



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

Key Source Module

High quality and performance key generator and distributor module



What is Key Source Module?

KSM is a comprehensive solution designed to solve the problems of key **generation** and **distribution** both with confidence and performance. KSM solves the problems of high quality key generation, using own-technology hardware random number generators. It is possible to program self-designed key formats in a simple and operative manner.

Presented as an autonomous hardware device used by an application, the system can be easily installed and can operate with a minimum of maintenance. Its simplicity allows its strict management and control.

KSM allows for fast integration in scenarios that need administration and use controlled by restrictive policies. Its administration and use model offer the highest level of flexibility, always guaranteeing control in the configuration and operation.

Applications

KSM is a complete solution to solve the problems of generation and distribution of quality keys for cryptography and other protected protocols of communications. Other environments of application include the simulation and system tests, uses in games of chance and resolution of mathematical problems

What are its advantages?

Generation of random numbers by means of self-designed hardware devices. The entropy contributed by stochastic physical phenomena sampled by hardware devices in KSM allows to rely on true non-determinist random series. This

represents a fundamental qualitative step, opposite to the techniques based on the use of pseudorandom series, possibly fed with random seeds.

Key generation based on true "high quality" random series. All usable random series coming from the RNGs pass extremely strict randomness tests before being used for keys generation. For comparison purposes, the randomness tests used demand a much higher level of quality than the required in FIPS 140.

Sensible information secure storage and batch processing. KSM has been designed to allow secure storing of validated random series and prime number generated inside its protected cryptographic module. The use of prevalidated series and prime numbers drastically accelerates the generation of keys in batch processing.

A **design based on standard** makes possible the immediate integration in open architectures, minimizing any integration existing cost.

Customer support

The KSM solution can be associated to a **Maintenance Program**. This Program includes qualified technical assistance, as well as availability for fast substitution of equipment when any hardware failure occurs.





Technical Specifications

Key Characteristics

Random generators

- Based on sampling of the noise effect in p-n unions.
- Three independent hardware sources available.
- Integrated hardware bias correction.

Integrated randomness tests

- Serial test
- Bigrams
- Increasing and decreasing rounds
- Serial correlation
- Frequencies
- Poker
- Length of rounds
- Monotonic series

Prime numbers generation

- Strong primes with length between 128 and 4096 bits.
- Configurable Rabin-Miller primality test.

Secure information storing

- 50 Mbytes of internal store for validated random series and prime numbers.
- Active intrusion detection and zeroization system.

Certificaciones

- Certified by the Centro Criptológico Nacional*, Spain.

Keys generation

- RSA (512 to 4096 bits).
- Diffie-Hellman parameters with prime P between 512 and 4096 bits.
- Format description language for private keys
 - Many binary and private textual formatting options based on macros.
 - Formatting available for dumping on printer and serial port.
 - Basic macro formatting and complex transformations available with plug-in applications.

Administration and protection

- Access control managed by KSM.
- Physical administration policy enforced.
- Administration with removable secure pinpad (device only needed during administration tasks).
- Advanced authentication and optional biometric authentication mechanisms.
- Active intrusion detection and zeroization system inside the cryptographic module (according to FIPS 140 specification).

Audit

- Users and administrators logging of activities.
- Log database located inside the cryptographic module of KSM.



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