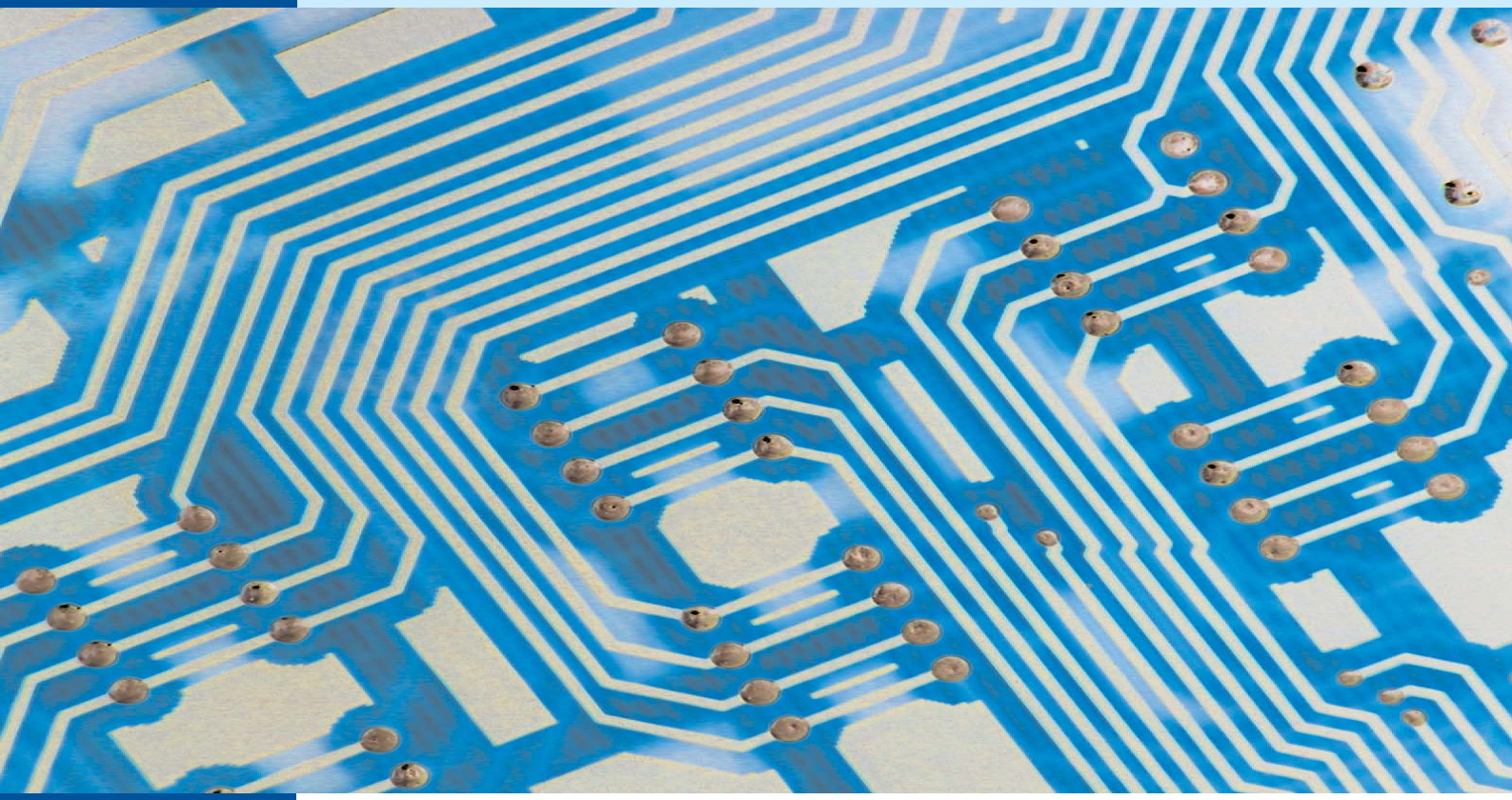

myHSM, the smart card HSM solution

An easy to use, highly secure, cost effective Hardware Security Module supporting all EMV related functions.

The HSM (Hardware Security Module) is a cornerstone component in EMV migration, responsible for securely storing the secret keys and processing cryptographic computations.

myHSM provides all the features needed for EMV in full compliance with standards: issuer key generation, card production (SDA and DDA), card issuance, transaction processing and clearing.

Also ready for e-commerce and online authentication applications, myHSM can verify most of the available cryptograms including ISO 9797-1 and MasterCard SecureCode CAP.

Designed both for production and test uses, my HSM is dramatically easy to use: all operations can be carried out in only one step, yet allowing for any type of computation, even the most complex.

The security of the myHSM module is guaranteed by a FIPS 140-2, level 3 certification, which meets the highest standards of security currently available.

Thanks to smart card technology, Iteon is proud to offer myHSM for only a fraction of the price of other HSMs. The use of a standard smart card platform instead of proprietary hardware allows us to propose great security at a low price.

myHSM is based on a flexible architecture allowing for the integration of new cryptographic algorithm or security methods, upon request.

EMV Transaction Processing and Clearing

- Authorisation Request Cryptogram (ARQC)
- Authorisation Response Cryptogram (ARPC)
- Transaction Cryptogram (TC)
- Application Authentication Cryptogram (AAC)

EMV Cryptograms supported

- MasterCard Cryptogram with M/Chip 2.1 and EMV 2000 session key derivation methods
- Visa Cryptogram version 10, 14
- JCB Cryptogram version 01, 02, 03

Online Authentication

- MasterCard CAP authentication token verification
- Generic ISO 9797-1 MAC generation and verification

EMV Issuer Cryptography and Card Issuance

- Signing of Static Data for Static Data Authentication
- IC Card secret key derivation

Key management

- Secure key storage
- Key - Profile Separation
- Mechanisms for key exchange
- Detailed key usage control
- Split secrets
- Control of key custodians: PIN code, smart card authentication

Algorithms supported

- DES, triple-DES
- RSA
- SHA-1

Form factor

- ISO 7816 smart card, card format (ID-1)
- ISO 7816 smart card, mini-SIM format (ID-0)
- USB token

Standards

- EMV 2000, ICC specifications for payment systems, version 4.0, December 2000
- EMV 2000, Issuer and application security guidelines, version 1.2, July 2003
- EMV Card Personalization Specification, version 1.0, June 2003
- Global Platform specifications for Key Management System (KMS) and Key Profile
- ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes Part 1: Mechanisms using a block cipher
- MasterCard, M/Chip 4 Card Application for Credit and Debit, version 1.0, October 2002
- Visa ICC, Card Specification, version 1.4.0, October 2001
- MasterCard SecureCode, 3-D Secure Chip Authentication Program (CAP), version 1.0, March 2003

Security

- FIPS 140-2 level 3 certified cryptographic module

myHSM product catalog

- ref#04149-01 - **Starter kit**: includes end-user licence, one myHSM module, documentation, basic PC software
- ref#04149-02 - **myHSM module**, card (ID-0) format
- ref#04149-03 - **myHSM module**, card (ID-1) format
- ref#04149-04 - **myHSM module**, USB token format
- ref#04149-05 - **security officer access card**

Iteon
6, rue Camille-Desmoulins
92300 Levallois-Perret - France

Phone: +33.1.5676.6026
Fax: +33.1.4759.0736

Email: info@iteon.net

www.iteon.net