4.4.9	**Copy audit trails** (Ref.: 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.	**FMT_MTD.1**	**Management of TSF data** See 7.4 for text. Assignment: copy to specifiable storage medium. Assignment: audit trail files.

7.4.4.10	**Alarm if unable to record** (Ref.: 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.	**FAU_ STG.3**	**Action in case of possible audit data loss** **FAU_STG.3.1** The TSF shall take [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*]. Note: generate an alarm added as an assignment.
	The TOE shall provide the authorized administrator with the ability to manage the audit trail at any time during the operation of the TOE.	**FMT_MTD.1**	**Management of TSF data** See 7.4 for text.
		PBC_DYN.1 **Added**	**Dynamic control of audit** PBC_DYN.1,1 The TSF shall provide [selection: *authorised users]* with the capability to perform the following actions at any time during normal TOE operation: enable or disable auditable events change the selection of attributes to be audited, c) manage the audit trail.
7.4.4.11	**Select users** (Ref.: ECMA-205 6.3.6). It shall be possible to selectively account for the actions of one or more users.	**FAU_SEL.1**	**Selective audit** See 7.4.4 for text. Note: User identity selected.
7.4.4.12	**Dynamic control** (Ref.: 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.	**PBC_DYN.1** **Added**	**Dynamic control of audit** 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.

7.4.4.13	**Audit tools** (Ref.: ECMA-205 6.3.8). Tools to examine the audit trail for the purpose of audit shall exist and be documented.	**FAU_SAR.1**	**Audit review** FAU_SAR.1.1 The TSF shall provide [selection: *authorized users*] with the capability to read [assignment: *list of audit information*] from the audit records. FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
	These tools shall allow the actions of one or more users to be identified selectively.	**FAU_SAR.3**	**Selectable audit review** FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: *searches, sorting, ordering*] of audit data based on [assignment: *multiple criteria with logical relations*].
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 to the extend that causal relations between events on different systems become traceable.	**FPT_STM.1**	**Reliable time stamps** FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.
		PBC_SYN.1	**Synchronization** PBC_SYN.1.1 The TSF shall be able to provide the capability to determine the order in which security relevant events occurred.
7.4.5	**Object reuse**		
7.4.5.1	**Object reuse** (Ref.: 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.	**FDP_RIP.2**	**Full residual information protection** FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] all objects.
7.4.6	**Accuracy**		
7.4.6.1	**TOE software integrity** (Ref.: 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.	**FPT_TST.1**	**TSF testing** FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, under the conditions [assignment: conditions at which self test should occur]*] to demonstrate the correct operation of the TSF. FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data. FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.
7.4.6.2	**Data integrity** (Ref.: ECMA-205 6.5.2). The TOE shall make available a mechanism to verify the integrity of data, e.g. checksum.	**FDP_SDI.1**	**Stored data integrity monitoring** FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

