



## Common Criteria v3.1 EAL2 Developer Evidence

The Common Criteria (CC) version 3.1 requires that the sponsor and/or developer present the evidence described in this checklist for successful EAL2 Common Criteria evaluation.

The assurance components at evaluation assurance level 2 (EAL2) are:

Assurance Class	Assurance Family	Assurance Components
Secure Target evaluation	ASE	ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_REQ.2 ASE_SPD.1 ASE_TSS.1
Development	ADV	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1
Guidance	AGD	AGD_OPE.1 AGD_PRE.1
Life-cycle support	ALC	ALC_CMC.2 ALC_CMS.2 ALC_DEL.1
Tests	ATE	ATE_COV.1 ATE_FUN.1 ATE_IND.2*
Vulnerability assessment	AVA	AVA_VAN.2*

\* Note that there is no sponsor and/or developer evidence requirement for evaluation of this component.

## 1 Security Target (ASE) Evaluation

Security Target (ST) conformant to Protection Profiles (PPs), if appropriate.

## 2 Development (ADV)

### 2.1 Security Architecture (ADV\_ARC)

Description of the security architecture of the Target of Evaluation (TOE) at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design documents, including:

- describing the security domains maintained by the TSF consistently with the SFRs.
- describing how the TSF initialization process is secure.
- demonstrating that the TSF protects itself from tampering.
- demonstrating that the TSF prevents bypass of the SFR-enforcing functionality.

### 2.2 Functional Specification (ADV\_FSP)

A functional specification (FSP) that includes:

- identification of all TOE Security Functionality Interfaces (TSFIs).
- description of all TSFIs in terms of their purpose, method of use, and parameters.
- for each Security Functional Requirement (SFR)-enforcing TSFI, description of the SFR-enforcing actions associated with the TSFI
- for each SFR-enforcing TSFI, description of direct error messages resulting from processing associated with the SFR-enforcing action.
- mapping of TSFIs to SFRs.

### 2.3 TOE Design (ADV\_TDS)

TOE design documentation that includes:

- description of the structure of the TOE in terms of subsystems.
- identification of TSF subsystems vs. non-TSF subsystems.
- description of behavior of each SFR-supporting and SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.
- high-level description of SFR-enforcing behavior of SFR-enforcing subsystems.
- description of interactions among the TSF subsystems, including among SFR-enforcing subsystems, and between the SFR\_enforcing subsystems and other subsystems of the TOE.
- mapping of TSFIs described in the FSP to the TSF subsystems.

## 3 Guidance (AGD)

### 3.1 Preparative Procedures (AGD\_PRE)

Customer documentation (e.g., user manuals) covering all activities needed to transform the delivered TOE into its evaluated configuration in the environment as described in the ST, including:

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

### 3.2 Operational Procedures (AGD\_OPE)

Customer documentation (e.g., user manuals) covering all activities needed during the operation of the TOE in its evaluated configuration, including for each user role:

- the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
- how to use the available interfaces provided by the TOE in a secure manner.
- available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
- for 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.
- describe the security measures to be followed in order to fulfill the security objectives and the operational environment as described in the ST.

All possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operations.

## 4 Life-cycle Support

### 4.1 Configuration Management (ALC\_CMC and ALC\_CMS)

The following evidence:

- Evidence that the Target of Evaluation (TOE) is labeled with its unique reference.
- Evidence that references to the TOE are consistent.
- Unique identification of the configuration items.
- Description of the method used to uniquely identify different versions of configuration items (this may be presented as a CM plan, but a CM plan, per se, is not required at EAL2).
- Configuration lists identifying items maintained under configuration management, to include at a minimum: the TOE itself, the parts that comprise the TOE, and the evaluation evidence required by the Security Assurance Requirements in the ST.

## 4.2 Delivery (ALC\_DEL)

Documentation of the developer process to:

- deliver the TOE or parts of the TOE to the consumer.
- maintain security when distributing versions of the TOE to the consumer.

## 5 Testing (ATE)

### 5.1 Test Coverage (ATE\_COV)

Evidence of test coverage showing the correspondence between the tests identified in the test documentation and the TSFIs identified in the FSP.

### 5.2 Functional Tests (ATE\_FUN)

Test documentation consisting of:

- test plan – identifies the tests to be performed, describes the scenarios for performing each test including any ordering dependencies on the results of other tests.
- expected test results – describes the expected outputs from successful execution of the tests.
- actual test results – actual results, which are expected to be consistent with the expected test results.