winbond

TrustME® Security Solution

Vision Statement

以綠色半導體技術豐富人類生活的隱形冠軍

Be a hidden champion in providing sustainable semiconductors to enrich human life.

winbond

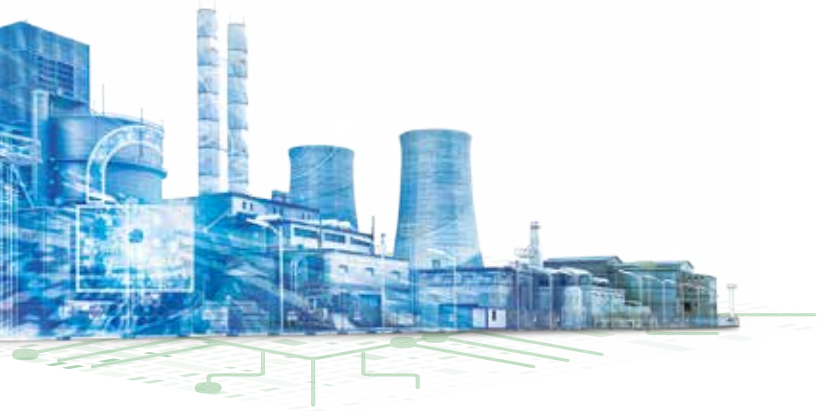
WINBOND'S TrustME®

Application Scope

Winbond introduced the first certified Secure Flash to protect connected devices across several markets

Automotive

- GPS
- Wi-Fi
- Cloud



Industry 4.0

- Sensors
- Robots
- Servers

IoT

- Smart Camera
- Smart Door Locks
- Home Energy Console

winbond
We Deliver

A Leading Specialty & Secure Memory Supplier

A heavy investment on security infrastructure and technology

All manufacturing sites are certified for Common Criteria EAL 5+ products

Active participation in standard bodies and security forums

W75F

Winbond TrustME® W75F Certified Secure Flash Solution

Winbond's W75F Secure Flash Solution is the first secure flash memory device to gain a Common Criteria (CC) EAL5+ certificate. It can be used for secure eXecute-in-Place (XiP) and can protect the confidentiality and integrity of code and data in IoT devices, integrated UICC, integrated Secure Element , Artificial Intelligence (AI) platforms, integrated Hardware Security Modules (HSM) for automotive subsystems. The W75F provides the industry's most secure external storage for code and data. It offers a dependable solution for manufacturers of connected devices who want to defend their products against threats such as replay, roll-back, man-in-the-middle, sniffing, side-channel attack and fault injection attack.

