NTNU

CC part 3 - Example: EAL3

Objectives:

- **to gain maximum assurance from positive security engineering at the design stage**

- **to obtain a moderate level of independently assured security**

- **a thorough investigation of the TOE and it's development without substantial reengineering**

NTNU

Example - EAL3

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

NTNU

Example - EAL3

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
- a vulnerability analysis

NTNU

Example - EAL3

Further assurance is provided through:

- the use of development environment controls
- TOE configuration management
- evidence of secure delivery procedures.

NTNU

Rationale - EAL 3

EAL3 represents a meaningful increase in assurance from **EAL2** by requiring **more complete testing coverage** of the **security functionality, mechanisms** and/or **procedures** that provide some **confidence** that the **TOE** will not **be tampered with** during development

NTNU

EALs, Ver. 3.1

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_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**	**2**	**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

NTNU

ADV_ARC.1 Security architecture description

Dependencies:

- **ADV_FSP.1 Basic functional specification**
- **ADV_TDS.1 Basic design**

Developers action elements ADV_ARC.1.n.D

The developer shall:

- **design and implement the TOE so that the security features of the TSF cannot be bypassed**
- **design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities**
- **provide a security architecture description of the TSF**

NTNU

ADV_ARC.1 Security architecture description

Content and presentation elements ADV_ARC.1.n.C

The security architecture description shall:

- **be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.**
- **describe the security domains maintained by the TSF consistently with the SFRs.**
- **describe how the TSF initialisation process is secure.**
- **demonstrate that the TSF protects itself from tampering.**
- **demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.**

NTNU

ADV_ARC.1 Security architecture description

Evaluator action elements ADV_ARC.1.nE:

The evaluator *shall:*

- ***confirm*** **that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ADV_FSP.3 Functional specification with complete summary

Dependencies:

- **ADV_TDS.1 Basic design**

Developers action elements –

The developer shall:

- **provide a funtional specification**
- **provide a tracing from the functional specification to the SFRs**

NTNU

ADV_FSP.3 Functional specification with complete summary

Content and presentation elements -

The functional specification shall:

- **completely represent the TSF.**
- **describe the purpose and method of use for all TSFI.**
- **identify and describe all parameters associated with each TSFI.**
- **describe the SFR-enforcing actions associated with the TSFI.**
- **describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.**
- **summarise the non-SFR-enforcing actions associated with each TSFI.**
- **demonstrate that the SFRs trace to TSFIs in the functional specification.**

NTNU

ADV_FSP.3 Functional specification with complete summary

Evaluator action elements:

The evaluator *shall*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**
- ***determine* that the functional specification is an accurate and complete instantiation of the SFRs.**

NTNU

ADV_TDS.2 Architectural design

Dependencies:

- **ADV_FSP.3 Functional specification with complete summary**

Developers action elements; The developer shall:

- **Provide the design of the TOE**
- **Provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design**

NTNU

ADV_TDS.2 Architectural design

Content and presentation elements:

The design shall:

- **describe the structure of the TOE in terms of subsystems.**
- **identify all subsystems of the TSF.**
- **describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.**
- **describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.**
- **summarise the non-SFR-enforcing behaviour of the SFR-enforcing subsystems.**
- **summarise the behaviour of the SFR-supporting subsystems.**
- **provide a description of the interactions among all subsystems of the TSF.**
- **demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.**

NTNU

ADV_TDS.2 Architectural design

Evaluator action elements:

The evaluator *shall*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**
- ***determine* that the design is an accurate and complete instantiation of all security functional requirements.**

NTNU

AGD_OPE.1 Operational user guidance

Dependencies:

- **ADV_FSP.1 Basic functional specification**

Developers action elements; The developer shall provide:

- **operational user guidance**

NTNU

AGD_OPE.1 Operational user guidance

Content and presentation elements (1 of 2):

The operational user guidance shall

- **describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.**
- **describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.**
- **describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.**
- **for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.**

NTNU

AGD_OPE.1 Operational user guidance

Content and presentation elements (2 of 2):

