Utimaco's hardware security module CryptoServer 2000 can serve as EPSS Security Platform (EPS) in MasterCard Europe's EPS Net.

ESP Functionality available on the CryptoServer:

Magnetic Stripe Card Production Functionality

Card production functionality required for Pay Now/Pay Later products on magnetic stripe cards:

- PIN Generation (according to ISO 9564-1: 1991)
- PVV Generation (according to the MasterCard/Visa algorithm and, on demand, also according to issuer-proprietary algorithms)
- CVC Generation (according to the MasterCard Europe algorithm and, on demand, also according to issuer-proprietary algorithms):
  - CVC1 Generation
  - CVC2 Generation

Magnetic Stripe Card Authorization Functionality

Authorization functionality required for Pay Now/Pay Later products on magnetic stripe cards:

- PIN Verification using PVV (according to MasterCard/Visa PVV algorithm and, on demand, also according to issuer-proprietary algorithms)
- CVC Verification (according to the MasterCard Europe algorithm and, on demand, also according to issuer-proprietary algorithms):
  - CVC1 Verification
  - CVC2 Verification

Chip Card Authorization Functionality (according to EMV 2000)

Authorization functionality required for Pay Now/Pay Later products on chip cards, compliant to the EMV 2000 standard:

- PIN Verification On-line
- ARQC Verification
- ARPC Generation
- TC Verification
- AAC Verification
- Secure Messaging (MAC Calculation and/or Message Encryption)
- DAC Verification (Data Authentication Code)
- IDN Verification (ICC Dynamic Number)

Here all cryptogram verification respectively generation commands (ARQC Verification, ARPC Generation, TC Verification, AAC Verification) and the Secure Messaging functionality are implemented according to the M/Chip 4 scheme (MasterCard, recommended in EMV 2000 specification). Implementations of MasterCard's M/Chip 2.1 scheme or the UKIS scheme (UK ICC Specification) are available on demand.

Functionality for the Integration with EPS Net

The following functionality block is mandatory for the communication between the ESP and the NSPs (Network Security Platforms) within the EPS Net. For this purpose keys have to be exported which secure the exchange of ISO 8583 messages and PIN blocks between NSPs and ESP.

- Export of dedicated Triple-DES Keys (encrypted and integrity protected):
  - MAC Generation Key
  - MAC Verification Key
  - PIN Block Encryption Key
- PIN Block Decryption and PIN Verification (for different PIN block formats, using this PIN Block Encryption Key)
- MAC Generation and Validation (using the MAC Generation Key and MAC Verification Key)

Functionality for On-behalf Services offered by MasterCard Europe:

This functionality block is recommended for issuers which use the MasterCard Europe's On-behalf Authorization Services for their authorization system. It comprises Key Management functionality intended to exchange operational keys between the ESP and MasterCard Europe.
It can be chosen between a key hierarchy of three levels or of two levels:

For the three-level key hierarchy method, the (symmetric) operational keys which will be transported from the ESP to MasterCard Europe are secured by a (symmetric) transport key pair. This transport key pair will be imported in the ESP by a public key method.
For the realization of this method, the following commands are available:

- Generation of RSA key pair (issuer-owned public key)
- Import of a MasterCard Europe-owned public key (in form of a - self-certified - EMV certificate)
- Import of check value of MasterCard Europe-owned public key
- Export of issuer-owned public key (self-certified with EMV certificate)
- Export of check value of issuer-owned public key
- Import of transport key pair (encrypted and signed with the resp. public keys)
- Export of operational keys (secured by transport key pair: encrypted and MAC authenticated):

For the two-level key hierarchy method, first a (symmetric) transport key pair goes – following the 3-persons rule - from MasterCard Europe to the ESP; later the (symmetric) operational keys go – secured with the transport key pair - from the ESP to MasterCard Europe.
Thus the following commands are available:

- Import of transport key pair in 3 components (over directly connected PIN-Pad, fitting for 3-persons rule)
- Export of operational keys (secured by transport key pair: encrypted and MAC authenticated)

Optional functionality block which is available on demand:

Functionality required for Electronic Purse (Clip):

- PIN Verification On-line
- Linked Load Transaction (Load Authorization and Verification):
  - Load S_1 MAC Verification
  - Load S_2 MAC Generation
  - Load S_3 MAC Verification
- Unlinked Load Transaction (Load Authorization and Verification):
  - Load S_1 MAC Verification
  - MAC_{LSAM} Verification
  - Unlinked Load S_2 MAC Generation
  - Load S_3 MAC Verification
  - $R2_{LSAM}$ Verification
- Unload Transaction:
  - Unload S_1 MAC Verification
  - Unload S_2 MAC Generation
  - Unload S_3 MAC Verification
- Currency Exchange Transaction:
  - Currency Exchange S_1 Verification
  - Currency Exchange S_2 Generation
  - Currency Exchange S_3 Verification
- Purchase Completion Transaction:
  - S_6 MAC Verification
  - S_6' MAC Verification
  - S_6'' MAC Verification
- Secure Messaging (if recommended in future)