CCN

Centro Criptológico Nacional

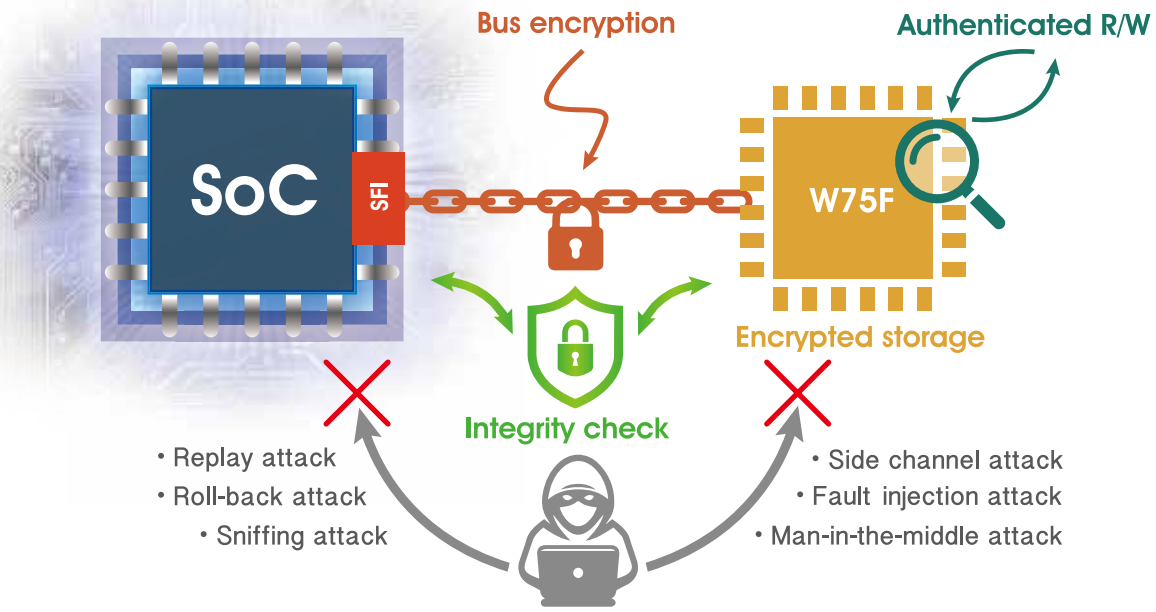
CERTIFICATE

CCN-CC-008/2017

Winbond TrustME™ Secure Element

W76S(2/4)MR(KD/DN/Q1/Q3/4F) version A

03 TrustME® Security



- The world's first Secure Flash device, Common Criteria EAL5+ certified
- Bolt-on security for IoT, Automotive and Artificial Intelligence (AI) platforms
- Complementary solution for Arm®v8-M and Arm®v8-A TEE sub-system
- In-band integrity check protects the interface
- Flexible secure memory architecture

Flash Density	Product Series	Voltage	Certificate	Feature	Package
4M bit 16M bit 32M bit	W75F	1.65-1.95V	CC EAL 5+	• Secure eXecute-in-Place (XiP) • Tamper and SCA/DPA Resistant • Code and Data Confidentiality and Integrity • Mutual Authentication with SoC • Secure SPI Quad/Octal Interface • Shared Memory Architecture for Multiple-Domains • AEC-Q100 with AG2 Qualification Available or Upon Request • 21 MByte/sec Secured and Authenticated Throughput • 100,000 Program/Erase Cycles • 20-year Data Retention • Temperature Range : -40°C to 105°C	WQFN32 5x5mm WLCSP

KGD

We also offer KGD (Known Good Die) products. For further information please contact: TrustME@winbond.com

W76S

Winbond TrustME® W76S Secure Element/eUICC Solution

Winbond W76S secure element is an innovative solution which includes 4MB Secure Flash whose memory size can be scaled to meet designers' requirement. W76S comes with Arm® SecurCore™, SC000™ 32-bit RISC with a core clock up to 100MHz and Memory Protection Unit (MPU). Various coprocessors, crypto, such as 3DES, AES 128/192/256, RSA-2048/4096, and ECC 521, True RNG and side-channel attacks (SCA) LICENSED DPA COUNTERMEASURES are used in W76S to advance the security features. W76S has passed Common Criteria EAL5+, EMVCo and CFNR (China Financial National Rising Authentication) certification. It can also be used for the embedded UICC (eUICC) application, supporting multi-profiles, remote provisioning, at the same time, save footprint on the PCB. The eUICC will bring benefit to the growth and enhances operational efficiency of the M2M ecosystem.


EMVCo

EMVCo Product Approval

(IC)


CCN

CERTIFICATE


服务认证证书

华邦电子股份有限公司

北京中金国盛认证有限公司

Premium Content Protection

- Usage of individual secret key per title
- Limiting number of playbacks/shares

Internet of things (IoT)

Electronic Wallet

- Mobile payment
- Software secure solution

Winbond TrustME®

Secure Boot

- Protect boot code from modifications
- Secure execution storage vs. Root-of-Trust e.g. TPM

Support AG2 (Automotive)

