



BY DAVID RICETTO • INSIDE SECURE

STRATEGIES AND TECHNOLOGIES ARE AVAILABLE TO HELP ENGINEERS DEVELOP AND IMPLEMENT SECURITY MEASURES TO PREVENT COUNTERFEIT PRODUCTS FROM ENTERING THE SUPPLY CHAIN.

Product counterfeiting has been an issue in many industries, from consumer products to ICs. In many instances, the counterfeit products affect only the bottom line and a company's reputation. High-end luxury consumer goods, such as handbags, wristwatches, and other products, are among the most susceptible to counterfeiting, and the brand holders spend large amounts of money to trace and eliminate the counterfeit products and the people responsible to ensure that fake products don't sully their brands. The IACC (International Anticounterfeiting Coalition) estimates that brand holders lose approximately \$600 billion of revenue annually due to counterfeiting. According to Michael Danel, the secretary general of the World Customs Organization, if terrorism did not exist, counterfeiting would be the most important criminal act of the early 21st century.

The effect of counterfeiting is always greater than the value of the counterfeit product itself. By damaging consumers' perception of the performance, reliability, and safety of branded devices, counterfeiting tarnishes brand image, customer loyalty, and satisfaction. It also has broader negative effects, such as reducing the value of intellectual capital, eroding profitability, and stifling innovation. It hurts not only the companies making the components but also the financial health and ability to invest in future innovation of all companies across multiple industries—from intellectual-property-right holders of the embedded software, firmware, and codecs in these devices to proprietary SOC architectures.

Furthermore, counterfeits of electronic components and system-level products as well as mechanical products and prescription medications can also affect personal safety and security. Counterfeiters often sell an inferior product as the genuine article, and the fake products typically fail to meet the full range of genuine product specifications and performance standards. Unfortunately, counterfeit electronic products, including ICs and battery packs, have also found their way into military, health, and transportation systems, and those systems could fail in the field, jeopardizing military and civilian lives.

SECURITY OPTIONS

Engineers can use multiple approaches to preventing counterfeit products from functioning in a system and thus prevent potential damage. At the simplest level, a product such as a battery or an ink cartridge can include an electronic signature that the host system must recognize for the product to work. To add an extra layer of security, the product can include an encrypted identifier to ensure that the counterfeiters cannot duplicate the signature.

Containers holding prescription medications or stand-alone mechanical products also could be "tagged" by attaching a secure electronic ID tag. These tags can prevent counterfeit products from entering the supply chain. Manufacturers in the luxury-goods market can embed contactless tags that contain a security handshake in an ID tag that either attaches to or is permanently embedded in the product. The tag must also be small and be avail-

AT A GLANCE

At the simplest level, a product such as a battery or an ink cartridge can include an electronic signature that the host system must recognize for the product to work.

Properly implemented authentication using asymmetric cryptography—the core technology behind digital signatures and certificates—offers the robust protection that can thwart counterfeiters.

Whether designers use an off-the-shelf product or design their own, the chip they use should include a secure RISC CPU; a hardware random-number generator; a hardware cryptographic-acceleration engine; a secured block of nonvolatile memory for secure storage of keys, certificates, user data, and other information; and communication interfaces, such as I²C or 1-Wire.

Only an authentic product with knowledge of the private key can produce a correct digital signature.

able in various form factors to accommodate the shape of various products—wine bottles, handbags, or jewelry, for example.

Various approaches can be used to minimize the influx of counterfeit products into the supply chain. Technologies such as holograms and simple RFID transmitters are no longer adequate because counterfeiters keep up to date on the latest copying and code-breaking techniques. Using sophisticated manufacturing equipment and technologies, well-organized groups have now shifted their targets to include more low-margin, high-volume products, such as consumer electronics and consumables.

One of the main trade-offs of these authentication systems is the cost of protection versus the value of the protected product. This trade-off is especially critical when it comes to relatively low-cost products, such as toner cartridges, batteries, and other consumables. This cost factor has played a major role in preventing consumer-electronics manufacturers from successfully employing what is perhaps the best technology for protecting their products: asymmetric authentication.

