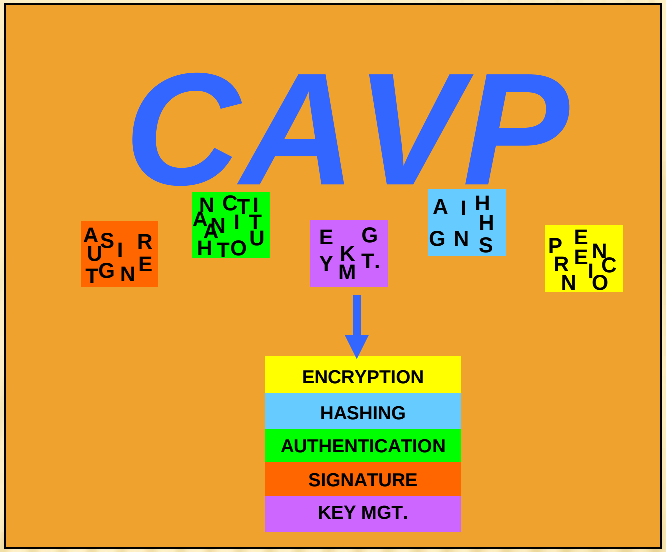
THE CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM



5th Annual NIST IT Security Automation Conference

Sharon Keller
Director, NIST CAVP
October 27, 2009

CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM (CAVP)

- Purpose: Provide assurance that cryptographic algorithm implementations adhere to the specifications detailed in the associated cryptographic algorithm standards.

- Established by NIST and the Communications Security Establishment Canada (CSEC) in 2003
  - Originally part of CMVP – algorithm validation tests were not standardized
  - With increased number of approved Federal Information Processing Standards (FIPS-Approved) and NIST-recommended cryptographic algorithms, formed as separate program

CAVP'S RELATIONSHIP WITH THE CMVP

- The validation of cryptographic algorithm implementations is a prerequisite to the validation of cryptographic module

- With the passage of the Federal Information Security Management Act of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards.

- U.S. Federal organizations must use validated cryptographic modules which in turn means that the cryptographic algorithms implemented in the module must be validated.

CAVP FUNCTIONS

- A suite of validation tests is designed for each Approved* cryptographic algorithm (called the Algorithm’s Validation System) to thoroughly test the algorithm’s
  - specifications,
  - components,
  - features, and
  - functionality

**FIPS-Approved and NIST-Recommended*

Algorithm Complexity Example

Special Publication 800-56A

Discrete Logarithm Cryptography(DLC)
Finite Field Cryptography (FFC)
Elliptic Curve Cryptogr

Key Agreement Schemes (KAS)	
FFC	ECC
	Full Unified Model
	Full MQV
	Ephemeral Unified Model
	One-Pass Unified Model
	One-Pass MQV

Key Agreement Roles
Initiator
Responder

Key Confirmation Roles
Provider
Recipient

Key Confirmation Types

Tests every combination of key agreement scheme – key agreement role-, (key confirmation role-key confirmation type, if KC). Within each combination, there is a section for each parameter set and SHA algorithm supported