7.4.6.3	**Security parameters status report** (Ref.: 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.	**FMT_MTD.1**	**Management of TSF data** See 7.4 for text. Assignment: generate a status report- Assignment: values of settable security parameters.
7.4.6.4	**Flow control at the boundaries** The TOE shall provide mechanisms for controlling the boundaries of ist 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.	**FPT_RCV.1** **FDP_IFC.1** **FDP_IFF.1**	**Simple security attributes** **FDP_IFF.1.1** The TSF shall enforce the [assignment: information flow control SFP] to enforce at least the following types of subject and information security. attributes: [assignment: the minimum number and type of security attributes]. **FDP_IFF.1.2** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. **FDP_IFF.1.3** The TSF shall enforce the [assignment: additional information flow control SFP rules]. **FDP_IFF.1.4** The TSF shall provide the following [assignment: list of additional SFP capabilities]. **FDP_IFF.1.5** The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows]. **FDP_IFF.1.6** The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. Assignment: List attributes to exclude irregular interference with the commercial environment.
7.4.7	**Availability and reliability**		
7.4.7.1	**Recovery** (Ref.: ECMA-205 6.6.1). Procedures or mechanisms shall be provided to allow recovery after a TOE failure or other discontinuity.	**FPT_RCV.1**	**Manual recovery** FPT_RCV.1.1 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.
7.4.7.2	**Data backup** (Ref.: ECMA-205 6.6.2). Procedures shall be provided for software and data backup and restoration.	**PBC_BKP.1**	**Backup** PBC_BKP.1.1 The TSF shall provide procedures 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.	**FRU_RSA.1**	**Maximum quotas** FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [assignment: controlled resources] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*]. Assignment: communication resources
7.4.7.4	**Transmission blockage.** Alternate communication channels shall be provided to recover from transmission blockage.	**FRU_FLT.1**	**Degraded fault tolerance** FRU_FLT.1.1 The TSF shall ensure the operation of [assignment: list of TOE capabilities] that will be maintained when the following failures occur: [assignment: list of type of failures]. Assignment: alternate communication channels. Assignment: transmission blockage.
7.4.7.5	**Denial of service** Mechanisms shall be present to mitigate the possibility of intentional denial of service.	**FIA_UID.1** **FIA_UAU.1** **FDP_ACC.1** **FDP_SDI.1** **FDP_IFC.1** **FAU_GEN.1** **FRU_RSA.1**	**Subset information flow control** FDP_IFC.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by SFP].
7.4.8	**Key management** (if cryptographic means are applied by the TOE) Note: The Common Criteria key management functional components do not line up exactly with the ECMA-271 requirements below, but taken as a whole, they provide for comprehensive key management services.		
7.4.8.1	**Key generation.** The key generation shall be based on state-of-the-art cryptographic techniques which ensure the unpredictable generation of strong keys.	**FCS_CKM.1**	**Cryptographic key generation** FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. Refinement added.
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.	**FCS_CKM.1**	**Cryptographic key generation** The key generation shall be based on state-of-the-art cryptographic techniques to ensure the unpredictable generation of strong keys.

7.4.8.3	**Key confirmation.** The security management shall support a key distribution technique which addresses the integrity or confidentiality of the keying information as required.	**FCS_CKM.2**	**Cryptographic key distribution** FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*]. Refinement added.
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).	**FCS_CKM.2**	**Cryptographic key distribution** The security management shall support a key distribution technique addressing the integrity and confidentiality of the keying information as required. Refinement added.
7.4.8.5	**Key revocation.** The security management shall support the revocation of distributed keys by technical or organizational means (Key revocation process).	**FCS_CKM.4**	**Cryptographic key destruction** FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].
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.	**FCS_CKM.3**	**Cryptographic key access** FCS_CKM.3.1 The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*]. Refinement added.
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.	**FCS_CKM.2**	**Cryptographic key distribution** The security management shall support a key distribution technique addressing the integrity and confidentiality of the keying information as required. Refinement added.
8.4	**CB-Class security functionalities**		
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 COFC).	**FDP_ACF.1**	**Security attribute based access control** See 7.4.2 for text.
	The business role qualification data of the Originator or Destination shall be automatically distributed.	**FCS_CKM.2**	**Cryptographic key distribution** See 7.4.8.3 for text.

8.4.1.2	**Consistency.** Consistency of related access control parameters for business actions shall be provided over all systems.	**FPT_TDC.1**	**Inter-TSF TSF data consistency** FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted IT product. FPT_TDC.1.2 The TSF shall use [assignement: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product. Assignment: access control parameters for business actions.
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.	**FCO_NRO.1**	**Selective proof of origin** FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [assignment: *list of information types*] at the request of the [selection: *originator, recipient,* [assignment: *list of third parties*]. FCO_NRO.1.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the Originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies. FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of origin*].
8.4.2.2	**Non-repudiation of the Destination.** The TOE shall support dedicated mechanisms for the non-repudiation of the Destination.	**FCO_NRR.1**	**Selective proof of receipt** FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [assignment: *list of information types*] at all times. FCO_NRO.2.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the Originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies. FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of origin*].

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.	**FCO_NRO.1**	**Selective proof of origin** The TOE shall support dedicated mechanisms for the non-repudiation of the Originator.
		FCO_NRR.1	**Selective proof of receipt** The TOE shall support dedicated mechanisms for the non-repudiation of the Destination.
	The Destination shall, if requested, send an attestation of reception when information was received under the agreed upon conditions such as integrity or confidentiality.	**FCO_NRR.1**	**Selective proof of receipt** The TOE shall support dedicated mechanisms for the non-repudiation of the Destination. Refinement added.
	If delivery was not accomplished, the Originator or Destination shall be notified by the transport service for the reasons of failed delivery	**PBC_NDD.1**	**Notification of non-delivery** PBC_NDD.1 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.	**FPT_STM.1**	**Reliable time stamps** FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.
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.	**FAU_STG.1**	**Protected audit trail storage** FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion. FAU_STG.1.2 The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records. Note: prevent selected.
	The stored timing information shall enable the tracing of business process actions on different systems.	**FPT_TDC.1**	**Inter-TSF basic TSF data consistency** FPT_TDC.1.1 The TSF shall enforce the consistent interpretation of [assignment: *list of TSF data types*] between this TSF and another trusted IT product. FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product. Assignment: logs of business transactions.

9.4	**PB-Class security functionalities**	**Component**	
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 has to be established. The system shall be able to verify this chain to the roots.	**FIA_UAU.5**	**Multiple authentication mechanisms** FIA_UAU.5.1 The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support user authentication. FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]. E - COFC text assigned as rule.
		FCS_CKM.2	**Cryptographic key distribution** The security management shall support a key distribution technique addressing the integrity and confidentiality of the keying information as required.
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.	**FPR_ANO.1**	**TSF anonymity** FPR_ANO.1.1 The TSF shall ensure that [assignment: *set of users and/or subjects*], [selection: *including, excluding*] authorised users, are unable to determine the user identity bound to [assignment: *list of subjects and/or operations and/or objects*].
		FPR_PSE.1	**Reversible pseudonymity** FPR_PSE.1.1 The TSF shall ensure that [assignment: *set of users and/or subjects*], [selection: *including, excluding*] authorised users, are unable to determine the user identity bound to [assignment: *list of subjects and/or operations and/or objects*]. FPR_PSE.1.2 The TSF shall be able to provide [assignment: *number of aliases*] aliases of the user name to [assignment: *list of subjects*].
	Dedicated techniques shall be supported to prevent the unauthorized monitoring of the logged system user's activities.	**FPR_UNO.1**	**Unobservability** FPR_UNO.1.1 The TSF shall ensure that [assignment: *set of users and/or subjects*], [selection: *including, excluding*] authorised users, are unable to observe the operation [assignment: *list of operations*] on [assignment: *list of objects*] by another user or subject.

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.	**FAU_STG.1**	**Protected audit trail storage** 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.
		FPT_TDC.1	**Inter-TSF TSF data consistency** 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. Assignment: logs of business transactions.
		PBC_SYN.1	**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.
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).	**FCO_NRO.1**	**Selective proof of origin** The TOE shall support dedicated mechanisms for the non-repudiation of the Originator.
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).	**FCO_NRR.1**	**Selective proof of receipt** The TOE shall support dedicated mechanisms for the non-repudiation of the Destination.
9.4.3.4	**Uniqueness of original**. Security mechanisms, such as watermarking, bill of lading scheme, ticketing, etc. shall be provided.	**FDP_DAU.1**	**Basic data authentication** FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *list of objects or information types*]. FDP_DAU.1.2 The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information. Assignment: unique objects.

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 certificate content shall be verified.	**FCS_CKM.2**	**Cryptographic key distribution** The security management shall support a key distribution technique addressing the integrity and confidentiality of the keying information as required.
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.	**FCO_NRO.2**	**Enforced proof of origin** 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.
		FCO_NRR.2	**Enforced proof of receipt** 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.
	The protocol shall prevent replay attacks.	**FPT_RPL.1**	**Replay detection and correction** 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. Assignment: commitment data, certificates.
9.4.5	**Trust center security functionalities (key management).** Note: The functionality of the four ECMA-271 key management requirements does not line up exactly with the four Common Criteria cryptographic key management components. However, taken as a whole, both sets of functional requirements can be used to specify a comprehensive set of key management services.		

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 public key which was authentically transmitted to the registration entity are assigned. The entity responsible for the registration process is called Registration Authority (RA).	**FCS_CKM.1**	**Cryptographic key generation** See 7.4.8.1 for text. Refinement added.
	The RA shall provide adequate means for the authenticity and integrity of the stored registration data.	**FCS_CKM.3**	**Cryptographic key access** See 7.4.8.6 for text. Refinement added.
	If a user's key has been broken, the new key shall be generated independent from the broken keys	**FCS_CKM.1**	**Cryptographic key generation** See 7.4.8.1 for text. Refinement added.
	In addition the transmission of key exchange information shall be independent from the broken keys.	**FCS_CKM.2**	**Cryptographic key distribution** See 7.4.8.3 for text. Refinement added.
9.4.5.2	**Certification.** The certification process generates the legal binding 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 the business process.	**FCS_CKM.2**	**Cryptographic key distribution** The security management shall support a key distribution technique addressing the integrity and confidentiality of the keying information as required. Refinement added.
	The CA shall provide adequate means for the authenticity and integrity of the stored certification data.	**FCS_CKM.3**	**Cryptographic key access** 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. Refinement added.
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.	**FCS_CKM.2**	**Cryptographic key distribution.** The security management shall support a key distribution technique addressing the integrity and confidentiality of the keying information as required. Refinement added.

