GM1130 Host Security Module

文档参考号：GMN14BJ0403011

北京江南歌盟科技有限公司

BEIJING JIANGNAN GEMEN TECHNOLOGY CO., LTD.

二○一四年七月

GM1130 HOST SECURITY MODULE

The GM1130 HSM is a tamper-resistant device that provides the cryptographic facilities necessary for securing transactions in financial networks.
The HSM is used to secure a multitude of financial applications around the world ranging from ATM and POS networks to interbank funds transfer and share dealing systems. It is available in standard and high speed variants with a wide range of connectivity options and protocols allowing connection to all types of host systems.

GM1130 HSM

Figure1: GM1130

HSM Features

- **Protect PIN Security and Data Integrity**
- **Ensure message transfered saftly**
- **Safeguard sensitive data stored**
- **Supports ATM, EFTPOS, EMV(Europay, Mastercard and Visa), and Chip Card Applications**
- **Visa/MasterCard/American Express PIN and Card Verification Functions**
- **Triple-DES DUKPT**
- **Support Smart Card Zone Master Key Distribution**
- **Evaluate FIPS 140-2 Level 3 and ISO 13491 Security Standards**
- **DES, Triple DES, RSA, MD5/SHA-1**
- **RSA key generation, signing and verification**
- **Supports EMV2000, ANSI, ISO, FIPS, VISA/Mastercard, ECBS Standards**

Performance Functions

Issuing card

- Generated PIN and encrypted PIN stored in host database
- Generate VISA PVV and CVV, MasterCard CVC, American Express CSC
- Provide multiplicity of Storage formats of encrypted PIN
- Support PIN mailer printing

Transaction processing

- Transfer encrypted PIN、transform PIN in network-node
- Verify VISA CVV, MasterCard CVC, American Express CSC
- Transfer and store sensitivity encrypted data
- Provide to generate and verify MAC, comply with ANSI X9.9、ANSI X9.19
- Verify PIN according to storage format

Keys management

- Using a random process generating keys，comply with ANSI X9.17
- Product and print key components, compose of keys or distribute of keys
- Store and protect keys' security
- Store the encrypted keys, support 64、128、192bits keys at same time，encryption algorithm in accordance with ANSI X3.106
- Generate, transform and Verify keys

The Host Security Module is:

- Used by all major card associations
- Used for ATM, POS, corporate banking, card issuing, funds transfer and stock/share trading
- Easily customized for user applications
- Available with support for a wide range of connectivity options and transaction protocols.
- Available in various speed variants to give required transaction throughput.
- Triple DES capable, using two and three keys, for all functions including the processing of PIN blocks.
- Integrated within all major financial industry solution providers applications.
- Certified to the most rigorous security standards.

Typical HSM Applications

ATM Interchange

The HSM is designed for the ATM interchange environment and is in use in many of the world’s major ATM interchange networks. The HSM can be customized to suit individual networks and, if needed, the particular requirements of each member of the network. The wide and growing variety of host interfaces in the HSM means that the needs of each member's system can be readily accommodated. In particular, the AMEX, VISA and MasterCard commands are an integral part of all standard functionality.

EFTPOS

The HSM supports a number of EFTPOS (Electronic Funds Transfer at Point of Sale) systems in use around the world. The Derived Unique Key Per Transaction are also available.

Card Production Facility

The HSM is suitable for use within the client card production area. It can provide a secure means of generating cryptographic card values such as VISA's CVV (Card Verification Value), MasterCard's CVC (Card Verification Code) and American Express CSC (Card Security Code) as well as securely generating PINs and PIN mailers.

Data Integrity

The integrity of information transmitted around and stored within systems is of paramount importance to its users. The integrity of information generated at remote terminals can be secured, using message authentication codes (MACs). The HSM is compatible with Smart Card terminals. A number of applications such as Cash Management.

Technical Specifications

MODEL	GM1130
Cryptographic Support	DES and Triple DES Algorithms - Provide PIN encryption and message authentication capabilities. RSA Algorithm - Provides high-level key management including remote key loading for ATMs, and supports the generation and validation of digital signatures. RSA key length is selectable from 192 to 2048 bits. Local Master Key Components - These are stored on Smart Cards (ISO 7816) for secure storage or distribution.
Security Certification	The HSM evaluation at FIPS 140-2 level 3.
Communication Interface	TCP/IP 10M~100M bps Async 115K bps Transparent Async
Typical Performance (Visa PVV Verify)	7000 times/sec
Pin Mailer printing	Support serial/parallel
Dimensions	Height: 68 mm Width: 430 mm Depth: 360 mm Weight: 8 kg

Power	Voltage: 90-132 VAC and 175-264 VAC, auto-selected Frequency: 50 Hz Power: 35 W (maximum)
Environmental	Operating Temperature: 0℃to50℃ Humidity: 5% to 90%, non-condensing