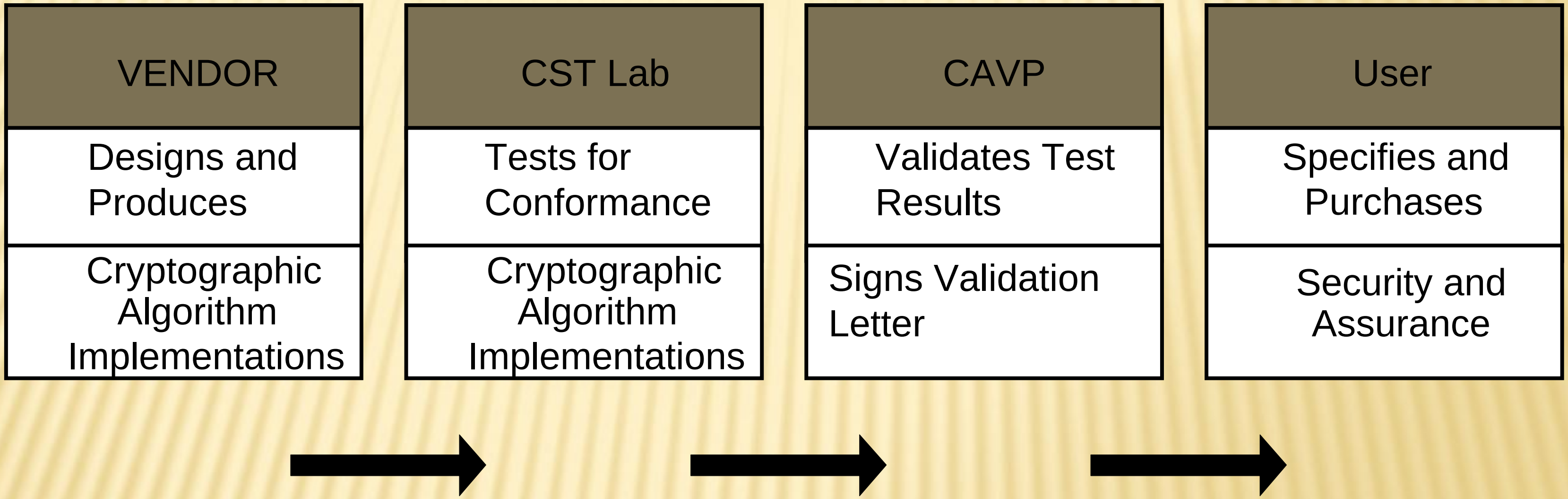
Parameter Size Sets (determines bit length of field ord bit length of subgrou minimum bit length function output, minimum MAC key size (for KC), minimum MacLen (for KC))	
FFC	ECC
FA	EA
FB	EB
FC	EC
	ED
	EE

SHA algorithms supported
SHA1 SHA224 SHA256 SHA384 SHA512

MACs supported (KC) with attributes
CMAC HMAC CCM

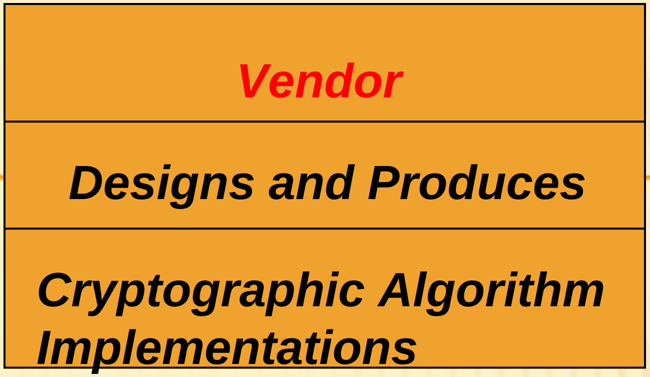
Tests key pair generation,
assurance of validity of keys,
FFC and ECC Diffie-Hellman Primitive (Z)
MQV Primitives (Z)
Concatenation Key Derivation Function
ASN.1 Key Derivation Function

Cryptographic Algorithm Validation Process



VENDOR	CST Lab	CAVP	User
Designs and Produces	Tests for Conformance	Validates Test Results	Specifies and Purchases
Cryptographic Algorithm Implementations	Cryptographic Algorithm Implementations	Signs Validation Letter	Security and Assurance

Cryptographic Algorithm Validation Process (cont.)



Vendor

Designs and Produces

Cryptographic Algorithm Implementations

- Implements cryptographic algorithms that comply with the requirements specified in the applicable FIPS Publication or NIST Special Publications.
- Validation of this implementation is mandatory for it to be used by the United States Federal Government.
  - FIPS 140 - a mandatory standard for the protection of sensitive data
  - Federal Information Security Management Act of 2002

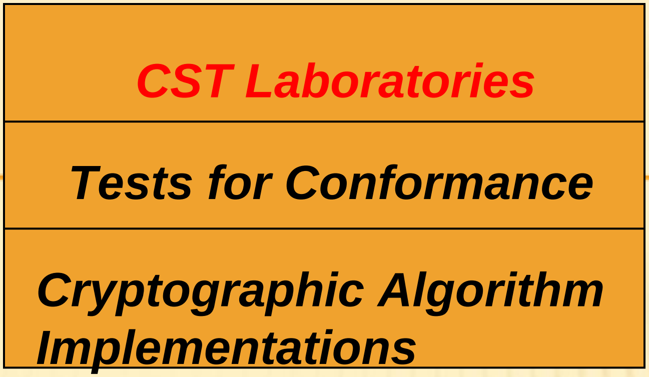
Cryptographic Algorithm Validation Process (cont.)

