ISO/IEC-19790 (2012_cor2015) Security requirements for cryptographic modules

ISO/IEC-24759_2017 Test requirements for cryptographic modules

FIPS 140-3 Implementation Guidance (IG)

SP 140-3 Derived Test Requirements (DTR) (March 2020)

FIPS 140-3 CMVP Management Manual (Sept 2020)

FIPS 186-4 Digital Signature Standard (DSS) (July 2013)

FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (August 2015)

SP 800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping (Dec 2012)

SP 800-52 rev 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (August 2019)

SP 800-56A rev3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (April 2018)

SP 800-56B rev2 Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography (March 2019)

SP 800-56C rev2 Recommendation for Key-Derivation Methods in Key-Establishment Schemes (April 2020)

SP 800-90A rev1Recommendation for Random Number Generation Using Deterministic Random Bit Generators (June 2015)

SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation (Jan 2018)

SP 800-131A rev2 Transitioning the Use of Cryptographic Algorithms and Key Lengths(March 2019)

SP 800-132 Recommendation for Password-Based Key Derivation: Part 1: Storage Applications (Dec 2010)

SP 800-135 rev1 Recommendation for Existing Application-Specific Key Derivation Functions (Dec 2011)

SP 800-140 CMVP series