Protection Profile for QQQQ

Version: 1.0
2015-08-14
National Information Assurance Partnership

Revision History

Version	Date	Comment
Round 1	2015-04-23	First draft of version 1.0 for comment
1.0	2015-08-14	Release - first version released

Contents

Appendix A - Implementation-Dependent Requirements

Implementation-Dependent Requirements are dependent on the TOE implementing a particular function. If the TOE fulfills any of these requirements, the vendor must either add the related SFR or disable the functionality for the evaluated configuration.

Appendix B - Inherently Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this Protection Profile. However, these requirements are not featured explicitly as SFRs and should not be included in the . They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by Part 1, **8.2 Dependencies between components**.
This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the Protection Profile provides evidence that these controls are present and have been evaluated. Requirement Rationale for Satisfaction FIA_UAU.1 - Timing of authentication implicitly requires that the OS perform all necessary actions, including those on behalf of the user who has not been authenticated, in order to authenticate; therefore it is duplicative to include these actions as a separate assignment and test. FIA_UID.1 - Timing of identification implicitly requires that the OS perform all necessary actions, including those on behalf of the user who has not been identified, in order to authenticate; therefore it is duplicative to include these actions as a separate assignment and test. FMT_SMR.1 - Security roles specifies role-based management functions that implicitly defines user and privileged accounts; therefore, it is duplicative to include separate role requirements. FPT_STM.1 - Reliable time stamps explicitly requires that the OS associate timestamps with audit records; therefore it is duplicative to include a separate timestamp requirement. FTA_SSL.1 - TSF-initiated session locking defines requirements for managing session locking; therefore, it is duplicative to include a separate session locking requirement. FTA_SSL.2 - User-initiated locking defines requirements for user-initiated session locking; therefore, it is duplicative to include a separate session locking requirement. FAU_STG.1 - Protected audit trail storage defines a requirement to protect audit logs; therefore, it is duplicative to include a separate protection of audit trail requirements. FAU_GEN.2 - User identity association explicitly requires that the OS record any user account associated with each event; therefore, it is duplicative to include a separate requirement to associate a user account with each event. FAU_SAR.1 - Audit review requires that audit logs (and other objects) are protected from reading by unprivileged users; therefore, it is duplicative to include a separate requirement to protect only the audit information.

Appendix C - Entropy Documentation and Assessment

This appendix describes the required supplementary information for the entropy source used by the OS. The documentation of the entropy source should be detailed enough that, after reading, the evaluator will thoroughly understand the entropy source and why it can be relied upon to provide sufficient entropy. This documentation should include multiple detailed sections: design description, entropy justification, operating conditions, and health testing. This documentation is not required to be part of the TSS.

Appendix D - Design Description

Documentation shall include the design of the entropy source as a whole, including the interaction of all entropy source components. Any information that can be shared regarding the design should also be included for any third-party entropy sources that are included in the product.
The documentation will describe the operation of the entropy source to include, how entropy is produced, and how unprocessed (raw) data can be obtained from within the entropy source for testing purposes. The documentation should walk through the entropy source design indicating where the entropy comes from, where the entropy output is passed next, any post-processing of the raw outputs (hash, XOR, etc.), if/where it is stored, and finally, how it is output from the entropy source. Any conditions placed on the process (e.g., blocking) should also be described in the entropy source design. Diagrams and examples are encouraged.
This design must also include a description of the content of the security boundary of the entropy source and a description of how the security boundary ensures that an adversary outside the boundary cannot affect the entropy rate.
If implemented, the design description shall include a description of how third-party applications can add entropy to the RBG. A description of any RBG state saving between power-off and power-on shall be included.

