

**Cryptographic Module
Validation Program**
**-Experience from FIPS 140-2
Validation-**

Tetsuo Nakakawaji
Information Technology R&D Center
Mitsubishi Electric Corporation

Outline

- HSM Overview
 - Design concept
 - Functionality
 - Features
- CMVP Validation Process
 - Security Policy
 - To meet FIPS 140-2 Level 3
- Lesson learned

HSM "TURBOMISTY" Overview

Full size PCI board HSM (Hardware Security Module)



Design Concept

- High security to meet FIPS 140-2 Level 3
- Balance between cost and performance
- Flexibility
 - Algorithm can be added/modified by updating software on the board
- Load balance using multiple HSMs in single machine
- Standard API = PKCS#11

Functionality

- Asymmetric Ciphers :
RSA(key pair generation , signing , encryption)
- Symmetric Ciphers : DES , 3DES , MISTY
- Hash Algorithms : MD5 , SHA-1
- Message Authentication Codes (for SSL):
SSL3-SHA1-MAC , SSL3-MD5-MAC
- Secure Key Backup
- Stores Private keys , Public keys , Certificates

Features

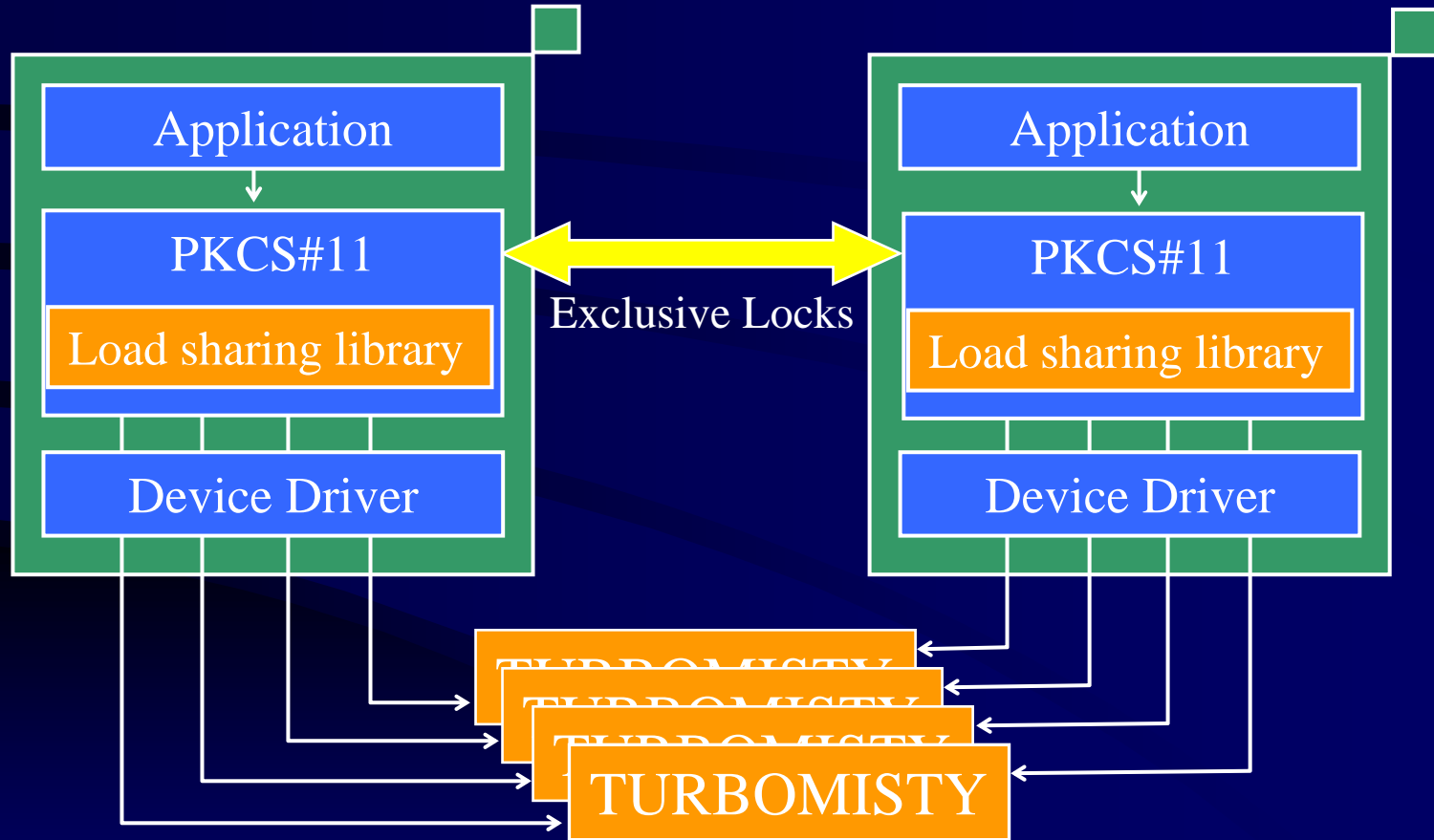
- Tamper resistant key protection
(Corresponds to FIPS140-1 Level3)
 - Physical protection
 - Detects tamper and deletes all keys
When the board is pulled out or,
the cover on the board is removed or broken.

