DATASHEET

5G/3GPP Subscriber Authentication Solutions With Entrust nShield® HSMs

Enable quantum-ready protection across your communication infrastructure.

Overview

Create a unified ecosystem across your critical infrastructure with Entrust nShield hardware security modules (HSMs) that offer crypto-agility straight out the box.

Our Entrust nShield HSMs create scalability, seamless failover, and load balancing to support your organization's protection and performance requirements.

With our HSMs, you can unlock:

- Strong, granular controls over access and usage of keys
- Support for micro-service software architecture for dynamic application scalability
- Regulatory compliance across your infrastructure with FIPS 140-2/3 and Common Criteria certifications, plus NIST-approved algorithms for post-quantum readiness

Opting for quantum-ready modules gives your organization the ability to not only protect the critical data within your subscriber network today but also offer the best protection from quantum threats in the future.

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
- Supports secure key generation and UICC data personalization while helping protect chip and base station networks
- Compatible with cloud and containerized environments, allowing telecom operators to secure scalable solutions without compromising efficiency
- HSMs enforce strict access controls and manage cryptographic key usage to safeguard subscriber IDs

CHALLENGE

Mobile communication infrastructure is expanding, and the rapid growth of IoT (Internet of Things) means networks must support billions of connected devices powering smart energy, smart homes, smart cities, and connected vehicles.

Alongside evolving consumer habits and demands, new use cases and access types are emerging. Communication service providers (CSPs) and regulators worldwide are calling for stronger security and trust across their networks to protect sensitive data and identities.

The urgency is amplified by the looming quantum threat: NIST (National Institute of Standards and Technology) will deprecate RSA and ECC by 2030, making cryptographic agility and post-quantum readiness a critical priority for mobile networks today.

SOLUTION

The 5G standard, defined by 3GPP, introduced major security enhancements to address vulnerabilities in earlier generations.

Earlier mobile networks were susceptible 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.

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

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

To enable these protections, operators must securely generate and safeguard cryptographic keys. Global best practice – and a requirement in many regional standards such as ENISA's 5G security guidelines – is to use HSMs as a root of trust. As networks prepare for the post-quantum era, HSMs must also support crypto-agility to handle new algorithms and future transitions.

THE ENTRUST DIFFERENCE

Quantum-Ready Security

Entrust nShield HSMs deliver high-performance, crypto-agile protection for today's 5G networks and tomorrow's post-quantum era. Built on flexible architecture, nShield HSMs can be updated to support evolving cryptographic standards, including NIST-approved post-quantum algorithms.

Certified to FIPS 140-3 and Common Criteria standards, our HSMs help operators meet regulatory requirements while ensuring the strongest protection for subscriber identities and network infrastructure. Built for crypto-agility, nShield HSMs can be updated to support evolving cryptographic standards, including hardware acceleration of NIST-approved post-quantum algorithms, future-proofing your network against emerging quantum threats.

Scalability

- Entrust's nShield Security World architecture delivers strong, granular controls over key access and usage, ensuring separation between tamper-protected hardware and cryptographic keys. Keys are abstracted from HSM memory constraints and stored externally in encrypted form, maintaining full protection outside the HSM.
- This architecture provides high scalability and supports integration with automated, orchestrated service environments – while enabling crypto-agility for future algorithm updates, including post-quantum cryptography.

High Performance

Entrust nShield 5 HSMs deliver exceptional performance for 3GPP algorithms, with indicative speeds such as:

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

Dual-HSM configurations can significantly boost MILENAGE and TUAK signature/authentication throughput. Built on a flexible FPGA architecture, nShield HSMs are designed for crypto-agility, supporting NIST-approved post-quantum algorithms to future-proof your network against emerging threats.

The CSP Advantage

Cryptographic Security Platform

The Entrust Cryptographic Security Platform (CSP) unifies PKI, HSM, key and secret management, and certificate lifecycle management into a single solution. CSP provides centralized visibility and control over your cryptographic estate, enabling compliance, automation, and crypto-agility at scale.

As networks prepare for the post-quantum era, CSP helps operators manage cryptographic transitions efficiently, delivering a secure foundation for 5G and beyond.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION