

Migrating smoothly to EMV



CRYPT2Pay™

When it comes to payment transactions, security is one of the most important issues. Banks and financial institutions may suffer considerable financial losses in case of fraud. Reliable and flexible protection solutions are required which integrate into payment systems. In close collaboration with major international banking networks, financial institutions and strategic partners, Bull has designed a range of Hardware Security Modules called CRYPT2Pay™ that meet today's market requirements.

CRYPT2Pay™ is a high performance encryption device designed to protect withdrawal and payment transactions, carried out with a bank or private card, contact or contactless, and all operations made in bank card processing centres (production and printing of PIN code mailers, data preparation for card personalization and transaction switching between different networks).

The CRYPT2Pay™ product range uses the latest cryptographic technology. It adapts to different uses with a high level of reliability. With CRYPT2Pay™, financial institutions may download the applications they need.

Already chosen by several major European banks, CRYPT2Pay™ brings the security indispensable for payment transactions.

The CRYPT2Pay™ product range provides the following applications:

- Transaction acquisition;
- EMV and magnetic stripe authorisation (VISA, MasterCard, American Express);

- PIN management;
- PIN printing;
- Card audit and PIN unblock: PAYDiag Server;
- Applications for private cards;
- 3-D Secure™ issuance and authorization;
- EMV and magnetic stripe data preparation;
- Key Management Centre.

In addition, new functions can be easily uploaded on the HSM to ensure upgrading to the latest market evolutions.

CRYPT2Pay™ is a universal module available in low, medium and high speed, offering a large variety of options and connection protocols.

A European leader in integrated security

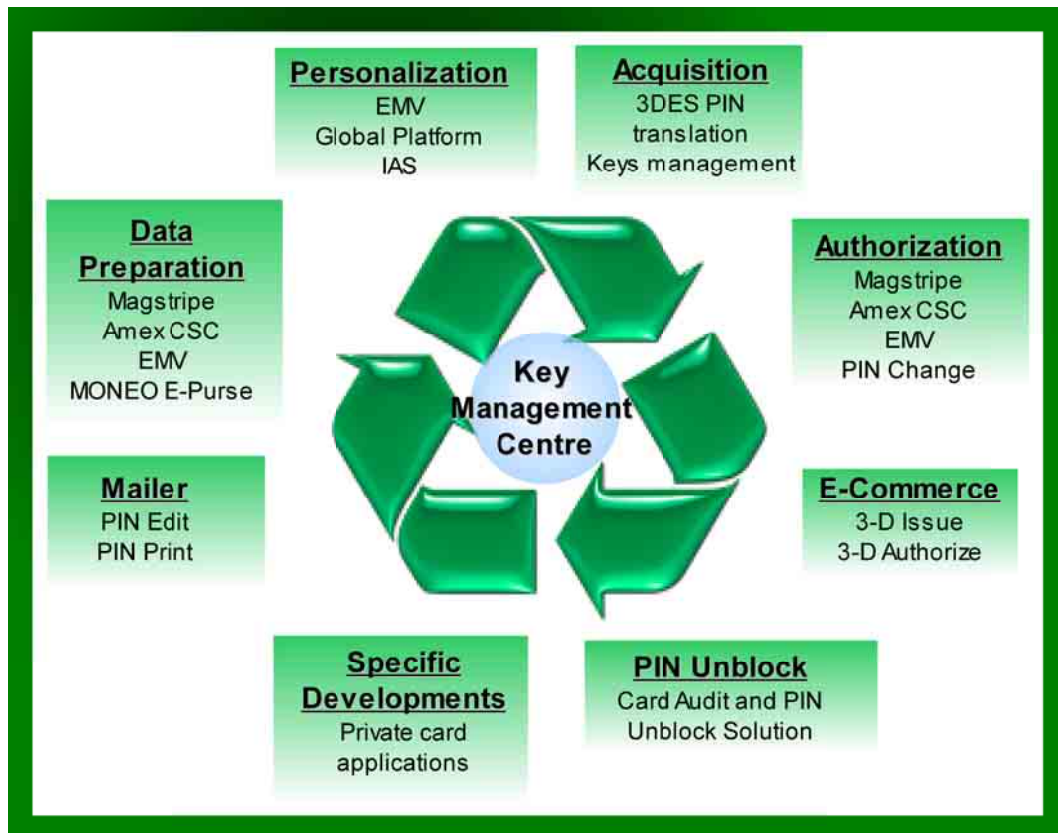
Bull has built up a unique body of expertise in information systems security, bringing together consulting and systems integration expertise and an in-depth understanding of corporate security technologies.