- PKCS#11 API
- Hardware random number generator
- Multiple platform

WindowsNT 4.0 , Windows2000 , Solaris7 , HP-UX 11.0

- New algorithms could be added by updating the F/W. (ECC etc.)

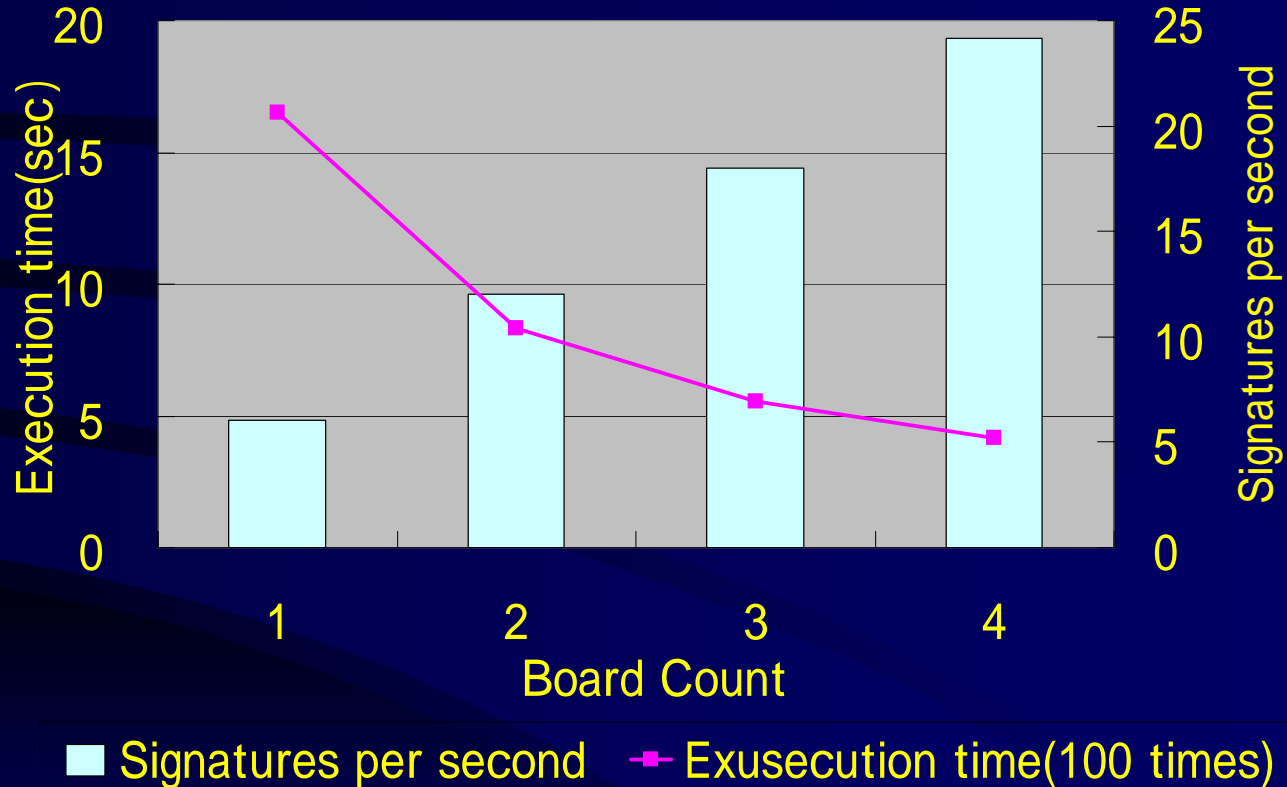
- Load sharing processing
(Multiple threads / Multiple processes)



