5G/3GPP Subscriber Authentication Solutions with Entrust nShield® Hardware Security Modules (HSMs)

Get high assurance protection of cryptographic keys for 5G/3GPP subscribers and improve trust across your communication infrastructure

HIGHLIGHTS

- Facilitate regulatory compliance and deliver the highest levels of data and application security for enterprises, financial institutions, and governments (NIST FIPS 140-2/3 standards as well as Common Criteria).
- Get strong, granular controls over access and usage of keys, allowing separation of tamper-protected hardware and keys.
- Create a unified ecosystem that delivers scalability, seamless failover, and load balancing.
- Support for micro-service software architecture for dynamic application scalability and maximum HSM utilization.

FEATURES

- Support 5G/3GPP subscriber authentication features MILENAGE, TUAK, and SIDF via standard firmware and API
- Generate subscriber long-term keys using high-quality TRNG entropy inside FIPS 140-3 HSM
- Enable support for PKI functions used for chip or SIM key generations, personalizing UICC data as well as protecting base station networks
- Compatible with cloud and containerized environment options, allowing telecom operators to secure scalable solutions without compromising on operational efficiency
- HSM by design offers strict access control policies, controlling the generation and use of cryptographic keys to protect subscriber IDs

Ensure the future of your communications infrastructure

CHALLENGE

Today's mobile communications infrastructure is undergoing unprecedented growth. The rapid rollout of the Internet of Things (IoT) continues at pace, which requires networks to handle billions of connected devices associated with smart energy, smart homes, smart cities, and connected cars.

Alongside changing consumer mobile communications habits and the need to support IoT, there are emerging use cases, different access types, and increasing demand from communication service providers (CSPs) and communication authorities around the globe for improved security and trust across their communication infrastructure.

SOLUTION

3GPP – a partnership project bringing together standards development organizations from around the globe – defined the 5G specification, which has addressed many of the security threats that exist on previous mobile technologies, introducing new mutual authentication capabilities and enhanced subscriber identity protection.

The 5G standard adopted three major security improvements in AuC1/ARPF2 functionality:

- Mutual authentication
- Encryption of inter/intra-network traffic
- End-subscriber ID protection

Previous generations of mobile networks were vulnerable to man-in-the-middle attacks where false base stations or Stingrays were used by nefarious actors to conduct eavesdropping attacks. One of the major vulnerabilities that made such attacks possible was that the subscriber identifier, IMSI, was sent in the clear, unprotected. This vulnerability is addressed in 5G through various means, the most important of which is the introduction of the concealed subscriber identifier. 5G cellular systems utilize a cryptographic key as a subscriber's long-term ID.

Around the globe, telco operators recognize that the best-practice approach to generate and protect cryptographic keys is in a hardware security module (HSM). The use of HSMs is recommended in national and regional standards such as the European Union Agency for Cybersecurity (ENISA) Security in 5G Specifications.

THE ENTRUST DIFFERENCE

Compliance

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 entire nShield product line is certified to the NIST FIPS 140-2/3[1] standard as well as Common Criteria.

1. nShield 5 FIPS 140-3 certification (currently in coordination).

Ensure the future of your communications infrastructure

Scalability

nShield Security World key management architecture provides strong, granular controls over access and usage of keys, allowing separation of tamper-protected hardware and keys. The cryptographic keys are abstracted from the memory constraints of the HSM and stored externally, while fully protected using encryption, external to the HSM. Security World provides a highly scalable architecture while also supporting integration with highly automated and orchestrated service environments.

High Performance

nShield 5 HSMs support 3GPP algorithms natively in firmware producing the following indicative performance speeds:

- ECIES key wrapping ~1,850 TPS
- MILENAGE signature or authentication ~8,000 TPS
- MILENAGE key generation ~3,100 TPS
- TUAK signature or authentication ~7,800 TPS
- TUAK key generation ~3,100 TPS

A dual HSM configuration can offer significant improvement in MILENAGE and TUAK signature/ authentication performance results.

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 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

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223