

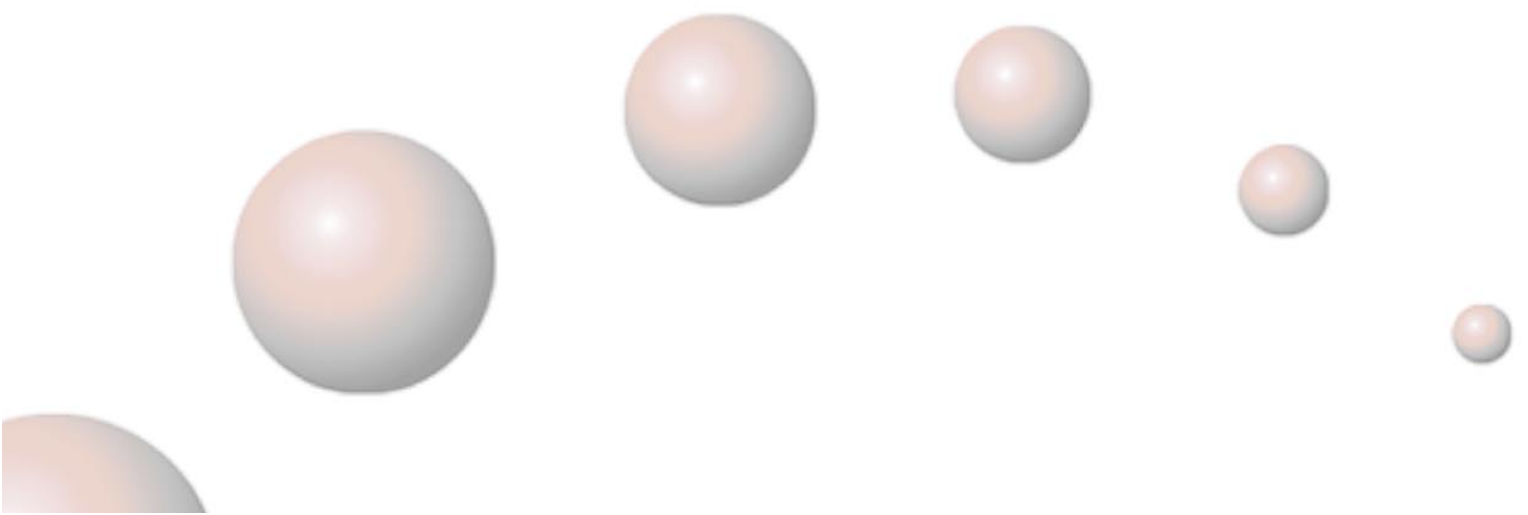


Asset Custodian Manager

Advanced Crypto Module
(ACM)²

(Version 1.0)

Technical Specifications



Integration with products

(ACM)² is a service provider that is easily integrated with software applications needing integral key management, rationalization and an acceleration of cryptographic processing.

At present, integration is immediate with the following products:

- KeyOne CA, Safelayer Secure Communications S.A.
- Entrust Authority, Entrust Inc.
- UniCERT CA, Baltimore Technologies
- CertValidator, CertCo, Inc.
- Sun ONE Certificate Server (IPlanet Certificate Management System), Sun Microsystems, Inc.

Connectivity with products

Applications can use the services offered by (ACM)² by means of a specific PKCS#11 v2.01 token.

At the moment, new interfaces are in development to guarantee integration with new commercial products and to offer alternatives for connectivity for customers' specific applications. Developments in process include connectivity with products based in:

- Microsoft CryptoAPI
- OpenSSL

Integral security

(ACM)² is a product designed to provide customers with the maximum level of confidence by guaranteeing compliance with demanding industry security standards. Taking advantage both of physical and logical security services, the product is able to meet the FIPS 140 level 3 standard.

The standard 140 of the Federal Information Processing Standard (FIPS) of the National Institute of Standards and Technology (NIST) establishes a security model recognized by the industry and allows an objective comparison between the existing commercial cryptographic modules. In the practice, the industry recognizes a FIPS 140 level 3 as a guarantee of proper management of high sensibility cryptographic material (identity private keys of certification authorities, registry authorities, entities that validate certificates, etc.).

The cryptographic module of (ACM)² is in validation stage, in an independent laboratory accredited by NIST, to obtain the level 3 FIPS 140 certification.