Performance

- RSA digital signing
 - 1024bit 170 msec
 - 2048bit 1050 msec
- RSA key pair generation (average)
 - 1024bit 9 sec
 - 2048bit 97 sec

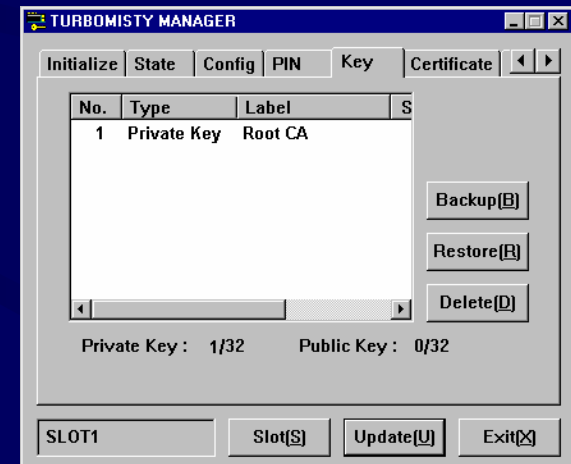
- RSA digital signing (Load sharing , 1024bit)



- Load sharing is also possible in case of connecting with SSL server
 - Connected with Netscape iPlanet Web Server
 - Detail performance analysis is undergoing...

