National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NIST and US Civilian Agency Cryptography

Matthew Scholl

Group Manager, Computer Security Division, ITL, NIST

Agenda:

- What is Crypto?
- What is Good Crypto?
- How you can Find the Good Stuff?
- When Good Crypto Goes Bad?

What is Crypto?

- Algorithms (the hard stuff)
- Key Management (the really hard stuff)
- Implementation (the hardest stuff)

The Algorithms

- Algorithms authorized for use by the US Civilian Agencies are specified in
  - FIPS 186-3 Secure Hash Standards
  - FIPS 197 Advanced Encryption Standard
  - FIPS 198-1 Keyed Hash Message Authentication Code

The Algorithms

- AES, TDEA, DSA, RSA, ECDSA and then,
- Modes of Operation: (Nine Total,)
- Modes provide algorithmic implementation for specific cryptographic needs;
  - Confidentiality (ECB, CBC, OFB, CFB, CTR, XTS-AES)
  - Authentication (CMAC)
  - Confidentiality and Authentication (CCM and GCM)

Key Management (SP 800-57)

- Key Establishment Schemes
  - Key Derivation Functions
  - Key Agreement Schemes
  - Key Transports
  - Key Wrapping
  - Key Confirmations
  - Random Number Generation
- Key Life spans (crypto periods)
- Public/Private Keys
  - Key Distribution
  - Key Validation
  - Key Revocation

Implementations

- Passwords/Pins/Entropy
- Authentication and Authorizations
- Communication Channels
- The other protections...
  - Physical/Environmental/Side Channel etc

What is Good Crypto?

- Does the product do what is claimed?
- Does it conform to standards?
- Was it independently tested?
- Is the product secure?

Good Crypto Metrics

- **Cryptographic Modules Surveyed (during testing)**
  - 48.8% Security Flaws discovered
  - 96.3% FIPS Interpretation and Documentation Errors
- **Algorithm Validations (during testing) (DES, Triple-DES, DSA and SHA-1)**
  - 8.5% Security Flaws
  - 65.1% FIPS Interpretation and Documentation Errors
- **Areas of Greatest Difficulty**
  - Physical Security
  - Self Tests
  - Random Number Generation
  - Key Management

Using FIPS Validated Cryptographic Modules

- Cryptographic modules *may* be embedded in other products
  - Applicable to hardware, software, and firmware cryptographic modules
  - Must use the validated version and configuration
  - e.g. software applications, cryptographic toolkits, postage metering devices, radio encryption modules
- Does not require the validation of the larger product
  - Larger product is deemed compliant to requirements of FIPS 140-2

When Good Crypto Goes Bad

- Cryptography used to protect sensitive information
- Attackers are becoming smarter and computers are becoming more powerful
- Many commonly used crypto algorithms broken (e.g., DES broken about 1998, and SHA-1 weakened by attacks in 2005)
- Defensive measures? Use other algorithms and larger key sizes

The Good, The Bad, The Ugly

- Problem? How to transition?
- Solution: Be flexible and plan ahead
  - Strategy originally proposed in Draft SP 800-57, Part 1 in 2003
  - SP 800-57, Part 1 completed in 2005; revisions in 2006 and 2007
  - Goal: to transition from a security strength of 80 bits to 112 bits by 2013
    - Some algorithms no longer recommended
    - Larger key sizes required

Purpose of SP 800-131:

- To bring more specific transition details to the attention of the Federal government agencies and the public
- Written from the point of view of the CMVP: what new validations are allowed vs. what already-validated implementations will continue to be allowed
- Will be used to develop validation guidance documents

Encryption:

- Algorithms **no longer approved after 2013**:
  - Two-key Triple DES
  - SKIPJACK
- Algorithms (and key sizes) still **approved**
  - Three-key Triple DES
  - AES 128,192 and 256

Hash Functions (FIPS 180-3):

