

Comprehensive secure solutions for EMV card issuance and mobile secure element provisioning with centralized key management

- Delivers full lifecycle management for card and mobile applications using HSMs to protect critical assets
- Keeps issuers in control while delivering flexibility to outsource specific tasks
- Scales easily to meet emerging performance and integration requirements
- Reduces the time required to introduce new payment products
- Simplifies security audit compliance by using the market leading FIPS-certified nCipher nShield Connect HSM



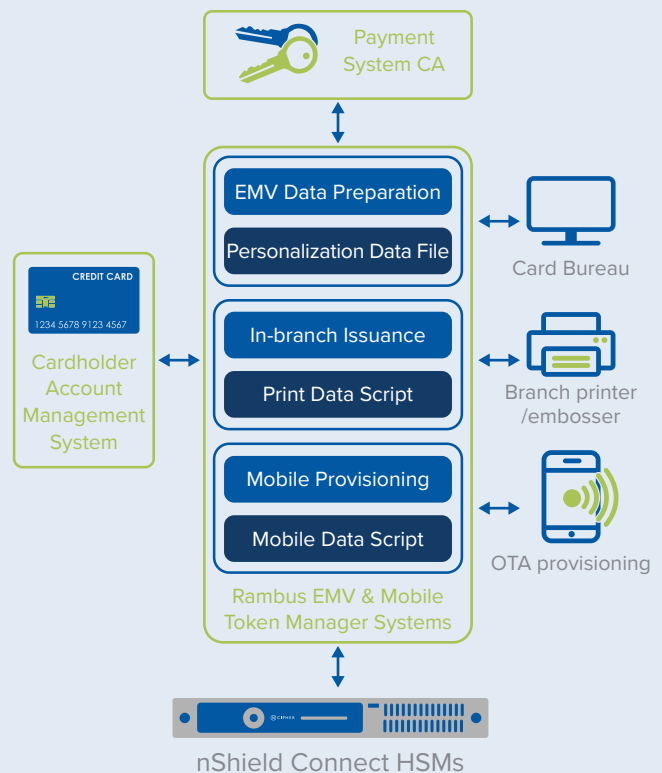
Rambus payment token issuance solutions with security assured by nCipher nShield Connect

CHALLENGES OF MAGNETIC STRIPE TO EMV MIGRATION

Most issuers have traditionally produced magnetic stripe cards in-house. The EMV standard introduces considerably higher levels of security and more complex key management, requiring enhancements to existing issuer security and risk management procedures. Mobile NFC applications, although based on EMV, differ significantly from cards in relation to device provisioning, creating numerous new technical and commercial challenges for issuers. An integrated solution set that provides a consistent management platform for EMV cards and mobile secure element applications while leveraging the proven legacy infrastructure will deliver security and efficiency while keeping the issuer in control.

HARDWARE-BASED KEY MANAGEMENT PROTECTING CRITICAL ASSETS

At the heart of any issuance solution for payment cards and mobile devices is strong key management with keys and sensitive data (such as PINs) protected at all times by hardware security modules (HSMs). Most issuers retain control of the master keys and certificates required for EMV cards, performing the EMV data preparation process in-house while reducing costs by outsourcing the subsequent personalization stage to a trusted bureau.



Rambus payment token issuance solutions with security assured by nCipher nShield Connect

HSMs underpin the secure transfer of keys and data between the issuer and the bureau. This process can be leveraged when creating secure content for mobile phone applications providing economies of scale and ensuring that sensitive data is protected during transmission across the mobile network.

RAMBUS TOKEN MANAGEMENT SYSTEMS FOR CARD AND MOBILE NFC APPLICATIONS

Rambus makes extensive use of nCipher nShield Connect to create secure lifecycle management systems for both EMV payment cards and mobile NFC secure elements. The solutions are modular, delivering the high levels of security and certifications demanded by the payments industry.

Rambus EMV Token Manager manages and controls any EMV contact or contactless card throughout its lifecycle, supporting all applications and their associated cryptographic keys. A modular approach enables issuers to start with a basic configuration and enhance incrementally to satisfy additional business and technology requirements such as instant card issuance at a bank branch. In addition to the issuance options, issuers can perform a range of post issuance tasks such as changing the risk parameters on the card or upgrading the applications. EMV Token Manager is easy to integrate with third party systems (typically operated by processors and card bureaus) where the issuer chooses to outsource certain tasks.

Rambus Mobile Token Manager provides issuers with choices on how to participate in the NFC ecosystem, including which tasks to outsource. It covers all aspects of managing security domains, mobile applications and the associated key management infrastructure, facilitating dynamic changes to suit new business models or requirements. Central recording of all application activity is provided, enabling data to be shared with other third party systems. Strong key management and protection of sensitive data is essential due to the mobile provisioning process taking place over-the-air (OTA) rather than inside a highly controlled secure personalization bureau for traditional payment cards. Mobile Token Manager offers high levels of flexibility and modularity, enabling issuers to reduce costs and support future market requirements.

BENEFITS DELIVERED BY NSHIELD CONNECT:

The nCipher nShield Connect is a high-performance network-attached hardware security module (HSM) that delivers secure cryptographic services as a shared resource for distributed application instances and virtual machines. With nShield Connect, issuers have a cost-effective way to establish appropriate levels of physical and logical controls for their server-based systems where software-based cryptography fails to meet risk management and security requirements.

Some of the main benefits that nShield Connect delivers to Rambus and ultimately to the end users of the token management solutions are as follows:

- Generates keys and data securely for all EMV card and mobile applications with no cleartext exposure outside the HSM security boundary – the fundamental trust model for chip-based payment tokens especially where issuers need to share sensitive information with third party service providers
- Provides high levels of cryptographic performance, scalability and resilience – essential for a mission critical issuance environment
- Enables Rambus to use the CodeSafe Developer Toolkit to create and run sensitive operations within the HSM, eliminating common threats to the application host platform – offering on-going flexibility to meet new requirements without reliance on vulnerable software-based cryptography
- Delivers highly secure installation and personalization of applications, both card and mobile-based – developed using industry standards and algorithms simplifying overall system conformance to the various EMV, PCI and payment system certification and/or audit requirements
- Implements strong role-based user authentication and key separation - ensuring isolation of data encryption/decryption, verification, authentication and authorization keys and helping to prevent exposure of sensitive data during the issuance process

Further information on Rambus Payments solutions can be found at: www.rambus.com/mobile-payments

Further information on the nCipher nShield Connect can be found at: www.ncipher.com/nshield

Search: nCipherSecurity



©nCipher - April 2019 • PLB8222

www.ncipher.com