Vendor
Designs and Produces
Cryptographic Algorithm Implementations

- Vendor contacts a NVLAP* Accredited Cryptographic and Security Testing (CST) Laboratory requesting validation of their implementation.
  - 18 accredited testing laboratories

*National Voluntary Laboratory Accreditation Program

Cryptographic Algorithm Validation Process (cont.)



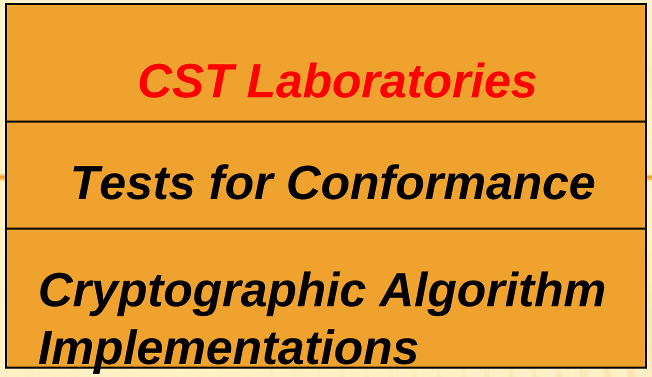
CST Laboratories

Tests for Conformance

Cryptographic Algorithm Implementations

- Independently tests cryptographic algorithm implementations
- Laboratory collects the necessary information from the vendor pertaining to the algorithm implementation.
  - Example: If vendor implements AES, laboratory needs to know
    - the modes of operation implemented (ECB, CBC, CFB, OFB, CCM, CMAC, GCM, GMAC)
    - the states implemented (Encrypt, Decrypt)
    - the key sizes implemented (128, 192, 256)

Cryptographic Algorithm Validation Process (cont.)



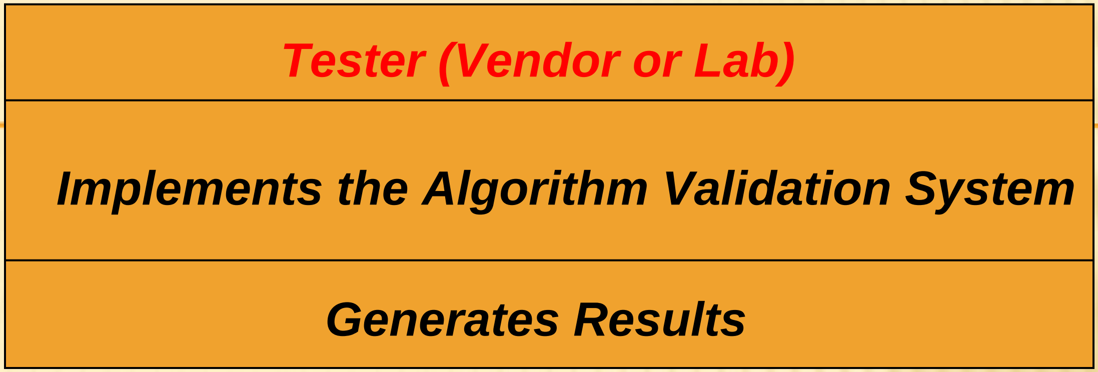
CST Laboratories

Tests for Conformance

Cryptographic Algorithm Implementations

- Laboratory generates input vectors for each test in the suite of validation tests described in the algorithm’s Validation System
- Laboratory sends these input vectors to the tester of the algorithm implementation (tester can be vendor or lab)

Cryptographic Algorithm Validation Process (cont.)



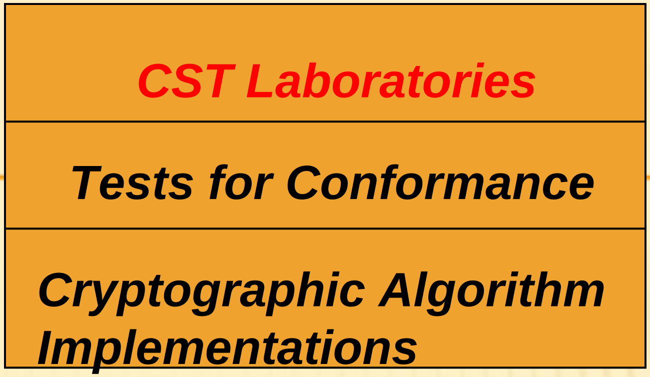
Tester (Vendor or Lab)

Implements the Algorithm Validation System

Generates Results

- Tester implements the test suite for the algorithm. The test suite is described in the algorithm validation system document located on the web.
- For example: For AES, the algorithm validation test suite is described in the AESAVS (AES Algorithm Validation System) document.
- The input vectors are input into the tests and the resulting answers are sent to the laboratory to determine their correctness.

