

COMMITTEE DRAFT ISO/IEC CD 15408-5		Reference document: SC 27 N18754	
Date: 2018-06-25		Supersedes document N18704, WG 3 N1475	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)		Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: 2018-08-20 Please submit your comments via the online balloting application by the due date indicated.	
ISO/IEC CD 15408-5 Title: IT-Security techniques – Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements Project: ISO/IEC 15408-5 (revision)			
Explanatory Report			
Status	SC 27 Decision	Reference documents	
		Input	Output
For details regarding previous development stages refer to 2 nd page of this explanatory report.			
ISO/IEC NP 15408-5 by subdivision Evaluation criteria for IT security -- Part 5 NWIP	53 rd WG 3 meeting, Oct. 2016, Recommendations 6, 15 (N16800 = WG 5 N600).	Expert contr. (WG 3 N1368, N1371, N1373).	SP report (WG 3 N1363); Call f. editor (WG 3 N1387 = N16886); Liaisons to: CCDB (WG 3 N1330); The Open Group (WG 3 N1332); Text f. NWIP (N16967 [replaces N16883]).
ISO/IEC 15408-5 1 st WD	54th WG 3 meeting, April 2017, Recommendations 5,10 11, 14 (N17041 = WG 3 N1413).	SoV (N17029).	Liaisons to: CCDB (WG 3 N1391); The Open Group (WG 3 N1394); ISO/TC 22/SC 32 (N17373); Text f. 1st WD (WG 3 N1439).
ISO/IEC 15408-5 2 nd WD	55th WG 3 meeting, October / November 2017, Recommendations 8, 10 (N17666 = WG 3 N1494).	SoCom (WG 3 N1473); Draft DoC (WG 3 N1501).	Editor's report (WG 3 N1465); Liaisons to: CCDB (WG 3 N1455); ISO/TC 22/SC 32 (N18103); DoC (WG 3 N1462); Text f. 2nd WD (WG 3 N1475).
ISO/IEC 15408-5 1 st CD	56 th WG 3 meeting, April 2018, Recommendations 8, 10 (N18471 = WG 3 N1557) / 30 th SC 27 Plenary, April 2018, Resolution 6 (N18710)	SoCom (WG 3 N1534); Late Com (WG 3 N1566).	Liaison to: CCDB (WG 3 N1521); DoC (WG 3 N1527); Text f. 1 st CD (N18754).
CD Registration and Consideration			
In accordance with resolution 6 (see SC 27 N18710) of the 30th SC 27 Plenary meeting held in Wuhan, China, 2018-04-23/24 the hereby attached document has been registered with the ISO Central Secretariat (ITTF) as 1st Committee Draft (CD) and is being circulated for a 1st CD 8 weeks letter ballot closing by			
2018-08-20			
Medium: http://isotc.iso.org/livelink/livelink/open/jtc1sc27			
No. of pages: 2 + 44			

Explanatory Report (2nd page)			
Status	SC 27 Decision	Reference documents	
		Input	Output
Study Period IT security testing, evaluation and assurance standards and techniques	51 st WG 3 meeting, Oct. 2015, Recommendations 5, 6 (N15594 = WG 3 N1251).		Terms of Reference (WG 5 N1258); 1 st /2 nd call f. contr. (WG 3 N1259 /1317)..
	52 nd WG 3 meeting, April 2016, Recommendation 5, 7 (N16026 = WG 3 N1296).	Expert contr. (WG 3 N1299, 1301).	3 rd call f. contr. (WG 3 N1377); Rapporteur's report (WG 3 N1320); Liaison to: CCDB (WG 3 N1266).

ISO/IEC JTC 1/SC 27/WG 3 N18754

Date: 2018-06-22

ISO/IEC WD 15408-5:####(EN)

ISO/IEC JTC 1/SC 27 IT Security techniques

Secretariat: DIN

**IT security techniques — Evaluation criteria for IT security — Part 5:
Pre-defined packages of security requirements**

**Techniques de sécurité IT — Critères d'évaluation pour la sécurité des technologies
de l'information — *Partie 5 : Paquets prédéfinis d'exigences de sécurité***

CD stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

25	Contents	Page
26	Foreword.....	iv
27	Introduction	v
28	1 Scope.....	1
29	2 Normative references	1
30	3 Terms and Definitions	1
31	4 Evaluation Assurance Levels.....	2
32	4.1 Family Name	2
33	4.2 Evaluation assurance level (EAL) overview.....	2
34	4.2.1 Relationship between assurances and assurance levels.....	2
35	4.3 Evaluation assurance level (EAL) objectives	4
36	4.4 Evaluation assurance level packages	5
37	4.4.1 Evaluation assurance level 1 (EAL1) - functionally tested	5
38	4.4.2 Evaluation assurance level 2 (EAL2) - structurally tested.....	7
39	4.4.3 Evaluation assurance level 3 (EAL3) - methodically tested and checked.....	8
40	4.4.4 Evaluation assurance level 4 (EAL4) - methodically designed, tested and	
41	reviewed	9
42	4.4.5 Evaluation assurance level 5 (EAL5) – semiformally verified designed and	
43	tested	11
44	4.4.6 Evaluation assurance level 6 (EAL6) – verified design and tested	13
45	4.4.7 Evaluation assurance level 7 (EAL7) - formally verified design and tested	14
46	5 Composed Assurance Packages.....	17
47	5.1 Family Name	17
48	5.2 Composed assurance package (CAP) overview	17
49	5.2.1 Relationship between assurances and assurance levels.....	17
50	5.3 Composed assurance package (CAP) objectives.....	18
51	5.4 Packages in the CAP family	20
52	5.4.1 Composition assurance level A (CAP-A) - Structurally composed	20
53	5.4.2 Composition assurance level B (CAP-B) - Methodically composed	21
54	5.4.3 Composition assurance level C (CAP-C) - Methodically composed, tested and	
55	reviewed	23
56	6 Composite Product Package.....	24
57	6.1.1 Composite Product (COMP).....	24
58	7 Protection Profile Assurance (PPA).....	25
59	7.1 Family Name	25
60	7.2 PPA family overview	25
61	7.3 PPA family objectives.....	26
62	7.4 PPA Packages.....	26
63	7.4.1 Direct Rationale PP (PPA-DR).....	26
64	7.4.2 Protection Profile Assurance Package - Standard (PPA-STD)	26
65	8 Security Target Assurance (STA).....	27
66	8.1 Family Name	27
67	8.2 STA family overview.....	27
68	8.3 STA family objectives	28
69	8.4 STA Packages.....	28
70	8.4.1 Direct Rationale ST (STA-DR)	28
71	8.4.2 Security Target Assurance Package - Standard (STA-STD)	29
72	Annex A (informative) Composition (ACO)	30
73		

READ ME FIRST

Editor's general notes for this draft.

Red text in a box are the Editors' comments.

Some editorial changes have also been introduced in order to comply with the [ISO/IEC Directives part 2:2018](#)

The editors are aware that the figures are of low quality. In the final documents high quality images will be used. The Editors hope that they are legible in this draft.

The Editor thanks the WG 3 contributors for their contributions and support during the editing cycle.

84 Foreword

85 ISO (the International Organization for Standardization) and IEC (the International
86 Electrotechnical Commission) form the specialized system for worldwide standardization.
87 National bodies that are members of ISO or IEC participate in the development of International
88 Standards through technical committees established by the respective organization to deal with
89 particular fields of technical activity. ISO and IEC technical committees collaborate in fields of
90 mutual interest. Other international organizations, governmental and non-governmental, in
91 liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and
92 IEC have established a joint technical committee, ISO/IEC JTC 1.

93 The procedures used to develop this document and those intended for its further maintenance
94 are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria
95 needed for the different types of document should be noted. This document was drafted in
96 accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see
97 www.iso.org/directives).

98 Attention is drawn to the possibility that some of the elements of this document may be the
99 subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such
100 patent rights. Details of any patent rights identified during the development of the document will
101 be in the Introduction and/or on the ISO list of patent declarations received (see
102 www.iso.org/patents).

103 Any trade name used in this document is information given for the convenience of users and does
104 not constitute an endorsement.

105 For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and
106 expressions related to conformity assessment, as well as information about ISO's adherence to
107 the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see
108 www.iso.org/iso/foreword.html.

109 This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology,
110 Subcommittee SC 27, IT Security techniques.

111 A list of all parts in the ISO/IEC 15408 series can be found on the ISO website.

112 Any feedback or questions on this document should be directed to the user's national standards
113 body. A complete listing of these bodies can be found at www.iso.org/members.html.

114 This is the **first** edition of ISO/IEC 15408-5.

115 A list of all parts in the ISO/IEC **15408** series can be found on the ISO website.

116 Introduction

117 This document provides pre-defined packages of security requirements. Such security
 118 requirements may be useful for stakeholders as they strive for conformity between evaluations.
 119 Packages of security requirements may also help reduce the effort in developing PPs and STs.

120 Part 1 of ISO/IEC 15408 defines the term “package” and describes the fundamental concepts.

121 This document presents:

- 122 • *evaluation assurance level (EAL)* family of packages that specify pre-defined sets of security
 123 assurance components that may be referenced in PPs and STs and which specify
 124 appropriate security assurances to be provided during an evaluation of a TOE.
- 125 • *composition assurance (CAP)* family of packages that specify sets of security assurance
 126 components used for specifying appropriate security assurances to be provided during an
 127 evaluation of composed TOEs.
- 128 • *composite product (COMP)* package that specifies a set of security assurance components
 129 used for specifying appropriate security assurances to be provided during an evaluation of
 130 a composite product TOEs.
- 131 • *Protection Profile Assurance (PPA)* family of packages that specify sets of security assurance
 132 components used for specifying appropriate security assurances to be provided during a
 133 protection profile evaluation.
- 134 • *Security Target Assurance (STA)* family of packages that specify sets of security assurance
 135 components used for specifying appropriate security assurances to be provided during a
 136 Security Target evaluation.

