ST33G1M2A, ST33G1M2M
Secure automotive and M2M microcontrollers

Embedded Secure solutions for connected cars

ST's Secure Element families have a proven track record ensuring high security in markets such as banking, identity, consumer Trusted Platform Modules as well as high-end SIM, NFC SWP-SIM, eSIM or eSE for mobile phones and other consumer applications.

Based on Arm® SecurCore® SC300 32-bit RISC core, our ST33G1M2A and ST33G1M2M secure microcontrollers ensure high-quality security solutions for both Industrial- and Automotive-grade applications.

With the growth of connected cars and the automotive industry's roadmap towards autonomous driving as well as the rise of new digital technologies in Industry 4.0 applications, an increasing number of platforms are vulnerable to physical or cyber-attacks.

Security being at the heart of such new challenges, ST is committed to the development of secure solutions to cover most requirements for the new area of digital technologies.

KEY FEATURES

- ARM® Cortex®-M3 or ARM® SecurCore® SC300 cores
- Common Criteria EAL5+ certified
- Strong remote authentication
- Root of Trust management
- Secure firmware update
- Key management
- Cryptographic services

KEY APPLICATIONS

- Connectivity & M2M modules
- Secure Element
- Immobilizers
- Secure gateways
- Secure positioning
- In-car communications

SECURE CONNECTIVITY

More and more objects, devices, machines, and automotive systems are being connected and communicate through cellular networks using 2G, 3G, and 4G technologies. ST's enhanced secure microcontrollers use SIM technology to enable communication with cellular networks, playing a key role in M2M (machine-to-machine) applications.
ST33G1M2A and ST33G1M2M secure microcontrollers comply with the GSMA Remote SIM provisioning specification enable OTA firmware downloads and the life management of different MNO profiles.

SECURE ELEMENT

Built on an ARM® SecurCore® SC300 core, ST33G1M2A and ST33G1M2M secure MCUs offer additional security features to help protect engine control units (ECU) and gateways against advanced forms of attacks. AEC-Q100-qualified, these platforms bring security into M2M and Automotive applications.
The tamper-resistant ST33 platforms, certified Common Criteria EAL5+, offer large memory capacity, multiple communication interfaces and certified cryptographic libraries in different form factors such as SIM modules, DFN, and TSSOP packages.
Developers will appreciate ST's Flash technology that shortens development time and improves time to market.

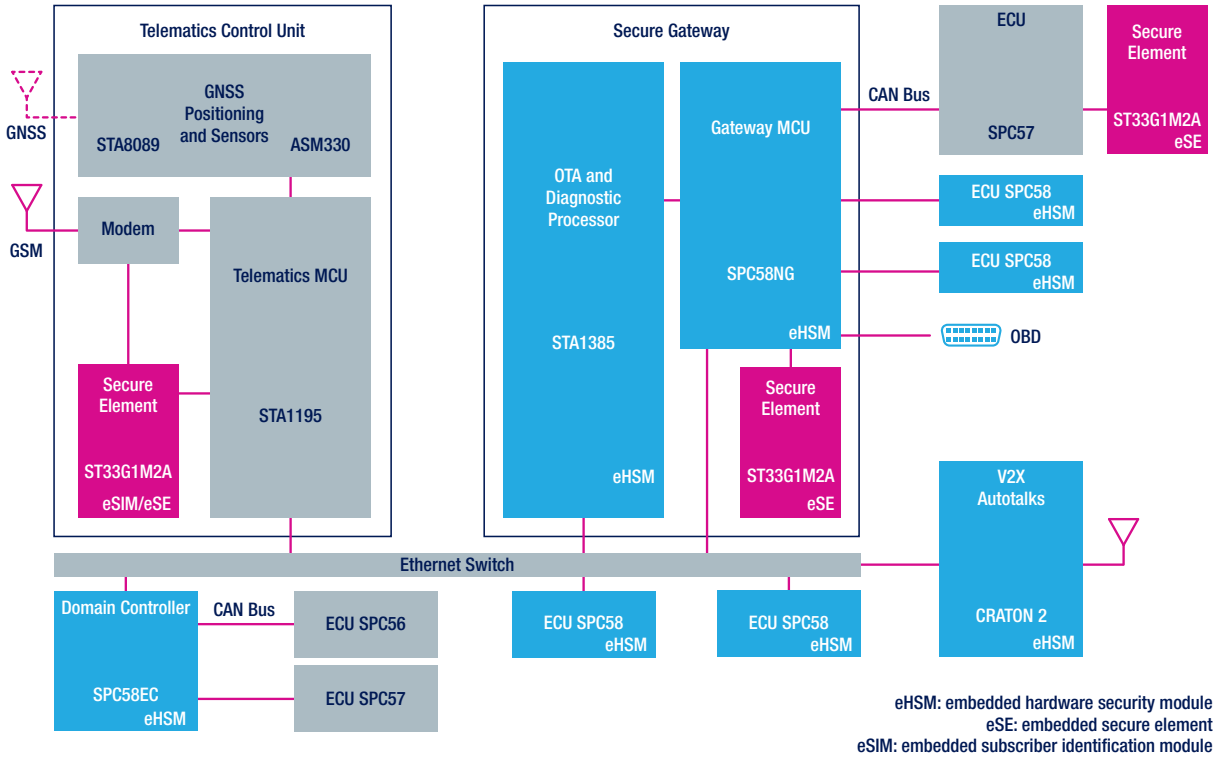
TRUSTED PLATFORM MODULES

Based on proven ST33 Secure Element hardware and a strong leadership in TPM solutions for PC and consumer sectors, ST offers unique Trusted Computing Solutions for the automotive market including secure gateways and telematic control units.
Developers can rely on TPM's proven open standard, with existing security protection profiles, auditable by independent third parties.
In compliance with Common Criteria EAL4+, FIPS 140-2 level 2 and TCG requirements, ST's ST33 TPM platform provides protection against physical and logical attacks. It includes embedded functions that cover tamper resistance, Root of Trust creation, platform and firmware integrity, remote attestation or health checks, mutual authentication, key management and storage, secure software updates, as well as multiple cryptographic services in order to protect users' assets.

ST33 & AUTOMOTIVE SOLUTIONS

Security being a matter of scale, ST33G1M2A secure microcontroller is offered as a security enhancer in pair with in-house Automotive MCUs. It strengthens eHSM hardware and software solutions as well as supports multiple security standards such as the EVITA Project and Secure Hardware Extension (SHE).

SECURE AUTOMOTIVE SOLUTIONS



eHSM: embedded hardware security module
eSE: embedded secure element
eSIM: embedded subscriber identification module