1. Record Nr. UNINA9910695284903321

Autore	Keller Sharon
Titolo	Modes of operation validation system for the Triple Data Encryption Algorithm (TMOVS) [[electronic resource]] : requirements and procedures / / Sharon Keller
Pubbl/distr/stampa	Gaithersburg, MD : , : U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, , [2000]
Edizione	[Rev. Apr. 2000.]
Descrizione fisica	xvi, 299 pages : digital, PDF file
Collana	NIST special publication ; ; 800-20
Altri autori (Persone)	KellerS. S
Soggetti	Computer programs - Validation - Standards Data encryption (Computer science) - Standards
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Title from title screen (viewed on July 20, 2006). "Original date: October 1999."
Nota di bibliografia	Includes bibliographical references.
Sommario/riassunto	The National Institute of Standards and Technology (NIST) Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS) specifies the procedures involved in validating implementations of the Triple DES algorithm in ANSI X9.52 - 1998, Triple Data Encryption Algorithm Modes of Operation. Successful completion of the tests contained within the TMOVS is required to claim conformance to ANSI X9.52-1998.The TMOVS is designed to perform automated testing on Implementations Under Test (IUTs). This publication provides a brief overview of the Triple DES algorithm and introduces the basic design and configuration of the TMOVS. Included in this overview are the specifications for the two categories of tests which make up the TMOVS, i.e., the Known Answer tests and the Modes tests. The requirements and administrative procedures to be followed by those seeking formal NIST validation of an implementation of the Triple DES algorithm are presented. The requirements described include the specific protocols for communication between the IUT and the TMOVS, the types of tests which the IUT must pass for format NIST

validation, and general instruction for accessing and interfacing the TMOVS. An appendix with tables of values and results for the TDES Known Answer tests is also provided.