137 The audience for this document includes consumers, developers, and evaluators of secure IT
 138 products.

IT security techniques — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements

1 Scope

This document provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders.

EXAMPLE

Examples of provided packages include the evaluation assurance levels (EAL) and the composed assurance packages (CAPs).

Editor's Note:

At this time, no pre-defined packages of security functional requirements have been identified for inclusion in ISO/IEC 15408-5. The Study Period indicated that Experts may contribute SFR packages during this revision of ISO/IEC 15408.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *IT security techniques — Evaluation criteria for IT security — Part 1: Introduction and general requirements*

ISO/IEC 15408-2, *IT security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

ISO/IEC 15408-3, *IT security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *IT security techniques — Methodology for IT security evaluation*

3 Terms and Definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

171 4 Evaluation Assurance Levels

172 4.1 Family Name

173 The name of this family of packages is *Evaluation Assurance Levels (EAL)*.

174 4.2 Evaluation assurance level (EAL) overview

175 The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of
176 assurance obtained with the cost and feasibility of acquiring that degree of assurance. ISO/IEC
177 15408 approach identifies the separate concepts of assurance in a TOE at the end of the evaluation,
178 and of maintenance of that assurance during the operational use of the TOE.

179 It is important to note that not all families and components given in ISO/IEC 15408-3 are included
180 in the EALs. This is not to say that these do not provide meaningful and desirable assurances.
181 Instead, it is expected that these families and components will be considered for augmentation of
182 an EAL in those PPs and STs for which they provide utility. Additionally, some classes found in
183 ISO/IEC 15408-3 are not relevant for the EAL packages. (For example, the APE and ACO classes.)

184 A set of assurance components have been chosen for each EAL package.

185 A higher level of assurance than that provided by a given EAL can be achieved by:

- 186 a) including additional assurance components from other assurance families; or
- 187 b) replacing an assurance component with a higher-level assurance component from the same
188 assurance family.

189 4.2.1 Relationship between assurances and assurance levels

190 Figure 1 illustrates the relationship between the SARs and the assurance levels defined in ISO/IEC
191 15408. While assurance components further decompose into assurance elements, assurance
192 elements cannot be individually referenced by assurance levels. Note that the arrow in the figure
193 represents a reference from an EAL to an assurance component within the class where it is defined.

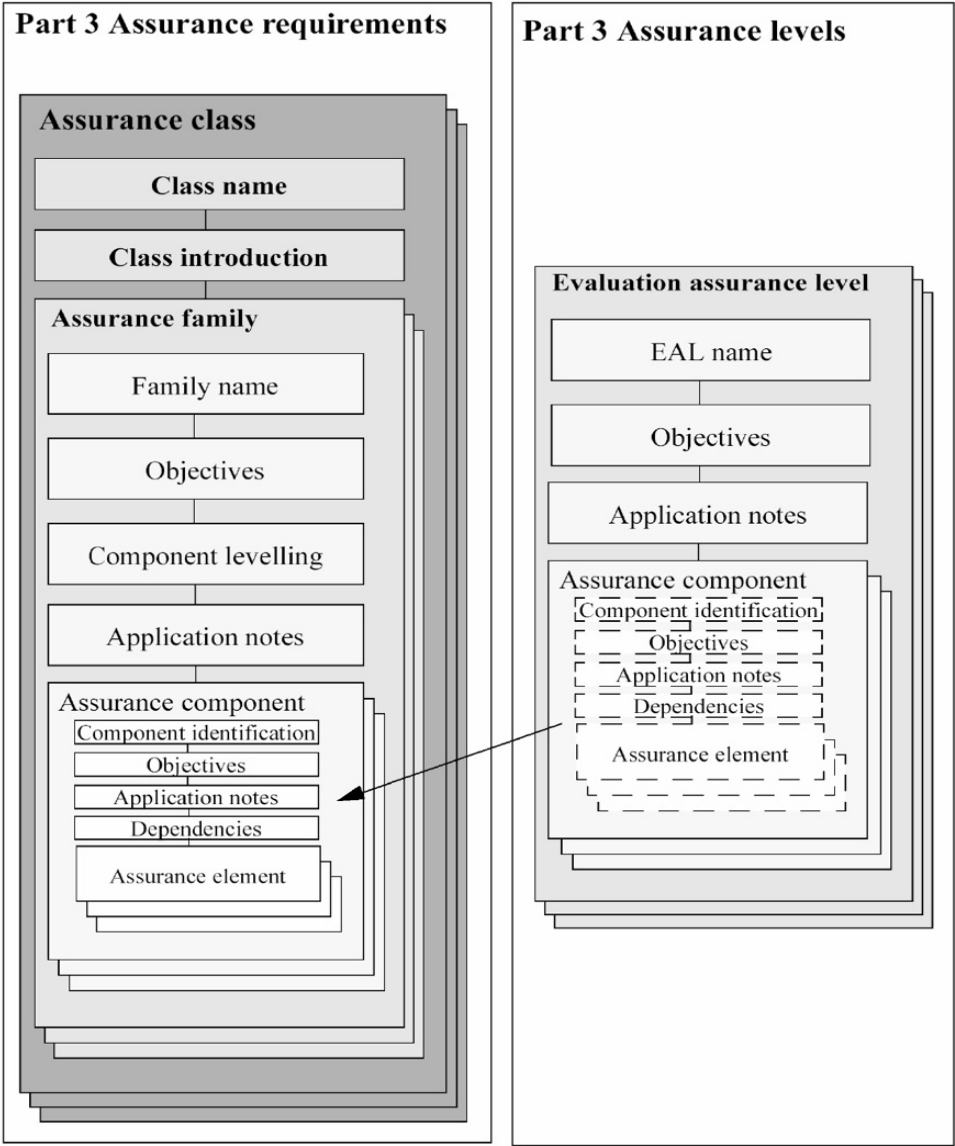


Figure 1 — Assurance and assurance level association

Table 1 represents a summary of the EAL packages. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

Editors' Note:

The Editors solicit comments in regard to the inclusion of ALC_PTD in the EAL tables.

203

Table 1 — Evaluation assurance level summary

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_PTD	??	??	??	??	??	??	??
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

204

205 4.3 Evaluation assurance level (EAL) objectives

206 As outlined in the next subclause, seven hierarchically ordered evaluation assurance levels are
 207 defined in ISO/IEC 15408 for the rating of a TOE's assurance. They are hierarchically ordered
 208 inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance
 209 from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component
 210 from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition
 211 of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in ISO/IEC 15408-3. More precisely, each EAL includes no more than one component of each assurance family and all the assurance dependencies of every component are addressed.

The notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in ISO/IEC 15408, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognized by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

NOTE An EAL cannot be augmented if it is included in an ST that claims exact conformance to a PP.

4.4 Evaluation assurance level packages

The following subclauses provide definitions of the EALs, highlighting differences between the specific requirements and the prose characterisations of those requirements using bold type.

4.4.1 Evaluation assurance level 1 (EAL1) - functionally tested

4.4.1.1 Package Name

The name of the package is: *Evaluation assurance level 1 (EAL1) - functionally tested*.

4.4.1.2 Package Type

This is an assurance Package.

4.4.1.3 Package overview

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.

4.4.1.4 Package objectives

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

This EAL provides a meaningful increase in assurance over unevaluated IT.

4.4.1.5 Assurance components

Table 2 gives the assurance components included in EAL 1.

Table 2 — EAL1

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

4.4.2 Evaluation assurance level 2 (EAL2) - structurally tested

4.4.2.1 Package Name

The name of the package is: *Evaluation assurance level 2 (EAL2) –structurally tested*.

4.4.2.2 Package Type

This is an assurance Package.

4.4.2.3 Package overview

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

4.4.2.4 Objectives

EAL2 provides assurance by a **full** security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation **and a basic description of the architecture of the TOE**, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, **evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.**

EAL2 also provides assurance through **use of a configuration management system and evidence of secure delivery procedures.**

This EAL **represents** a meaningful increase in assurance **from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.**

4.4.2.5 Assurance components

Table 3 gives the assurance components included in EAL 2.

Table 3 — EAL2

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system

Assurance Class	Assurance components
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

290

291 **4.4.3 Evaluation assurance level 3 (EAL3) - methodically tested and checked**292 **4.4.3.1 Package Name**293 The name of the package is: *Evaluation assurance level 3 (EAL3) –methodically tested and checked.*294 **4.4.3.2 Package Type**

295 This is an assurance Package.

296 **4.4.3.3 Package overview**

297 EAL3 permits a conscientious developer to gain maximum assurance from positive security
 298 engineering at the design stage without substantial alteration of existing sound development
 299 practices.

300 EAL3 is applicable in those circumstances where developers or users require a moderate level of
 301 independently assured security and require a thorough investigation of the TOE and its
 302 development without substantial re-engineering.