Cryptographic Algorithm Validation Process (cont.)



CST Laboratories

Tests for Conformance

Cryptographic Algorithm Implementations

- CST Laboratory checks the results for accuracy.
- If the results are not correct, lab informs the vendor that the implementation does not meet the requirements of the standard
- If the results are correct, the testing laboratory requests that the CAVP validate the algorithm implementation
  - Lab sends results of tests with the validation request to NIST CAVP

Cryptographic Algorithm Validation Process (cont.)

CAVP
Validates Test Results
Officially Validates Cryptographic Algorithm Implementation

- CAVP checks the results for accuracy
- Determines if the implementation is compliant with the specifications in the cryptographic algorithm standard.

Cryptographic Algorithm Validation Process (cont.)

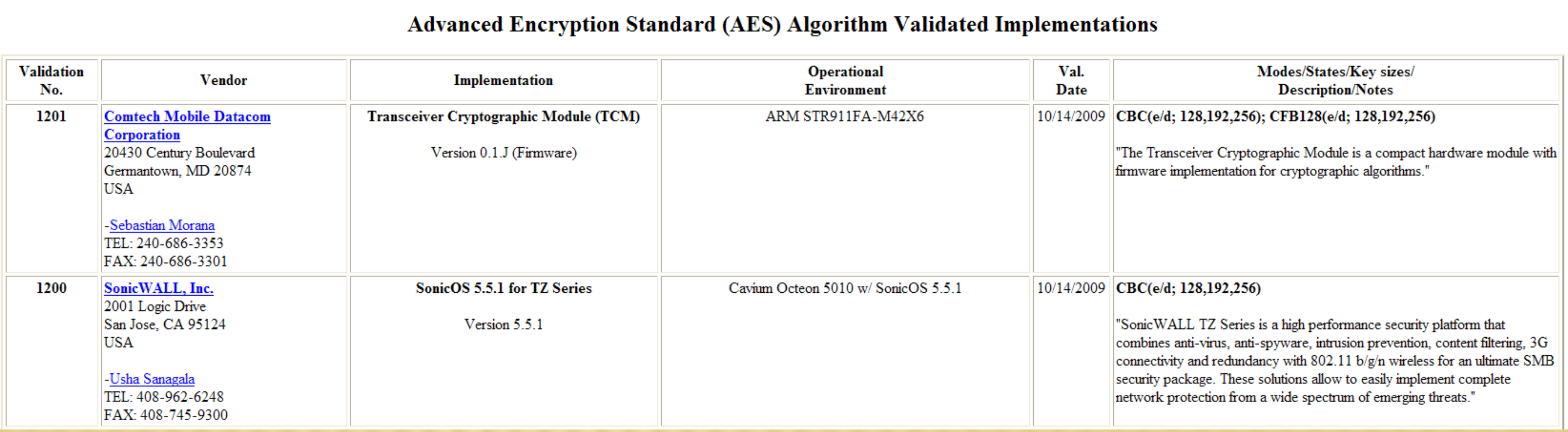
CAVP

Validates Test Results

Officially Validates the Cryptographic Algorithm Implementation

- Posts the official validation on the website
  - Validated cryptographic algorithm implementations are located at

    csrc.nist.gov/groups/STM/cavp/validation.html
- This implementation may now be used in cryptographic modules used by the U.S. Government.