SECURITY SERVICES



Architect of an Open World™

Crypt2Pay™ functions



Acquisition

With CRYPT2Pay™, banks can migrate smoothly to EMV by implementing triple DES on their payment systems (VISA, MasterCard, European standard key management).

Authorization

CRYPT2Pay™ provides secure mechanisms to manage either smart card (contact or contactless) or legacy magstripe card transactions.

E-Commerce

VISA developed the Three-Domain Secure protocol to improve on-line transaction

performance, and accelerate the growth of e-commerce. The protocol, also used by MasterCard, is based on authentication of the card holder by the card issuer.

PIN Unblock Solution

PAYDiag Server

Card Audit and PIN Unblock

In close collaboration with financial institutions, Bull has designed a fast and inexpensive solution to deal with blocked cards. Under the control of the authenticated branch manager, the EMV card is audited and the PIN unblock operation is carried out. Banks save card replacement costs and the customer returns

satisfied with a working card. The benefits of the central management server are ease of use for the branch manager and the user friendly PC or POS display.

Specific Developments

Thanks to its customer based experience, Bull has designed a package to meet customer development needs at lower costs.

A highly-skilled team is available to provide assistance to operators and their application programmers.

Mailer

To print PIN codes on a secure envelope, two architectures may be implemented. The PIN Edit function decrypts a PIN block and returns the PIN to the server which controls the printer.

The PIN print function decrypts a PIN block and prints it on a printer connected to its serial port.

Data preparation

CardLink Data Preparation Solution

CRYPT2Pay™ is fully integrated into the

CRYPTOMATHiC CardLink solution. CardLink is a system for preparing EMV data, which is used for issuing single and multi-application smart cards. The solution interfaces with major card management systems.

Securing banking networks

With more than 25 years in financial security, Bull has gained considerable professional experience in securing banking networks. Bull's teams can provide financial institutions with integration

services, architecture consulting, worldwide maintenance and support services. Thanks to a network of recognised partners, Bull takes an active part in implementing comprehensive payment systems with renowned software publishers such as ACI Worldwide, ATOS Worldline, CRYPTOMATHiC, e-Funds, Jware Technologies, Magellan, S2M, Steria and others. Many banks and card centres worldwide already rely on Bull's technology and experience.

Security, flexibility, scalability	Cryptography	Technical features
<ul style="list-style-type: none"> • Tamper resistant design: MEPS 2 approved, FIPS 140-2 level 3+; • Several coprocessor speeds: 90 PVV / 200 PVV / 2000 PVV; • Multi-purpose HSM with different customizable packages. <p style="text-align: center;">Full compliance</p> <ul style="list-style-type: none"> • EMV 4.2 CPA; • Visa VIS 1.4.0; • MasterCard Mchip 4.0; • AMEX CSC™; • 3-D Secure™; • PayPass; • PayWave. 	<ul style="list-style-type: none"> • DES: DES and triple DES keys; <ul style="list-style-type: none"> • Encryption and Decryption; • MAC computation and verification; • RSA: Keys up to 2048 bits: <ul style="list-style-type: none"> • Key pair generation; • Encryption and Decryption; • Signature generation and verification; • SHA-1, SHA-256: hashing functions; • HMAC: encryption and decryption; • AES: 128, 192 and 256 bit keys; • ECDSA: Key generation. 	<ul style="list-style-type: none"> • Performance: 90 - 200 – 2000 PVV tps; • Voltage: 85-264 Vac; • Frequency: 47-63 Hz; • Humidity: 30% - 70% non condensing; • Operating temperature: 10/45°C; • Dimension: 440x270x65 mm; • Weight : 9 Kg.

