Digital signatures eliminate product cloning threats

15th January 2015 SEGGER Microcontroller GmbH & Co. KG Nat Bowers

Digital signatures can help to eliminate the threat of product cloning.

By Dirk Akemann, SEGGER Microcontroller.

Embedded systems are an integral part of many modern investment, industrial and consumer products. Unless preventive technological protection is provided, sophisticated technologies enable attacks to be made on hardware and software in embedded systems. SEGGER emSecure is the first digital signature software package designed specifically for embedded systems. The toolkit is hardware independent and provides a complete set of high-level functions which allow the developer to easily add a digital signature to a product and provide a high level of security.

The emSecure software package allows creation and verification of digital signatures. One important application is to make it impossible to create a clone of an embedded device by copying hardware and/or firmware. And it can do much more, such as verifying the authenticity of firmware updates for embedded devices, licenses, serial numbers or other sensitive data - a must for critical devices such as election machines, medical devices, industrial controls, financial applications and many others. Based on RSA asymmetric encryption (Figure 1) with 2 keys (public and private key), it cannot be broken by reverse engineering.

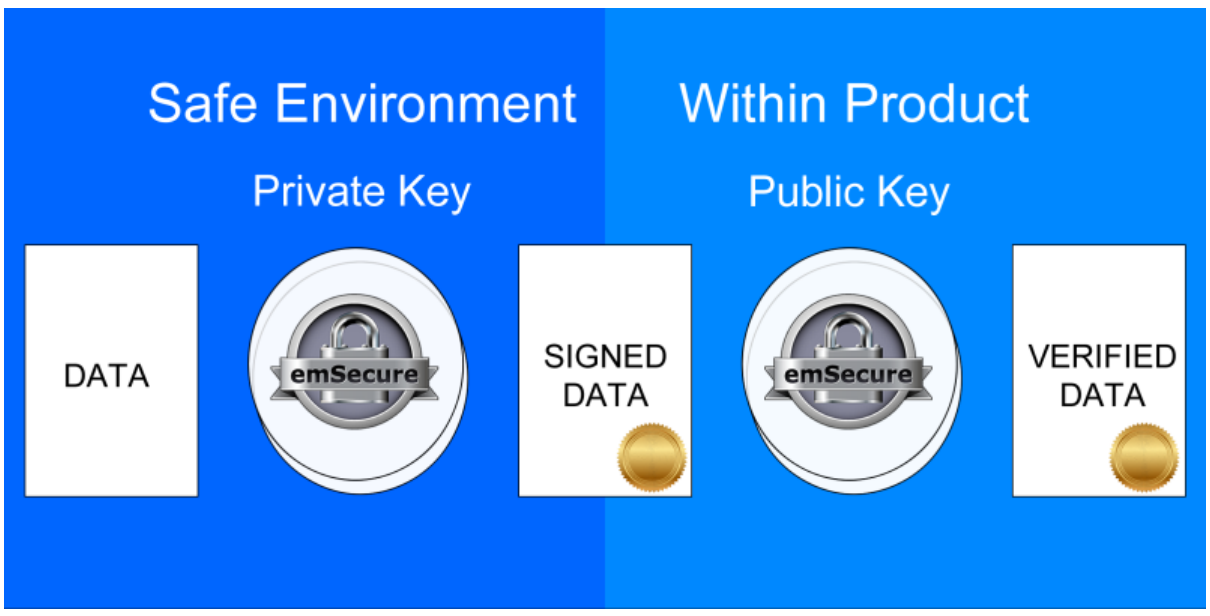

Figure 1 - Working principle of emSecure

The source code from emSecure has been created from the ground up for embedded systems in order to achieve a small memory footprint, high performance and be very portable. emSecure is a very complete package, including all the necessary functionality for the generation and verification of digital signatures, and its use is not restricted to embedded systems.

Secure firmware update

CRCs (Cyclic Redundancy Checks) and hash functions are in general a good way to ensure that a data transmission such as a firmware download has worked flawlessly. They can also be used to make sure that an image has not changed when stored in flash memory. However, they do not add much security, as an attacker can easily compute the CRC or hash value of a modified firmware. The important difference with digital signatures is that the digital signature is based on an asymmetric encryption algorithm (RSA): The digital signature — as used in emSecure — cannot be forged by analysing the verification code in the firmware. The digital signature can only be generated with the private key (Figures 1 and 2), which is not contained in the firmware. In addition to the integrity check, which is also provided with CRCs and hash functions, a digital signature assures the authenticity of the provider of the signed data, as only he can create a valid signature.

