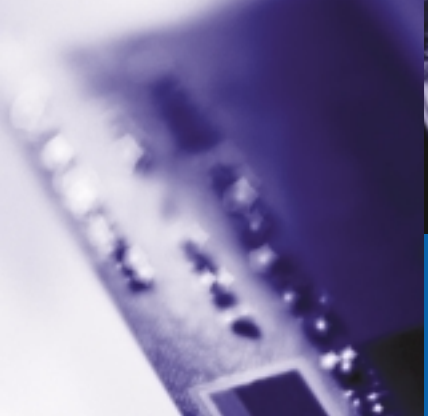


payShield™

HARDWARE SECURITY MODULE FOR E-PAYMENTS

PRODUCT | DATA SHEET

PAYMENT SECURITY IN FIPS 140-2 LEVEL 3 HARDWARE

Today's on-line payment industry has increasingly become a target for fraud. To address rising levels of disputed transactions, the card associations have introduced advanced security controls, including improved authentication techniques that demand sophisticated hardware-based cryptographic processing.

The payShield hardware security module (HSM) is designed to meet the stringent security requirements of the on-line payments industry, strengthening the security of card and PIN authentication systems by securing transaction processes in a FIPS 140-2 Level 3* validated tamper-resistant environment. In addition to providing increased security, payShield can dramatically increase transaction throughput by processing high volumes of symmetric and asymmetric cryptographic operations, an important requirement of the latest e-payment initiatives such as 3-D Secure.

*Federal Information Processing Standard (FIPS) 140-2 Level 3 is the international security standard for cryptographic modules

Cardholder authentication

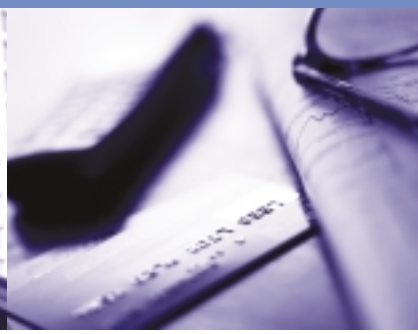
Supported by the major card associations, cardholder authentication provides a secure mechanism to better establish the identity and therefore legitimacy of a person presenting a payment card for a transaction. The process, whether applied to on-line or traditional store purchases, provides assurance that the buyer is indeed the authorized cardholder. By using nCipher's payShield HSM, issuing banks, payment processors and solution providers can ensure that cryptographic operations used in the card authentication process are performed inside a FIPS 140-2 Level 3 secure device and are therefore protected from attack.

FEATURE	BENEFIT
SECURE CARDHOLDER AUTHENTICATION	In a single HSM, payShield handles all hardware secured cryptographic functions required for cardholder authentication initiatives, such as 3-D Secure, eliminating the need to purchase multiple HSMs
EMV AUTHENTICATION FOR SMART CARDS	payShield supports next-generation payment initiatives such as the validation of smart card transactions on Internet-based or point-of-sale (POS) systems
SECURE MESSAGING	Cryptography is used to ensure both the secrecy and the integrity of messages flowing within the payment system. By using payShield, information is digitally signed within the HSM for increased protection
HIGH SPEED CRYPTOGRAPHIC PROCESSING	Cryptographic acceleration is a key feature of all nCipher HSMs, allowing organizations to improve transaction throughput during the card authorization process, thus reducing delays while boosting system capacity
FIPS 140-2 LEVEL 3 KEY GENERATION, PROTECTION AND MANAGEMENT	Protected within FIPS 140-2 Level 3 validated tamper-resistant hardware, cryptographic keys are never exposed – minimising vulnerability and meeting industry privacy requirements
COMPREHENSIVE CRYPTOGRAPHIC SUPPORT	payShield combines high speed processing support for both symmetric and asymmetric operations within a single physical device. DES, Triple-DES, AES and RSA keys can be managed under a common management framework and security policy, reducing complexity and operational cost
SHAREABLE CRYPTOGRAPHIC RESOURCE	Provides flexible security for multiple server and multi-site installations, lowering the overall cost of deploying cryptographic hardware
FAILOVER CAPABILITY	Supports the use of dual HSMs for resiliency, transparently passing processing activities to a second payShield device in the event of failure

nCIPHER™

payShield™

Split knowledge and dual control provide a mechanism for sharing responsibility across an administrative team



ADVANCED HSM MANAGEMENT

The payShield HSM exploits nCipher's proven Security World key management framework. This combines advanced cryptographic techniques for the generation, backup and recovery of cryptographic keys. Split knowledge and dual control provide a mechanism for sharing responsibility across an administrative team avoiding the threat of a single "super-user", a vital capability for the protection and secure management of keys used for payment processing. Most security functions are controlled through an intuitive graphical user interface.

CUSTOMIZED SECURITY

The combination of nCipher's developer toolkits and broad range of supported software APIs means that the payShield platform can be expanded even further to enable more sophisticated security solutions. This flexibility enables the integration of customized encryption, decryption, or signing functions.

Rack mounted, network connected payShield

INDUSTRY APPLICATION

ePayments

The 3-D Secure specification mandates the use of FIPS certified hardware for storage and management of cryptographic keys. payShield provides a single HSM solution that supports Visa's 3-D Secure Cardholder Authentication Verification Value (CAVV) using the Visa Card Verification Value (CVV) method, as well as MasterCard's SPA Account Authentication Value (AAV) and Card Authentication Program (CAP).