Appendix E - Entropy Justification

There should be a technical argument for where the unpredictability in the source comes from and why there is confidence in the entropy source delivering sufficient entropy for the uses made of the RBG output (by this particular OS). This argument will include a description of the expected min-entropy rate (i.e. the minimum entropy (in bits) per bit or byte of source data) and explain that sufficient entropy is going into the OS randomizer seeding process. This discussion will be part of a justification for why the entropy source can be relied upon to produce bits with entropy.
The amount of information necessary to justify the expected min-entropy rate depends on the type of entropy source included in the product.
For developer provided entropy sources, in order to justify the min-entropy rate, it is expected that a large number of raw source bits will be collected, statistical tests will be performed, and the min-entropy rate determined from the statistical tests. While no particular statistical tests are required at this time, it is expected that some testing is necessary in order to determine the amount of min-entropy in each output.
For third-party provided entropy sources, in which the OS vendor has limited access to the design and raw entropy data of the source, the documentation will indicate an estimate of the amount of min-entropy obtained from this third-party source. It is acceptable for the vendor to “assume” an amount of min-entropy, however, this assumption must be clearly stated in the documentation provided. In particular, the min-entropy estimate must be specified and the assumption included in the ST.
Regardless of type of entropy source, the justification will also include how the DRBG is initialized with the entropy stated in the ST, for example by verifying that the min-entropy rate is multiplied by the amount of source data used to seed the DRBG or that the rate of entropy expected based on the amount of source data is explicitly stated and compared to the statistical rate. If the amount of source data used to seed the DRBG is not clear or the calculated rate is not explicitly related to the seed, the documentation will not be considered complete.
The entropy justification shall not include any data added from any third-party application or from any state saving between restarts.

Appendix F - Operating Conditions

The entropy rate may be affected by conditions outside the control of the entropy source itself. For example, voltage, frequency, temperature, and elapsed time after power-on are just a few of the factors that may affect the operation of the entropy source. As such, documentation will also include the range of operating conditions under which the entropy source is expected to generate random data. It will clearly describe the measures that have been taken in the system design to ensure the entropy source continues to operate under those conditions. Similarly, documentation shall describe the conditions under which the entropy source is known to malfunction or become inconsistent. Methods used to detect failure or degradation of the source shall be included.

Appendix G - Health Testing

More specifically, all entropy source health tests and their rationale will be documented. This includes a description of the health tests, the rate and conditions under which each health test is performed (e.g., at start, continuously, or on-demand), the expected results for each health test, and rationale indicating why each test is believed to be appropriate for detecting one or more failures in the entropy source.

Appendix H - Acronyms

AES Advanced Encryption Standard ANSI American National Standards Institute API Application Programming Interface ASLR Address Space Layout Randomization CESG Communications-Electronics Security Group CMC Certificate Management over CMS CMS Cryptographic Message Syntax CN Common Names CRL Certificate Revocation List CSA Computer Security Act DEP Data Execution Prevention DES Data Encryption Standard DHE Diffie-Hellman Ephemeral DNS Domain Name System DRBG Deterministic Random Bit Generator DSS Digital Signature Standard DT Date/Time Vector DTLS Datagram Transport Layer Security EAP Extensible Authentication Protocol ECDHE Elliptic Curve Diffie-Hellman Ephemeral ECDSA Elliptic Curve Digital Signature Algorithm EST Enrollment over Secure Transport FIPS Federal Information Processing Standards DSS Digital Signature Standard HMAC Hash-based Message Authentication Code HTTP Hypertext Transfer Protocol HTTPS Hypertext Transfer Protocol Secure DSS Digital Signature Standard IETF Internet Engineering Task Force IP Internet Protocol ISO International Organization for Standardization IT Information Technology ITSEF Information Technology Security Evaluation Facility NFC Near Field Communication NIAP National Information Assurance Partnership NIST National Institute of Standards and Technology OCSP Online Certificate Status Protocol OID Object Identifier OMB Office of Management and Budget OS Operating System PII Personally Identifiable Information PKI Public Key Infrastructure PP Protection Profile RBG Random Bit Generator RFC Request for Comment RNG Random Number Generator RNGVS Random Number Generator Validation System SAN Subject Alternative Name SAR Security Assurance Requirement SFR Security Functional Requirement SHA Secure Hash Algorithm S/MIME Secure/Multi-purpose Internet Mail Extensions SIP Session Initiation Protocol SWID Software Identification TLS Transport Layer Security URI Uniform Resource Identifier URL Uniform Resource Locator USB Universal Serial Bus XCCDF eXtensible Configuration Checklist Description Format XOR Exclusive Or

Appendix I - Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
EP	Extended Package
FP	Functional Package
OE	Operational Environment
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
cPP	Collaborative Protection Profile

Appendix J - Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012. • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012. • Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CEM]	Common Evaluation Methodology for Information Technology Security - Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
[CESG]	CESG - End User Devices Security and Configuration Guidance
[CSA]	Computer Security Act of 1987, H.R. 145, June 11, 1987.
[OMB]	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, OMB M-06-19, July 12, 2006.