303 **4.4.3.4 Objectives**

304 **EAL3** provides assurance by a full security target and an analysis of the SFRs in that ST, using a
 305 functional and interface specification, guidance documentation, and an **architectural description**
 306 of the **design** of the TOE, to understand the security behaviour.

307 The analysis is supported by independent testing of the TSF, evidence of developer testing based
 308 on the functional specification **and TOE design**, selective independent confirmation of the
 309 developer test results, and a vulnerability analysis (based upon the functional specification, TOE
 310 design, security architecture description and guidance evidence provided) demonstrating
 311 resistance to penetration attackers with a basic attack potential.

312 **EAL3** also provides assurance through **the use of development environment controls, TOE**
 313 configuration management, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from **EAL2** by requiring **more complete testing coverage** of the **security** functionality and **mechanisms and/or procedures that provide some confidence that the TOE will not be tampered with during development.**

4.4.3.5 Assurance components

Table 4 gives the assurance components included in EAL 3.

Table 4 — EAL3

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

4.4.4 Evaluation assurance level 4 (EAL4) - methodically designed, tested and reviewed

4.4.4.1 Package Name

The name of the package is: *Evaluation assurance level 4 (EAL4) –methodically designed, tested and reviewed.*

4.4.4.2 Package Type

This is an assurance Package.

4.4.4.3 Package overview

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, although rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

4.4.4.4 Objectives

EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and **complete** interface specification, guidance documentation, a description of the **basic modular** design of the TOE, and **a subset of the implementation**, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, **implementation representation**, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with **an Enhanced-Basic** attack potential.

EAL4 also provides assurance through the use of development environment controls and **additional** TOE configuration management **including automation**, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from **EAL3** by requiring more **design description**, the **implementation representation for the entire TSF**, and **improved** mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

4.4.4.5 Assurance components

Table 5 gives the assurance components included in EAL 4.

Table 5 — EAL4

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance components
	ALC_TAT.1 Well defined developer tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

356

357 **4.4.5 Evaluation assurance level 5 (EAL5) – semiformally verified designed and tested**358 **4.4.5.1 Package Name**359 The name of the package is: *Evaluation assurance level 5 (EAL5) – semiformally designed and tested.*360 **4.4.5.2 Package Type**

361 This is an assurance Package.

362 **4.4.5.3 Package overview**

363 EAL5 permits a developer to gain maximum assurance from security engineering based upon
364 rigorous commercial development practices supported by moderate application of specialist
365 security engineering techniques. Such a TOE will probably be designed and developed with the
366 intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5
367 requirements, relative to rigorous development without the application of specialized techniques,
368 will not be large.

369 EAL5 is therefore applicable in those circumstances where developers or users require a high level
370 of independently assured security in a planned development and require a rigorous development
371 approach without incurring unreasonable costs attributable to specialist security engineering
372 techniques.

373 **4.4.5.4 Objectives**

374 **EAL5** provides assurance by a full security target and an analysis of the SFRs in that ST, using a
375 functional and complete interface specification, guidance documentation, a description of the
376 design of the TOE, and the implementation, to understand the security behaviour. **A modular TSF
377 design is also required.**

378 The analysis is supported by independent testing of the TSF, evidence of developer testing based
379 on the functional specification, TOE design, selective independent confirmation of the developer

380 test results, and **an independent** vulnerability analysis demonstrating resistance to penetration
 381 attackers with **a moderate** attack potential.

382 **EAL5** also provides assurance through the use of **a** development environment controls,
 383 and **comprehensive** TOE configuration management including automation, and evidence of secure
 384 delivery procedures.

385 This EAL represents a meaningful increase in assurance from **EAL4** by requiring **semiformal**
 386 **design descriptions, a more structured (and hence analysable) architecture**, and improved
 387 mechanisms and/or procedures that provide confidence that the TOE will not be tampered with
 388 during development.

389 4.4.5.5 Assurance components

390 Table 6 gives the assurance components included in EAL 5.

391 **Table 6 — EAL5**

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.1 Implementation representation of the TSF
	ADV_INT.2 Well-structured internals
	ADV_TDS.4 Semi-formal modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.2 Compliance with implementation standards
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.4 Methodical vulnerability analysis

4.4.6 Evaluation assurance level 6 (EAL6) – verified design and tested

4.4.6.1 Package Name

The name of the package is: *Evaluation assurance level 6 (EAL6) –semiformally verified design and tested.*

4.4.6.2 Package Type

This is an assurance Package.

4.4.6.3 Package overview

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.

4.4.6.4 Objectives

EAL6 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, the design of the TOE, and the implementation to understand the security behaviour. **Assurance is additionally gained through a formal model of select TOE security policies and a semiformal presentation of the functional specification and TOE design.** A modular, **layered and simple** TSF design is also required.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, TOE design, selective independent confirmation of the developer test results, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a **high** attack potential.

EAL6 also provides assurance through the use of a **structured** development process, **development** environment controls, and comprehensive TOE configuration management including **complete** automation, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from **EAL5** by requiring **more comprehensive analysis**, a **structured representation of the implementation**, more **architectural structure (e.g. layering)**, **more comprehensive independent vulnerability analysis**, and improved **configuration management and development environment controls**.

4.4.6.5 Assurance components

Table 7 gives the assurance components included in EAL 6.

Table 7 — EAL6

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF

Assurance Class	Assurance components
	ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security model policy
	ADV_TDS.5 Complete Semi-formal modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.3 Compliance with implementation standards – all parts
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.2 Ordered functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

4.4.7 Evaluation assurance level 7 (EAL7) - formally verified design and tested

4.4.7.1 Package Name

The name of the package is: *Evaluation assurance level 7 (EAL7) –formally verified design and tested.*

4.4.7.2 Package Type

This is an assurance Package.

4.4.7.3 Package overview

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

4.4.7.4 Objectives

EAL7 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, the design of the TOE, and a **structured presentation** of the implementation to understand the security behaviour.

439 Assurance is additionally gained through a formal model of select TOE security policies and a
 440 semiformal presentation of the functional specification and TOE design. A modular, layered and
 441 simple TSF design is also required.

442 The analysis is supported by independent testing of the TSF, evidence of developer testing based
 443 on the functional specification, TOE design **and implementation representation, complete**
 444 independent confirmation of the developer test results, and an independent vulnerability analysis
 445 demonstrating resistance to penetration attackers with a high attack potential.

446 **EAL7** also provides assurance through the use of a structured development process, development
 447 environment controls, and comprehensive TOE configuration management including complete
 448 automation, and evidence of secure delivery procedures.

449 This EAL represents a meaningful increase in assurance from **EAL6** by requiring more
 450 comprehensive analysis **using formal representations and formal correspondence**, and
 451 **comprehensive testing**.

452 4.4.7.5 Assurance components

453 Table 8 gives the assurance components included in EAL 7.

454 **Table 8 — EAL7**

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF
	ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security model policy
	ADV_TDS.6 Complete Semi-formal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.3 Compliance with implementation standards – all parts
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem definition

Assurance Class	Assurance components
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.4 Testing: implementation representation
	ATE_FUN.2 Ordered functional testing
	ATE_IND.3 Independent testing - complete
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

455

5 Composed Assurance Packages

5.1 Family Name

The name of this family of packages is *Composed Assurance Packages (CAP)*.

5.2 Composed assurance package (CAP) overview

The structure of the CAPs is similar to that of the EALs. The main difference between these two types of package is the type of TOE they apply to; the EALs applying to component TOEs and the CAPs applying to composed TOEs.

Figure 2 illustrates the CAPs and associated structure defined in this document. Note that while the figure shows the contents of the assurance components, it is intended that this information would be included in a CAP by reference to the actual components defined in ISO/IEC 15408.

Some dependencies identify the activities performed during the evaluation of the dependent component on which the composed TOE activity relies. Where it is not explicitly identified that the dependency is on a dependent component activity, the dependency is to another evaluation activity of the composed TOE.

A higher level of assurance than that provided by a given CAP can be achieved by:

a) including additional assurance components from other assurance families; or

b) replacing an assurance component with a higher-level assurance component from the same assurance family.

The ACO: Composition components included in the CAP assurance packages should not be used as augmentations for component TOE evaluations, as this would provide no meaningful assurance for the component.

5.2.1 Relationship between assurances and assurance levels

Figure 2 illustrates the relationship between the SARs and the composed assurance packages defined in ISO/IEC 15408. While assurance components further decompose into assurance elements, assurance elements cannot be individually referenced by assurance packages. Note that the arrow in the figure represents a reference from a CAP to an assurance component within the class where it is defined.

