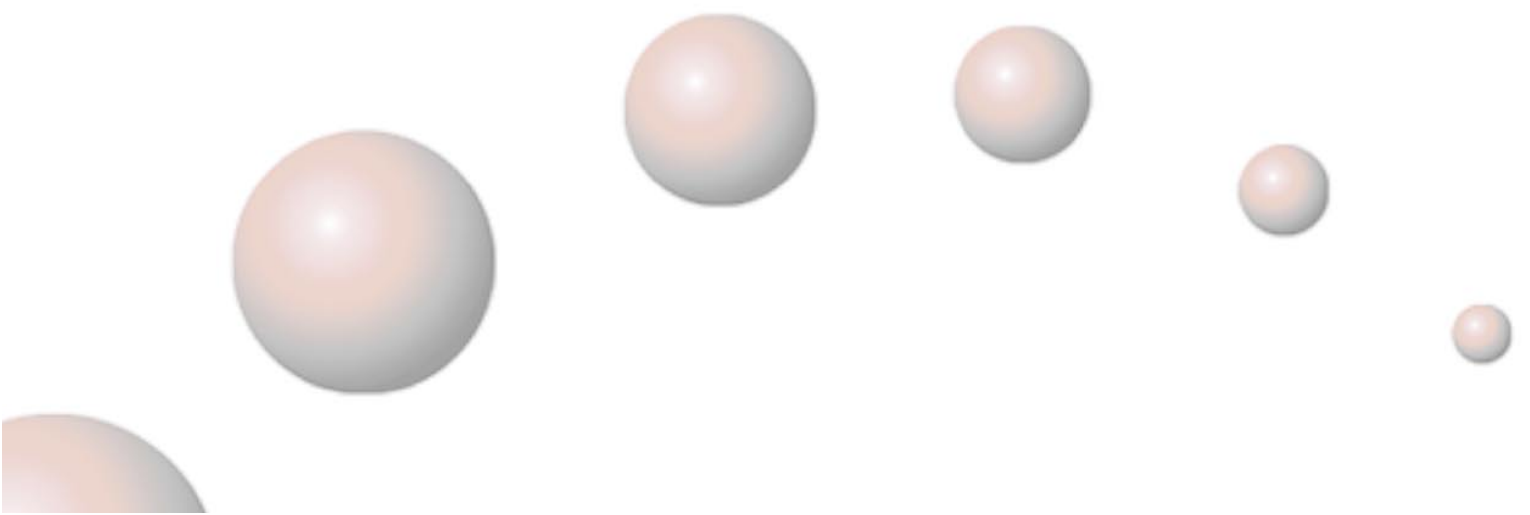




# Key Source Module

Version 1.0

## **Technical Specifications**



## Key Source Module (KSM) features

KSM is a solution designed to solve and simplify the problem of quality keys generation in cryptography.

The system provides **true random numbers** and **prime numbers** for its use in highly demanding environments in terms of **control** and **quality** in random data.

Its core includes hardware equipment designed to generate, check and validate the quality of the obtained random series, as well as strong prime numbers.

The product is intended to serve as a highly reliable solution for environments where cryptographic services are used and where keys are extremely sensitive or generated in large batch processes.

KSM guarantees controlled response times for key generation operations in massive batch tasks. An internal system validates random and prime numbers works continuously. It generates, validates and securely stores random and prime numbers until requested to be extracted and used.

## Comprehensive Solution

KSM includes an autonomous **physical device** that can be used by means of an **application**, used for the extraction of random numbers, prime numbers, cryptographic keys and a variety of secondary parameters. The available capabilities for the configuration of the application are such that permit:

- Generation of RSA keys with lengths between 512 and 4096 bits, with strong prime numbers and with configurable public exponent values.
- Generation of Diffie-Hellman parameters with prime parameter length between 512 and 4096 bits.
- Extraction of prime numbers and true random numbers from KSM.
- Private key generation and formatting using a macro-based language and optional plug-ins.

The application allows the extraction of the information generated using different standard formats:

- RSA keys in PKS#1 format or PKCS#12 encapsulation.
- Prime numbers in ASN.1 DER format or PKCS#12 encapsulation.
- Diffie-Hellman Parameters in ASN.1 DER format or PKCS#12 encapsulation.
- Random private keys in any format.

Any random private key can be sent to different outputs: a file, a parallel port device or a serial port device, for its injection into dedicated equipment.

## Advantages

- **True random** generation of bit streams. Unlike most commonly used procedures of generation of pseudorandom numbers, KSM provides 3 hardware generators of true random numbers. This guarantees the quality of the obtained keys in terms of predictability. An orthodox use of pseudorandom number generators implies the contribution of real random numbers (the seed numbers) from the outside of the system. KSM provides true random number generators without any external need: **they do not require any maintenance.**
- **Batch processing** for the statistical validation of random numbers and strong prime numbers. Being able to serve “high quality” random numbers and strong primes implies the use of strict and heavy-weighted algorithms. KSM validates and generates strong prime numbers continuously and serves that stored and validated information to the user on a request basis, guaranteeing reduced response times without compromising quality.
- Technology based on **standards**. The product, since its conception, has been designed to comply with standards. As an open architecture, the system can be integrated with third-party products.

## Connectivity

KSM provides an application development environment that facilitates integrations compliant with customers needs. Successful integrations can be performed under highly demanding security requirements. The development environment is a highly productive tool that easily enables taking advantage of all benefits of KSM.

KSM offers different connectivity options for its integration with different technologies.

## Integral security

KSM is designed to offer the highest level of confidence to customers by guaranteeing the most demanding security levels. The design of the product has been done according to physical and logical security standards.

The cryptographic module of KSM is compliant with the physical and logical requirements demanded by the NIST FIPS PUB 140 standard for its security level 3.

The Federal Information Processing Standard (FIPS) 140 standard of the National Institute of Standards and Technology (NIST) is an industry market recognized model that allows for the comparison between the existing offer of cryptographic modules. In a pragmatic way, the industry

recognizes the level 3 of security as a guarantee for the management of highly sensitive cryptographic material.

Main characteristics of the cryptographic module of KSM 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 sensible information: true random numbers and strong primes are generated, validated and stored inside the cryptographic module until they are used.
- Logical protection of sensible information: any true random number or strong prime that goes through the cryptographic perimeter does it inside a cryptogram, only useful to the authorized user.
- Protection of sensible information: all sensible information (true random numbers, strong primes and keys) 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 cycle of life of the product. Created after the first activation of the intrusion detection system while in factory, neither the manufacturer can access its value.

## **Flexibility and secure management**

The KSM management system is designed to allow a simple and powerful administration model. The product enforces the physical presence of administrators for management tasks. Establishment of policies that involve task delegations are also possible for daily operations.

## **Simple configuration**

KSM has been conceived as an autonomous and specialized system for an easy deployment and configuration. These characteristics support the control of the general security level of the scenarios where the product is integrated. The physical KSM equipment is connected to the operative system with a data cable, and receives standard power feed. The physical security perimeter includes the whole set KSM –equipment that hosts the application.

Maintenance of KSM can be easily performed, being its insertion and removal possible with a minimum previous qualification.

## **Non-tampering product delivery warranty**

KSM has a built-in certification system of non-manipulation. Any unit manufactured or revised by authorized technicians is delivered to the customer with a deactivated alarm marker, non-repeatable during the service cycle of life of the system.