- SHA-1:
  - OK for digital signature generation thru 2013
  - OK for digital signature verification beyond 2013
  - OK for other applications beyond 2013 (e.g., HMAC, RNGs, KDFs)
- SHA-224, SHA-256, SHA-384, SHA-512:
  - OK for all applications (including digital signature generation and verification)

Digital Signatures:

- Transition from 186-2 to 186-3 by 2013
- FIPS 186-2 certificates will continue to be valid, subject to the requirements for appropriate security strengths:
  - Signature generation: ≥ 112 bits of security (e.g., ≥ 2048-bit keys for DSA and RSA; ≥ 224-bit keys for ECDSA)
  - Signature verification: ≥ 80 bits of security when generated
- **The invalidation of the algorithm certificates will affect all currently-validated FIPS 186-2 DSA implementations, as well as those implementations of RSA and ECDSA that only use SHA-1 for digital signature generation**

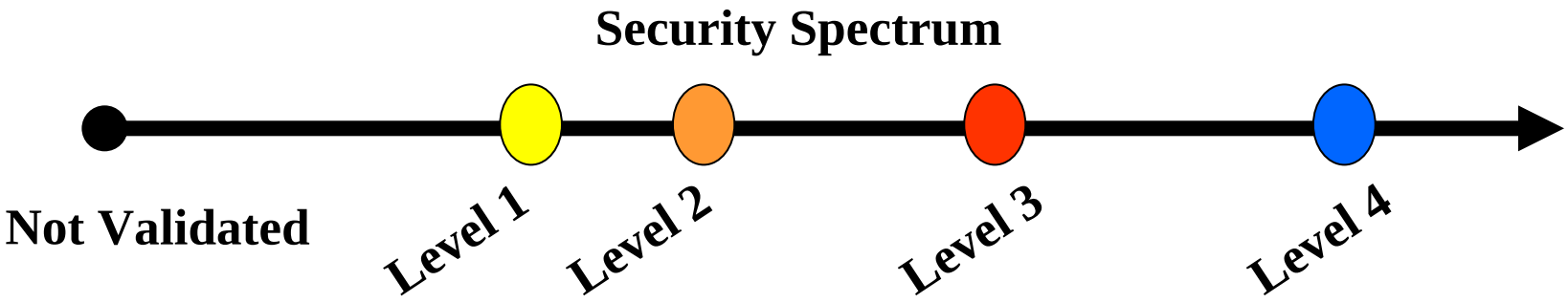
Random Number Generation:

- RNGs specified in FIPS 186-2, ANS X9.31-1998 and ANS X9.62-1998:
  - No new validations after 2013
  - Already-validated implementations OK thru 2015
- RNGs specified in SP 800-90
  - Approved beyond 2013
  - Part of a larger effort within ANSI
  - Provides more guidance, including requirements for achieving higher security strengths