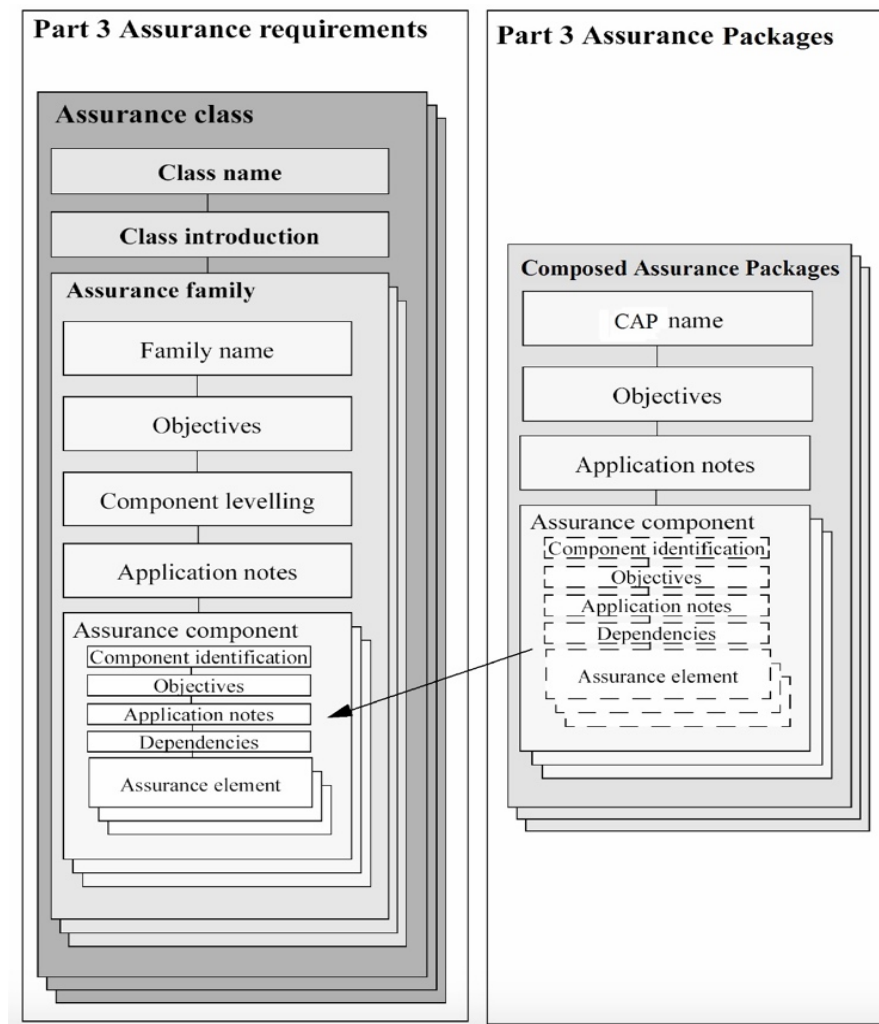


Figure 2 — Assurance and composed assurance package association

5.3 Composed assurance package (CAP) objectives

The Composed Assurance Packages (CAPs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance for composed TOEs.

It is important to note that there are only a small number of families and components from part 3 of ISO/IEC 15408 included in the CAPs. This is due to their nature of building upon evaluation results of previously evaluated entities (base components and dependent components), and is not to say that these do not provide meaningful and desirable assurances.

CAPs are to be applied to composed TOEs, which are comprised of components that have been (are going through) component TOE evaluation (see Annex B). The individual components will have been certified to an EAL or another assurance package specified in the ST. It is expected that a basic level of assurance in a composed TOE will be gained through application of EAL1, which can be achieved with information about the components that is generally available in the public domain. (EAL1 can be applied as specified within to both component and composed TOEs.) CAPs provide an alternative approach to obtaining higher levels of assurance for a composed TOE than application of the EALs above EAL1.

While a dependent component can be evaluated using a previously evaluated and certified base component to satisfy the IT platform requirements in the environment, this does not provide any

formal assurance of the interactions between the components or the possible introduction of vulnerabilities resulting from the composition. Composed assurance packages consider these interactions and, at higher levels of assurance, ensure that the interface between the components has itself been the subject of testing. A vulnerability analysis of the composed TOE is also performed to consider the possible introduction of vulnerabilities as a result of composing the components.

Table 9 represents a summary of the CAPs. The columns represent a hierarchically ordered set of CAPs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next subclause, three hierarchically ordered composed assurance packages are defined in ISO/IEC 15408 for the rating of a composed TOE's assurance. They are hierarchically ordered inasmuch as each CAP represents more assurance than all lower CAPs. The increase in assurance from CAP to CAP is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements). These increases result in greater analysis of the composition to identify the impact on the evaluation results gained for the individual component TOEs.

These CAPs consist of an appropriate combination of assurance components as described in Clause 6 of ISO/IEC 15408-3:20XX. More precisely, each CAP includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

The CAPs only consider resistance against an attacker with an attack potential up to Enhanced-Basic. This is due to the level of design information that can be provided through the ACO_DEV, limiting some of the factors associated with attack potential (knowledge of the composed TOE) and subsequently affecting the rigour of vulnerability analysis that can be performed by the evaluator. Therefore, the level of assurance in the composed TOE is limited, although the assurance in the individual components within the composed TOE may be much higher.

Table 9 shows a summary of the composed assurance packages.

Editor's Note:

The inclusion of the ALC_DEL, DVS, FLR, LCD and TAT families seems redundant. The tables miss other complete Classes, so why include these unused families?

Editor proposes deletion of these rows.

If no comments are received on this, the editor's proposal will be accepted and presented in the next draft.

Table 9 — Composition assurance level summary

Assurance class	Assurance Family	Assurance Components by Composition Assurance Package		
		CAP-A	CAP-B	CAP-C
Composition	ACO_COR	1	1	1
	ACO_CTT	1	2	2
	ACO_DEV	1	2	3
	ACO_REL	1	1	2
	ACO_VUL	1	2	3

Guidance documents	AGD_OPE	1	1	1
	AGD_PRE	1	1	1
Life-cycle support	ALC_CMC	1	1	1
	ALC_CMS	2	2	2
	ALC_DEL			
	ALC_DVS			
	ALC_FLR			
	ALC_LCD			
	ALC_TAT			
Security Target evaluation	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD		1	1
	ASE_TSS	1	1	1

537 5.4 Packages in the CAP family

538 5.4.1 Composition assurance level A (CAP-A) - Structurally composed

539 5.4.1.1 Package Name

540 The name of the package is: *Composition assurance level A (CAP-A) –Structurally composed.*

541 5.4.1.2 Package Type

542 This is an assurance Package.

543 5.4.1.3 Package overview

544 CAP-A is applicable when a composed TOE is integrated and confidence in the correct security
545 operation of the resulting composite is required. This requires the cooperation of the developer of
546 the dependent component in terms of delivery of design information and test results from the
547 dependent component certification, without requiring the involvement of the base component
548 developer.

549 CAP-A is therefore applicable in those circumstances where developers or users require a low to
550 moderate level of independently assured security in the absence of ready availability of the
551 complete development record.

552 5.4.1.4 Objectives

553 CAP-A provides assurance by analysis of a security target for the composed TOE. The SFRs
554 in the composed TOE ST are analysed using the outputs from the evaluations of the
555 component TOEs (e.g. ST, guidance documentation) and a specification for the interfaces
556 between the component TOEs in the composed TOE to understand the security behaviour.

557 The analysis is supported by independent testing of the interfaces of the base component
558 that are relied upon by the dependent component, as described in the reliance information,
559 evidence of developer testing based on the reliance information, development information

and composition rationale, and selective independent confirmation of the developer test results. The analysis is also supported by a vulnerability review of the composed TOE by the evaluator.

CAP-A also provides assurance through unique identification of the composed TOE (i.e. IT TOE and guidance documentation).

5.4.1.5 Assurance components

Table 10 gives the assurance components included in CAP-A.

Table 10 — CAP-A

Assurance Class	Assurance components
ACO: Composition	ACO_COR.1 Composition rationale
	ACO_CTT.1 Interface testing
	ACO_DEV.1 Functional description
	ACO_REL.1 Basic reliance information
	ACO_VUL.1 Composition vulnerability review
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification

5.4.2 Composition assurance level B (CAP-B) - Methodically composed

5.4.2.1 Package Name

The name of the package is: *Composition assurance level B (CAP-B) –Methodically composed*.

5.4.2.2 Package Type

This is an assurance Package.

5.4.2.3 Package overview

CAP-B permits a conscientious developer to gain maximum assurance from understanding, at a subsystem level, the effects of interactions between component TOEs integrated in the composed TOE, whilst minimising the demand of involvement of the base component developer.

578 CAP-B is applicable in those circumstances where developers or users require a moderate level of
 579 independently assured security, and require a thorough investigation of the composed TOE and its
 580 development without substantial re-engineering.

581 5.4.2.4 Objectives

582 **CAP-B** provides assurance by analysis of a **full** security target for the composed TOE. The SFRs in
 583 the composed TOE ST are analysed using the outputs from the evaluations of the component TOEs
 584 (e.g. ST, guidance documentation), a specification for the interfaces between the component
 585 TOEs **and the TOE design (describing TSF subsystems) contained** in the
 586 composed **development information** to understand the security behaviour.

587 The analysis is supported by independent testing of the interfaces of the base component that are
 588 relied upon by the dependent component, as described in the reliance information **(now also**
 589 **including TOE design)**, evidence of developer testing based on the reliance information,
 590 development information and composition rationale, and selective independent confirmation of
 591 the developer test results. The analysis is also supported by a vulnerability **analysis** of the
 592 composed TOE by the evaluator **demonstrating resistance to attackers with basic attack**
 593 **potential**.

594 **This CAP represents a meaningful increase in assurance from CAP-A by requiring more**
 595 **complete testing coverage of the security functionality.**

596 5.4.2.5 Assurance components

597 Table 11 gives the assurance components included in CAP-B.

598 **Table 11 — CAP-B**

Assurance Class	Assurance components
ACO: Composition	ACO_COR.1 Composition rationale
	ACO_CTT.2 Rigorous interface testing
	ACO_DEV.2 Basic evidence of design
	ACO_REL.1 Basic reliance information
	ACO_VUL.2 Composition vulnerability analysis
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.2 Parts of the TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives for the operational environment
	ASE_REQ.2 Stated security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

599

5.4.3 Composition assurance level C (CAP-C) - Methodically composed, tested and reviewed

5.4.3.1 Package Name

The name of the package is: *Composition assurance level C (CAP-C) –Methodically composed, tested and reviewed.*

5.4.3.2 Package Type

This is an assurance Package.