- **identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.**
- **for each user role, describe the security measures to be followed in order to fullfil the security objectives for the operational environment as described in the ST.**
- **be clear and reasonable.**

NTNU

AGD_OPE.1 Operational user guidance

The evaluator *shall*

- ***confirm*** **that the information provided meets all requirements for content and presentation of evidence.**

NTNU

AGD_PRE.1 Preparative procedures

Dependencies: None

Developers action elements; The developer shall:

- **provide the TOE including its preparative procedures**

NTNU

AGD_PRE.1 Preparative procedures

Content and presentation elements -

The preparative procedures shall:

- **describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.**
- **describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.**

NTNU

AGD_PRE.1 Preparative procedures

Evaluator action elements -

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**
- **apply the preparative procedures to confirm that the TOE can be prepared securely for operation.**

NTNU

ALC_CMC.3 Authorization controls

Dependencies:

- **ALC_CMS.1 TOE CM coverage**
- **ALC_DVS.1 Identification of security measures**

Developers action elements; The developer shall:

- **provide the TOE and a reference for the TOE**
- **provide CM documentation**
- **use a CM system**

NTNU

ALC_CMC.3 Authorization controls

Content and presentation elements:

- **The TOE shall be labeled with its unique reference.**
- **The CM documentation shall describe the method used to uniquely identify the configuration items.**
- **The CM system shall uniquely identify all configuration items.**
- **The CM system shall provide measures such that only authorised changes are made to the configuration items.**
- **The CM documentation shall include a CM plan.**
- **The CM plan shall describe how the CM system is used for the development of the TOE.**
- **The evidence shall demonstrate that all configuration items are being maintained under the CM system.**
- **The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.**

NTNU

ALC_CMC.3 Authorization controls

Evaluator action elements:

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ALC_CMS.3 Implementation representation CM Coverage

Dependencies: None

Developers action elements;
The developer shall:

- **provide a configuration list for the TOE**

ALC_CMS.3 Implementation representation CM Coverage

Content and presentation elements:

- **The configuration list shall include:**
  - **the TOE itself**
  - **the evaluation evidence required by the SARs**
  - **the parts that comprise the TOE**
  - **the implementation representation.**
- **The configuration list shall uniquely identify the configuration items.**
- **For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.**

NTNU

ALC_CMS.3 Implementation representation CM Coverage

Evaluator action elements -

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ALC_DEL.1 Delivery procedures

Dependencies: None

Developers action elements -
The developer shall:

- **document procedures for delivery of the TOE or parts of it to the consumer**
- **use the delivery procedures**

NTNU

ALC_DEL.1 Delivery procedures

Content and presentation elements -

The delivery documentation shall:

- **describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.**

NTNU

ALC_DEL.1 Delivery procedures

Evaluator action elements -

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence**

NTNU

ALC_DVS.1 Identification of security measures

Dependencies: None

Developers action elements -
The developer shall:

- **produce development security documentation**

NTNU

ALC_DVS.1 Identification of security measures

Content and presentation elements -

The development security documentation shall:

- **describe all 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.**

NTNU

ALC_DVS.1 Identification of security measures

Evaluator action elements -

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**
- ***confirm* that the security measures are being applied.**

NTNU

ALC_LCD.1 Developer defined life-cycle model

Dependencies: None

Developers action elements - The developer shall:

- **establish a life-cycle model to be used in the development and maintenance of the TOE**
- **provide life-cycle definition documentation**

NTNU

ALC_LCD.1 Developer defined life-cycle model

Content and presentation elements:

The life-cycle definition documentation shall:

- **describe the model used to develop and maintain the TOE.**
- **provide for the necessary control over the development and maintenance of the TOE.**

NTNU

ALC_LCD.1 Developer defined life-cycle model

Evaluator action elements -

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ASE_CCL.1 Conformance claims

Dependencies:

- **ASE_INT.1 ST introduction**
- **ASE_ECD.1 Extended components definition**
- **ASE_REQ.1 Stated security requirements**

Developers action elements –
The developer shall provide:

