Secure Flash Memory Enabling Trust & Providing Scalability

- Hardware security is the foundation of cyber security
- Secure storage is the core of hardware security
- Security by design

Certified Secure Flash = Trusted & Proven Solution

Security Level

- High
- Substantial
- Basic

TrustME® Secure Flash

**W75F** (High Security)
- ePayment
- eID
- Smart Meter
- iUICC
- Automotive, V2X, Car Key
- Android Strongbox-Related

**W77Q** (Substantial Security)
- Smart Home
- IoT
- Automotive
- AI
- Smart Meter
- Wearable
- WiFi, Bluetooth
- Industrial-IEC 62443 Compliant

**W25Q NOR Flash** • General Purpose
Secure Over-The-Air Firmware Update
Resilience
Root-of-Trust
Secure Storage
Secure SPI Channel

Drop-in Replacement
- Secure Over-The-Air Firmware Update
- Resilience
- Root-of-Trust
- Secure Storage
- Secure SPI Channel

Resilience

Remote Authorized Service
TCP/IP
MCU
SPI

End-to-End Secure Channel