Thus, more advanced security technologies are necessary to prevent the illegal copying of products. These more-robust approaches employ strong cryptographic techniques and strong authentication to protect some high-value products. Until now, however, these approaches have been too costly and complex to implement in lower-cost, high-volume products, such as ink and toner cartridges for printers and batteries for mobile devices. Such technologies add cost and complexity to the products they protect, and designers must walk the fine line between the product's cost and the overhead to protect the product.

For instance, a host can include an embedded, secure microcontroller to communicate with a secure chip in the ink/toner cartridge or the battery pack. The controller incorporates firmware to allow strong authentication between the printer and the cartridge or the system and the battery pack and can lock out cloned counterfeit products. Such a scheme, though, requires a communication channel between the printer and the cartridge or the host and the battery, and that requirement means the use of at least one or two more pins on both ends, which also drives up the system cost.

Going wireless can help eliminate the pins but can be a slightly higher-cost approach. For example, NFC technology, using the NFC-enabled product and standardized secure contactless tags and readers, can play a role in this market. Manufacturers can use such approaches to protect themselves and consumers by strengthening the anticounterfeiting arsenal.

GO ASYMMETRIC

Properly implemented authentication using asymmetric cryptography—the core technology behind digital signatures and certificates—offers the robust protection that can thwart counterfeiters. Asymmetric cryptography has proved to be so useful that it has become a common part of everyday life. Every Internet e-commerce Web site using a secure server employs asymmetric cryptography to secure transactions.

Asymmetric algorithms employ a public key and its corresponding, intrinsically linked private key. A counterfeiter cannot derive one key based on knowledge of the other key. Thus, only a toner

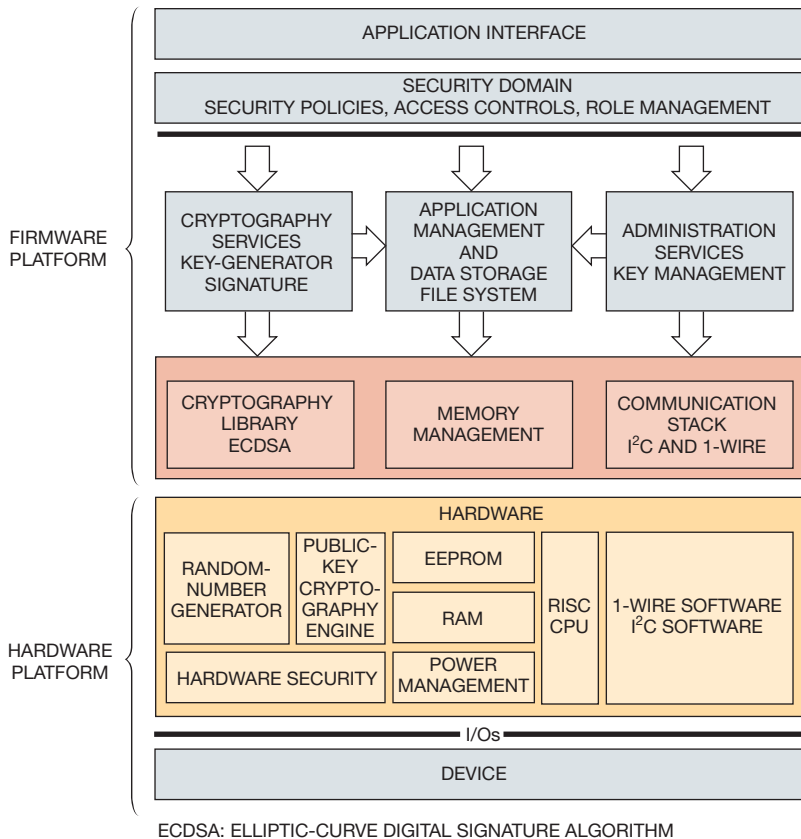


Figure 1 A security IC contains a dedicated cryptographic engine, a random-number generator, a RISC CPU, and simple serial I/O. Firmware layers above the hardware manage the memory, communications, and cryptographic library (courtesy Inside Secure).