- **a conformance claim**
- **a conformance claim rationale**

NTNU

ASE_CCL.1 Conformance claims

Content and presentation elements (1 of 2):

The conformance claim shall:

- **contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.**
- **describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.**
- **describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.**
- **be consistent with the extended components definition.**
- **identify all PPs and security requirement packages to which the ST claims conformance.**

NTNU

ASE_CCL.1 Conformance claims

Content and presentation elements (2 of 2):

- **describe any conformance of the ST to a package as either package-conformant or package-augmented.**
- **demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.**
- **demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.**
- **demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.**
- **demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.**

NTNU

ASE_CCL.1 Conformance claims

Evaluator action elements:

The evaluator *shall :*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ASE_ECD.1 Extended component definition

Dependencies: None

Developers action elements -
The developer shall provide:

- **a statement of security requirements**
- **an extended components definition**

NTNU

ASE_ECD.1 Extended component definition

Content and presentation elements:

The statement of security requirements shall

- **identify all extended security requirements.**
- **define an extended component for each extended security requirement.**
- **describe how each extended component is related to the existing CC components, families, and classes.**
- **use the existing CC components, families, classes, and methodology as a model for presentation.**
- **consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.**

NTNU

ASE_ECD.1 Extended component definition

Evaluator action elements:

The evaluator *shall*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**
- ***confirm* that no extended component can be clearly expressed using existing components.**

NTNU

ASE_INT.1 ST introduction

Dependencies: None

Developers action elements:

- **The developer shall provide an ST introduction**

NTNU

ASE_INT.1 ST introduction

Content and presentation elements:

The ST introduction shall

- **contain an ST reference, a TOE reference, a TOE overview and a TOE description.**
- **uniquely identify the ST.**
- **identify the TOE.**
- **summarise the usage and major security features of the TOE.**
- **identify the TOE type.**
- **identify any non-TOE hardware/software/firmware required by the TOE.**
- **describe the physical scope of the TOE.**
- **describe the logical scope of the TOE.**

NTNU

ASE_INT.1 ST introduction

Evaluator action elements

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**
- ***confirm* that the TOE reference, the TOE overview, and the TOE description are consistent with each other.**

ASE_OBJ.2 Security objectives

Dependencies:

- **ASE_SPD.1 Security problem definition**

Developers action elements –
The developer shall provide:

- **a statement of security objectives**
- **a security objectives rationale**

NTNU

ASE_OBJ.2 Security objectives

Content and presentation elements:

The statement of security objectives shall:

- **describe the security objectives for the TOE and the security objectives for the operational environment.**
- **trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.**
- **trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.**
- **demonstrate that the security objectives counter all threats.**
- **demonstrate that the security objectives enforce all OSPs.**
- **demonstrate that the security objectives for the operational environment uphold all assumptions.**

NTNU

ASE_OBJ.2 Security objectives

Evaluator action elements -

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence**

NTNU

ASE_REC.2 Derived security requirements

Dependencies:

- **ASE_OBJ.2 Security objectives**
- **ASE_ECD.1 Extended components definition**

Developers action elements –
The developer shall provide:

- **a statement of security requirements**
- **a security requirements rationale**

NTNU

ASE_REC.2 Derived security requirements

Content and presentation elements (1 of 2):

The statement of security requirements shall:

- describe the SFRs and the SARs.
- define all subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs
- identify all operations on the security requirements.
- assume that all operations are performed correctly.
- assume that each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

NTNU

ASE_REC.2 Derived security requirements

Content and presentation elements (2 of 2):

The security requirements rationale shall:

- **trace each SFR back to the security objectives for the TOE.**
- **demonstrate that the SFRs meet all security objectives for the TOE.**
- **explain why the SARs were chosen.**
- **the statement of security requirements shall be internally consistent.**

NTNU

ASE_REC.2 Derived security requirements

Evaluator action elements

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ASE_SPD.1 Security problem definition

Dependencies: None

Developers action elements:

- **the developer shall provide a security problem definition**

NTNU

ASE_SPD.1 Security problem definition

Content and presentation elements:

The security problem definition shall:

- **describe the threats.**
- **describe all threats in terms of a threat agent, an asset, and an adverse action.**
- **describe the OSPs.**
- **describe the assumptions about the operational environment of the TOE.**

NTNU

ASE_SPD.1 Security problem definition

Evaluator action elements:

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ASE_TSS.1 TOE summary specification

Dependencies:

- **ASE_INT.1 ST introduction**
- **ASE_REQ.1 Stated security requirements**

Developers action elements:

- **The developer shall provide a TOE summary specification**

NTNU

ASE_TSS.1 TOE summary specification

Content and presentation elements:

The TOE summary specification shall:

- **describe how the TOE meets each SFR.**

NTNU

ASE_TSS.1 TOE summary specification

Evaluator action elements:

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**
- ***confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.**

NTNU

ATE_COV.2 Analysis of coverage

Dependencies:

- **ADV_FSP.2 Security enforcing functional specification**
- **ATE_FUN.1 Functional testing**

Developers action elements –
The developer shall provide:

- **an analysis of the test coverage**

NTNU

ATE_COV.2 Analysis of coverage

Content and presentation elements -

The analysis of the test coverage shall:

- **demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.**
- **demonstrate that all TSFIs in the functional specification have been tested.**

NTNU

ATE_COV.2 Analysis of coverage

Evaluator action elements:

The evaluator ***shall***

- ***confirm*** that the information provided meets all requirements for content and presentation of evidence.

NTNU

ATE_DPT.1 Testing: basic design

Dependencies:

- **ADV_ARC.1 Security architecture description**
- **ADV_TDS.2 Architectural design**
- **ATE_FUN.1 Functional testing**

Developers action elements –
The developer shall provide:

- **the analysis of the depth of testing**

NTNU

ATE_DPT.1 Testing: basic design

Content and presentation elements –

The analysis of the depth of testing shall:

- **demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.**
- **demonstrate that all TSF subsystems in the TOE design have been tested.**

NTNU

ATE_DPT.1 Testing: basic design

Evaluator action elements -

The evaluator *shall:*

- ***confirm*** **that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ATE_FUN.1 Functional testing

Dependencies:

- **ATE_COV.1 Evidence of coverage**

Developers action elements –
The developer shall:

- **test the TSF and document the result**
- **provide test documentation**

NTNU

ATE_FUN.1 Functional testing

Content and presentation elements:

The test documentation shall

- **consist of test plans, expected test results and actual test results.**
- **identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.**
- **show the anticipated outputs from a successful execution of the tests.**
- **be consistent with the expected test results**

NTNU

ATE_FUN.1 Functional testing

Evaluator action elements:

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**

NTNU

ATE_IND.2 Independent testing - sample

Dependencies:

- ADV_FSP.2 Security enforcing functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_COV.1 Evidence of coverage
- ATE_FUN.1 Functional testing

Developers action elements; The developer shall:

- provide the TOE for testing

NTNU

ATE_IND.2 Independent testing - sample

Content and presentation elements:

- **The TOE shall be suitable for testing.**
- **The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.**

NTNU

ATE_IND.2 Independent testing - sample

Evaluator action elements –

The evaluator *shall:*

- ***confirm* that the information provided meets all requirements for content and presentation of evidence.**
- ***execute* a sample of tests in the test documentation to verify the developer test results.**
- ***test* a subset of the TSF interfaces to confirm that the TSF operates as specified.**

NTNU

AVA_VAN.2 Vulnerability analysis

Dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.1 Basic functional specification
- ADV_TDS.1 Basic design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures

Developers action elements; The developer shall:

- provide the TOE for testing

NTNU

AVA_VAN.2 Vulnerability analysis

Content and presentation elements:

- **The TOE shall be suitable for testing.**

NTNU

AVA_VAN.2 Vulnerability analysis

Evaluator action elements -

The evaluator *shall:*

- ***confirm*** **that the information provided meets all requirements for content and presentation of evidence.**
- ***perform*** **a search of public domain sources to identify potential vulnerabilities in the TOE.**
- ***perform*** **an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.**
- ***conduct*** **penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.**