5.4.3.3 Package overview

CAP-C permits a developer to gain maximum assurance from positive analysis of the interactions between the components of the composed TOE, which, though rigorous, do not require full access to all evaluation evidence of the base component.

CAP-C is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity composed TOEs and are prepared to incur additional security-specific engineering costs.

5.4.3.4 Objectives

CAP-C provides assurance by analysis of a full security target for the composed TOE. The SFRs in the composed TOE ST are analysed using the outputs from the evaluations of the component TOEs (e.g. ST, guidance documentation), a specification for the interfaces between the component TOEs and the TOE design (describing TSF **modules**) contained in the composed development information to understand the security behaviour.

The analysis is supported by independent testing of the interfaces of the base component that are relied upon by the dependent component, as described in the reliance information (now including TOE design), evidence of developer testing based on the reliance information, development information and composition rationale, and selective independent confirmation of the developer test results. The analysis is also supported by a vulnerability analysis of the composed TOE by the evaluator demonstrating resistance to attackers with **Enhanced-Basic** attack potential.

This CAP represents a meaningful increase in assurance from **CAP-B** by requiring more **design description and demonstration of resistance to a higher attack potential**.

5.4.3.5 Assurance components

Table 12 gives the assurance components included in CAP-C.

Table 12 — CAP-C

Assurance Class	Assurance components
ACO: Composition	ACO_COR.1 Composition rationale
	ACO_CTT.2 Rigorous interface testing
	ACO_DEV.3 Detailed evidence of design
	ACO_REL.2 Reliance information
	ACO_VUL.3 Enhanced-Basic Composition vulnerability analysis
AGD: Guidance documents	AGD_OPE.1 Operational user guidance

Assurance Class	Assurance components
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.2 Parts of the TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives for the operational environment
	ASE_REQ.2 Stated security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

631

632 **6 Composite Product Package**633 **Editor Note:**

634 The editor proposes the following initial draft text for the “Composition package” using the
635 XXX_COMP families that have been added to CD1 for Part 3.

636 The Editor solicits comments in regard to this proposal.

637 **6.1.1 Composite Product (COMP)**638 **6.1.1.1 Package name**

639 The name of the package is *Composite Product (COMP)*.

640 **6.1.1.2 Package type**

641 This package is an *assurance package*.

642 **6.1.1.3 Package overview**

643 COMP provides assurance that a composite product TOE has been assembled and evaluated
644 according to the relevant criteria.

645 **6.1.1.4 Objectives**

646 COMP is applicable when composition techniques according to ISO/IEC 15408-1, 13 have been
647 specified. The objective is to ensure that the TOE has been composed taking into account the
648 requirements given in ISO/IEC 15408-1 and ISO/IEC 15408-3 and that the evaluation of security
649 targets, life cycle requirements, design and vulnerability analysis for the composed TOE have been
650 performed according to the criteria specified in ISO/IEC 15408-3. Providing assurance that
651 potential contradictions and inconsistencies have been taken into account.

652 **6.1.1.5 Security assurance components**

653 The security assurance components given in Table 15 are included in the package.

654

Table 13 — COMP

Assurance Class	Assurance components
ASE: Security Target Evaluation	ASE_COMP.1 Consistency of composite product Security Target
ALC: Life-cycle support	ALC_COMP.1 Integration of the application into the underlying platform and Consistency check for delivery and acceptance procedures
ADV: Development	ADV_COMP.1 Design compliance with the platform certification report, guidance and ETR_COMP
ATE: Tests	ATE_COMP.1 Composite product functional testing
AVA: Vulnerability analysis	AVA_COMP.1 Composite product vulnerability assessment

655

656 7 Protection Profile Assurance (PPA)

657 7.1 Family Name

658 The name of this family of packages is *Protection Profile Assurance (PPA)*.

659 7.2 PPA family overview

660 The Protection Profile Assurance (PPA) family provides two assurance packages for PP evaluation.

661 a) Assurance package for evaluating direct rationale PPs

662 b) Assurance package for evaluating standard PPs

663 These assurance packages provide the components that are used in the evaluation of each type of
664 Protection Profile described in ISO/IEC 15408-1.

665 Table 14 represents a summary of the PPAs. The columns represent the set of PPAs, while the rows
666 represent assurance families. Each number in the resulting matrix identifies a specific assurance
667 component where applicable.

668 These PPAs consist of an appropriate combination of assurance components as described in Clause
669 7 of part 3 of ISO/IEC 15408:20XX. More precisely, each PPA includes no more than one component
670 of each assurance family and all assurance dependencies of every component are addressed.

671

Table 14 — PPA summary

Assurance class	Assurance family	Assurance Components by Protection Profile Assurance Package	
		Direct Rationale PP (PPA-DR)	Standard PP (PPA-STD)
Protection Profile evaluation	APE_CCL	1	1
	APE_ECD	1	1
	APE_INT	1	1
	APE_OBJ	1	2
	APE_REQ	1	2
	APE_SPD	1	1

672

673 **7.3 PPA family objectives**

674 The PPA objectives are to support the provision of assurance through evaluation that a protection
 675 profile conforms with the requirements given in ISO/IEC 15408.

676 **7.4 PPA Packages**677 **7.4.1 Direct Rationale PP (PPA-DR)**678 **7.4.1.1 Package name**

679 The name of the package is *Protection Profile Assurance Package - Direct Rationale (PPA-DR)*.

680 **7.4.1.2 Package type**

681 This package is an *assurance package*.

682 **7.4.1.3 Package overview**

683 PPA_DR provides assurance by evaluation of a Direct Rationale Protection Profile, using the criteria
 684 specified in ISO/IEC 15408-3.

685 **7.4.1.4 Objectives**

686 PPA-DR is applicable when a Direct Rationale PP is evaluated. It may be used to verify that a Direct
 687 Rationale PP conforms with the requirements of ISO/IEC 15408-1

688 **7.4.1.5 Security assurance components**

689 The security assurance components given in Table 15 are included in the package.

690

Table 15 — PPA-DR

Assurance Class	Assurance components
APE: Protection Profile Evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements

691

692 **7.4.2 Protection Profile Assurance Package - Standard (PPA-STD)**693 **7.4.2.1 Package name**

694 The name of the package is *Protection Profile Assurance Package – Standard PP (PPA-STD)*.

695 **7.4.2.2 Package type**

696 This package is an *assurance package*.

7.4.2.3 Package overview

PPA_STD provides assurance by evaluation of a standard Protection Profile, using the criteria specified in ISO/IEC 15408-3.

7.4.2.4 Objectives

PPA-STD is applicable when a Standard PP is evaluated. It may be used to verify that a Standard PP conforms with the requirements of ISO/IEC 15408-1.

7.4.2.5 Security assurance components

PPA_STD provides assurance by evaluation of a standard Protection Profile, as specified in ISO/IEC 15408-1.

Table 16 — PPA-STD

Assurance Class	Assurance components
APE: Protection Profile Evaluation	APE_INT.1 PP Introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.2 Security objectives
	APE_ECD.1 Extended component definition
	APE_REQ.2 Security requirements

8 Security Target Assurance (STA)**8.1 Family Name**

The name of this family of packages is *Security Target Assurance (STA)*.

8.2 STA family overview

The Security Target Assurance (STA) family provides two assurance packages for ST evaluation.

a) Assurance package for evaluating direct rationale STs

b) Assurance package for evaluating standard STs

These assurance packages provide the components that are used in the evaluation of each type of Security Target described in ISO/IEC 15408-1.

Table 17 represents a summary of the STA packages. The columns represent the set of STAs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

These STAs consist of an appropriate combination of assurance components as described in Clause 9 of part 3 of ISO/IEC 15408:20XX. More precisely, each STA includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

723

Table 17 — STA summary

Assurance class	Assurance family	Assurance Components by Security Target Assurance Package	
		Direct Rationale ST (STA-DR)	Standard ST (STA-STD)
Security Target Evaluation	ASE_INT	1	1
	ASE_CCL	1	1
	ASE_SPD	1	2
	ASE_OBJ	1	2
	ASE_ECD	1	1
	ASE_REQ	1	2
	ASE_TSS	1	2

724

8.3 STA family objectives

726 The STA objectives are to support the provision of assurance through evaluation that a protection
 727 profile conforms with the requirements given in ISO/IEC 15408.

8.4 STA Packages**8.4.1 Direct Rationale ST (STA-DR)****8.4.1.1 Package name**

731 The name of the package is *Security Target Assurance Package - Direct Rationale (STA-DR)*.

8.4.1.2 Package type

733 This package is an *assurance package*.

8.4.1.3 Package overview

735 STA_DR provides assurance by evaluation of a Direct Rationale Security Target, using the criteria
 736 specified in ISO/IEC 15408-3.