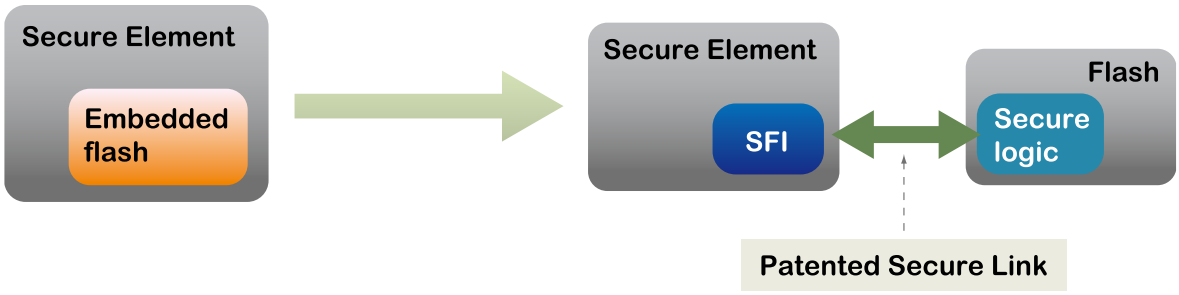
GSMA Remote Provisioning

- Support OTA technology to lower international roaming switching cost between countries
- GlobalPlatform UICC Card Architecture
- 32-bit CPU based on the Arm® SecurCore™ SC000™

Biometric Information Authenticity

- Fingerprint storage

Winbond's Patented Architecture



Uniquely Paired Secure Controller and Secure Flash Memory

- Added digital logic to flash device to protect secure flash interface and create secure link between integrated IP and flash
- Flash device from Winbond as a security companion device

Cost Effective, Two Separate Devices

- Standard flash memory process
- Standard CMOS process for the controller

Scalable Large Flash Density to Enable Application Innovation

Flash Density	Product Series	Voltage	Clock (MHz)	Feature	Package
2M Byte 4M Byte	W76S	1.65-3.6V	100	• 32-bit CPU based on Arm® SecurCore™ SC000™ Core • 32KB RAM • 2MB/4MB Secure Flash • Compatible with Java Card Specification 3.x • Crypto Accelerators for 3DES, AES, RSA, ECC, SHA, TRNG • GSMA Remote Provisioning Specifications Compliant • GlobalPlatform UICC Card Architecture Support • AG2 Support • SWP, SPI, ISO 7816, I2C, GPIOs • Temperature Range: -40°C to 105°C • CC EAL5+ Certificate • EMVCo Approval • CFNR Certificate	WQFN32 5x5 mm WSON12 4x4.2 mm SON8(MFF2) 6x5mm WSON8 4x4.2 mm

