IGI Online MICS CA

Cosa Serve....

Background

- Cosa e' una CA Online MICS:
  - *A MICS is an automated system to issue X.509 formatted identity assertions (certificates) based on pre-existing identity data maintained by a federation or large organization*
  - *….Given valid identity assertions, the MICS generates X. 509 certificates for these entities that are fully compatible with certificates that would be issued to similar end-entities under the Classic Authentication Profile*
  - E' definita nell'apposito profilo EuGridPMA *https://www.eugridpma.org/guidelines/MICS/IGTF-AP-MICS-1.2-clean.pdf*

Normativa EuGridPMA (Profilo MICS)

- Redazione del CP/CPS
- HSM conforme a FIPS 140-2 (>= Level 3)
- Operativita' conforme a FIPS 140-2 (>= Level 3)
  - "The MICS CA system is designed to be an on-line system, i.e. the issuing machine may be connected (directly or indirectly) to a network or other computer device. If so, it must be equipped with at least a FIPS 140 level 3 capable Hardware Security Module (HSM) or equivalent, and the CA system must be operated in FIPS 140 level 3 mode to protect the CA's private key"
- Dal punto di vista architetturale:
  - *An authentication/request server containing also the HSM hardware, connected to a dedicated network that only carries traffic destined for the CA and is actively monitored for intrusions and is protected via a packet-inspecting stateful firewall*

CP/CPS

- E' il documento che descrive come viene gestita la CA
  - Riconoscimento iniziale e mantenimento delle identita' (ruolo della RA e interazione RA-IdM)
  - Quali tipi di certificati emette e regole di "*Identity Translation*"
  - Formato ed uso dei certificati (attributi, estensioni etc..)
  - Life cycle dei certificati (emissione, re-keying, revoca)
  - Gestione operativa (generazione delle chiavi, procedure di firma, sicurezza fisica, controlli sul personale ...)
  - Procedure di auditing esterno e self-auditing
  - Piano di business continuity
  - Pubblicazione delle informazioni
  - Altri aspetti legali
- RFC 3647 (*Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework*)

Esempio: CP/CPS di Terena TCS

Circa 50 pagine

ND EDUCATION NETWORKING ASSOCIATION

HSM (Hardware Security Module)

- Definizione: "*Una Black box hardware/software inserita/connessa a un PC che fornisce funzioni crittografiche in modo fisicamente e logicamene sicuro*"
  - Generazione di chiavi
  - Storage di chiavi e materiale crittografico
  - Operazioni di cifratura/decifratura
  - …

Esempio:
IBM 4765 Cryptographic Security Module

FIPS 140-2

- FIPS: Federal Information Processing Standards
  - Definisce le caratteristiche di sicurezza di un modulo crittografico utilizzato per la protezione delle informazioni “sensibili” in ICT
    - Algoritmi crittografici utilizzati
    - Interfacce e porte di accesso al servizio
    - Controllo degli accessi fisici /Authn-Authz degli operatori
    - Gestione e life cycle del materiale crittografico
    - Sicurezza fisica ed ambientale
      - Resistenza elettromagnetica
      - Resistenza termica
    - Descrizione “finite state model” delle operazioni
    - Operativita’ (sistemi operativi)
    - …
  - 4 livelli di sicurezza

FIPS 140-2 Obiettivi

- Proteggere il modulo da operazioni non autorizzate
- Impedire la divulgazione dei CSPs
- Rivelare e impedire la modifica non autorizzata del materiale crittografico e dei CSPs
- Rivelare possibili errori sulle operazioni del modulo al fine di evitare la divulgazione dei CSPs*.

* CSP = Critical Security Parameters = dati (PIN, passwords, chiavi) che, se divulgati, compromettono le funzionalita' del modulo crittografico

FIPS 140-2 Level 3 (profilo MICS)

- FIPS 140-2 Level 2 + ...
  - Tamper Resistance (capacita' di resistere ai tentativi di compromissione)
  - Possibilita' di cancellazione automatica dei dati critici in caso di violazione (*".. questo sistema si autodistruggera' entro ...."*)
  - Controllo degli accessi "Identity based" oltre che "Role Based" (*l'utente Riccardo Brunetti puo' eseguire queste e quelle operazioni*)
  - I dati devono transitare da e per l'HSM su canali dedicati (porte ed interfacce specifiche)
  - Software e firmware eseguibili su un comune PC desktop "general purpose" con:
    - SO valutato EAL3 (o maggiore)

In breve

- Per realizzare una CA Online serve:
  - Acquistare un modulo HSM certificato FIPS 140-2 Livello >=3 (stima costo ~ 10 KEuro)
  - Acquistare una WS dedicata con un buon livello di ridondanza HW (RAID, doppio alimentatore ecc..) su cui installare il HSM (stima costo ~ 5KEuro)
  - Un SO EAL >=3 (Red Hat Enterprise Linux 5, Windows 7/Server 2008...)*
  - Un locale ad accesso controllato dentro cui mettere il CA-Server, che sia production-level (UPS, sistema antincendio ecc..)
  - Un firewall che regoli l'accesso di rete alle porte strettamente necessarie al funzionamento del CA-Server
  - Redigere il CP/CPS
  - Almeno 2 persone istruite alle operazioni di manutenzione e/o gestione per quanto possa essere necessario (presumibilmente e' richiesta una frazione piccola del tempo)
  - ....Convincere EuGridPMA

