Mobile cloud payments from Rambus using Entrust nShield Connect HSMs

Rambus

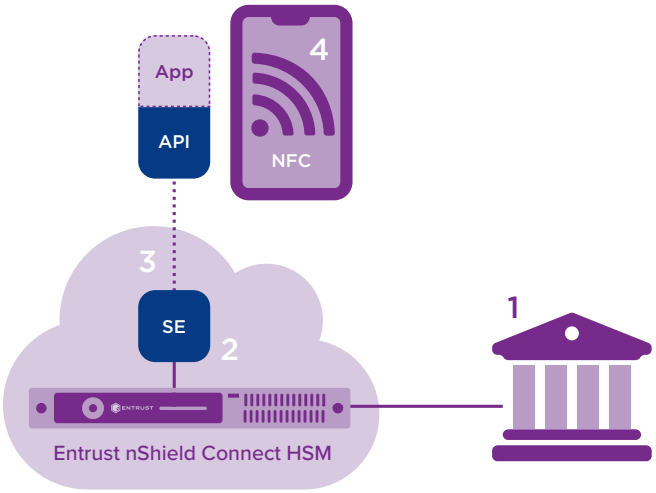
Take direct control of your mobile payments strategy by storing credentials in the cloud using host card emulation (HCE)

HIGHLIGHTS

- Reduces the cost and complexity of provisioning NFC mobile payments for issuers by removing the need for a third party to access a secure element (SE) inside the mobile device
- Uses certified hardware security modules (HSMs) in generation, storage and distribution of keys and sensitive data for maximum protection against compromise
- Works seamlessly with existing point-of-sale (POS) terminals by leveraging the EMV contactless card acquiring infrastructure
- Scales easily supporting any card, application and payment scheme without the memory storage limitations of a device-based SE

Physical secure elements: high cost and high complexity

An SE inside a mobile device provides a secure location for the storage of payment credentials and sensitive data. The operational challenges with SEs are that new trust infrastructures and additional business relationships are necessary to provision the payment application, resulting in higher costs. Issuers have total control over payment cards, but in the mobile world, it is a highly complex challenge to support all types of consumer-owned mobile devices and maintain a secure implementation over time.



Rambus solution components

1. Real time and/or batchfile import of card and personalization data
2. HSM protects all keys and sensitive data
3. Secure connection
4. A Rambus client API SDK allows for a smooth integration to existing mobile wallet applications

LEARN MORE AT ENTRUST.COM/HSM

Mobile cloud payments from Rambus using Entrust nShield Connect HSMs

HCE has simplified mobile provisioning

Since certain mobile platforms now allow applications to communicate directly with the NFC controller, which was formerly the exclusive role of the SE, issuers do not need a third party to provision mobile devices. This can be done directly using cryptographic keys and payment credentials secured using HSMs in their private cloud or data center. Emulating a payment card in the mobile device using HCE technology gives issuers immediate control over the "card" applications and payment credentials, and facilitates real-time risk management.

How Rambus and Entrust help issuers launch mobile NFC payment solutions quickly and securely

The SE was originally considered the environment in the mobile device for secure storage of applications and credentials. The technical complexity in supporting all mobile device handset/operating system permutations, the need for new business relationships (at additional cost to issuers) and operational challenges relating to post deployment support and/or liability has largely hindered widespread adoption. By moving the SE to a remote environment, bank issuers can directly provision their payment applications to an SE (in their own secure private cloud) without any third parties being involved.

Using software-based cryptography inside the mobile device as part of the payment ecosystem simplifies the device provisioning process, making it easier to get payment capability to consumers. However, it adds requirements for secure credential management in the issuer cloud as well as real-time risk management to minimize fraud losses during transaction authorization.

The Entrust nShield® HSM plays a critical role in the security of the Rambus Secure Element in the Cloud solution which leverages HCE technology and ensures that all keys and sensitive data are protected during creation, storage and in transit between the private cloud and the mobile device.

Rambus Secure Element in the Cloud

Rambus's Secure Element in the Cloud, an international patent pending solution, emulates an EMV mobile payment via a remote SE and provides the functionality to complete an EMV payment transaction using a standard EMV contactless POS terminal. When a consumer makes a purchase, payment credentials are accessed from the remote SE. A response is then generated and communicated through the mobile device to the POS terminal. The data is presented in the same format as that used in standard EMV transactions and hence there is no impact on the acquiring infrastructure. Using tokenization, payments can be made even when no data connection can be established. Some of the important security features that are available to the issuer include:

- Secure channel between the cloud and the mobile device to protect sensitive keys and data during both device provisioning and subsequent use in making payment transactions
- Extensive use of TrustZone in the mobile device to enable the payment application to generate the EMV cryptograms in real-time where necessary without risk of exposing sensitive data to the mobile operating system
- Flexible PAN and token options to enable the issuer to decide how many transactions can be allowed to take place offline before online authorization is necessary

Mobile cloud payments from Rambus using Entrust nShield Connect HSMs

- Simple integration with existing bank mobile banking platform, maximizing investment in existing infrastructure and leveraging existing secure customer registration and activation processes

Entrust nShield Connect HSMs

The Entrust nShield Connect HSM is a high-performance network-attached appliance that delivers secure cryptographic services as a shared resource for distributed application instances and virtual machines. With nShield Connect HSMs, 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 HSMs delivers to Rambus and ultimately to the consumers making mobile payments underpinned by the Secure Element in the Cloud solution are:

- Provides high levels of cryptographic performance, scalability and resilience – essential for a mission-critical mobile provisioning environment
- Supports the latest cryptographic algorithms and key management schemes to provide issuer flexibility for the mobile application – designed to future-proof the solution as standards emerge
- Implements strong role-based user authentication and key separation – helping to prevent exposure of sensitive data during the provisioning process

Benefits for issuers

Hosting the SE in the cloud reduces the cost of provisioning NFC mobile payments, offering a range of operational and business benefits to issuers:

- Simplifies the application provisioning process especially when using flexible off-the-shelf solutions such as Secure Element in the Cloud to reduce time to market
- Enables sophisticated risk management before, during and after the transaction to help minimize fraudulent attacks
- Keeps issuers in control by providing a valuable addition to their proven mobile banking infrastructure
- Supports a layered approach to security by keeping the option to use a SE in the future (in conjunction with HCE) for applications or situations requiring additional levels of assurance
- Delivers an immediate revenue stream via transaction fees which align with those for contactless card transactions

www.rambus.com/mobile-payments

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com