

Common Criteria v3.1 EAL4 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 EAL4 Common Criteria evaluation.

The assurance components at evaluation assurance level 4 (EAL4) 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.4 ADV_IMP.1 ADV_TDS.3
Guidance	AGD	AGD_OPE.1 AGD_PRE.1
Life-cycle support	ALC	ALC_CMC.4 ALC_CMS.4 ALC_DEL.1 ALC_DVS.1 ALC_LCD.1 ALC_TAT.1
Tests	ATE	ATE_COV.2 ATE_DPT.2 ATE_FUN.1 ATE_IND.2*
Vulnerability assessment	AVA	AVA_VAN.3*

* 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 completely represents the TSF including:

- description of the purpose and method of use for all TSFI.
- identification and description of all parameters associated with each TSFI.
- for each Security Functional Requirement (SFR)-enforcing TSFI, description of all actions associated with each TSFI.
- for each SFR-enforcing TSFI, all direct error messages that may result from an invocation of each TSFI.
- summary of SFR-supporting and SFR-non-interfering actions associated with each TSFI.
- mapping of TSFIs to SFRs.

2.3 Implementation Representation (ADV_IMP)

The following evidence:

- The implementation representation for the entire TSF in the form used by the development personnel, to a level of detail such that the TSF can be generated without further design decisions.
- Mapping demonstrating correspondence between the TOE design description and a sample of the implementation representation.

2.4 TOE Design (ADV_TDS)

TOE design documentation that includes:

- description of the structure of the TOE in terms of subsystems.
- description of the TSF in terms of modules.
- identification and description of all TSF subsystems.

- description of interactions among all subsystems of the TSF.
- mapping from the subsystems of the TSF to the modules of the TSF.
- description of each SFR-enforcing module in terms of its purpose and interaction with other modules.
- description of each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.
- description of each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.
- mapping of all behavior described in the TOE design to the TSFIs that invoke it.

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 (ALC)

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.
- A CM plan that describes how the CM system is used for the development of the TOE and the procedures used to accept modified or newly-created configuration items as part of the TOE.
- Description of the method used to uniquely identify different versions of configuration items.
- Evidence that the CM system provides automated measures to allow only authorized changes to the configuration items.
- Evidence that the CM system supports production of the TOE by automated means.
- Evidence that demonstrates that all configuration items are being maintained under the CM system and that the CM system is being operated in accordance with the CM plan.
- Configuration lists identifying items maintained under configuration management, to include at a minimum: the TOE itself, the parts that comprise the TOE, the evaluation evidence required by the Security Assurance Requirements (SARs) in the ST, and the implementation representation.

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.

4.3 Development Security (ALC_DVS)

Development security documentation that describes 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.

4.4 Life-cycle Definition (ALC_LCD)

Life-cycle definition documentation that describes the model used to develop and maintain the TOE.

4.5 Tools and Techniques (ALC_TAT)

Documentation of development tools including:

- definition of each development tool used for implementation.
- documentation of each development tool that defines the meaning of all statements, conventions, and directives used in the implementation and unambiguously define the meaning of all implementation-dependent options.

5 Testing (ATE)

5.1 Test Coverage (ATE_COV)

Analysis of test coverage including demonstration of correspondence between tests identified in the test documentation and the TSFIs identified in the FSP showing that all TSFIs in the FSP have been tested.

5.2 Testing Depth (ATE_DPT)

Analysis of testing depth including demonstration of correspondence of tests identified in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design showing that:

- all TSF subsystems in the TOE design have been tested.
- the SFR-enforcing modules in the TOE design have been tested.

5.3 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.