

**Preliminary Assessment Report**

**January 2024**

**Version 0.1**

|  |  |
| --- | --- |
| TOE Name |  |
| PP/cPP/EAL |  |
| Flaw Remediation Level (ALC\_FLR) |  |
| Lead Evaluator |  |
| Developer Point-of-Contact |  |
| Version No. of the Preliminary Assessment Report |  |

Notes for the following tables:

* The preliminary assessment shall be performed by the CCTL’s lead evaluator as part of the deliverables for the application package.
* The developer shall acknowledge the result of this Preliminary Assessment Report by signing off the report.

|  |  |
| --- | --- |
| **Application summary** | **Comment** |
| **Lead Evaluator’s comments** |  |
| **Lead Evaluator’s Signature/Date** |  |
| **Developer’s comments** |  |
| **Developer’s Signature/Date** |  |

|  |
| --- |
| **TOE Overview** |
| Include the TOE description such as TOE name, usage of TOE, TOE type, TOE model/family series (with explanation on the differences between the models/family series), all components of TOE etc. |
|  |
| **Non-TOE** |
| Include the complete and detailed identification of the non-TOE hardware/software/firmware such as model, version, requirements etc. |
|  |
| **TOE Operational Environment** |
| Description of TOE Operational Environment include Diagram if any. |
|  |
| **TOE Security Features** |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N** | **Item/Section** | **Assessment Pass/Fail** | **Justification** |
| 1 | CAF provided, duly completed and meets all mandatory requirements of the CAF. |  |  |
| **2.1 Conformance Claims** | | | |
| 2.1.1 | ST and TOE are compliant with a valid CC version.  CCV3.1R5 version is the last from the 3.1 series, and may optionally be used for evaluation starting no later than the 30th of June 2024. |  |  |
| **2.2 TOE Overview** | | | |
| 2.2.1 | Evaluator shall examine the TOE security functions to determine that it contains all the expected security functions of its TOE type.  For example, a data diode TOE shall provide information flow control . |  |  |
| 2.2.2 | Evaluator shall examine the TOE operational environment to determine that it is consistent with the TOE type.  For example, it may not be reasonable for an encrypted portable storage solution to be assumed for use in a physically secure environment. |  |  |
| 2.2.3 | Evaluator shall examine the TOE Overview to determine the accuracy of the TOE’s Physical Scope and all non-TOE hardware/software/firmware required by the TOE are identified. |  |  |
| **2.3 Security Problem Definition (applicable for Security Target evaluation only)** | | | |
| 2.3.1 | Evaluator shall examine the defined assets within the ST to determine that assets are clearly defined and not misleading to reader. (if applicable) |  |  |
| 2.3.2 | Evaluator shall examine the sufficiency of the assets for the TOE type and TOE operational environment. (if applicable) |  |  |
| 2.3.3 | Evaluator shall examine the defined threats to determine that it is clear and not misleading to reader. (if applicable) |  |  |
| 2.3.4 | Evaluator shall examine the sufficiency of the threats for the TOE type and TOE operational environment and that all threats are sufficiently addressed by countermeasures. (if applicable) |  |  |
| 2.3.5 | Evaluator shall examine all assumptions to determine that it is clear and not misleading to reader. (if applicable) |  |  |
| 2.3.6 | Evaluator shall examine the reasonableness of the assumption for the TOE operational environment. (if applicable) |  |  |
| **2.4 Security Functional Requirement (SFR) coverage** | | | |
| 2.4.1 | Evaluator shall examine the TOE summary specification to determine the sufficiency of the SFR. |  |  |
| **3 Security Requirements** | | | |
| 3.1 | Evaluator shall examine the Cryptography Algorithm(s) and Network Protocol(s) used.  All Cryptography Algorithm(s) and Network Protocol(s) are implemented based on best practices. |  |  |
| 3.2 | Evaluator shall identify publicly known vulnerabilities related to TOE (e.g., CVEs, NVDs data bases).  Evaluator shall list the search keywords used, as well as provide the search result.  In case where publicly known vulnerabilities are found, developer shall confirm that all known vulnerabilities have been fixed for this version of TOE or that the vulnerabilities do not affect the TOE. |  |  |
| **4 Developer’s Document[[1]](#footnote-2)** | | | |
| 4.1 | Evaluator shall check the completeness of the design document for Class ADV: Development evaluation. |  |  |
| 4.2 | Evaluator shall check the completeness of the guidance documentation for Class AGD: Guidance Documents evaluation. |  |  |
| 4.3 | Evaluator shall check the completeness of the procedure documentation for life-cycle of TOE for Class ALC: Life-cycle support evaluation. |  |  |
| 4.4 | Evaluator shall check the completeness of the test documentation for Class ATE: Tests evaluation. |  |  |

1. The readiness of the developer’s documentation is crucial for meeting the project schedule. The CCTL is required to assess the suitability and completeness of the developer’s documentation to determine whether the evaluation could be conducted in accordance with the CEM and within the proposed time frame. [↑](#footnote-ref-2)