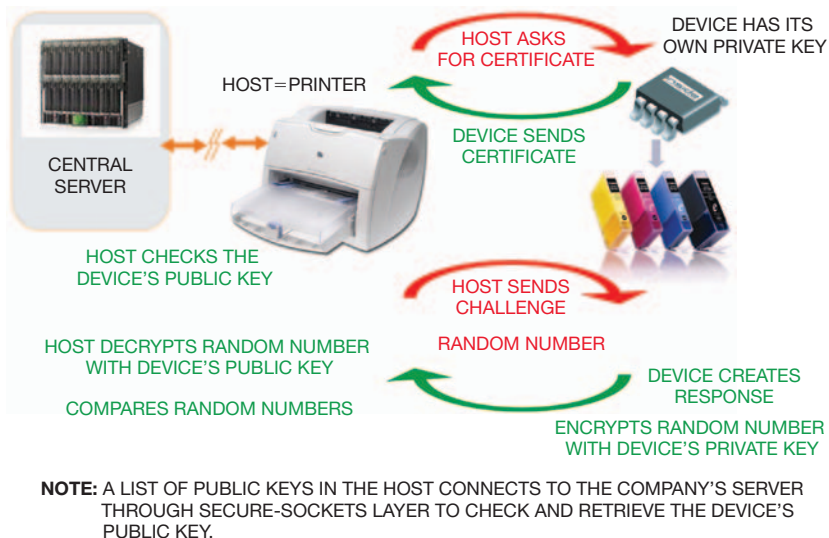


Figure 2 The IC uses its securely stored private key to compute the elliptic-curve digital signature of the challenge message and sends this digital signature back to the host. Using the corresponding public key, the host verifies the signature.

cartridge that “knows” the private key can respond correctly to a printer’s challenge, and the printer can determine this knowledge using only the corresponding public key. If a counterfeiter cannot obtain the private key, then a printer can “assume” that any toner cartridge responding correctly is authentic.

Although asymmetric cryptography offers superior security, it is by nature also demanding, complex, and costly to implement. The strength of technology provided by asymmetric cryptography is directly proportional to the key length used. As the key gets longer, however, so does the computational and software complexity. Increased complexity, in turn, demands more computational power, which demands larger, more complex and costly chips.

However, as the microprocessors available to counterfeiters wanting to hack these systems continue to become faster and cheaper, a key length that seemed adequate a few years ago may no longer offer adequate security, and the currently recommended RSA (Rivest/Shamir/Adleman) key size is 2048 bits. For this reason, effective asymmetric implementations have been too costly for all but the most high-end applications.

Enter the ECC (elliptic-curve cryptosystem), an emerging alternative to public-key cryptosystems, such as RSA, DSA (Digital Signature Algorithm), and Diffie-Hellman, for performing asymmetric authentication. ECC provides higher strength per bit than any other current cryptosystem, and the longer the key, the greater the difference. A 244-bit ECC key has the equivalent strength of a 2048-bit RSA key for secu-

rity; a 384-bit ECC key matches a 7680-bit RSA key. Greater strength for any given key length enables the use of shorter keys, resulting in significantly lower computational loads and memory requirements, faster computations, smaller chips, and lower power consumption—all beneficial for implementations of asymmetric authentication in low-cost systems.

IMPLEMENTING ECC REQUIRES A SIGNIFICANT INVESTMENT IN HARDWARE AND SOFTWARE, INVOLVING A TRADE-OFF BETWEEN THE COST OF PROTECTION AND THE PRODUCT’S VALUE.

