

## **Hardware Security Modules – What to Look For**

Web location: <http://www.cren.net/crenca/onepagers/hsm.html>

Draft 1.5, November 05, 2001

### **1. What is a Hardware Security Module (HSM)? How does it fit into my campus Certification Authority?**

A Hardware Security Module is a hardware-based security device that generates, stores and protects cryptographic keys. It provides the foundation for a high-level secure campus certification authority. Certification modules are also available in software, but a hardware device provides a higher level of security.

### **2. How do I know if a Hardware Security Module is secure enough for my applications? Are there any universal criteria for rating these devices?**

Yes, there are universal criteria for rating these devices. The criteria are documented in a Federal Information Processing Standard (FIPS) called FIPS 140-1 – Security for Cryptographic Modules.

This FIPS standard provides criteria for evaluating security modules – whether hardware, software, or some combination of hardware and software. The FIPS standard was developed collaboratively by the following agencies: the US National Institute of Standards and Technology (NIST), the US National Security Agency (NSA), and the Canadian Communications Security Establishment (CSE). Security devices are currently rated from FIPS 140-1 Level 1 to FIPS 140-1 Level 4. Higher standards may be developed in the future. The Level 4 standard is for the most rigorous security environments.

### **3. What is a FIPS 140-1 Level 3 Hardware Security Module?**

A FIPS 140-1 Level 3 Hardware Security Module Device meets the FIPS 140-1 Level 3 or higher standard by supporting cryptographic key generation and storage within a hardware environment. At this time, most institutional certificate authorities use a FIPS 140-Level 3 Hardware security module that cannot be physically accessed by unauthorized personnel.

### **4. Are there any advantages to using a FIPS 140-1 Level 3 Hardware Security Module rather than a software only security module?**

A FIPS 140-1 Level 3 validated cryptographic module has a number of significant security and operational advantages over an equivalent software-based cryptographic implementation. The most useful advantage is the more secure environment. The principal value of these hardware modules is that keys can be generated and stored in these boxes, and provide strong protection against removal from the box.

By using hardware root-key protection from the beginning of deployment, an organization can achieve FIPS 140-1 Level 3 security at the outset. The inherent risks associated with software are mitigated because the root key will be and will always have been stored in protected hardware.

For additional information see: <http://www.cren.net/crenca/onepagers/additionalhsm.html>

### **5. Why should a campus have a Hardware Security Module?**

The security and performance benefits offered by a hardware security device provide a critical component in the management and storage of private keys within a security infrastructure. HSMs also supply the infrastructure needed by the finance, government and healthcare sectors to conform to industry and regulatory standards.

## **6. What does the Hardware Security Module protect and secure?**

The heart of trust in a public key infrastructure is the certificate authority (CA) that holds the root cryptographic signing key of the certificate authority. This signing key is used to sign the public keys of certificate holders, and even more importantly, signs its own public key. If this key is compromised, all certificates signed by the certificate authority are suspect, and the CA's credibility is destroyed.

## **7. What are some of the additional protections of using a Hardware Security Module as part of a CA?**

The security of a certificate authority depends on the right tools and the processes [or policies](#) using those tools. Here are some of the specific protections that can be achieved when combining a hardware security module with effective institutional practices and processes.

- Hardware may be less susceptible to system failures and corruptions, such as viruses.
- The content of the hardware module can be backed up to other hardware devices. If one set of hardware is destroyed, a backup set remains either on a duplicate hardware device or in a spare token or card set dependant upon your HSM model. Protecting the content is achieved with the combination of the hardware protections and good operational practices.
- Hardware can protect against internal and external intruders by using two-factor authentication: both the hardware device and a password can be required activate the root key.
- Hardware provides a higher level of security than non-secure media such as backup tapes, floppy diskettes, or smart cards, since the latter can be easily removed or copied.
- Hardware enables you to keep track of the number and locations of copies of root keys that exist.
- Hardware can enable an institution to support controlled access to the activation and use of root keys. Access codes can be distributed among several people who must cooperate to gain access to the root key.

## **8. What are some of the specific disadvantages of a software module or a combination of software and physical barriers to protect a CA?**

Software or a combination of software and physical barriers to protect the root key has the following disadvantages.

- Software alone is vulnerable to viruses, inadvertent erasing, hackers, and complications from system failures.
- Physical barriers, such as vaults, and secured entrances are cost-prohibitive due to the expense of the initial investment and the on-going maintenance costs and do not adequately protect against insider attacks.
- Database backups of the certificate authority's directory may contain a copy of the root key on each backup media, which are not secure and easily copied. This results in multiple copies of root keys existing at any one time with no assurance that additional copies have not been made and removed.

## **9. What are some of the best practices for an HSM architecture**

Best practices are superior methods or strategies that are used by leading organizations to improve their security posture. See the following for a set of Best Practices on security assurance:

[http://www.chrysalis-its.com/news/library/industry\\_white\\_papers/dt\\_best\\_practices.pdf](http://www.chrysalis-its.com/news/library/industry_white_papers/dt_best_practices.pdf)

Acknowledgements: Thanks to Tina Bennett at Chrysalis for the foundation piece from which this FAQ was developed and to the reviewers, especially Ed Feustel at the Dartmouth College PKI lab.