Contact us: TrustME@winbond.com

Winbond TrustME® W77Q Secure Flash

SpiNOR Flash Compatible Memory Enabling Comprehensive, End-to-End Security

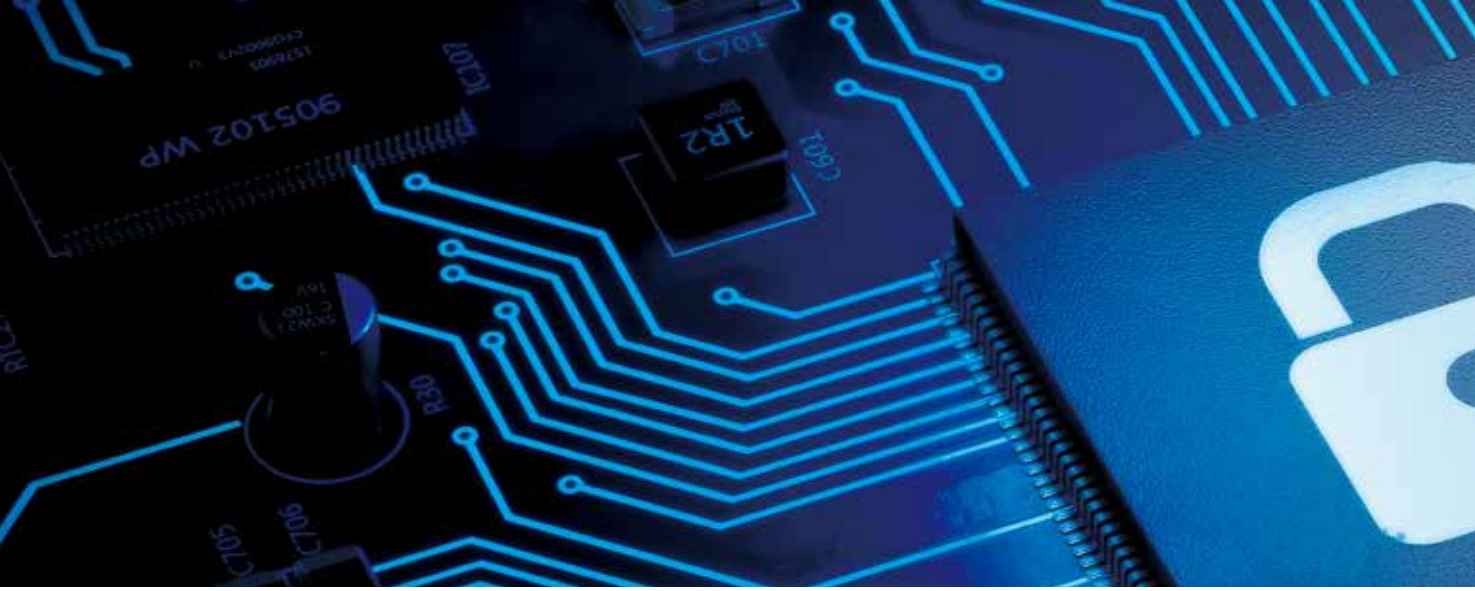
W77Q series of Secure Flash memory devices is a drop-in replacement for standard flash devices. It supports secure boot and system level resilience, and provides strong protection for operations such as over-the-air updates and device authentication. The new W77Q enables hardware root-of-trust and secure, encrypted data-storage and transfer capabilities. It ensures robust and secure over-the-air updates with end-to-end secure channel between the updating authority and the IoT device equipped with W77Q, even when the host processor is compromised.

Flash Density	Product Series	Voltage	Clock (MHz)	Feature	Package[1]
32 Mbit	W77Q	1.65-1.95V	66MHz at Double Transfer Rate/ 133MHz at Single Transfer Rate	• Hardware-based Root-of-Trust engine • Device attestation • Cryptographically secured write protection • Secure code updates with anti-rollback • Secure boot from Flash (Root-of-Trust) with fast execution • Secure eXecute-in-Place (XiP) of boot and application code • Authenticated watchdog timer • Authenticated and encrypted data transfer between the Flash and the host • Secure over-the-air update with end-to-end secure channel between the updating authority and W77Q even when the host processor is compromised • Secure interface: § Replay Protection Monotonic Counter (RPMC) • Incremental security § In-field fail safe configuration update § Secure symmetric key management • Secure unique device ID • 20-year data retention • 100,000 program/erase cycles • Operating temperature range of -40°C to 105°C	SOP16 (300-mil) WSON8 (6x5) 24-ball TFBGA

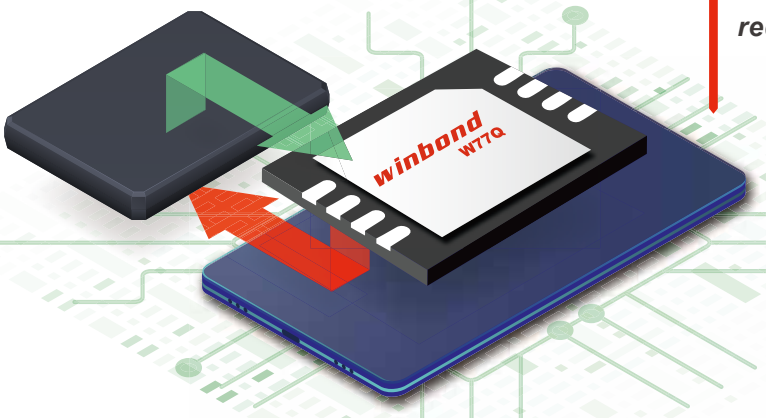
1. For other package and density, please contact: TrustME@winbond.com

KGD

We also offer KGD (Known Good Die) products. For further information please contact: TrustME@winbond.com