8.4.1.4 Objectives

738 STA-DR is applicable when a Direct Rationale ST is evaluated. It may be used to verify that a Direct
 739 Rationale ST conforms with the requirements of ISO/IEC 15408-1

8.4.1.5 Security assurance components

741 The security assurance components given in Table 18 are included in the package.

742

Table 18 — STA-DR

Assurance Class	Assurance components
ASE: Security Target Evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition

	ASE_OBJ.1 Security objectives for the operational environment
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements
	ASE-TSS.2 TOE Summary specification

743 8.4.2 Security Target Assurance Package - Standard (STA-STD)

744 8.4.2.1 Package name

745 The name of the package is *Security Target Assurance Package – Standard ST (STA-STD)*.

746 8.4.2.2 Package type

747 This package is an *assurance package*.

748 8.4.2.3 Package overview

749 STA_STD provides assurance by evaluation of a standard Security Target, using the criteria
750 specified in ISO/IEC 15408-3.

751 8.4.2.4 Objectives

752 STA-STD is applicable when a Standard Security Target is evaluated. It may be used to verify that a
753 Standard Security Target conforms with the requirements of ISO/IEC 15408-1.

754 8.4.2.5 Security assurance components

755 STA_STD provides assurance by evaluation of a standard Security Target, as specified in ISO/IEC
756 15408-1. The security assurance components given in Table 19 are included in the package.

757

758 **Table 19 — STA-STD**

Assurance Class	Assurance components
ASE: Security Target Evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.2 Stated security requirements
	ASE-TSS.2 TOE Summary specification

759

Annex A (informative)

Composition (ACO)

Editor Note:

The Editor believes that this Annex be moved into part 1 or part 3 as an informative annex since it contains the concepts and general information in support of the ACO composition technique.

If no comments are received on this topic, the editor's proposal will be accepted and presented in the next draft.

The goal of this annex is to explain the concepts behind composition evaluations and the ACO criteria. This annex does not define the ASE criteria; this definition can be found in clause 9 of ISO/IEC 15408-3:20XX.

A.1 Necessity for composed TOE evaluations

The IT market is, on the whole, made up of vendors offering a particular type of product/technology. Although there is some overlap, where a PC hardware vendor may also offer application software and/or operating systems or a chip manufacturer may also develop a dedicated operating system for their own chipset, it is often the case that an IT solution is implemented by a variety of vendors.

There is sometimes a need for assurance in the combination (composition) of components in addition to the assurance of the individual components. Although there is cooperation between these vendors, in the dissemination of certain material required for the technical integration of the components, the agreements rarely stretch to the extent of providing detailed design information and development process/procedure evidence. This lack of information from the developer of a component on which another component relies means that the dependent component developer does not have access to the type of information necessary to perform an evaluation of both the dependent and base components at EAL2 or above. Therefore, while an evaluation of the dependent component can still be performed at any assurance level, to compose components with assurance at EAL2 or above it is necessary to reuse the evaluation evidence and results of evaluations performed for the component developer.

It is intended that the ACO criteria are applicable in the situation where one IT entity is dependent on another for the provision of security services. The entity providing the services is termed the "base component", and that receiving the services is termed the "dependent component". This relationship may exist in a number of contexts. For example, an application (dependent component) may use services provided by an operating system (base component). Alternatively, the relationship may be peer-to-peer, in the sense of two linked applications, either running in a common operating system environment, or on separate hardware platforms. If there is a dominant peer providing the services to the minor peer, the dominant peer is considered to be the base component and the minor peer the dependent component. If the peers provide services to each other in a mutual manner, each peer will be considered to be the base component for the services offered and dependent component for the services required. This will require iterations of the ACO components applying all requirements to each type of component peer.

The criteria are also intended to be more broadly applicable, stepwise (where a composed TOE comprised of a dependent component and a base component itself becomes the base component of another composed TOE), in more complex relationships, but this may require further interpretation.

It is still required for composed TOE evaluations that the individual components are evaluated independently, as the composition evaluation builds on the results of the individual component evaluations. The evaluation of the dependent component may still be in progress when the composed TOE evaluation commences. However, the dependent component evaluation must complete before the composed TOE evaluation completes.

The composed evaluation activities may take place at the same time as the dependent component evaluation. This is due to two factors:

a) Economic/business drivers - the dependent component developer will either be sponsoring the composition evaluation activities or supporting these activities as the evaluation deliverables from the dependent component evaluation are required for composed evaluation activities.

b) Technical drivers - the components consider whether the requisite assurance is provided by the base component (e.g. considering the changes to the base component since completion of the component evaluation) with the understanding that the dependent component has recently undergone (is undergoing) component evaluation and all evaluation deliverables associated with the evaluation are available. Therefore, there are no activities during composition requesting the dependent component evaluation activities to be re-verified. Also, it is verified that the base component forms (one of) the test configurations for the testing of the dependent component during the dependent component evaluation, leaving ACO_CTT to consider the base component in this configuration.

The evaluation evidence from the evaluation of the dependent component is required input into the composed TOE evaluation activities. The only evaluation material from the evaluation of the base component that is required as input into the composed TOE evaluation activities:

a) Residual vulnerabilities in the base component, as reported during the base component evaluation. This is required for the ACO_VUL activities.

No other evaluation evidence from the base component activities should be required for the composed TOE evaluation, as the evaluation results from the component evaluation of the base component should be reused. Additional information about the base component may be required if the composed TOE TSF includes more of the base component than was considered to be TSF during component evaluation of the base component.

The component evaluation of the base and dependent components are assumed to be complete by the time final verdicts are assigned for the ACO components.

The ACO_VUL components only consider resistance against an attacker with an attack potential up to Enhanced-Basic. This is due to the level of design information that can be provided of how the base component provides the services on which the dependent component relies through application of the ACO_DEV activities. Therefore, the confidence arising from composed TOE evaluations using CAPs is limited to a level similar to that obtained from EAL4 component TOE evaluations. Although assurance in the components that comprise the composed TOE may be higher than EAL4.

A.2 Performing Security Target evaluation for a composed TOE

An ST will be submitted by the developer for the evaluation of the composed (base component + dependent component) TOE. This ST will identify the assurance package to be applied to the composed TOE, providing assurance in the composed entity by drawing upon the assurance gained in the component evaluations.

847 The purpose of considering the composition of components within an ST is to validate the
 848 compatibility of the components from the point of view of both the environment and the
 849 requirements, and also to assess that the composed TOE ST is consistent with the component STs
 850 and the security policies expressed within them. This includes determining that the component STs
 851 and the security policies expressed within them are compatible.

852 The composed TOE ST may refer out to the content of the component STs, or the ST author may
 853 chose to reiterate the material of the component STs within the composed TOE ST providing a
 854 rationale of how the component STs are represented in the composed TOE ST.

855 During the conduct of the ASE_CCL evaluation activities for a composed TOE ST the evaluator
 856 determines that the component STs are accurately represented in the composed TOE ST. This is
 857 achieved through determining that the composed TOE ST demonstrably conforms to the
 858 component TOE STs. Also, the evaluator will need to determine that the dependencies of the
 859 dependent component on the operational environment are adequately fulfilled in the composed
 860 TOE.

861 The composed TOE description will describe the composed solution. The logical and physical scope
 862 and boundary of the composed solution will be described, and the logical boundary(ies) between
 863 the components will also be identified. The description will identify the security functionality to be
 864 provided by each component.

865 The statement of SFRs for the composed TOE will identify which component is to satisfy an SFR. If
 866 an SFR is met by both components, then the statement will identify which component meets the
 867 different aspects of the SFR. Similarly, the composed TOE Summary Specification will identify
 868 which component provides the security functionality described.

869 The package of ASE: Security Target evaluation requirements applied to the composed TOE ST
 870 should be consistent with the package of ASE: Security Target evaluation requirements used in the
 871 component evaluations.

872 Reuse of evaluation results from the evaluation of component STs can be made in the instances that
 873 the composed TOE ST directly refers to the component STs. e.g. if the composed TOE ST refers to a
 874 component ST for part of its statement of SFRs, the evaluator can understand that the requirement
 875 for the completion of all assignment and selection operations (as stated in ASE_REQ.*.3C has been
 876 satisfied in the component evaluations.

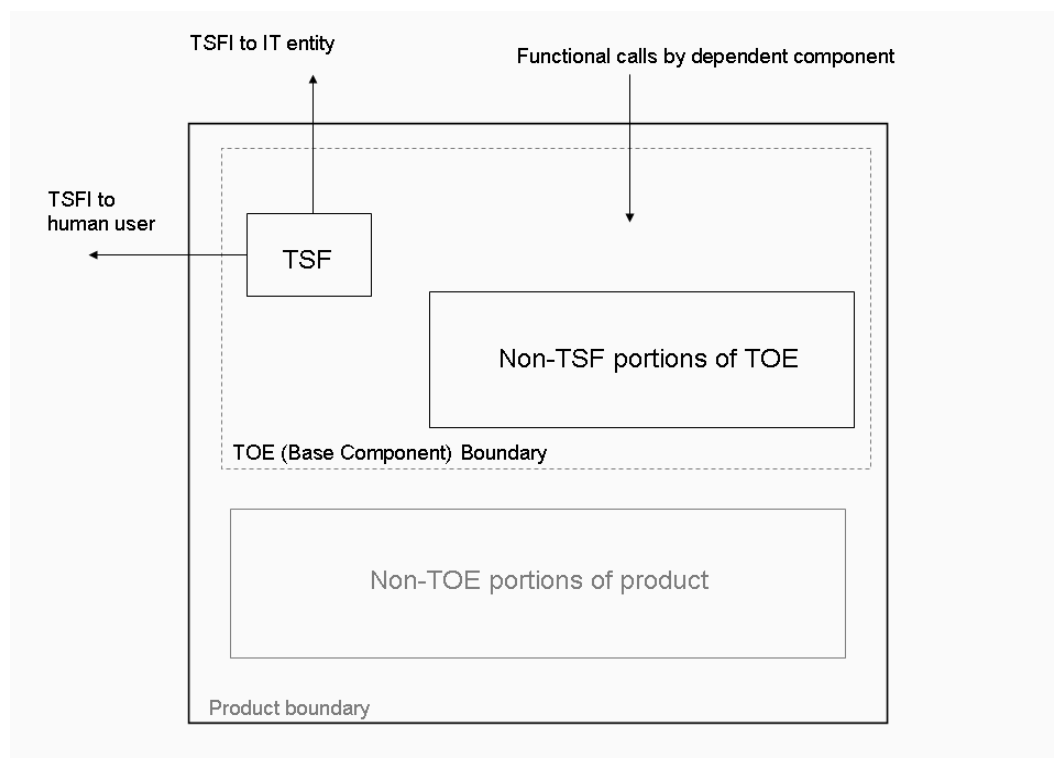
877 **A.3 Interactions between composed IT entities**

878 The TSF of the base component is often defined without knowledge of the dependencies of the
 879 possible applications with which it may be composed. The TSF of this base component is defined
 880 to include all parts of the base component that have to be relied upon for enforcement of the base
 881 component SFRs. This will include all parts of the base component required to implement the base
 882 component SFRs.

