Secure MCUs for pay-TV applications

STMicroelectronics

Conditional access and content protection

STMicroelectronics is the world's leading supplier of ICs for pay-TV and conditional access, and has extensive experience supplying 8- and 32-bit secure microcontrollers for conditional access to pay-TV providers.

Drawing on its expertise in security and non-volatile memories, ST is upgrading its pay-TV product family with the introduction of a new enhanced 8/16-bit microcontroller combined with EEPROM and a new 32-bit ARM SC300™ based microcontroller associated with high-density Flash storage.

Conditional access for pay-TV

Anticipating both upcoming cryptographic requirements and security features, ST continues to develop new, secure, state-of-the-art microcontrollers for pay-TV applications.

To meet the tough requirements of the pay-TV environment, all products are not only EAL5+ certified, but also integrate specific advanced security features gained from ST's long experience in custom, semi-custom and standard products for pay-TV.

ST's cryptographic coprocessors, associated with our proprietary cryptographic software libraries, present best-in-class timing and security performances.

The ST23 8/16-bit core family is based on the latest EEPROM technology, providing low- to mid-range pay-TV requirements. Products with additional peripherals such as full-speed USB 2.0, SPI interface and general-purpose inputs/outputs are available for future application trends.

For increased performance demands, ST's 32-bit core products, such as the ST33F1M, include state-of-the-art embedded Flash technology. They combine high security, high computation power and high-density storage capabilities.

Several standard-product families are proposed for pay-TV:

- ST23YSxx for symmetric cryptography with embedded EDES engine and software AES, based on a standard ISO 7816 interface.
- ST23YLxx which in addition offers a new hardware cryptographic coprocessor (Nescrypt) enabling best-in-class asymmetric cryptography computation.
- ST23YTxx also featuring asymmetrical cryptography, but with full-speed USB 2.0 and SPI interfaces, as well as GPIOs.
- ST33F1M: highly-secure 32-bit ARM SC300-based microcontroller combined with 1.2-Mbyte Flash storage. Also embeds Nescrypt cryptographic accelerator for best-in-class asymmetric cryptography.

Latest-generation secure MCUs for pay-TV

ST23YS family

- 8/16-bit CPU core
- 2- or 8-Kbyte EEPROM
- EDES engine
- ISO 7816-3 interface

ST23YL/ZL family, standard range

- 8/16-bit CPU core
- 18-, 48- or 80-Kbyte EEPROM
- Nescrypt cryptographic coprocessor
- EDES engine
- ISO 7816-3 interface

ST23YT family: USB, SPI range for conditional access tokens

- 8/16-bit CPU core
- 34- or 66-Kbyte EEPROM
- Nescrypt cryptographic coprocessor
- EDES engine
- ISO 7816, SPI, full-speed USB 2.0 interfaces plus GPIOs

ST33F1M for high-density storage

- ARM SC300 32-bit RISC core
- 1.2-Mbyte Flash for code and data storage
- Nescrypt cryptographic coprocessor
- EDES engine
- ISO 7816-3, SWP or SPI interface

ST23 secure MCUs for pay-TV

Part number	EEPROM (Kbytes)	Program memory	RAM (Kbytes)	Cryptography	Interface	Process
ST23YS02	2	32-Kbyte ROM	2	EDES, AES	ISO 7816-3, IART	0.13 µm
ST23YS08	8	108-Kbyte ROM	2	EDES, AES	ISO 7816-3, IART	0.13 µm
ST23YL18	18	196-Kbyte ROM	4+2	EDES, AES, RSA, ECC	ISO 7816-3, IART	0.13 µm
ST23ZL48	48	300-Kbyte ROM	6+2	EDES, AES, RSA, ECC	ISO 7816-3, IART	90 nm
ST23YL80	80	396-Kbyte ROM	6+2	EDES, AES, RSA, ECC	ISO 7816-3, IART	0.13 µm
ST23YT34	34	110-Kbyte ROM	5+2	EDES, AES, RSA, ECC	USB, ISO 7816-3, IART	0.13 µm
ST23YT66	66	210-Kbyte ROM	6+2	EDES, AES, RSA, ECC	USB, ISO 7816-3, IART, SPI, GPIOs	0.13 µm
ST33F1M	-	1.2-Mbyte Flash	30	EDES, AES, RSA, ECC	ISO 7816-3, SWP, SPI	90 nm

Packaging

ST has the unique ability to offer secure MCUs in form factors other than traditional micromodules. Packages, such as TSSOP20 and SO8N, combine integration and security. All these packages are ECOPACK versions, compliant with the European directive 200/95/EC relating to restrictions on hazardous substances (RoHS).

Security

The ST23YL/ZLxx, ST23YTxx and ST33F1M all benefit from hardware protection against the most recent attacks.

Order code: FLPAYTV1010