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.	**FCS_CKM.4**	**Cryptographic key destruction** The security management shall support the revocation of distributed keys by technical or organizational means (Key revocation process).
	The CA shall provide adequate means for the authenticity and integrity of the stored revocation data.	**FCS_CKM.3**	**Cryptographic key access** 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. Refinement added.

A.9 Mapping of CC functional components to E - COFC functionalities

This clauses shows that each functional components maps to at least one E - COFC security functionality.

Table A.14 – CC to E - COFC mapping

No	Component	Name	E - COFC reference(s)
1	FAU_GEN.1	Audit data generation	7.4.2.8, 7.4.4.2, 7.4.4.4, 7.4.4.7
2	FAU_GEN.2	User identity generation	7.4.4.1
3	FAU_SAR.1	Audit review	7.4.4.13
4	FAU_SAR.2	Restricted audit review	7.4.2.4
5	FAU_SAR.3	Selectable audit review	7.4.4.13
6	FAU_SEL.1	Selective audit	7.4.4.11
7	FAU_STG.2	Guarantees of audit trail availability	7.4.4.8, 8.4.2.5, 9.4.3.1
8	FAU_STG.3	Action in case of possible audit data éoss	7.4.4.10
9	FCO_NRO.2	Enforced proof of origin	7.4.1.3, 7.4.3.2, 8.4.2.1, 8.4.2.3, 9.4.3.2, 9.4.4.2
10	FCO_NRR.1	Selective proof of receipt	7.4.1.3, 7.4.3.2, 8.4.2.2, 8.4.2.3, 9.4.3.3, 9.4.4.2
11	FCS_CKM.1	Cryptographic key generation	7.4.8.1, 7.4.8.2, 9.4.5.1
12	FCS_CKM.2	Cryptographic key distribution	7.4.1.13, 7.4.8.3, 7.4.8.4, 7.4.8.7, 8.4.1.1, 9.4.1.1, 9.4.4.1, 9.4.5.1, 9.4.5.2, 9.4.5.3
13	FCS_CKM.3	Cryptographic key access	7.4.8.5, 9.4.5.1, 9.4.5.2, 9.4.5.4

Table A.14 – CC to E - COFC mapping (continued)

No	Component	Name	E - COFC reference(s)
14	FCS_CKM.4	Cryptographic key destruction	7.4.8.6, 9.4.5.4
15	FDP_ACC.1	Subset access control	7.4.2.2
16	FDP_ACF.1	Security attribute based access control	7.4.2.2, 7.4.2.3, 7.4.2.5, 7.4.2.6, 7.4.2.7, 7.4.2.10
17	FDP_DAU.1	Basic data authentication	9.4.3.4
17.1	FDP_IFC.1	Subset information flow control	7.4.6.4
17.2	FDP_IFF.1	Simple security attributes	7.4.6.4
18	FDP_ITT.1	Basic internal transfer protection	7.4.3.1, 7.4.3.3
19	FDP_RIP.2	Full residual information protection	7.4.5.1
20	FDP_SDI.1	Stored data integrity monitoring	7.4.6.2
21	FDP_UCT.1	Basic data exchange confidentiality	7.4.3.3
22	FDP_UIT.1	Data exchange integrity	7.4.3.1
23	FIA_AFL.1	Basic authentication failure handling	7.4.1.6
24	FIA_ATD.1	User attribute definition	7.4.1.4
25	FIA_SOS.1	Selection of secrets	7.4.1.11
26	FIA_UAU.1	Timing of authentication	7.4.1.1, 7.4.1.2, 7.4.2.1
27	FIA_UAU.3	Unforgeable authentication	7.4.1.3
28	FIA_UAU.5	Multiple authentication mechanisms	9.4.1.1
29	FIA_UAU.6	Re-authenticating	7.4.1.8
30	FIA_UAU.7	Protected authentication feedback	7.4.1.12
31	FIA_UID.1	Timing of identification	7.4.1.1, 7.4.1.12
32	FIA_USB.1	User-subject binding	7.4.4.1
33	FMT_MOF.1	Management of security functions behavior	7.4.4.3
34	FMT_MSA.1	Management of security attributes	7.4.1.4
35	FMT_MSA.2	Secure security attributes	Dependency of FCS_CKM.2
36	FMT_MSA.3	Static attribute initialization	7.4.2.6
37	FMT_MTD.1	Management of TSF data	7.4.1.5, 7.4.1.10, 7.4.4.9
38	FMT_SAE.1	Time-limited authorization	7.4.1.7, 7.4.1.13
39	FMT_SMR.2	Restricted security roles	7.4.2.4
40	FPR_ANO.1	Anonymity	9.4.2.1
41	FPR_PSE.1	Pseudonymity	9.4.2.1
42	FPR_UNO.1	Unobservability	9.4.2.1
43	FPT_AMT.1	Abstract machine testing	Dependency of FPT_TST.1
44	FPT_FLS.1	Failure with preservation of secure state	Dependency of FPT_FLS.1
45	FPT_ITC.1	Inter-TSF confidentiality during transmission	7.4.3.3
46	FPT_ITI.1	Inter-TSF detection of modification	7.4.3.1

