Functional Package for Transport Layer Security (TLS)

Version: 1.1
2019-03-01
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2018-12-17	First publication
1.1	2019-03-01	Clarifications regarding override for invalid certificates, renegotation_info extension, DTLS versions, and named Diffie-Hellman groups in DTLS contexts

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 - Acronyms

AES Advanced Encryption Standard CA Certificate Authority CBC Cipher Block Chaining CN Common Name DHE Diffie-Hellman Ephemeral DN Distinguished Name DNS Domain Name Server DTLS Datagram Transport Layer Security EAP Extensible Authentication Protocol ECDHE Elliptic Curve Diffie-Hellman Ephemeral ECDSA Elliptic Curve Digital Signature Algorithm GCM Galois/Counter Mode HTTP Hypertext Transfer Protocol IETF Internet Engineering Task Force IP Internet Protocol LDAP Lightweight Directory Access Protocol NIST National Institute of Standards and Technology RFC Request for Comment (IETF) RSA Rivest Shamir Adelman SAN Subject Alternative Name SCSV Signaling Cipher Suite Value SHA Secure Hash Algorithm SIP Session Initiation Protocol TCP Transmission Control Protocol TLS Transport Layer Security UDP User Datagram Protocol URI Uniform Resource Identifier URL Uniform Resource Locator

Appendix C - Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
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

Appendix D - Bibliography

Identifier	Title
[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.
[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.