883 The TSFI of this base component represents the interfaces provided by the TSF to the external
 884 entities defined in the statement of SFRs to invoke a service of the TSF. This includes interfaces to
 885 the human user and also interfaces to external IT entities. However, the TSFI only includes those
 886 interfaces to the TSF, and therefore is not necessarily an exhaustive interface specification of all
 887 possible interfaces available between an external entity and the base component. The base
 888 component may present interfaces to services that were not considered security-relevant, either
 889 because of the inherent purpose of the service (e.g., adjust type font) or because associated ISO/IEC
 890 15408 SFRs are not being claimed in the base component's ST (e.g. the login interface when no
 891 ISO/IEC 15408-2 FIA: Identification and authentication SFRs are claimed).

892 The functional interfaces provided by the base component are in addition to the security interfaces
 893 (TSFIs), and are not required to be considered during the base component evaluation. These often

894 include interfaces that are used by a dependent component to invoke a service provided by the
 895 base component. The base component may include some indirect interfaces through which TSFIs
 896 may be called, e.g. APIs that can be used to invoke a service of the TSF, which were not considered
 897 during the evaluation of the base component.



898
 899 **Figure A.1 — Base component abstraction**

900 The dependent component, which relies on the base component, is similarly defined: interfaces to
 901 external entities defined in the SFRs of the component ST are categorized as TSFI and are examined
 902 in ADV_FSP.

903 Any call out from the dependent TSF to the environment in support of an SFR will indicate that the
 904 dependent TSF requires some service from the environment in order to satisfy the enforcement of
 905 the stated dependent component SFRs. Such a service is outside the dependent component
 906 boundary and the base component is unlikely to be defined in the dependent ST as an external
 907 entity. Hence, the calls for services made out by the dependent TSF to its underlying platform (the
 908 base component) will not be analysed as part of the Functional specification (ADV_FSP) activities.
 909 These dependencies on the base component are expressed in the dependent component ST as
 910 security objectives for the environment.

911 This abstraction of the dependent component and the interfaces is shown in Figure A.2 below.

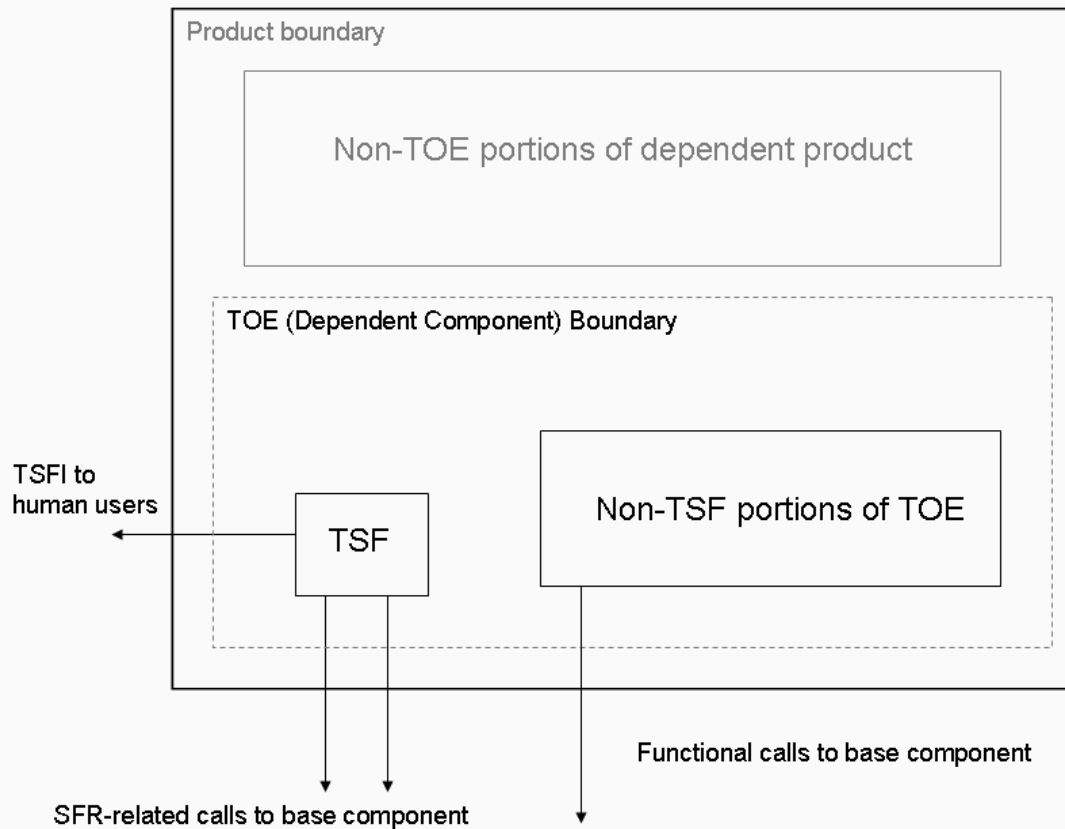


Figure A. 2 — Dependent component abstraction

When considering the composition of the base component and the dependent component, if the dependent component's TSF requires services from the base component to support the implementation of the SFR, the interface to the service will need to be defined. If that service is provided by the base component's TSF, then that interface should be a TSFI of the base component and will therefore already be defined within the functional specification of the base component.

If, however, the service called by the dependent component's TSF is not provided by the TSF of the base component (i.e., it is implemented in the non-TSF portion of the base component or possibly even in the non-TOE portion of the base component (not illustrated in Figure B.3), there is unlikely to be a TSFI of the base component relating to the service, unless the service is mediated by the TSF of the base component. The interfaces to these services from the dependent component to the operational environment are considered in the family Reliance of dependent component (ACO_REL).

The non-TSF portion of the base component is drawn into the TSF of the composed TOE due to the dependencies the dependent component has on the base component to support the SFRs of the dependent component. Therefore, in such cases, the TSF of the composed TOE would be larger than simply the sum of the components' TSFs.

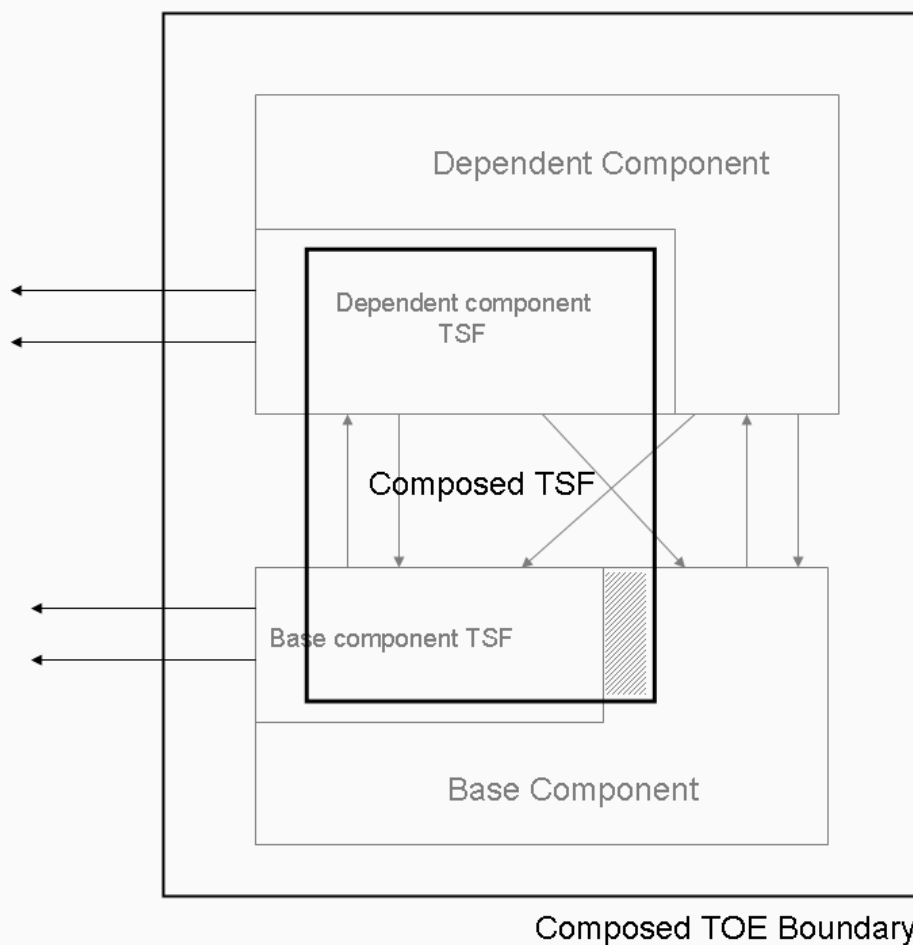


Figure A.3 — Composed TOE abstraction

It may be the case that the base component TSFI is being called in a manner that was unforeseen in the base component evaluation. Hence there would be a requirement for further testing of the base component TSFI.