FIPS 140-2: Security Areas

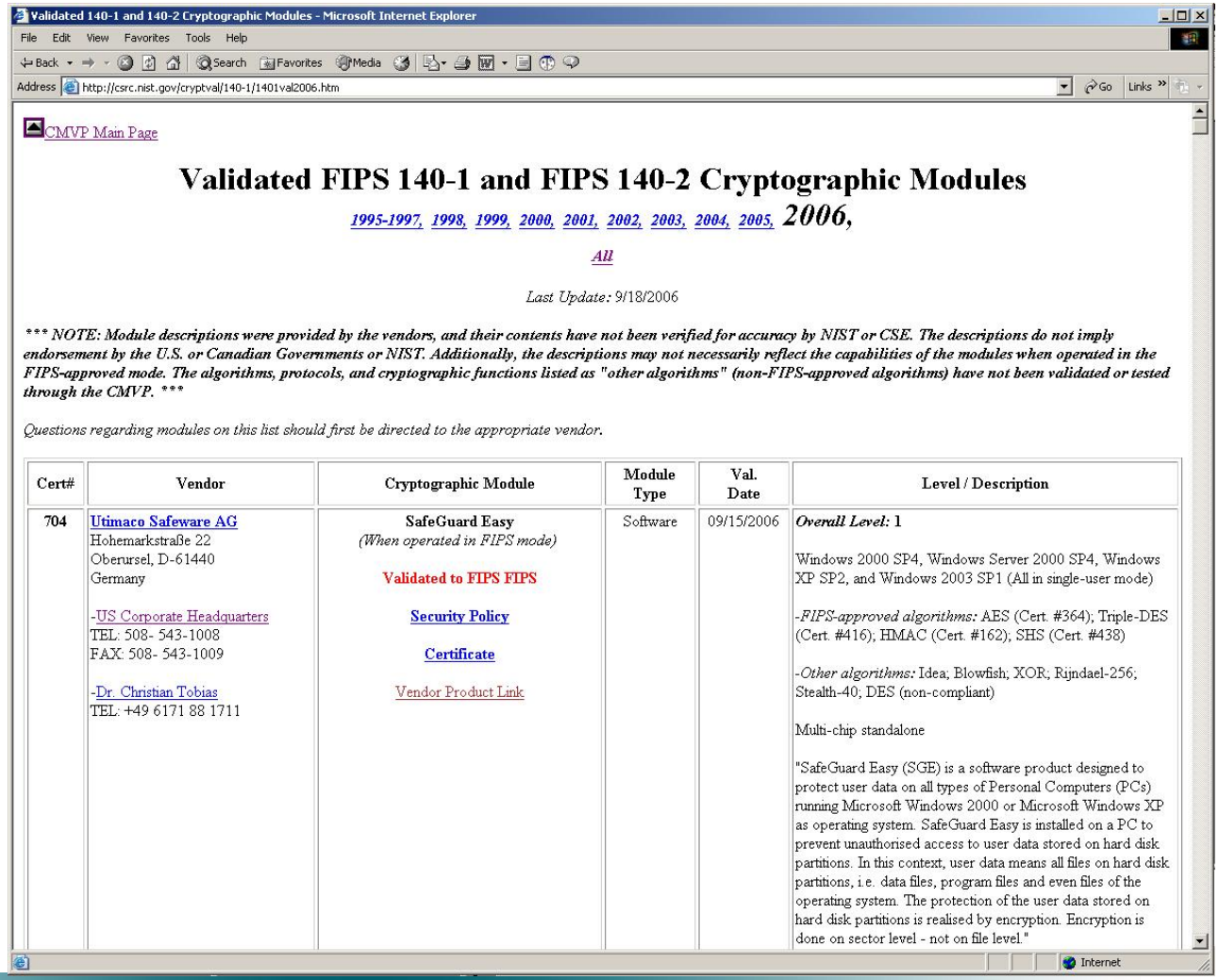
1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. EMI/EMC requirements
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks

FIPS 140-2: Security Levels



- Level 1 is the lowest, Level 4 most stringent
- Requirements are primarily cumulative by level
- Overall rating is lowest rating in all sections
- Validation is applicable when a module is configured and operated in accordance with the level to which it was tested and validated

- Certificate number
- Vendor Name
  - Address
  - Contact
- Module Name
  - Version
  - Security Policy
  - Certificate
- Module Type
- Validation Date
- Overall Level
  - Section Levels
  - Algorithms
  - Embodiment
  - Vendor supplied text



Validated 140-1 and 140-2 Cryptographic Modules - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://csrc.nist.gov/cryptval/140-1/1401val2006.htm