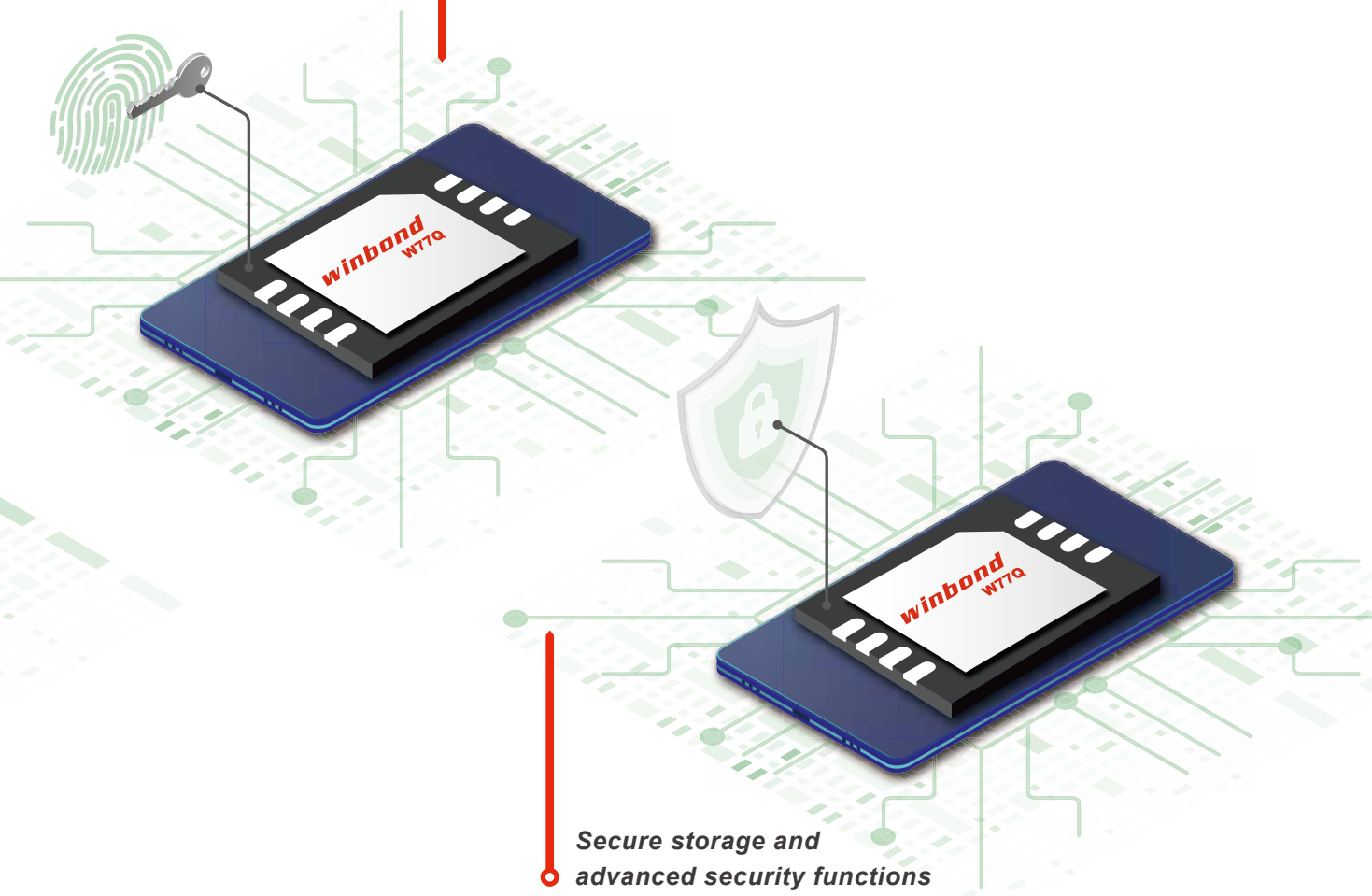


100% electrical and functional drop-in replacement for standard serial flash
Fast integration path with no need to redesign board or SoC