The possible interfaces are further described in the following diagram, Figure A.4, and supporting text.

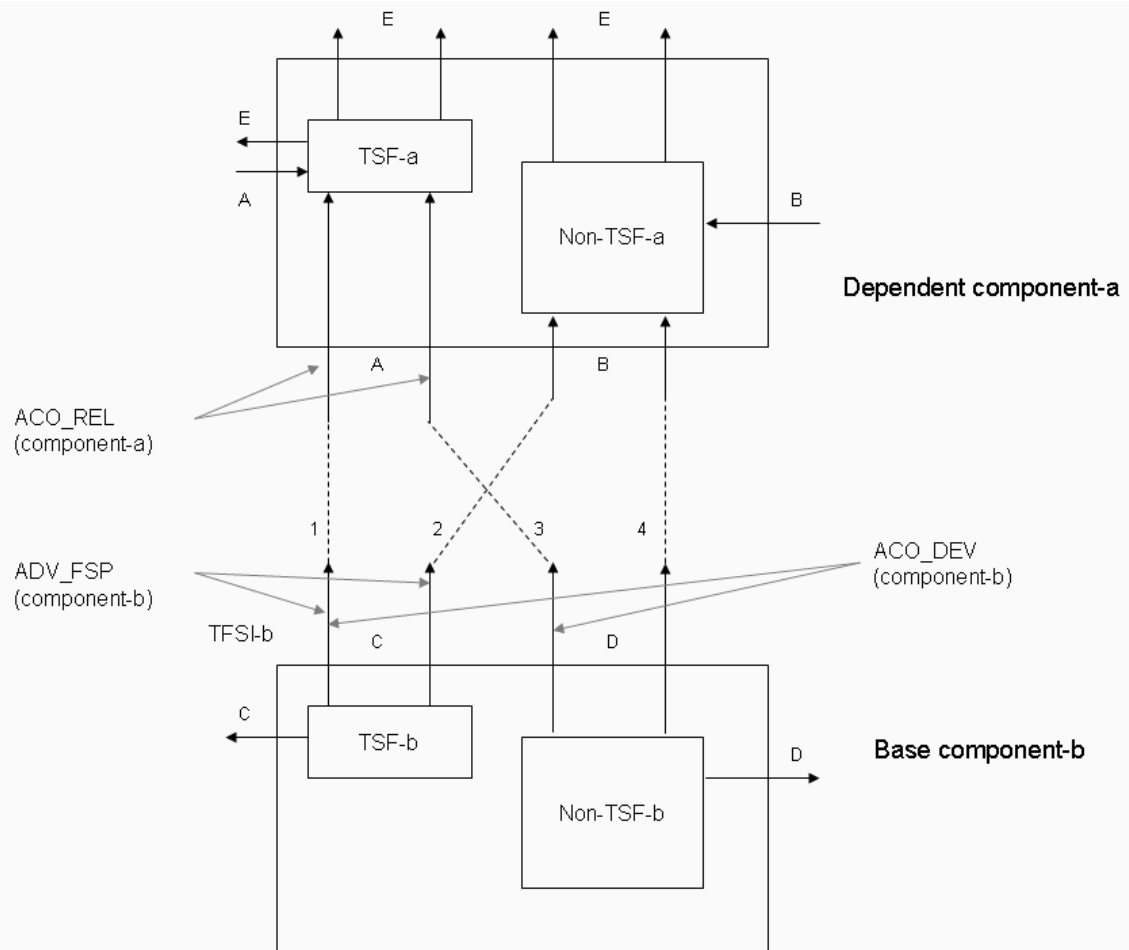


Figure A. 4 — Composed component interfaces

a) Arrows going into 'dependent component-a' (A and B) = where the component expects the environment to respond to a service request (responding to calls out from dependent component to the environment);

b) Arrows coming out of 'base component-b' (C and D) = interfaces of services provided by the base component to the environment;

c) Broken lines between components = types of communication between pairs of interfaces;

d) The other (grey) arrows = interfaces that are described by the given criteria.

The following is a simplification, but explains the considerations that need to be made.

There are components a ('dependent component-a') and b ('base component-b'): the arrows coming out of TSF-a are services provided by TSF-a and are therefore TSFIs(a); likewise, the arrows coming out of TSF-b ("C") are TSFIs(b). These are each detailed in their respective functional specs. component-a is such that it requires services from its environment: those needed by the TSF(a) are labelled "A"; the other (not related to TSF-a) services are labelled "B".

When component-a and component-b are combined, there are four possible combinations of {services needed by component-a} and {services provided by component-b}, shown as broken lines (types of communication between pairs of interfaces). Any set of these might exist for a particular composition:

- 956 a) TSF-a needs those services that are provided by TSF-b ("A" is connected to "C"): this is
 957 straightforward: the details about "C" are in the FSP for component-b. In this instance, the
 958 interfaces should all be defined in the functional specifications for the component-b.
- 959 b) Non-TSF-a needs those services that are provided by TSF-b ("B" is connected to "C"): this is
 960 straightforward (again, the details about "C" are in the FSP for component-b), but unimportant:
 961 security wise.
- 962 c) Non-TSF-a needs those services that are provided by non-TSF-b ("B" is connected to "D"): we
 963 have no details about D, but there are no security implications about the use of these interfaces, so
 964 they do not need to be considered in the evaluation, although they are likely to be an integration
 965 issue for the developer.
- 966 d) TSF-a needs those services that are provided by non-TSF-b ("A" is connected to "D"): this would
 967 arise when component-a and component-b have different senses of what a "security service" is.
 968 Perhaps component-b is making no claims about I&A (has no FIA SFRs in its ST), but component-a
 969 needs authentication provided by its environment. There are no details about the "D" interfaces
 970 available (they are not TSFI (b), so they are not in component-b's FSP).
- 971 Note: if the kind of interaction described in case d above exists, then the TSF of the composed TOE
 972 would be TSF-a + TSF-b + Non-TSF-b. Otherwise, the TSF of the composed TOE would be TSF-a +
 973 TSF-b.
- 974 Interfaces types 2 and 4 of Figure B.4 are not directly relevant to the evaluation of the composed
 975 TOE. Interfaces 1 and 3 will be considered during the application of different families:
- 976 a) Functional specification (ADV_FSP) (for component-b) will describe the C interfaces.
- 977 b) Reliance of dependent component (ACO_REL) will describe the A interfaces.
- 978 c) Development evidence (ACO_DEV) will describe the C interfaces for connection type 1 and the D
 979 interfaces for connection type 3.
- 980 A typical example where composition may be applied is a database management system (DBMS)
 981 that relies upon its underlying operating system (OS). During the evaluation of the DBMS
 982 component, there will be an assessment made of the security properties of that DBMS (to whatever
 983 degree of rigour is dictated by the assurance components used in the evaluation): its TSF boundary
 984 will be identified, its functional specification will be assessed to determine whether it describes the
 985 interfaces to the security services provided by the TSF, perhaps additional information about the
 986 TSF (its design, architecture, internal structure) will be provided, the TSF will be tested, aspects of
 987 its life-cycle and its guidance documentation will be assessed, etc.
- 988 However, the DBMS evaluation will not call for any evidence concerning the dependency the DBMS
 989 has on the OS. The ST of the DBMS will most likely state assumptions about the OS in its
 990 Assumptions subclause and state security objectives for the OS in its Environment subclause. The
 991 DBMS ST may even instantiate those objectives for the environment in terms of SFRs for the OS.
 992 However, there will be no specification for the OS that mirrors the detail in the functional
 993 specification, architecture description, or other ADV evidence as for the DBMS. Reliance of
 994 dependent component (ACO_REL) will fulfil that need.
- 995 Reliance of dependent component (ACO_REL) describes the interfaces of the dependent TOE that
 996 make the calls to the base component for the provision of services. These are the interfaces to which
 997 the base component is to respond. The interface descriptions are provided from the dependent
 998 component's viewpoint.

999 Development evidence (ACO_DEV) describes the interfaces provided by the base component, which
1000 respond to the dependent component service requests. These interfaces are mapped to the relevant
1001 dependent component interfaces that are identified in the reliance information. (The completeness
1002 of this mapping, whether the base component interfaces described represent all dependent
1003 component interfaces, is not verified here, but in Composition rationale (ACO_COR)). At the higher
1004 levels of ACO_DEV the subsystems providing the interfaces are described.

1005 Any interfaces required by the dependent component that have not been described for the base
1006 component are reported in the rationale for Composition rationale (ACO_COR). The rationale also
1007 reports whether the interfaces of the base component on which the dependent component relies
1008 were considered within the base component evaluation. For any interfaces that were not
1009 considered in the base component evaluation, a rationale is provided of the impact of using the
1010 interface on the base component TSF.