Table A.14 – CC to E - COFC mapping (concluded)

No	Component	Name	E - COFC reference(s)
47	FPT_ITT.1	Basic internal TSF data transfer protection	7.4.3.1, 7.4.3.3
48	FPT_RCV.1	Manual recovery	7.4.7.1
49	FPT_RPL.1	Replay detection	7.4.1.3, 7.4.3.2, 9.4.4.2
50	FPT_RVM.1	Non-bypassability of the TSP	7.4.2.9
51	FPT_SEP.1	TSF domain separation	7.4.1.11, 7.4.2.4
52	FPT_STM1	Reliable time stamps	7.4.4.14, 8.4.2.4
53	FPT_TDC.1	Inter-TSF basic TSF data consistency	8.4.1.2, 8.4.2.5, 9.4.3.1
54	FPT_TST.1	TSF testing	7.4.6.1
55	FRU_FLT.1	Degraded fault tolerance	7.4.7.4
56	FRU_RSA.1	Maximum quotas	7.4.7.3
57	FTA_SSL.1	TSF-initiated session locking	7.4.1.8
58	FTA_TAB.1	Default TOE access banners	7.4.1.5
59	FTA_TAH.1	TOE access history	7.4.1.5
60	FTA_TSE.1	TOE session establishment	7.4.1.9
61	FTP_ITC.1	Inter-TSF trusted channel	Dependency of FDP_UCT.1 and FDP_UIT.1
62	PBC_DYN.1	Dynamic control of audit	7.4.4.10, 7.4.4.12
63	PBC_NDD.1	Notification of non-delivery	8.4.2.3
64	PBC_BKP.1	Backup	7.4.7.2
65	PBC_SYN.1	Synchronization	7.4.4.14, 9.4.3.1

Annex B

Glossary

CC	Common Criteria [for IT Security Evaluation]
COTS	Commercial Off The Shelf
EAL	Evaluation Assurance Level
IT	Information Technology
NIST	National Institute of Standards and Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

Annex C

References

CC	Common Criteria Project, Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998.
COFC	ECMA, Commercially Oriented Functionality Class for Security Evaluation (COFC), Standard ECMA-205, December 1993.
CS2 PPG	Stoneburner, Gary, CS2 - Protection Profile Guidance for Near-Term COTS, Version 0.3, National Institute of Standards and Technology, July 13, 1998.
CS2 PPGR	Stoneburner, Gary, Rationale for CS2 - Protection Profile Guidance for Near-Term COTS, Version 0.3, National Institute of Standards and Technology, July 13, 1998.
E - COFC	ECMA, Extended Commercially Oriented Functionality Class for Security Evaluation (E - COFC), Standard ECMA-271, December 1997.
E - COFC PP	E - COFC Public Business Class Protection Profile, Version 0.31, 23 July 1998.
E - COFC PPR	E - COFC Public Business Class Protection Profile Rationale, Version 0.31, 23 July 1998.

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 Technical Report 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.