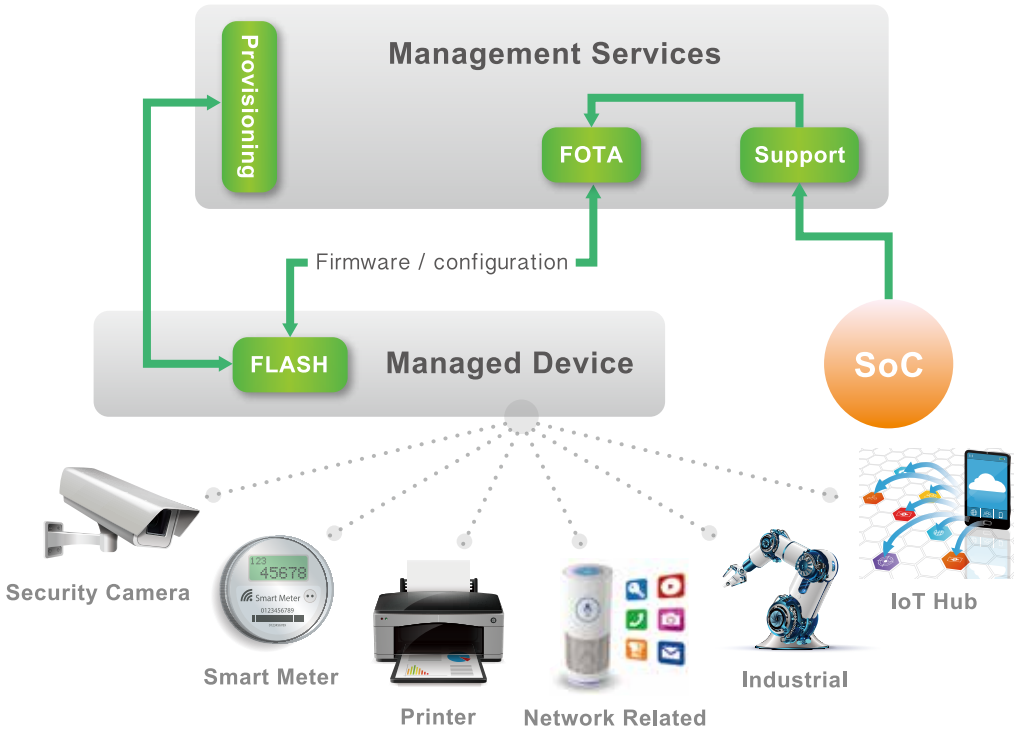
Secure over-the-air update support

Advanced security features
Automatic code and data authentication and fallback



Secure storage and
advanced security functions

ARCHITECTURE OVERVIEW



Root-of-Trust Secure Flash Memory

- Self code integrity check and secure boot
- Hacking detection
- System recovery (Resilience)

3rd Party Certified and Trusted Memory

- CC/EAL2 (in progress)
- SESIP (in progress)