CMVP Main Page

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules

1995-1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, ***2006,***

All

Last Update: 9/18/2006

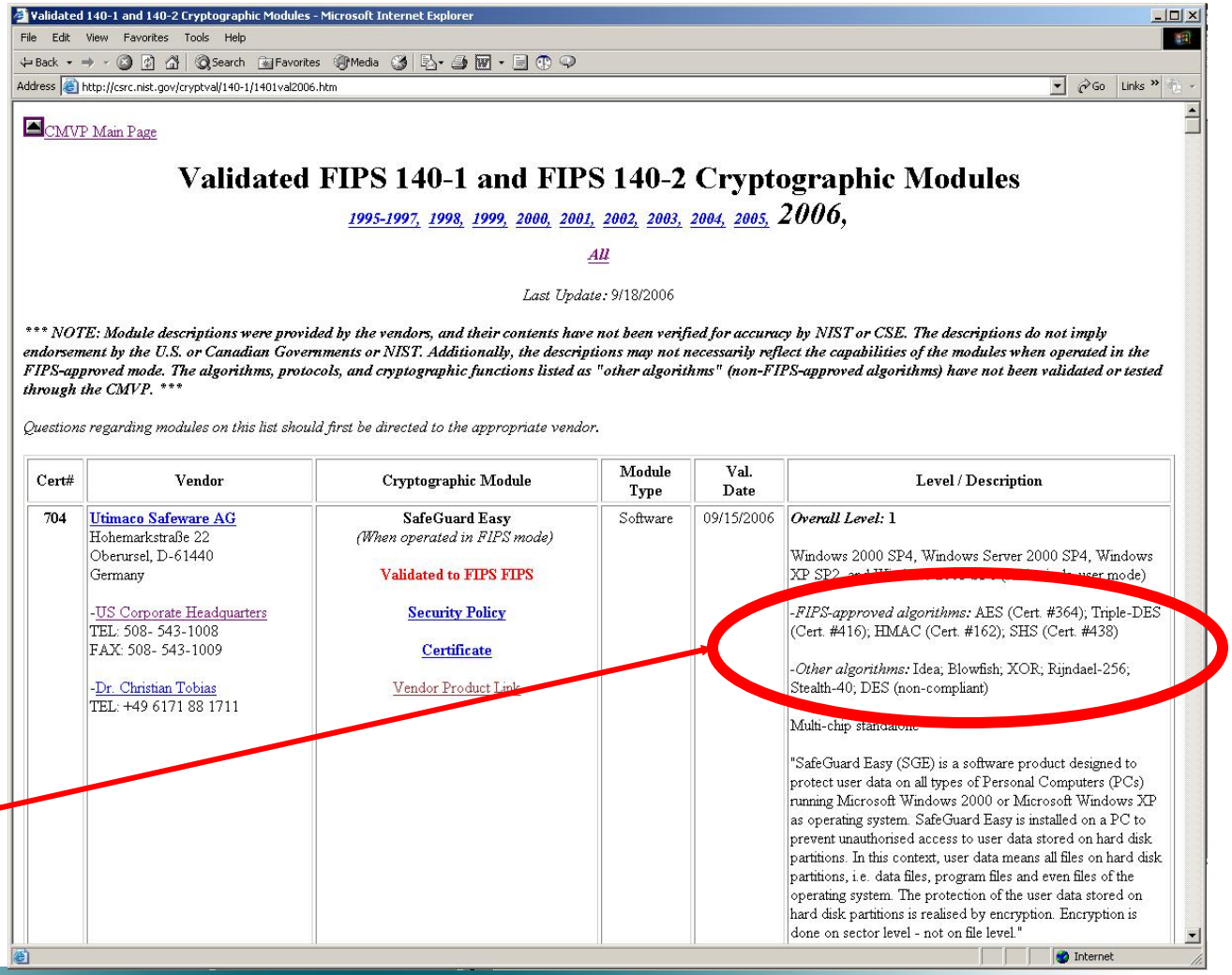
**** NOTE: Module descriptions were provided by the vendors, and their contents have not been verified for accuracy by NIST or CSE. The descriptions do not imply endorsement by the U.S. or Canadian Governments or NIST. Additionally, the descriptions may not necessarily reflect the capabilities of the modules when operated in the FIPS-approved mode. The algorithms, protocols, and cryptographic functions listed as "other algorithms" (non-FIPS-approved algorithms) have not been validated or tested through the CMVP. ****

Questions regarding modules on this list should first be directed to the appropriate vendor.

