



Tale of two Standards

M.R, MURALIDHARAN
CONSULTANT CDAC

Standards for Cryptographic Products

- ▶ National Institute of Standards and Technology (NIST)
- ▶ International Standards Organization (ISO)
- ▶ History of standards for Cryptographic products
- ▶ Certification ecosystems
- ▶ Issues/Options in adopting standards

National Institute of Standards and Technology - NIST

- ▶ Agency of the U.S. Department of Commerce, founded in 1901
- ▶ Builds Standards, Frameworks and Certification Program for use by US Govt., and Industry
- ▶ Famously know for Cyber Security Framework, Crypto module certification framework FIP 140-2/3 etc.
- ▶ Power to mandate other US agencies/dept. to follow its dict
- ▶ All standard publications are free and downloadable
- ▶ Free to use by any one

NIST - Standards Development process

- ▶ Driven by a strong in-house technically team
- ▶ Crypto algorithms are selected for standardization based on publicized requirement and contest
 - ▶ Selection of AES
 - ▶ Took almost 5 years from call for submission, 1997
 - ▶ NSA score
 - ▶ 3 conferences, 1998, 1999, 2000 to filter submission and select 15/5/1
 - ▶ Became Official Standard on December 6, 2001
 - ▶ Followed similar process for SHA, Light Weight Algorithm and PQC
- ▶ In spite of openness it got involved what is known as Dual_EC_DRBG algorithm controversy,
 - ▶ included in NIST standard SP 800-90A, allegations of a secret back door from National Security Agency (NSA)
 - ▶ After much furor it was withdrawn.

NIST Standards relating to Cryptographic Products

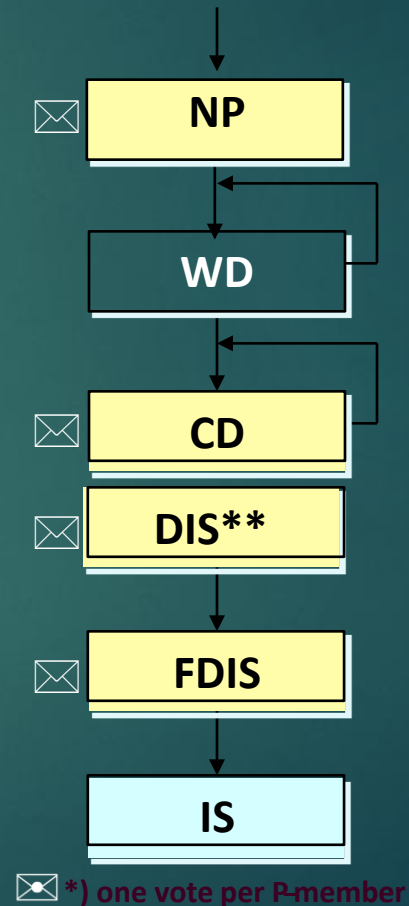
- ▶ Crypto Modules
 - ▶ FIPS 140 – 1/2/3
 - ▶ Describing 4 levels of security
 - ▶ Derived Testing Requirements (DTR) for FIPS 140
 - ▶ Implementation Guidance (IG)
 - ▶ Security Policy
- ▶ Algorithms
 - ▶ Symmetric, asymmetric (AES, RSA, DSA etc.)
 - ▶ Hash (SHA 1/2/3)
 - ▶ Many others (ASCON etc.,)

International Organization for Standardization- ISO

- ▶ independent, non-governmental international organization of national standards bodies to build global standards
- ▶ Currently has 173 national members
- ▶ Standards are built by broad agreement/consensus between members countries, every stage in standard development has voting
- ▶ Has evolved a elaborate process to bring new standards and making updates
- ▶ ISO standards documents are proprietary and must be purchased
- ▶ Unable to withstand pressure from sovereign countries and MNCs
 - ▶ allegations that one MNC influenced ISO during the standardization process of the Open XML (OOXML) document format (ISO/IEC 29500)