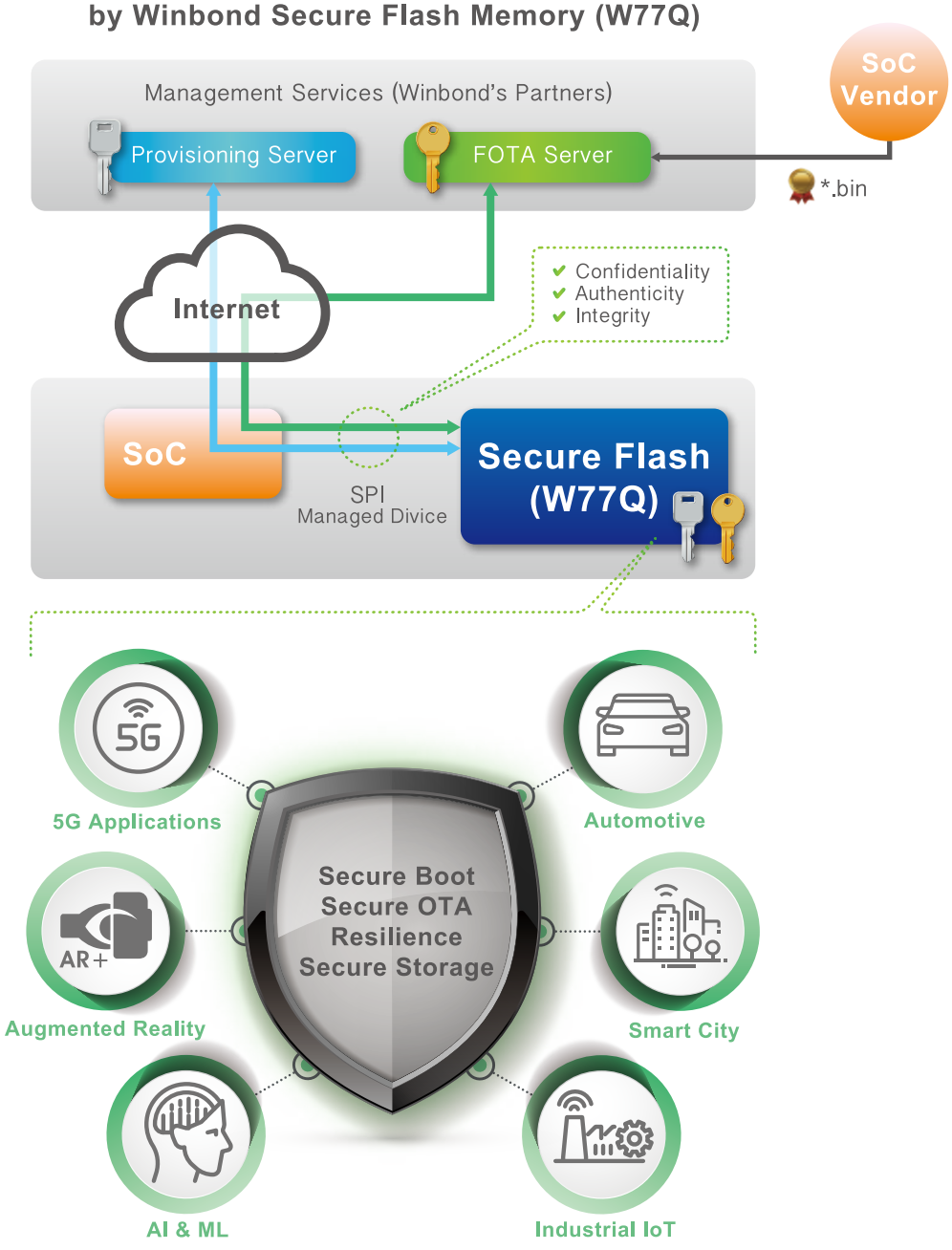
End-to-End Security Architecture

- Even with unsecure or compromised host processor
- Secure firmware over-the-air update
- Remote memory configuration for high / substantial / basic security demand

Drop in Replacement

- Compatible with standard flash memory
- Enables incremental security

End-to-End Security Application Example by Winbond Secure Flash Memory (W77Q)



