Oasis Smart SIM Securely Connects the Dots with Entrust nShield HSMs

Challenge

Oasis Smart SIM Embedded SIM cards (eSIMs) offer new ways to manage and deploy connectivity for both user-driven devices and machine-to-machine (M2M) communications, without the hassle of physical SIM cards. But these embedded SIM cards, provisioned over-the-air, must comply with critical regional regulations to ensure secure communications, like the GSMA Security Accreditation Scheme (SAS).

The GSMA SAS defines how to protect credentials that access the Mobile Operators Network and requires use of a hardware-based hardware security module (HSM) as the root of trust. By certifying its eSIMs, Oasis Smart could deliver a complete set of GSMA-certified services for mobile operators and device makers that take advantage of 4G and 5G connectivity and interoperable connectivity.

CUSTOMER PROFILE

Oasis Smart SIM provides both end-to-end and customized services to enable the deployment of global USIM technology connectivity and management. It offers a full set of services for embedded and reprogrammable SIMs, along with solutions for activation, connectivity, and subscription management. Oasis contributes to shaping the globally connected world by combining leading-edge USIM technology and disruptive business models in a migrated focus from products and solutions to software and services.

Objectives

- Meet security requirements of the GSMA SAS
- Create a secure, interoperable architecture that enables remote over-the-air provisioning and management of its M2M and consumer SIM/eSIMs
- Scale out solution blueprint globally

Technology and Services

- Entrust nShield HSM
- ECC library
- Entrust DPS training and support

Learn more about nShield HSMs at entrust.com

Oasis Smart SIM Case Study

> **Delivering a first-class digital-first user experience is now a requirement for service providers in order to win the connectivity battle. We design, develop, and certify solutions that are at the forefront of the industry requirements in term of functionality and security and, as well as ensuring we can attain the GSMA Security Accreditation Scheme requirements, Entrust nShield HSMs provide scalability and security. As an integral part of our solution blueprint, we recommend nShield HSMs and we look forward to strengthening our relationship with Entrust to be included more deeply into their ecosystem.**
>
> Patrick Cao, Chief Operating Officer, Oasis Smart SIM

Solution

Oasis Smart SIM developed its own key management system to support two GSMA-certified PKI deployments, backed by two Entrust nShield HSMs in a secure data center in France. To meet the GSMA SAS requirements, the HSMs were configured to operate in FIPS 140-2 Level 3 mode, an implementation that creates complexity in the Java Cryptography Extension interface.

Entrust engineers ensured that the nShield HSMs would meet these requirements and collaborated with Oasis Smart SIM to enable secure management of encryption keys and certificates to meet GSMA SAS certification requirements.

Results

Oasis Smart SIM has implemented a secure, interoperable architecture that enables remote over-the-air provisioning and management of its M2M and consumer SIM/eSIMs.

All sensitive data in this system are protected by nShield HSMs. These HSMs also provide elliptic curve cryptography (ECC) encryption, which is used in the authentication protocol between the remote eSIM and the Oasis Subscription Manager.

As a result, Oasis Smart SIM was the first European SME to obtain the GSMA SAS certification and is today ranked among the world's Top 10 eSIM solution providers.

Oasis Smart SIM Case Study

THE TRANSFORMATION

First France, and then the world

Oasis Smart SIM started by adding two nShield HSMs into its architecture. This enabled the company to successfully pass the GSMA SAS certification, at which point it started onboarding customers into the secure infrastructure.

The next steps in the Oasis Smart SIM roadmap include:

- Replicating this solution blueprint in multiple locations to support its customers globally
- Focusing on countries where data management regulations require local deployments
- Scaling up operations as the number of connected devices continues to grow

MEASURES OF SUCCESS

Ensuring security in a connected world

Through its Oasis eSIM Remote Provisioning Solution, Oasis Smart SIM enables every mobile operator and virtual mobile operator to provide global connectivity services and offers to manage their eSIM subscriptions with the highest level of security and interoperability.

In particular, the company:

- Implemented a secure, interoperable architecture that enables remote over-the-air provisioning and management of its M2M and consumer SIM/eSIMs
- Plans to roll out this solution blueprint globally

The Entrust advantage

Entrust nShield HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations. The purpose-built hardware devices are designed to generate, safeguard, and manage cryptographic keys on behalf of applications. The unique nShield Security World key management architecture enforces important separation of duties with dual controls that segregate security functions from administrative responsibilities.

For more information visit: **entrust.com/HSM**

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223