ISO processes - Project Development

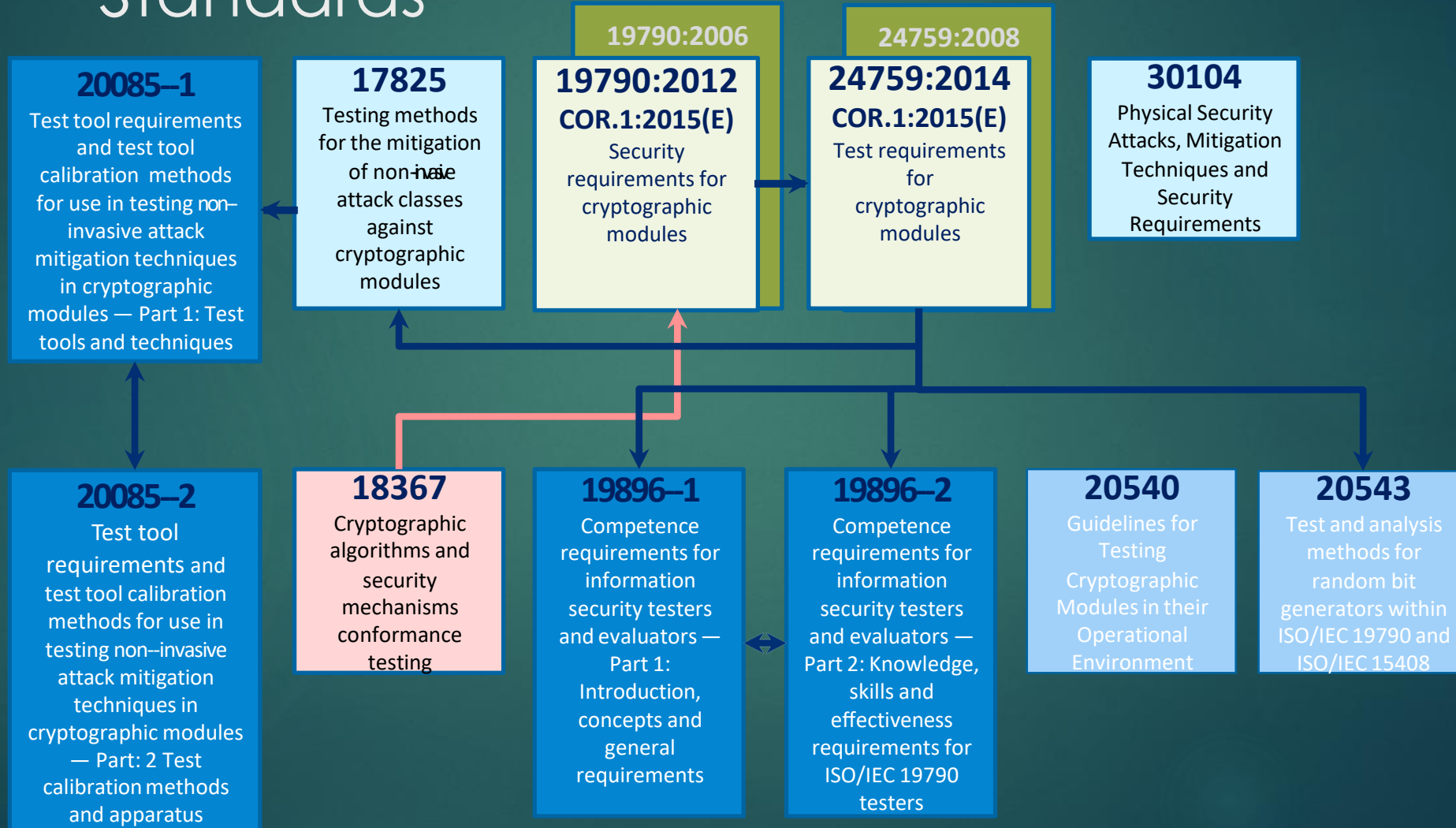
- Maturity level / state of standardization
 - Study Period / New Project (NP)
 - 3 month NP letter ballot^{*}
 - Working Draft (WD)
 - Committee Draft (CD)
 - 3 month CD ballot(s)
 - Draft International Standard (DIS)
 - 3 month DIS ballot (+ 2 months f. translation)
 - Final Draft International Standard (FDIS)
 - 2 month FDIS ballot
 - no more comments at this stage
 - International Standard (IS)
 - pre-review 3 years after publication (subsequent per 2 years prior to SR)
 - review every 5 years (via the Systematic Review at JTC 1 Level)
 - or after 'defect report'
 - Updates can be made via technical corrigendum's



ISO - Crypto Standards

- ▶ ISO/IEC JCT1 27 is the committee responsible for crypto standards
- ▶ Security Management Standards
 - ▶ ISO 27001
- ▶ Crypto module standards
 - ▶ ISO/IEC 19790 and other related standards
- ▶ Crypto Algorithms standards
 - ▶ Symmetric, Hash, Asymmetric etc. (AES,DES, RSA etc.,)
 - ▶ Testing of algorithms
 - ▶ Many more algorithms are standardized than NIST
- ▶ Lack of Certification Eco-System

Cryptographic Module Testing – ISO Standards



Related standards

- ▶ Certification Authority ISO/IEC 17021
- ▶ Common criteria evaluation ISO/IEC 15408:2014
- ▶ Laboratory accreditation ISO/IEC 17025:2017
- ▶ Evaluator competence
 - ▶ ISO/IEC 19896-1:2018 Introduction, concepts and general requirements
 - ▶ ISO/IEC 19896-2:2018 Knowledge, skills for ISO/IEC 19790 testers
 - ▶ ISO/IEC 19896-3:2018 for common criteria