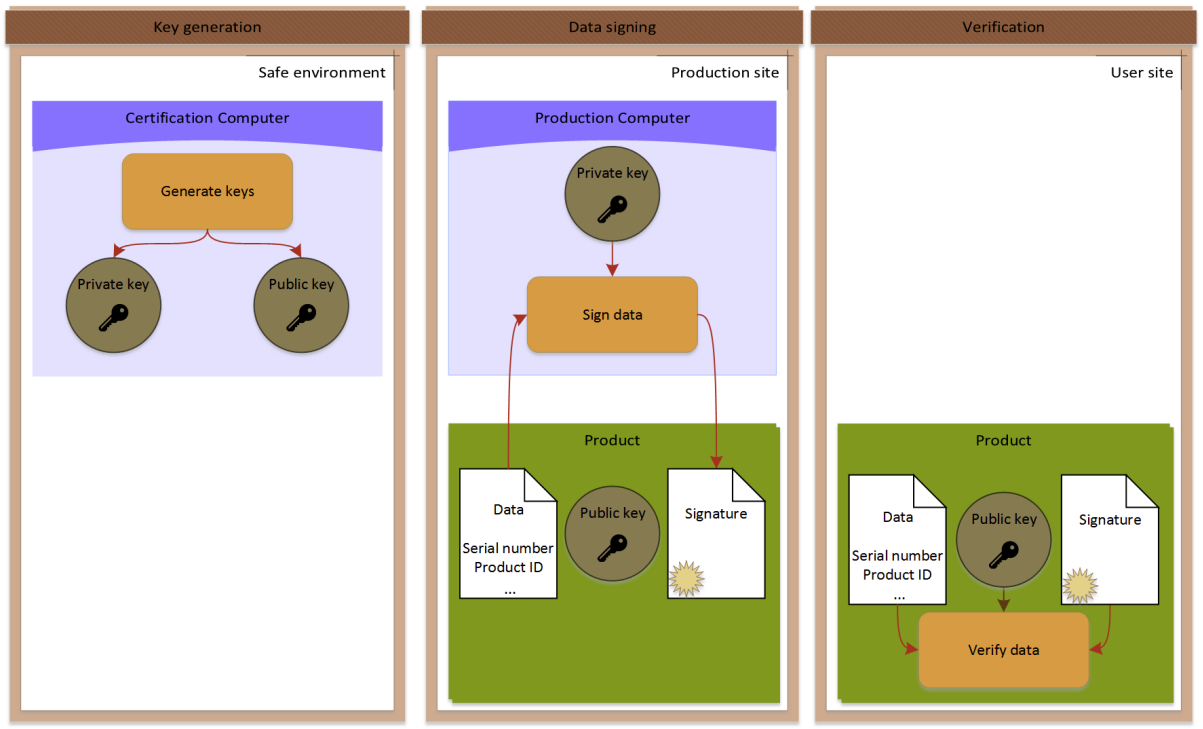

Figure 2 - emSecure provides OEMs an efficient solution to bring security in their production process

emSecure has a simple yet powerful API. It can be easily integrated into an existing application. The code is completely written in ANSI-C and can be used platform- and controller-independent. Key pairs can be generated on a computer, as well as on any embedded system itself. The generated keys can be exported into different formats to be stored in the application code or loaded from a key file. This allows portability and exchangeability between different platforms.

A complete package

emSecure is a complete package that comes with everything needed: A utility to generate the private and public keys, and create and verify digital signatures. All parts of the package conform to the relevant FIPS (Federal Information Processing Standard) specifications issued by NIST (National Institute of Standards and Technology). Verification functions using the test vectors provided in the FIPS 186-4 allow testing the implementation as well as the code produced by the compiler.

emSecure includes all basic applications needed for securing a product. Additional applications for benchmark and validations are also part of emSecure. The applications' source-code is included and provides an easy to use starting point for modifications and integration into other applications. The utilities are PC applications, ready-to-use for the one-time setup step to secure the related device. The example applications can be used ‘as is’, but are mainly included as a reference to include emSecure in the customer product.

emSecure is a very convenient and powerful solution for adding product security to an embedded device. Compared to Hardware-based approaches the software only solution provides space and costs advantages, as it reduces the BOM (for hardware encryption chips). Using emSecure requires relatively little effort (software only) compared to hardware approaches. In addition the new software package enables an easy ‘upgrade’ to protected firmware for existing products, prevents product cloning and tampering with the firmware. Developed with a focus on embedded systems, the software package is a hardware independent product which will work on PCs as well.