Side Bar: Get a Trusted Security Certificate

Jon Titus, Senior Technical Editor

Related Content:
Click here for Jon's April 2008 Embedded Systems article;
Security Goes Beyond Cryptograhy [1]

If you manufacture just a few embedded systems, you can come up with public/private keys and the information needed to authenticate the identity of each device. But if you plan to manufacture devices for a large market, you may need the help of a trusted certificate authority (CA) that issues digital certificates. Certicom, for example, recently started a DeviceCA program that will issue "bulk" digital certificates to standards bodies, professional organizations, or large OEMs. Those groups will sell certificates to other companies. So, if you have vending machines or ticket kiosks you can buy digital certificates to identify your products and provide a public/private key for each. The Certicom DeviceCA certificates work with elliptic-curve cryptography (ECC) and the Rivest-Shamir-Adleman (RSA) public-key algorithms.

"Suppose you produce electricity meters used on homes and industrial buildings," said Brian Neill, product manager at Certicom. "A utility company can read the meter through a wireless link. If someone hacks a meter to lie about energy use, someone can go out and manually read it. But if the meter can receive wireless commands to adjust a usage rate seasonally, you don't want someone to hack one meter and then change settings throughout a neighborhood. You want uniquely identified meters to respond only to commands sent by the utility company. This way, if one particular meter gets hacked, you can fix it or shut it off, and the other meters remain unaffected."
If you use just one key for all meters and a hacker gets that key, you have a "broken" metering system that requires distribution of a new key to each meter. To avoid this problem, manufacturers place a unique and secret key in each meter. "It's great to have that type of individual key, but you run into big headaches when you manufacture meters," explained Neill. "An off-shore manufacturer must program each meter with unique data. You can't have any duplicates o r mismatches. As you add complexity to a manufacturing process, you open room for errors. And you must ensure the security of the key 'injection' process, too."

A certificate authority creates unique IDs and keys and then certifies them. "Then when a device presents its unique ID, its public key, and its certificate, you can tell that Certicom -- and no one else -- has made this certificate," explained Neill. "Then when you 'talk' with a remote device over a secure link, you know you supplied the device at the other end and it has a chain of digital signatures that you can trace to a trusted source."

For more information of certificate authorities, see:
http://en.wikipedia.org/wiki/Certificate_authority [2]

Links:
[1] http://www.ecnmag.com/
[2] http://en.wikipedia.org/wiki/Certificate_authority