Never the twain shall meet

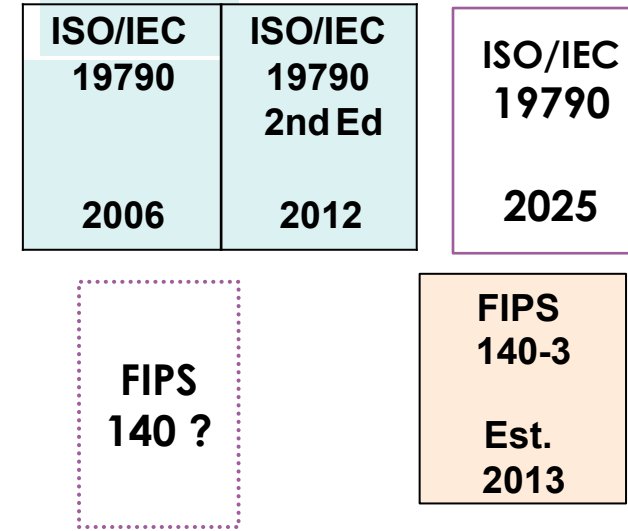
- ▶ Due to historical issues people thought NIST and ISO will not come together and cooperate
- ▶ For example,
 - ▶ NIST voted against its own standard (DES), such that it will not be adopted by ISO
 - ▶ Shock to ISO was so much it stopped all cryptographic standards activities for a decade or more
 - ▶ NIST has been in cryptographic activities for much long
 - ▶ experienced in dealing with Industry
 - ▶ Implementation Guidance
- ▶ NIST has developed very many standards which were adopted by American industry and govt. agencies, it is good as ISO
- ▶ **BUT HISTORY WAS CREATED with FIPS 140-3**

ISO and NIST comes together

- ▶ ISO was working on 19790 for some time
 - ▶ Basic ideas from FIPS 140-2 and made it better
 - ▶ Added lessons learned from Common criteria standard
 - ▶ Strengthened with Side Channel related clauses
- ▶ NIST was at crossroads for some time
 - ▶ FIPS 140-2 has been around many years and showing age related issues
 - ▶ IG was getting bigger than standard itself
 - ▶ Tried to come up with 5 level certification instead of 4 level
- ▶ But saner thoughts prevailed and it adopted ISO/IEC 19790 as FIPS 140-3 along with ISO/IEC 24759 as DTR
- ▶ NIST took care not change every thing but retain its independance and strength by additions and not delection

History and Evolution

Federal Standard 1027	FIPS 140 (Fed Std 1027)	FIPS 140-1	FIPS 140-2	FIPS 140-2 Change Notices
1982	Not Used	1994	2001	2002



ISO 19790 / FIPS 140-3

- ▶ Crypto products/modules are tested and certified for
- ▶ Eleven areas of areas of Security
 1. Cryptographic Module Specification
 2. Cryptographic Module Ports and Interface
 3. Roles, Services, and Authentication
 4. Software/Firmware Security
 5. Operational Environment
 6. Physical Security
 7. Non-Invasive Security
 8. Sensitive Security Parmeter Management
 9. Self-Tests
 10. Life Cycle Assurance
 11. Mitigation of Other Attacks
- ▶ Four level of increasing security strength

Certification and management

- ▶ NIST

- ▶ Stakeholders - Certification Authority CA, Cryptographic CSTL, Vendor
- ▶ Detailed documents/standard about function of each one of them
- ▶ Web publication of certified products
- ▶ Lifetime of Certificate

- ▶ ISO

- ▶ Every nation is free to adopt any standard with or without modification.
- ▶ Create its own process and procedure for certification
- ▶ How much of modification will be tolerated ?

- ▶ **Can we mix and match between these two ?**

Issues

- ▶ Too many algorithms in ISO standards
 - ▶ 4/5 in light weight algorithms
 - ▶ Where as NIST has been very conservative and did family planning
- ▶ Testing philosophy
 - ▶ NIST is simple and doable
 - ▶ ISO talks about black box/ grey box /white box testing
- ▶ Inclusion of side-channel and fault testing
 - ▶ Increased setup cost and running cost
- ▶ Need for high quality manpower

Crypto Module Certification framework needs,

- ▶ specialist group to address problems upfront and provide continuity
- ▶ Mix and match standards, processes and procedures
- ▶ Much work is to be done to understanding ramification of changes in specification
- ▶ Modify standards to suit our environment
- ▶ Evolve suitable Testing requirements

India needs strong regulatory framework

Technical competence

Bureaucratic will power

Steady fast Political support



Thank you