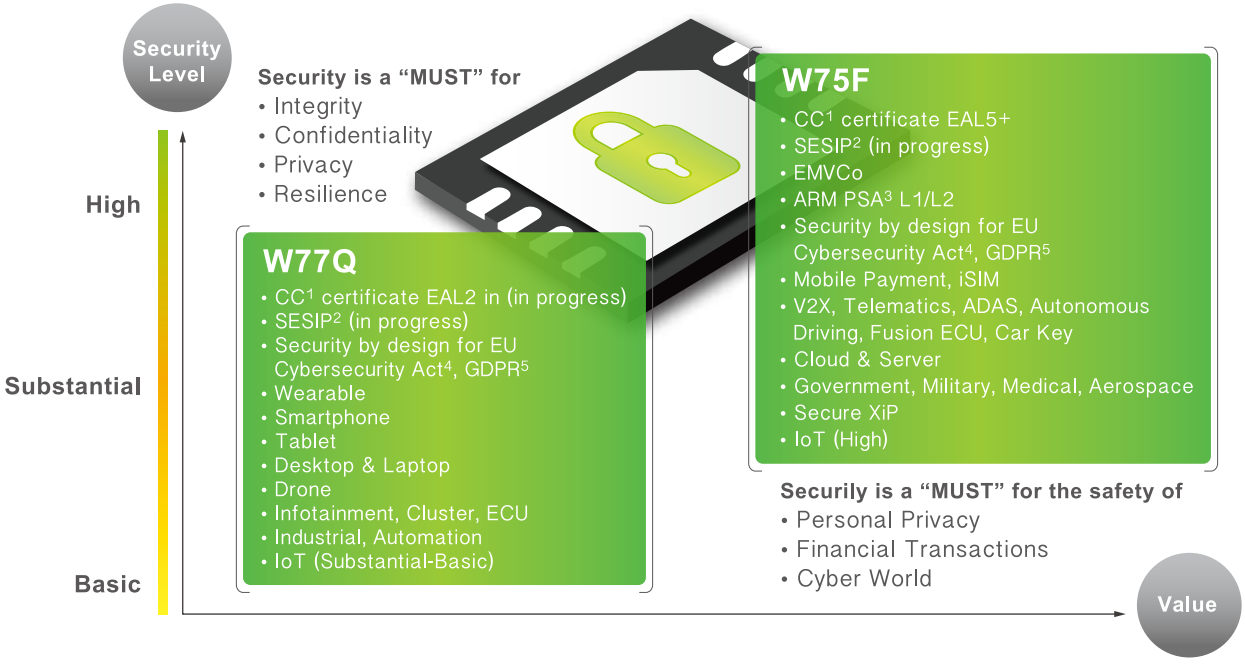
Business Benefits

- Drop-in replacement for standard flash
- Fast-time-to-market product development
- System resilience with protection, detection and recovery

winbond
We Deliver

Winbond's Portfolio Addresses All Levels of Resilience And Protection

W75F and W77Q can satisfy the composition certification scheme to save customer's effort and expedite time-to-market



1. Common Criteria (CC) for Information Technology Security Evaluation
2. The Security Evaluation Standard for IoT Platforms (SESIP) defines a standard for trustworthy assessment of the security of the IoT Platforms
3. Arm's Platform Security Architecture
4. The EU Cybersecurity Act establishes an EU-wide cybersecurity certification framework for digital products, services and processes.
5. The General Data Protection Regulation (EU) 2016/679 (GDPR)

winbond

WORLDWIDE SALES OFFICE

Winbond Electronics Corporation -CTSP Site
No. 8, Keya 1st Rd., Daya Dist.,
Central Taiwan Science Park,
Taichung City 42881, Taiwan
Tel：886-4-2521-8168

Jhubei Office
No. 539, Sec. 2, Wenxing Rd., Jhubei City,
Hsinchu County 30274, Taiwan
Tel：886-3-567-8168

Taipei Office
2F., No.192, Jingye 1st Rd., Zhongshan Dist.,
Taipei City 10462, Taiwan
Tel：886-2-8177-7168

Winbond Electronics Corporation America
2727 North First St., San Jose,
CA 95134, U.S.A.
Tel：1-408-943-6666

Winbond Electronics (Suzhou) Limited
Room 1206, Kingboard Plaza (Building B, 12 floor),
No.505, Guangming Road, Huaqiao Town,
Kunshan City, Jiangsu Province, China
Te：86-512-8163-8168

Winbond Electronics (Suzhou) Limited
-Shenzhen Branch office
8F Microprofit Building, Gaoxinnan 6 Road,
High-Tech Industrial Park,
Nanshan Dist. Shenzhen, P.R. China
Tel：86-755-3301-9858

Winbond Electronics (H.K.)Limited
Unit 9-11, 22F, Millennium City 2,
378 Kwun Tong Road, Kowloon, Hong Kong
Tel：852-2751-3126

Winbond Electronics Corporation Japan
Shin-Yokohama Square Bldg. 9F 2-3-12 Shin-Yokohama,
Kouhoku-ku,Yokohama, kanagawa 222-0033, Japan
Tel：81-45-478-1881

www.winbond.com