Advanced Encryption Standard (AES) Algorithm Validated Implementations

Validation No.	Vendor	Implementation	Operational Environment	Val. Date	Modes/States/Key sizes/ Description/Notes
1201	Comtech Mobile Datacom Corporation 20430 Century Boulevard Germantown, MD 20874 USA -Sebastian Morana TEL: 240-686-3353 FAX: 240-686-3301	**Transceiver Cryptographic Module (TCM)** Version 0.1.J (Firmware)	ARM STR911FA-M42X6	10/14/2009	**CBC(e/d; 128,192,256); CFB128(e/d; 128,192,256)** "The Transceiver Cryptographic Module is a compact hardware module with firmware implementation for cryptographic algorithms."
1200	SonicWALL, Inc. 2001 Logic Drive San Jose, CA 95124 USA -Usha Sanagala TEL: 408-962-6248 FAX: 408-745-9300	**SonicOS 5.5.1 for TZ Series** Version 5.5.1	Cavium Octeon 5010 w/ SonicOS 5.5.1	10/14/2009	**CBC(e/d; 128,192,256)** "SonicWALL TZ Series is a high performance security platform that combines anti-virus, anti-spyware, intrusion prevention, content filtering, 3G connectivity and redundancy with 802.11 b/g/n wireless for an ultimate SMB security package. These solutions allow to easily implement complete network protection from a wide spectrum of emerging threats."

Cryptographic Algorithm Validation Process (cont.)

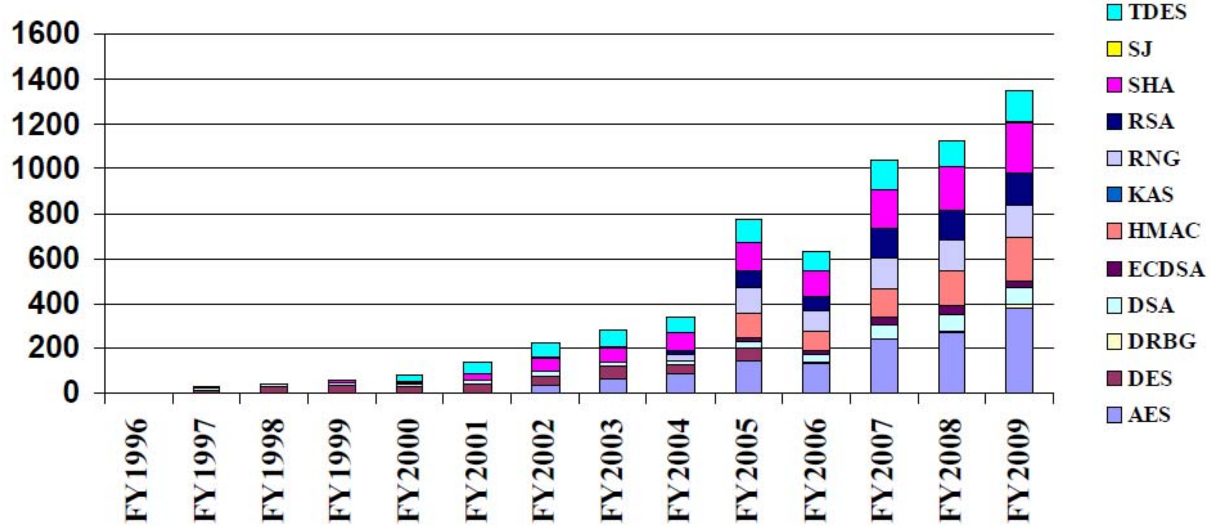
User

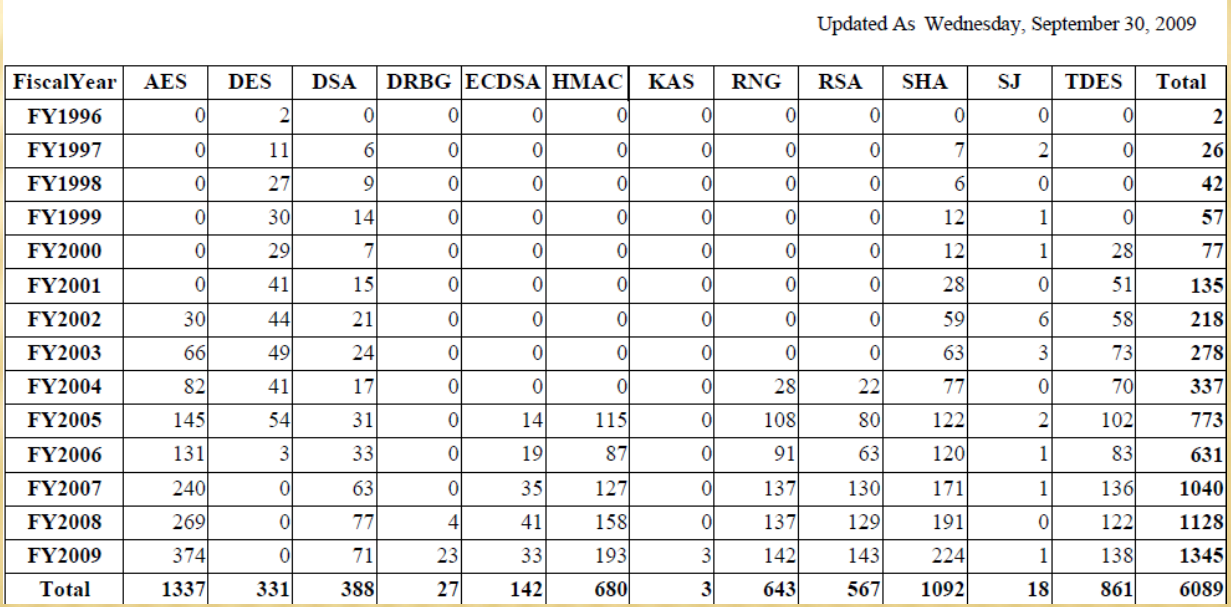
Specifies and Purchases

Security and Assurance

- Verifies that the cryptographic algorithm implementations have been validated inside a cryptographic module or a product considered for purchase and use by Federal Government.

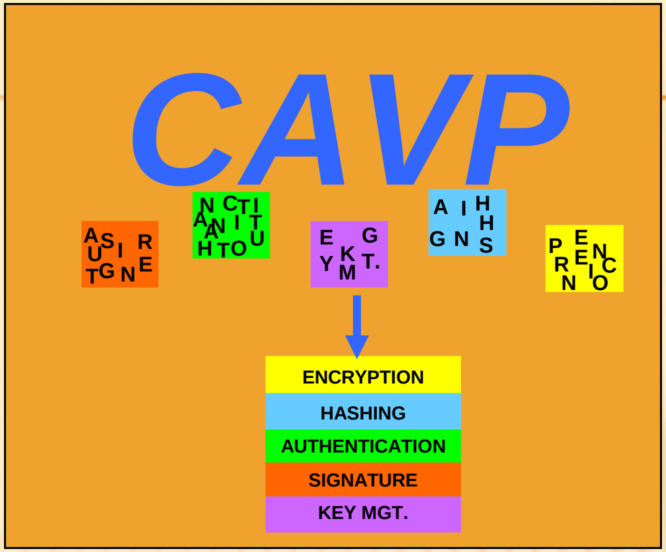
CAVP Validation Status By FYs





Updated As Wednesday, September 30, 2009

FiscalYear	AES	DES	DSA	DRBG	ECDSA	HMAC	KAS	RNG	RSA	SHA	SJ	TDES	Total
FY1996	0	2	0	0	0	0	0	0	0	0	0	0	**2**
FY1997	0	11	6	0	0	0	0	0	0	7	2	0	**26**
FY1998	0	27	9	0	0	0	0	0	0	6	0	0	**42**
FY1999	0	30	14	0	0	0	0	0	0	12	1	0	**57**
FY2000	0	29	7	0	0	0	0	0	0	12	1	28	**77**
FY2001	0	41	15	0	0	0	0	0	0	28	0	51	**135**
FY2002	30	44	21	0	0	0	0	0	0	59	6	58	**218**
FY2003	66	49	24	0	0	0	0	0	0	63	3	73	**278**
FY2004	82	41	17	0	0	0	0	28	22	77	0	70	**337**
FY2005	145	54	31	0	14	115	0	108	80	122	2	102	**773**
FY2006	131	3	33	0	19	87	0	91	63	120	1	83	**631**
FY2007	240	0	63	0	35	127	0	137	130	171	1	136	**1040**
FY2008	269	0	77	4	41	158	0	137	129	191	0	122	**1128**
FY2009	374	0	71	23	33	193	3	142	143	224	1	138	**1345**
Total	**1337**	**331**	**388**	**27**	**142**	**680**	**3**	**643**	**567**	**1092**	**18**	**861**	**6089**



CAVP

ENCRYPTION

HASHING

AUTHENTICATION

SIGNATURE

KEY MGT.

Thank You