The main characteristics of the cryptographic module of (ACM)² are the following:

- Physical protection of the perimeter of the cryptographic module by means of a self-designed strongbox.
- Self-developed active intrusion detection system that protects the physical perimeter of the cryptographic module. The system is always operative since its first activation in factory stage, its operation is continuum and independent of external power feed and provides for protection for 5 years without battery replacement.
- Evidence of intrusion in the protection box and removal evidence seals.
- Permanent indication of intrusion attempts with a luminous alarm.
- Physical protection of keys: keys are generated and used inside the cryptographic module only.
- Logical protection of keys: any key that goes through the cryptographic perimeter does it inside a "digital envelope", that can be opened only inside the cryptographic module.
- Protection of stored keys: any key stored inside the cryptographic module is encrypted by a module specific "master key". The encryption master key is generated and stored inside the cryptographic module and it cannot be extracted from it. Any equipment has a different master key during the life cycle of the product. Created after the first activation of the intrusion detection system while in factory, neither the manufacturer can access its value.

Flexibility establishing management policies

The (ACM)² management system is designed to allow multiple management models using distribution of knowledge for authentication. It is possible to assign different administrative tasks requiring up to four administrators.

Management tasks are independent from the life cycle of user keys. The use of (ACM)² services do not imply any capability for administration. The administration of (ACM)² systems do not mean the capability of possible generation, substitutions or use of user keys.

The product enforces physical presence of administrators for management tasks. Establishment of policies that involve tasks delegations are also possible for daily operations.

Complete management of the life cycle of keys

The (ACM)² basic service is the management of the complete life cycle of keys. Any key, since its creation inside a cryptographic module, is associated to a specific operation environment, in such a way that its use is limited exclusively to the set of cryptographic modules that composes the environment. Optionally, a key can be assigned to a new operation environment, if required and considered possible in a specific operational scenario, and only with express authorisation of the administrators of the involved environments.

The highest guarantee of control of the life cycle of keys can be obtained by persistent storing of private keys inside the cryptographic module. (ACM)² has a store of RSA keys with a capacity to 2000 keys.

Safe and flexible Exportation and Importation of keys

(ACM)² includes an exportation and importation system for keys. The exportation of a key consists of an extraction of a "digital envelope" from the inside of the cryptographic module that hosts the key. The importation consists on the inverse procedure, by which a digital envelope that contains a key is inserted in the cryptographic module for its use.

The key contained in a digital envelope can be unwrapped inside an (ACM)² only, and exclusively under previous authorisation of the administrators of the operation domain that owns the key.

There exist many operational uses for digital envelopes of keys, among others the most useful can be mentioned:

- dissemination of keys in scenarios with massive and increasing use of cryptographic resources
- replication of systems for fault-tolerant configurations and for distribution of cryptographic load in equipment clusters
- backup copies

A strict control is applied to the exportation and importation of keys. A digital envelope that holds a key generated by an equipment belonging to a certain domain cannot be imported by another equipment of a different domain if there is not a previous express consent from the administrators of both realms.

Available configurations

There exist different models of operation implantation of (ACM)² equipment intended to prevent important problems of exploitation that can degrade the level of service:

- Fault-tolerant configurations
- Redundant configurations
- Configurations to the distribution of Cryptographic load.

Fault-tolerant configurations allow the maintenance of the service even when sporadic failures can occur in the availability of (ACM)² equipment or even in auxiliary infrastructure systems.

Redundant configurations guarantee high availability of management and cryptography services. Clustering (ACM)² systems in a domain, together with the replication of its key stores guarantee high levels of availability. Mechanisms for detection of unavailability and setting up for alternative

service equipment, both automatic and manual, are offered as part of the standard packages for customers.

Configurations for the load distribution of cryptographic process allow, by means of relating (ACM)² units into clusters inside a domain, to distribute the process requests in order to guarantee a low response times and controlled latencies. The clusters of (ACM)² units can grow in number, by “warm” insertion of new units even while in-service, to adapt its processing capabilities to meet customers’ needs anytime, on a on-demand basis. Different strategies of processing load distribution are offered, together with the possibility of using third parties traffic balance systems.

All configuration methods mentioned, include the capability of “warm” insertion and extraction of (ACM)² units in a cluster while in-operation, without disturbances to the service.

Secure execution environment for applications

(ACM)² is a secure environment for processing and storage. It is possible to execute customers’ applications inside the cryptographic module, thus achieving for these and its associated data the highest level of protection.

Key management event recording

(ACM)² hosts a recording system for key-related events inside its cryptographic module. Any relevant event related to key administration can be recorded and checked by the administrators.

Non-tampering product delivery warranty

(ACM)² has a built-in certification system of non-manipulation. Any unit manufactured or revised by authorised technicians is delivered to the customer with an activated initial status hardware marker, non repeatable during the service life cycle of the system.