Nevertheless, implementing such a system requires specialized knowledge and a significant investment in hardware and software development. Again, the trade-off between the cost of implementing such technology and the value of what this technology is protecting has prevented most manufacturers from employing it.

BUY OR ROLL YOUR OWN?

Developing a custom chip or programming a microcontroller to execute the ECC can be a lengthy process. However, vendors including Infineon, Inside Secure, NXP, Renesas, and STMicroelectronics can deliver off-the-shelf security products. Most of these off-the-shelf products are based on technologies developed for the banking and smart-card industries.

Whether designers use an off-the-shelf product or design their own, the chip they use should include a secure RISC CPU; a hardware random-number generator; a hardware cryptographic-acceleration engine; a secured block of non-volatile memory for secure storage of keys, certificates, user data, and other information; and communication interfaces, such as I²C or 1-Wire (**Figure 1**).

These products should also include many dedicated anti-tampering schemes to protect against simple- and differential-power-analysis attacks and against physical attacks, including active shield, which actively protects your computer from trojans, spyware, adware, trackware, dialers, key loggers, and even some special kinds of viruses. It should also include environmental-protection systems, such as voltage, frequency, and temperature monitors; light protection; and secure management and access protection to prevent reverse-engineering or cloning. A collection of advanced-security firmware routines should ease the implementation of fully user-defined, nonvolatile storage of sensitive or secret data; set up identity-based authentication with user, administrator, and manufacturer roles; and perform authentication, digital-signature, and other advanced cryptographic operations using keys and data from the file system.

HOW DOES IT WORK?

The manufacturer of a toner cartridge or a battery embeds a chip such as an ASIC with similar features in each of its prod-

ucts. Each chip contains a private key and a certificate that has the approval of the printer, laptop, or mobile-phone manufacturer, as well as identifying information about the product, such as the model number. When a user inserts the consumable product into the host product, the host software first requests a random number from the IC's onboard random-number generator, along with a public key.

The host then combines that number with the public key to create a challenge message, which the host sends back to the accessory product. The IC uses its securely stored private key to compute the elliptic-curve digital signature of the challenge message and sends this digital signature back to the host. Using the corresponding public key, the host verifies the signature (**Figure 2**). Only an authentic product with knowledge of the private key can produce a correct digital signature. Using the result of the verification, the host decides whether to authenticate the accessory. The host can also determine whether this model number is correct for use with the host and could also use the product to track, for example, how many pages the printer has printed and use that information to send a replacement notification when the ink cartridge is nearly empty.

Manufacturers can implement a version of the security chip with an NFC interface, and this version can operate on induced power for a reader. Vendors would use this approach for products, such as wine bottles or designer handbags, for example, that have no built-in power source. Vendors can use dedicated readers at the point of purchase or even built-in NFC interfaces in the latest cell phones to activate the embedded NFC chip to authenticate the product. A typical NFC interface can transfer data at rates as high as 106 kbps, and such a chip might have a memory-storage capacity

of approximately 1.5 kbytes. **EDN**

AUTHOR'S BIOGRAPHY



David Richetto has more than 12 years of experience in the smart-card market and the development of secure ICs. He currently manages the application labs at Inside Secure (Aix-en-Provence, France) and the marketing activities for the company's anti-counterfeiting products. Previously, Richet-

to was application manager for smart-card and secure ICs at Atmel SMS, specializing in the SIM (subscriber-identity-module), bank, ID, and embedded-security markets. He has also managed the development of the first software layer of Gemplus (now Gemalto). He started his career at Motorola Semiconductor (now Freescale) in 1994 as a design engineer. Richetto has a degree in electronics and system engineering from École Nationale Supérieure d'Ingénieurs—Caen (Caen, France).

FOR MORE INFORMATION

Infineon

www.infineon.com

Inside Secure

www.insidesecond.com

IACC

www.iacc.org

NXP Semiconductors

www.nxp.com

Renesas

www.renesas.com

STMicroelectronics

www.st.com

World Customs

Organization
www.wcoomd.org