Secure MCUs for IT security

STMicroelectronics

System-on-chip for trusted services

STMicroelectronics has developed a unique portfolio of products to support the development and deployment of IT and PC peripherals.

With extensive experience in secure MCUs and system-on-chip (SoC) devices, combined with advanced inhouse packaging systems, ST provides innovative solutions for USB and TPM applications.

TPM solutions for PC motherboards

Trusted computing is set to become the major IT challenge for companies and governments, as computer systems become ever more complex and vulnerable, in an increasingly open and hostile environment. The trusted platform module (TPM) is a secure MCUs hardware component permanently located on the platform. The TPM standard, TPM v1.2, is defined by the Trusted Computing Group (TCG) for implementation on PC clients, PC server platforms, mobile phones or storage devices, among others. The TPM sits on the platform motherboard and provides the first link in the chain of trust. The TPM validates the integrity of the BIOS and the platform hardware, so it can then be used to verify platform boot and OS loading, as well as application integrity.

ST19NP18-TPM

At the forefront of trusted computing standards, the ST19NP18-TPM, which is the leading TCG 1.2 device for the major PC motherboard manufacturers, is now available with a 100 kHz I²C communication capability for embedded systems. This release of ST's TPM is compliant with the latest version of the TCG TPM v1.2 specification, and provides support for direct anonymous attestation (DAA) and secure field upgrades, in particular. The ST19NP18 is based on enhanced NVM technology and confirms ST's commitment towards advanced process technology.

USB connectivity solutions

Secure USB tokens are a clever, practical and cost-effective solution to ensure personal IT security and access control for corporate IT networks. A portable USB-based device allows users to carry their secure digital and biometric signatures wherever they go, so they can identify themselves securely on any digital appliance.They are particularly suitable for PC-based applications such as secure login, secure e-mail, digital signatures, secure Internet/extranet/ intranet and remote access.

USB tokens and cards with USB secure MCUs

With the 8-bit based ST19XT34 device, ST was the first company to release a secure microprocessor with combined ISO 7816 and USB interfaces. Since then, we have expanded our portfolio with a new range of USB products with enhanced features. These products are based on the new ST23 secure platform with its new cryptographic engine and libraries (RSA, ECC). The additional versatile GPIOs and serial communication capabilities allow you to develop applications with a user-friendly interface, or to emulate a CD-ROM for more secure application launching on a computer. Its rich USB interface provides for composite devices with various USB profiles or classes, such as CCID or mass storage which use native Windows drivers.

ST19NP18-TPM

- Single-chip trusted platform module
- Advanced CMOS EEPROM process with enhanced performances
- Embedded TPM firmware
- Full TPM solution with complete TCG-compliant software stack layers
- Asymmetric crypto-coprocessor
- Hardware-based SHA-1 accelerator
- Active security sensors
- 33 MHz LPC interface v1.1
- Five software-controlled GPIOs
- 100 kHz I²C interface

ST23YT66 and ST23YT34

- 8/16-bit ST23 secure core
- Full speed certified USB 2.0
  - USB libraries supplied by ST
  - CCID, HID and mass storage USB compliant
  - No external crystal needed for USB operations
  - Data transfer hardware accelerator
- Nescrypt cryptographic co-processor
- EDES engine
- True random number generator – AIS31
- Up to 12 general-purpose I/Os
- ISO 7813-3 and serial peripheral interface

ICs for IT security on ST19 and ST23 platforms

Application	Part number	EEPROM (Kbytes)	ROM (Kbytes)	RAM (Kbytes)	Cryptography	Interface
USB	**ST23YT66**	66	210	6 + 2	EDES, PKI	USB 2.0 12 Mbit/s, ISO 7816-3, SPI, GPIO
	ST23YT34	34	110	5 + 2	EDES, PKI	USB 2.0 12 Mbit/s, ISO 7816-3, GPIO
TPM	**ST19NP18-TPM**				EDES, PKI, SHA-1	LPC, GPIO, I²C 100 kHz, GPIO

Packaging

ST has the unique ability to offer secure MCUs in form factors other than traditional micromodules. Packages such TSSOP20 (for ST23YT66), SO8-Narrow (for ST23YT34), and TSSOP28 or QFN (for TPM) combine integration and security. All these packages are ECOPACK versions, compliant with the European directive 2002/95/EC relating to restrictions on hazardous substances (RoHS).