



Redes de Telefonía Móvil, S.A.
División Seguridad Lógica

Cryptographic Hardware to guard cryptographic material in Security Infrastructures

What is Advanced Crypto Module?

Advanced Crypto Module (ACM)² is a hardware platform designed to provide basic security services for applications in the certification, electronic signature, e-commerce and protection of information areas. It is specifically intended to manage, custody and use critical data (both public and private keys), preventing its interception and non-authorized use in highly demanding security environments.

Designed for the efficiency of cryptographic services, it is ready to provide hardware acceleration and to rationalize the use of resources in highly demanding contexts, in terms of performance for encryption, key generation and electronic signature applications.

The FIPS-140 level 3 compliance allows its adoption as a cryptographic key manager and generator/verifier of electronic signatures for certification authorities, OCSP responders, VPN agents, etc. It releases from cryptographic load the processors of web systems, e-commerce and application servers.

Protection and key management

(ACM)² provides complete management of the life cycle of sensible cryptographic material. In scenarios requiring maximum security, keys are generated, stored and used inside the protected cryptographic module, preventing any possibility of interception. The Secure Configuration Terminal of (ACM)² guarantees exclusive management of sensitive information, restricting its access to authorized personnel and allowing the implantation of flexible policies at the same time.

Availability and Performance

As a result of the experience obtained with previous products, (ACM)² allows the establishment of

Advanced Crypto Module



redundant configurations that assure high availability in real time by means of clustering techniques and key cloning procedures. These configurations allow, with no additional elements, the processing load distribution among equipment.

The integral approach in the product design provides extremely flexible configurations: an installation with only two units can act, simultaneously, as a High Availability Cluster and as a Load Balancer system for the most demanding customers' needs. Back-up of keys can be performed by Key Cloning to different (ACM)² units by a means of encrypted exportation of keys, all the above done with procedures compliant with the specifications of the FIPS 140 level 3 standard.

Use of standards and easy integration

In its standard package, (ACM)² is provided with a PKCS#11 interface for its immediate integration with applications (CA, WEB, VPN, etc.). In addition, (ACM)² has a proprietary toolkit; a complete API that makes easy the integration process with any kind of system or the development of new systems that need to use the services offered by (ACM)².

User support

The local manufacturing of this product and the support of an Integration and Development Team permit multiple services to be offered: from the design to the development of "ready to run" solutions for special applications. As an option, (ACM)² provides a Help-Desk and technical support, assuring a quick substitution of out-of-service units within Spain.





Technical Specifications

Available Algorithms

Public key algorithms

RSA

- ✓ Key generation (256 to 4096 bits).
- ✓ Generation and verification of electronic signatures.
- ✓ Encryption and decryption both with public and private keys.
- ✓ Padding:
 - PKCS#1 (v. 1.5)
 - no padding

DSA

- ✓ $2^{L-1} < p < 2^L$, with $512 \leq L \leq 1024$

Diffie Hellman

- ✓ Parameters generation (128 to 4096 bits primes).
- ✓ Derivation of keys.

Private key algorithms

- | | | |
|--------|--------|--------|
| ✓ DES | ✓ RC-2 | ✓ AES |
| ✓ 3DES | ✓ RC-4 | ✓ IDEA |

Hashing algorithms

- | | |
|-----------|--------|
| ✓ SHA-1 | ✓ MD-2 |
| ✓ SHA-256 | ✓ MD-5 |

Standards

- ✓ Certified by the Centro Criptológico Nacional*, Spain.
- ✓ FIPS 140 level 3 compliance.

Random Number Generators (RNGs)

- ✓ Three concurrent random numbers generators.
- ✓ Continuous checking of random numbers quality.
- ✓ Protection system against potential degradation of the RNGs random numbers quality.

Interfacing

- Supported connectivity
 - ✓ PKCS#11 v. 2.01 (Windows XP, 2003, 2000, NT 4.0, Solaris Sparc).
 - ✓ PKCS#11 v. 2.01 (Linux Intel in development).
 - ✓ Sun PKCS#11 Java provider (Win32 Intel & Sparc).
 - ✓ OpenSSL Engine (Win32 Intel & Sparc).
 - ✓ Application protocol documentation available (development toolkit available).
- 10/100 Mbps Ethernet data port.

*



Active protection

- ✓ Hardware active system for intrusion detection and "zeroization" of keys.

Administration

- ✓ Secure Configuration Terminal (SCT).
- ✓ Support for flexible policies management. Up to four administrators.
- ✓ Up to four administrators.
- ✓ Control of unit status.
- ✓ Control of key policies management.
- ✓ Event logging inside the "Network Security Process Unit" (NSPU).

Physical characterization

- Network Security Process Unit (NSPU)
 - ✓ The unit is presented as a device to be located inside a 19" rack (2U height).
 - ✓ Capable of operation both rack-assembled and desk-mounted.
 - ✓ Frontal Control Panel with physical control access for administration activities.
 - ✓ Frontal Information Panel for continuous control of the status of the NSPU.
- Secure Configuration Terminal (SCT)
 - ✓ Stand-alone device for the NSPU administration and control. It has an alphanumeric keyboard, display and control port.

Applications

- ✓ Certification infrastructure elements: Certification Authorities, Registry Authorities, OSCP Responders, etc.
- ✓ Acceleration of protocols with massive cryptography needs (SSL, TLS, SSH, SET, IPsec).
- ✓ Electronic commerce systems.
- ✓ Environments with storage and retrieval of sensitive and personal data.



Redes de Telefonía Móvil S.A.
División Seguridad Lógica
Avda. Castillos 1024
28918 Leganés. Madrid, Spain
Tel: +34 91 610 37 66
Fax: +34 91 610 68 22
<http://www.retemsa.com>