Cert#	Vendor	Cryptographic Module	Module Type	Val. Date	Level / Description
704	Utimaco Safeware AG Hohemarkstraße 22 Oberursel, D-61440 Germany -US Corporate Headquarters TEL: 508- 543-1008 FAX: 508- 543-1009 -Dr. Christian Tobias TEL: +49 6171 88 1711	SafeGuard Easy *(When operated in FIPS mode)* Validated to FIPS FIPS Security Policy Certificate Vendor Product Link	Software	09/15/2006	***Overall Level:*** 1 Windows 2000 SP4, Windows Server 2000 SP4, Windows XP SP2, and Windows 2003 SP1 (All in single-user mode) *-FIPS-approved algorithms:* AES (Cert. #364); Triple-DES (Cert. #416); HMAC (Cert. #162); SHS (Cert. #438) *-Other algorithms:* Idea; Blowfish; XOR; Rijndael-256; Stealth-40; DES (non-compliant) Multi-chip standalone "SafeGuard Easy (SGE) is a software product designed to protect user data on all types of Personal Computers (PCs) running Microsoft Windows 2000 or Microsoft Windows XP as operating system. SafeGuard Easy is installed on a PC to prevent unauthorised access to user data stored on hard disk partitions. In this context, user data means all files on hard disk partitions, i.e. data files, program files and even files of the operating system. The protection of the user data stored on hard disk partitions is realised by encryption. Encryption is done on sector level - not on file level."

Internet

- Certificate number
- Vendor Name
  - Address
  - Contact
- Module Name
  - Version
  - Security Policy
  - Certificate
  - Product Link
- Module Type
- Validation Date
- Overall Level
  - Section Levels and Operating Systems
  - Algorithms
  - Embodiment
  - Vendor supplied text



QUESTIONS ?

BACKGROUND

Issues re Impact and Implementation (1):

Q: How do I know what Crypto algorithms and key sizes I'm using?

A: Check the technical specifications for your product and/or its cryptographic module. Also, the Cryptographic Algorithm Validation Program certificate will state what cryptographic algorithms are included in the module (see http://csrc.nist.gov/groups/STM/cmvp/validation.html).

Issues re Impact and Implementation (2):

Q: I am currently using FIPS 140-validated cryptography, isn't that good enough?

A: Not quite; the product specifications and certificates should be checked. Transitions from specific algorithms and key sizes means that some certificates may need to be modified or invalidated. NIST plans to review previously-validated modules to remove the un-approved cryptography from our certificate listing, but this will take longer than the planned transition dates.

Issues re Impact and Implementation (7):

Q: How can I still verify signatures in my archives or from organizations that are using old algorithms or key sizes

A: The verification capability for these algorithms and key sizes will continue to be approved. The public keys for these signatures need to be saved (e.g., archived); The signing keys need to be destroyed to preclude further use.

Key Wrapping:

- Encryption of one key by another, possibly including an integrity mechanism
- No FIPS or NIST Recommendation yet.
- IG D.2: AES or Triple DES may be used to wrap keys using the specification on the NIST web site.
  - Two-key Triple DES OK thru 2013
  - AES and Three-key Triple DES OK

Deriving Keys from a Key (a.k.a. Key Derivation):

- Specified in SP 800-108
- HMAC–based KDF using any approved hash function OK (HMAC specified in FIPS 198-1)
- CMAC-based KDF (CMAC specified in SP 800-38B):
  - Two-key Triple DES OK thru 2013
  - AES and Three-key Triple DES OK

Message Authentication Codes:

- HMAC (FIPS 198-1 and SP 800-107):
  - Any approved hash function
  - Key lengths $\geq$ 80 bits OK thru 2013
  - Key lengths $\geq$ 112 bits OK beyond 2013
- CMAC (SP 800-38B):
  - Two-key Triple DES OK thru 2013
  - AES and Three-key Triple DES OK beyond 2013