Flexible Swissbit Solution

IoT security embedded in memory cards

As devices, machinery and manufacturing plants get smarter, they also become more vulnerable. When designing networked devices, machinery and production facilities, developers need to place more focus on security aspects. Swissbit now offers a flexible, hardware-based approach that includes TPM (Trusted Platform Module) and data encryption.

For IT- and data-security, systems communicating over the Internet or via their gateways in the IoT (Internet of Things), need to have a unique and non-cloneable identity. Systems must also be able to send, receive and store cryptographically and heavily secured data. Solutions involving only the use of software rarely offer sufficient protection. This presents developers and manufacturers with great challenges.

Swissbit, the storage and security expert, offers a new hardware-based approach. Developers of embedded systems for industrial applications know Swissbit as the only independent European manufacturer of flash memory products. Many see the Swiss company, producing in Germany, as their top choice for robust, durable SSDs with PCIs and SATA-interfaces, CompactFlash, USB-flash drives, SD and microSD memory cards and managed NAND BGAs.

Based on decades of experience in the protection of stored data, Swissbit has now developed a new advanced approach to security for embedded IoT devices. The thought process behind the development is that every device needs memory to act as a boot medium for log files, and data cache memory in case of network failures. These memory interfaces can and should have security features.

Security in memory card format

Swissbit's new security solution consists of a flash memory chip, produced and tested for industrial requirements. This chip is run using a special version of the durabit firmware with integrated AES 256-bit encryptor. The DP (Data Protection) version encrypts and protects all data in various ways (CD-ROM mode, PIN protection, hidden memory, WORM mode). For the hardware-based protection of the communication in the IoT, another security anchor is required. Swissbit's security modules come with solutions such as an Infineon/NXP Smart Card Chip CC EAL 5+/6+. An API, a SDK and a PKCS#11 library are available for application development.

Designating an ID to things

Security experts trust in microSD cards with secure element for encrypting mobile phone communications. Similar to the communication between people, the communication of the things in the Internet also needs to employ identification, authentication and authorization. In other words, how does a "thing" know that the data or data queries received from another "thing" are correct and that the source of a message is truly the system component that it claims to be? Swissbit security memory media, with secure element, provide applications and systems with a unique identity. "Things" get a counterfeit-proof ID and as such, networked systems can be protected from misuse,

“identity theft” and data access can be restricted. Smart cards, that are integrated onto memory cards, provide systems with non-cloneable identities, transforming them into uniquely identifiable M2M (machine-to-machine) communication participants, that can authenticate themselves and send and recieve cryptographically heavily secured data.

Another important device-specific application for these Swissbit solutions is Trusted Boot. Trusted Boot ensures that software can only be run on specific hardware or hardware classes. A secure flash memory card can be used to manage software licensing and feature activation. Access control, code encryption or digital signature allow the definition and management of different software configurations for products.

Retrofittable and future-proof

In comparison to a soldered TPM, the idea of a pluggable security module might at first seem unusual. However, older machinery and systems generally have a USB interface or interfaces for memory cards. Therefore, the big advantage of using pluggable security modules is that existing devices can easily be retrofitted and secured using Swissbit security memory.

This ability to retrofit devices offers another advantage in the constant race to keep up with cyber security. Attack and defense methods develop cyclically and harmonizing them with for example the project lifecycle of an industrial plant is challenging. A situation could arise where it necessary to allocate a new ID with improved cryptography technologies to the M2M communication participants. Swissbit’s retrofittable solution makes this possible.

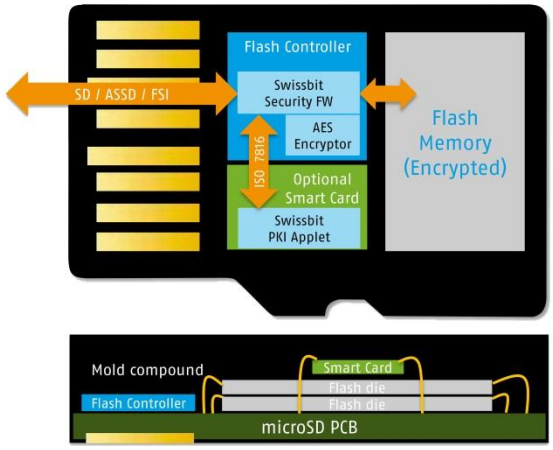
Outlook

In response to the rapidly increasing market demand for embedded IoT, Swissbit opened its new factory in October 2019, located in Berlin, Germany. This factory is equipped with state-of-the-art advanced 3D chip scale packaging technology, developing and producing customized system-in-package and multi-chip module designs for its customers. This technology facilitates not only the integration of microcontrollers, NAND chips and crypto chips, but also sensors, wireless chips and antennas. Using memory interfaces with TPM and encryption components for security solutions might only be the beginning, with the scope for the addition of further functionalities that can be miniaturized and integrated.

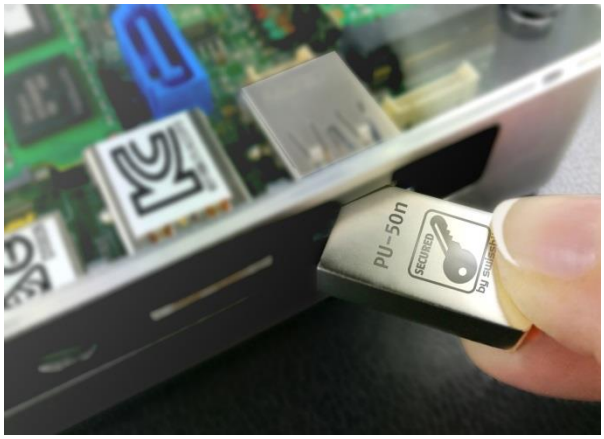
Current example TSE for POS systems

Swissbit’s business division for security products, Embedded IoT, will be at embedded world to present technical security equipment (TSE), for example tamper-proof recording of cash register data.

((Image source Swissbit))



The structure of a microSD card with security features.



Memory interfaces, such as USB, can be used to retrofit a TPM function.