Management

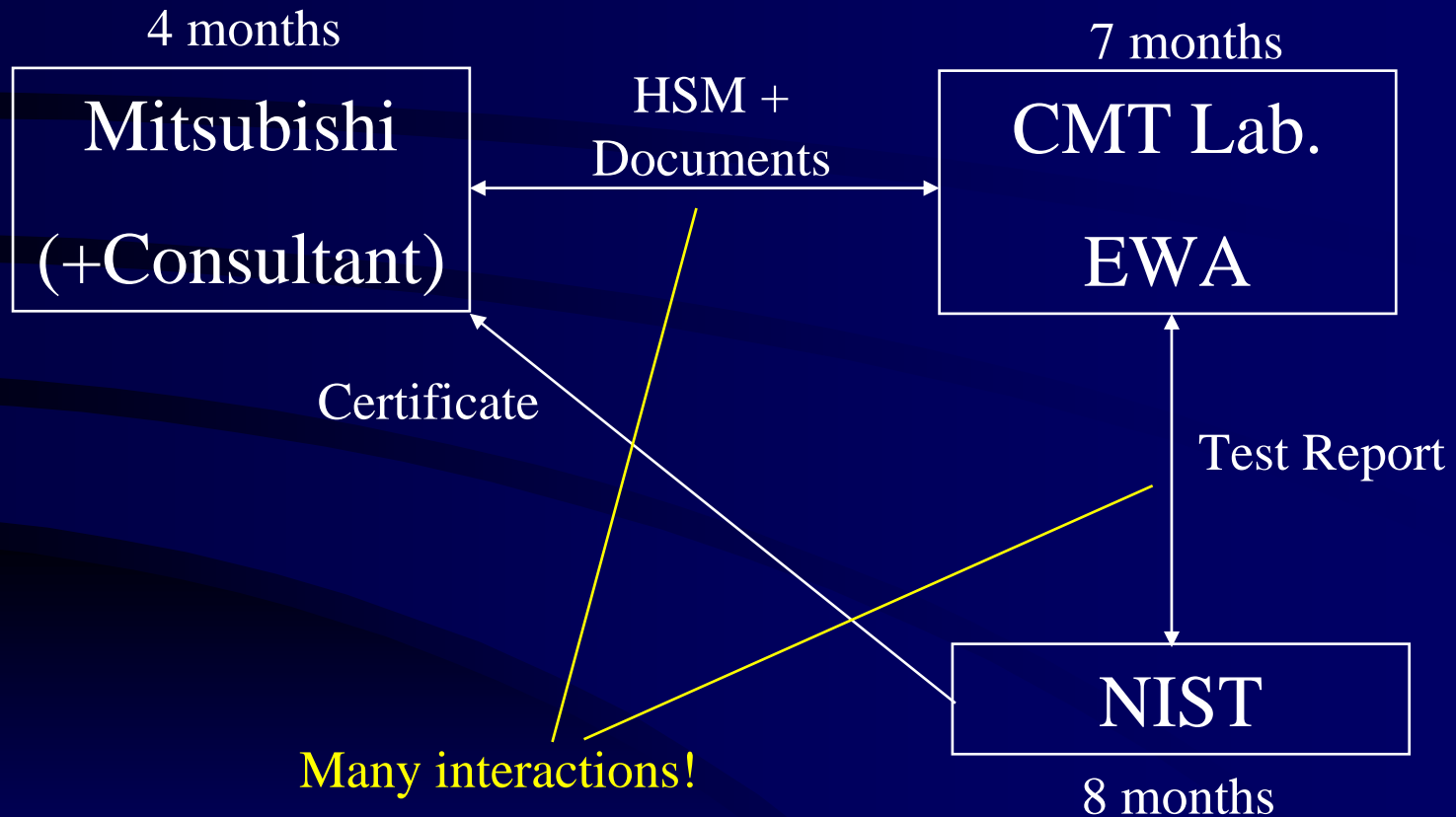
- HSM is managed by the Administrative Tool on the host.
 - Get states
 - Show information about stored keys and certificates
 - Backup/Restore Private Keys
 - Initialize
 - Update F/W



Specifications

- RSA key length
 - 512 - 2048 bit
- Number of keys and certificates
 - Private Key , Public Key : 32
 - Certificate : 64
- Full Size PCI Board
 - (PCI 2.1,33MHz Synchronous 32bit bus)
- Batteries : Keep about 8 years
 - (If the host computer runs 40 hours a week)

CMVP Validation Process



Documents for CMT Lab.

- Security Policy
- Product overview
- Manuals
- H/W Diagram
- Parts list
- S/W Source code
- and so on...

CMT Test Report

- Mitsubishi TurboMisty FIPS 140-2 Security Policy.pdf
- Draft FIPS 140-2 TurboMISTY Certificate.doc
- Mitsubishi TurboMISTY FIPS 140-2 CMT Report v1-1 Sign Sheet.pdf
- Mitsubishi TurboMISTY FIPS 140-2 CMT Report v1-1 Vendor Info.pdf
- Mitsubishi TurboMISTY FIPS 140-2 CMT Report v1-1.pdf -> Test Requirements basis

We've got it!

FIPS 140-2 Validation Certificate



The National Institute of Standards
and Technology of the United States
of America



Certificate No. 359



The Communications Security
Establishment of the Government
of Canada

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

TurboMISTY by Mitsubishi Electric Corporation (When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Designated Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

TM A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

Lesson learned...

- “White box” testing
 - Advantage: Security is ensured (all inside mechanisms are checked in detail)
 - Disadvantage: Time consuming
- Documentation is very important, especially “security policy”
 - Cryptographic boundary
 - Services and Roles
- Language/location barrier
 - Mutual certification is desirable