



### Generation of EMV/CEPS card holder files

This module will generate the personalization files of holder cards for the future credit/debit chip cards, Electrón, Visa Cash, electronic purse, etc. both for Visa and Mastercard, as well as other sort of defined cards or to be defined cards.

All generation processes make a strict verification of possible errors or incongruity guaranteeing a secure process.

### Generation of PSAM/LSAM holder files

As mentioned before, the needed output files to personalize chip cards for purse terminals CEPS will be generated, which means PSAM specification and also cards for purse load terminals (LSAM).

### Certificate and public key management of CAs for EMV

With this module we will be able to:

- Import Visa EMV public keys.
- Import MasterCard EMV public keys.
- Generate certificate request of the EMV issuing company.
- Import certificates of the EMV issuing company.

Generación de petición de certificado EMV Visa

BIN 500000

Clave Pública  
Longitud del módulo 896  
Exponente 3

Descripción del Certificado  
cert

Certificado  
Caducidad octubre de 2008

Identificador de Servicio CREDIT/DEBIT

Tracking Number 000001

OK Cancel

### Certificate and public key management of CAs for CEPS.

With this module we will be able to:

- Import public keys for issuing company and cardholder, both VISA and MasterCard
- Generate the certificate request of the CEPS issuing company to Visa and MasterCard's CAs.
- Import certificates of CEPS issuing company.
- Generate the cardholder's certificate request CEPS to Visa and Europay/MasterCard's CAs.
- Import certificates of CEPS cardholder.



### Cryptographic hardware management (HSM)

Allows for a security copy of all the RSA keys in file format, which are stored in the cryptographic module.

In this backup process we will take out from the HSM all asymmetric keys coded (ECB /3DES with triple key length) in order to safeguard these keys or make an exact copy of them in another HSM. You will also be able to manage a precise key with its own backup key.

In a key recovery process, the cryptographic module must have loaded the same backup key as the one that was loaded at the HSM which coded the RSA key file.

### Process control

This module will control the performance of the pre-personalization process, providing a file together with the pre-personalization one and a detailed report of the process results. (Audit log)

This file will show the operator who has accessed the application, as well as the access date, access time and any other performed operations.

### Technical Requirements

- Pentium II or higher with at least 64MB RAM and a free PCI slot.
- Windows NT Server or Workstation with Service Pack 5 or later.
- Internet Explorer 5.0 or posterior.
- Cryptographic Card Cryptosec (included).



Realia Technologies, S.L.  
C/ Orense, 68 Pl. 11  
28020 Madrid

Tif.: +34 - 91 449 03 30 / Fax: +34 - 91 579 56 06  
info@realsec.com  
www.realsec.com