

# Certicom and TI Announce Data Security for HF Tags

A system developed by the two companies uses public-key elliptic-curve cryptography (ECC) to encrypt a drug's National Drug Code (NDC). Supply-chain partners can read the encrypted tags to authenticate that the goods are genuine.

By Mary Catherine O'Connor

Nov. 13, 2006—[Certicom](#), a Mississauga, Ontario, provider of wireless-information security solutions, has announced a new security platform application for companies using passive, high-frequency ISO 15693 RFID tags to track and trace products in the retail supply chain. The system utilizes public-key elliptic-curve cryptography (ECC) to encrypt a drug's National Drug Code (NDC) written to a tag. Supply-chain partners can read the encrypted tags as they receive tagged goods, allowing them to authenticate that the goods are genuine product made by the manufacturer, not counterfeit. With the right software, the partners can then decrypt the encrypted part of the tag data if they need to.

Certicom collaborated with [Texas Instruments' RFID business division](#) to develop the RFID security solution, using TI's ISO 15693 tags to test the solution. The company says it can be deployed on any ISO 15693 tag. TI is working with TI to market the product, which it has dubbed Certicom Security for RFID Product Authentication. Certicom and TI are initially targeting the product to pharmaceutical manufacturers, though they say it could also help makers of other highly counterfeited goods—such as cosmetics, liquor and apparel—to authenticate their products.

"Pharma is the poster child [for product authentication with passive RFID], but there are other markets where this product can help," says Joseph Pearson, business development manager for Texas Instruments' RFID division. "We're excited about the solution and the technology that's going into it."

The authentication platform consists of hardware and software components. Certicom designed it to work with existing RFID-tagging systems. To deploy the platform, a manufacturer installs a device Certicom calls a signing appliance. This device sits on a company's manufacturing floor and receives EPCs as the firm's RFID software generates them in an item-level tagging operation. The application encrypts each EPC it receives, using the Certicom ECC digital signature (which complies with IEEE encryption standard 1363a-2004). This digital signature, encoded to the tag's user memory, masks only the product code section of the tag's EPC. The product code consists of the drug's NDC, a universal product identifier listed on the [National Drug Code Directory](#) maintained by the [FDA](#), accessible by the general public via the Internet. If the drugmaker's supply-chain partners, such as logistics firms or retailers, want to read the tag's EPC to automate or improve the accuracy of their receiving processes, they can do so with any interrogator capable of reading HF tags.

This allows a company to collect an item's EPC with the masked product code, which they can match to the same masked code in an advance shipment notice. However, if that supply-chain partner also wanted to determine the NDC of the product being shipped, and to pull the full EPC data into an electronic-pedigree program for pharmaceuticals, it would need to install Certicom's authentication software on any readers used

to decrypt the drug's NDC.

Certicom's authentication platform cannot be used on existing UHF EPC Gen 2 tags, because Gen 2 chips do not currently offer enough user memory to store the 352 bits required for the 96-bit EPC and 256-bit digital signature. Tony Walters—Certicom's director of business development—says Certicom and TI are actively working with the EPCglobal working group that is currently developing a Gen 2 standard for an item-level tag. Their goal is to persuade the organization to ensure that the item-level Gen 2 standard holds enough user memory to facilitate the Certicom authentication scheme.

Pearson says TI's ISO 15693-compliant HF chips come with different memory sizes, but all offer enough to accommodate the EPC and digital signature—some as much as 2,000 bits of memory.

Pharmaceutical companies are starting to use RFID to track and trace their products at the item level. Some, such as Pfizer, are using HF tags at the item level (and UHF tags for cases and pallets), while others utilize UHF at the item level.

Pearson says the Certicom approach will work for companies falling on either side of another dichotomy among pharmaceutical companies using RFID: whether to encode a drug's NDC directly to the tag, or to encode a pointer on the EPC referring to the NDC in a separate database. Some retailers want the NDC encoded to the tag so they can identify the product without having to link to a separate network to access the code, he says, thus saving time and money. Others worry that putting drug codes on tags might make consumers susceptible to a loss of privacy if a tag were to be read by an unauthorized third party who then identified the drug by looking up its code in the National Drug Code Directory.

Since the Certicom software runs directly on the supply-chain partner's reader, it could be used off-network if the encrypted NDC were encoded directly to the tag. In either case, it would encrypt the NDC to protect consumer privacy more securely. TI and Certicom are demonstrating the solution this week at the RFID Healthcare Industry Adoption Summit in Washington, D.C. The conference ends Wednesday, Nov. 15.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved