FIME®

One Action. **A billion transactions.**

Security Services

FOR NFC HANDSET MANUFACTURERS

Secure your handset

A SECURE HANDSET IS KEY

Robust security is the key to protect the end-user against fraud and security breaches. The security of the handset is essential to ensuring the overall trustworthiness of the Near Field Communication (NFC) ecosystem.

KEY SECURITY FOCUS FOR MOBILE HANDSET

- Secure handset underlying hardware/software (TEE).
- Providing protection for secure applications within the handset (TEE).
- Gaining compliance to security standards.

Common Criteria GLOBALPLATFORM®

+ KEY BENEFITS

- Prove the security of your handset to your partners and customers.
- Avoid brand, image and reputation damage in case of fraud or security issues.
- Reduce your incurred costs for fraud and security issues.
- Protect end-users against fraud and security breaches.
- Improve end-user's trust in NFC services.
- Drive end-user acceptance of NFC solutions.

Security Services
FOR NFC HANDSET MANUFACTURERS

LEARN MORE

www.fime.com/smart-devices-testing.html

FIME CONTACTS

Americas	fimeinsidesalesnalac@fime.com
Asia Pacific	fimeinsidesalesap@fime.com
China	fimeinsidesaleschina@fime.com
EMEA	fimeinsidesalesemea@fime.com
India	fimeinsidesalessa@fime.com
Japan	fimeinsidesalesjapan@fime.com
Korea	fimeinsidesaleskorea@fime.com

FIME HELPS YOU GAIN SECURITY EVIDENCE FOR YOUR HANDSET

The most important part of a handset regarding security is the TEE, as specified by GlobalPlatform. It is a secure operating system implemented in the mobile's main application processor, which is co-embedded with a classic mobile operating system (called the rich OS).

Trusted applications, on top of a TEE, offer security services to the client applications that are on top of the classic mobile OS (rich OS).

The TEE can be tested regarding compliance to GlobalPlatform specifications, and certified against Common Criteria or GlobalPlatform security requirements.

Security services for secure handsets

Support areas	Security requirements	Type of service
Design centre Manufacturing plant	• ISO 27001 • Physical and logical security requirements • Security expertise	• Security audit • Penetration testing
Mobile device	• Common criteria	• Security evaluation
	• Security expertise	• Security assessment
Trusted Execution Environment (TEE)	• Common criteria • GlobalPlatform	• Security evaluation
	• Security expertise	• Security assessment

Product life-cycle phase	Type of service
Analysis / definition	• Risk analysis • Security requirements development • Security target development
Design	• Product design review
Integration / validation	• Source code review • Vulnerability analysis • Dedicated test tool development
Continuity of operations	• Technological watch for NFC security issues to ensure that you keep abreast regarding new vulnerabilities, countermeasures and workarounds

Why choose FIME?

- FIME is recognised in the NFC ecosystem by key certification bodies as a global test tool provider and a major test laboratory.
- FIME has developed expertise in mobile security, dealing with issues spanning from the UICC to the handset.
- FIME participates in the GlobalPlatform TEE Security Working Group and manages the TEE Attack Expert Working Group.
- FIME has been established as a major player within the secure chip industry since 1995.
- FIME is able to provide you with both functional and security testing as a global service offer.
- Quality is our priority.
- Most of FIME's worldwide laboratories are ISO 17025 accredited.

A global solution

FIME has developed a comprehensive portfolio of testing solutions to support handset manufacturers in their NFC product development cycle.

This offer encompasses a full range of functional and security testing for the secure elements, Trusted Execution Environment (TEE), mobile handsets, mobile applications including HCE, Token Service Provider (TSP) and Trusted Service Manager (TSM).

Beyond this standard testing portfolio, FIME experts can develop dedicated tests to future-proof your development.