EMV smart card support

EMV is a smart card standard developed by Europay, MasterCard and Visa to address the universal aspects of chip card issuance and acceptance. The standard provides the bridge from traditional magnetic strips to chip-based smart cards for debit and credit payments. payShield supports the Authorization Request and Response cryptograms used in smart card based authentication.

EFTPOS

The payShield HSM supports functionality to provide key management and PIN-based functions relating to EFTPOS system deployment. The functionality supports debit, credit and smart cards for authorization and processing in an on-line EFTPOS system.

ATM PIN processing

PIN processing functions are supported by payShield, including PIN generation, translation and authentication. Customized formats can be easily developed due to the flexibility of the payShield architecture. payShield supports verification, generation and translation using both the Visa PVV and IBM 3624 formats.

HARDWARE SECURITY MODULE FOR E-PAYMENTS

TECHNICAL SPECIFICATIONS

Customized formats can be easily developed due to the flexibility of the payShield architecture

Cardholder authentication functions

- Visa's 3-D Secure Cardholder Authentication Verification Value (CAVV) using the Visa Card Verification Value (CVV) method
- MasterCard SPA Account Authentication Value (AAV) for 3-D Secure
- MasterCard CVC and CVC2 card validation codes
- MasterCard Card Authentication Program (CAP)

EMV functions supported

- Authorization Request Cryptogram (ARQC) verification
- Authorization Response Cryptogram (ARPC) generation
- Transaction Certificate/Application Authorization Cryptogram TC/AAC generation

PIN functions

- Verification, generation and translation using both the Visa PVV and IBM 3624 formats

Key-loading

Key-loading is provided using the VeriFone SC552 hand-held secure smart card reader/writer (sold separately, in pairs). These devices provide a secure smart card reader, display and keyboard, and are used to transfer key segments onto smart cards for transfer into the payShield HSM. Used as a pair, they enable split-knowledge key management.

Direct connected (SCSI) payShield with key-loading hand-held terminal

Cryptographic algorithms supported

Symmetric ciphers

- Triple-DES (two and three key)
- AES - Rijndael
- Arc Four (compatible with RC4)
- CAST
- DES

Public key ciphers

- DSA
- El Gamal
- RSA

Key exchange mechanisms

- DH
- DES / DES3 XOR

Hash and HMAC functions

- MD2
- MD5
- RIPEMD 160
- SHA-1
- HMAC-SHA1

OS Support

- Solaris
- Windows
- HP-UX
- AIX
- Linux

APIs

Access to the payShield payments functions is through a native C and Java API. In addition payShield supports a range of API's for general cryptographic functions. These include:

- PKCS #11
- Microsoft CryptoAPI
- Java JCE/JCA
- nCipher nCore API (C or Java)

payShield™ HARDWARE SECURITY MODULE FOR E-PAYMENTS

PRODUCT SPECIFICATIONS

CONNECTIVITY	FORM FACTOR	SHAREABLE/DEDICATED	PERFORMANCE STANDARD	PERFORMANCE ULTRA
10/100 ETHERNET	19" RACK MOUNT	SHAREABLE or DEDICATED	PVV - 200 RSA - 150	PVV - 500 RSA - 400
SCSI	5.25" DRIVE BAY OR EXTERNAL ENCLOSURE	DEDICATED	PVV - 200 RSA - 150	PVV - 500 RSA - 400

Actual system performance depends on application software version, server platform type and other factors.

10/100 Ethernet

Connectivity
- 1 or 2 10/100 Ethernet
- RS232, mini-DIN serial connection
- PS/2 Keyboard connection

User Interface
- High Resolution LCD
- Dual 'Soft' menu keys
- Scroll / select knob

Mechanical
- Weight 6.4 Kg
- Standard 1U rack mount [19" x 1 3/4" x 17 1/4"], (482mm x 44mm x 440mm)

Electrical
- Input voltage 100-240 AC auto switching 50-60 Hz (nominal)
- Maximum Power Consumption: 460 watts (4 amps at 115 volts AC)

Certification
- FCC: CFRA47, Part 15, Subpart B, Class A
- CE: EN 55022, Class A; EN 55024-1; EN 60950
- UL : 1950

Temperature / Humidity (Operational):
+10 to +35°C; 10 to 85% relative humidity, non condensing

SCSI

Connectivity
Fast wide SCSI 2 (also called SCSI 3) with a high density micro-D 68 connector can be mounted in a server's 5.25" drive bay or in a dedicated external enclosure.

Electrical
- Maximum power consumption 3.0 amps at 5 Volts.

Certification
- FCC: CFRA47, Part 15, Subpart B, Class A
- CE: EN 55022, Class A; EN 55024-1; EN 60950

Temperature / Humidity (Operational):
+10 to +35°C; 10 to 85% relative humidity, non condensing

NCDS/HSMPS/OCT2003

nCipher Inc.
500 Unicorn Park Drive
Woburn, MA 01801 USA
Tel: +1 (781) 994 4000
E-mail: ussales@ncipher.com

nCipher Corporation Ltd.
Jupiter House, Station Rd.
Cambridge, CBI 2JD UK
Tel: +44 (0) 1223 723600
E-mail: int-sales@ncipher.com

nCipher Corporation Ltd.
15th Floor, Cerulean Tower,
26-1 Sakuragaoka-cho, Shibuya-ku,
Tokyo 150 8512 Japan
Tel: +81 3 5456 5484
E-mail: int-sales@ncipher.com

Visit our Web site at www.ncipher.com – today!

Redefining cryptographic security

nCIPHER™