# Authentication Gets Personal

BY STEPHEN EVANCZUK

Continued breakdowns in password-based security systems have led to increased use of more sophisticated authentication systems by financial institutions and other potential high-value targets of cyberattacks. Within emerging authentication solutions, hardware-based crypto ICs provide a protective foundation for secure access to physical and virtual resources.

Attacks on supposedly secure systems have exposed widespread weakness to infiltration by individual hackers, criminal syndicates, and even state-backed groups. Financial and retail sectors have gained unwanted attention for loss of personal information on a massive scale. Yet, security weaknesses in medical, transportation, and energy sectors ultimately pose a greater danger to personal and public safety with potential life-threatening consequences.

**Wearable technology promises to transform security into a more personal experience.**

Highly secure systems depend on authentication methods that combine three key factors for identification: passwords (what you know), an access card (what you have), and a fingerprint (what you are). Outside of high-security facilities, however, system security usually relies on simple password protection. Yet, password security is notoriously weak: Users too often use common or predictable passwords, often relying on the same weak password across multiple systems and services. In fact, in a 2013 security bulletin, the FDA cited simple password protection as a weak link in medical device security systems, recommending the use of more robust authentication methods not only for life-sustaining devices but also for any device connected to medical networks.

Emerging efforts such as NTT Docomo's Portable SIM and Bionym's Nymi wearable device hope to bring sophisticated authentication services into everyday life. Portable SIM seeks to upgrade traditional SIM technology with a wearable device that incorporates SIM, NFC, and Bluetooth to authenticate users not only for cell phone use, but also for unlocking doors, starting vehicles, and other common activities.

Bionym looks to build an even more robust security foundation with its wrist-worn Nymi device. Unlike simple heart rate monitors, the Nymi captures the user's actual ECG waveform. Unique to every individual, the ECG augments authentication with the notion of "who you are" — the "Holy Grail" of multifactor authentication. Furthermore, because this biometric process requires direct attachment to the individual, chances of forgery or spoofed data are remote.

Trusted authentication only begins with unique biometric identification, relying on communication methods designed to prevent interception of trusted signals for replay or use in man-in-the-middle attacks, for example. Authentication methods such as challenge-response require an external device (such as a wearable) to confirm its own identity to a host, typically using a shared secret to establish a trusted communications link. In the past, implementing advanced authentication algorithms remained limited to national agencies or large companies able to afford hardware capable of executing crypto functions in real time. Today, however, engineers can find hardware support for authentication ranging from processors with built-in crypto accelerators to dedicated authentication chips.

For example, MCUs in Microchip Technology's PIC32MZ family integrate a hardware crypto engine designed to accelerate encryption, decryption, and authentication algorithms. Dedicated chips such as Maxim Integrated's DS28E35 and Atmel's CryptoAuthentication IC family provide hardware-accelerated authentication capabilities, while Atmel's CrytoMemory chips provide crypto acceleration and secure key storage.

In fact, silicon-based security continues to evolve rapidly in response to growing demand for better protection. More ICs offer features such as secure boot, protected memory and hardware-based virtualization, and designers can expect to find security integrated more tightly into a growing array of devices.