*(vedi anche prodotti specifici nella slide alla fine)

Esempio CA Online del CERN (Ack: Roberto Cecchini)

More slides

FIPS 140-2 Level 1

- Nessuna richiesta di sicurezza fisica
- Richieste di livello base per il controllo degli accessi e di rete (normale ambiente production-level)
- Utilizzo di un algoritmo specificato in uno standard approvato per la crittografia dei dati (*Approved security function)*
- Software e firmware eseguibili su un comune PC desktop “general purpose” senza particolari caratteristiche
- Nessuna richiesta specifica per il SO

FIPS 140-2 Level 2

- FIPS 140-2 Level 1 + ...
  - Tamper Evidence (capacita' di evidenziare i tentativi di compromissione)
  - Controllo degli accessi "role-based" per gli operatori (*l'utente X puo' eseguire queste operazioni*)
  - Software e firmware eseguibili su un comune PC desktop "general purpose" con:
    - SO valutato EAL2 (o maggiore)

FIPS 140-2 Level 4

- FIPS 140-2 Level 3 + ...
  - Ancora maggiore resistenza ai tentativi di manipolazione
  - Cancellazione automatica dei dati in caso di violazione (*".. questo messaggio si autodistruggera' entro ...."*)
  - Protezione per sbalzi di corrente/tensione/temperatura
  - Software e firmware eseguibili su un comune PC desktop "general purpose" con:
    - SO valutato EAL4 (o maggiore) (DigitPA, certificatori accreditati)
  - Indicato per operare in condizioni di assenza di protezione fisica del sistema.

FIPS 140-2 Riassunto

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

FIPS 140-2 Porte

- Ogni informazione gestita dal modulo HSM deve transitare in una delle porte fisiche o logiche specificate per quel modulo
- 4 tipi di porta devono essere specificate:
  - Data Input
  - Data Output
  - Control Input
  - Status Output
- Per i security level 3 e 4:
  - Le porte fisiche o logiche utilizzate per l' I/O di materiale crittografico in chiaro, per le procedure di autenticazione e per i CSPs devono essere dedicate (possibilmente direct-attached).

FIPS 140-2 Authn e Ruoli

- Un modulo crittografico conforme deve poter permettere di autenticare e autorizzare un operatore (e deve essere operato in questo modo)
  - *Role-Based*:
    - E' richiesta una procedura di selezione (esplicita o implicita) del ruolo dell'operatore.
  - *Identity-Based*:
    - E' richiesta una procedura di identificazione dell'operatore oltre che di selezione (esplicita o implicita) del ruolo
- Per Security Level 3 e 4:
  - Necessaria *Identity-Based*

FIPS 140-2 Ruoli

- *User Role*: per le operazioni approvate di routine del servizio (i.e. operazioni crittografiche)
- *Crypto Officer Role*: per le operazioni crittografiche di inizializzazione (i.e. generazione delle chiavi della CA), per le operazioni di gestione dei CSPs e per le operazioni di (self)auditing.
- *Maintenance Role*: per le operazioni di mantenimento dell'hardware e del software. (N.B. quando il modulo e' in maintenance i dati CSPs devono essere azzerati)

FIPS 140-2 Sicurezza Fisica

- Single-Chip: Smart Cards
- Multiple-Chip Embedded: Schede di espansione (PCI) montate su PC
- Multiple-Chip Standalone: HW dedicato

	General Requirements for all Embodiments	Single-Chip Cryptographic Modules	Multiple-Chip Embedded Cryptographic Modules	Multiple-Chip Standalone Cryptographic Modules
Security Level 1	Production-grade components (with standard passivation).	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
Security Level 2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.	Hard opaque tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage.
Security Level 4	EFP or EFT for temperature and voltage.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization circuitry.	Tamper detection/ response envelope with tamper response and zeroization circuitry.

FIPS 140-2 Gestione delle chiavi crittografiche

- Fornisce le specifiche su come deve essere gestito il life-cycle delle chiavi e del materiale CSPs
  - RNG (Random Number Generator)
  - Storage delle chiavi
  - I/O delle chiavi
  - Azzeramento delle chiavi

FIPS 140-2 Sistemi Operativi

- Security Level >=3:
- IL SO deve:
  - Permettere un controllo delle operazioni (execute, modify, read, enter) sui CSPs “role-based”
  - Permettere di proteggere i processi crittografici
  - Permettere di loggare le operazioni crittografiche e sui CSPs (lunga lista di eventi da loggare)
  - Certificato EAL >=3
    - Red Hat Enterprise Linux 5 (EAL 4+)
    - Windows 7/Server 2008
    - ….
- Ci sono anche prodotti specifici
  - Red Hat Certificate System (http://www.redhat.com/certificate_system/)
  - DogTag (http://pki.fedoraproject.org/wiki/PKI_Main_Page)