

SecureRF Announces Temperature-Logging EPC Tag with Data Protection

The semi-passive tag uses the company's Algebraic Eraser and public and private keys to encrypt temperature history or other data an end user might want to secure.

By Mary Catherine O'Connor

April 6, 2007—In late 2005, [SecureRF](#), a data security startup in Westport, Conn., says it created a breakthrough design that will provide strong data security for EPC tags. To bring such a tag to market, the company is now developing a silicon chip with the additional memory required to support its data security engine, the Algebraic Eraser. The company has just unveiled its first product: a semi-passive Lightweight Multistream Encryption (LIME) EPC tag with an integrated temperature sensor. The tag's sensor measures the temperature periodically, then logs those readings in onboard memory.

SecureRF says the LIME tag is well suited for pharmaceutical supply chain applications, or others in which end users require or benefit from data security in addition to temperature tracking. The company is currently offering the LIME tag as a collection of discrete components, combined onto an 8-by-3-centimeter circuit board. This includes an off-the-shelf EPC Gen 2 inlay, a temperature sensor, a field-programmable gate array (a device containing programmable logic components and programmable interconnects), a microprocessor (on which the Algebraic Eraser software resides) and a battery. SecureRF claims the Algebraic Eraser is faster, requires less computing power and consumes less energy than existing methods of encrypting data (see [SecureRF Creates New Encryption Method](#)).

While data saved to standard Gen 2 tags can be locked, it cannot be encrypted because the EPC protocol requires that the EPC be available for singulating tags. For a SecureRF tag—either the LIME tag or any future tag the company might develop—to be used in an EPC network, it must be readable just like any other Gen 2 tag. Thus, explains Mike McGregor, SecureRF's vice president of engineering, the LIME tag does not encrypt its EPC data. The additional data saved to the tag, however—primarily its temperature history, or other data an end user might want to protect, such as a drug identification or other identification codes—can be encrypted using SecureRF's asymmetric encryption.

This requires a public key, stored in the EPC tag's user memory and presented to the reader, and a private key, encoded into the Algebraic Eraser software running on the tag's microprocessor. It also calls for both public and private keys stored in SecureRF software called the secure reader host. This software can be deployed either on a reader's user memory (assuming the interrogator has enough processing power to support it), or on the server, running middleware linking the tag data to back-end systems. Alternatively, the secure reader host can run on a separate piece of hardware, on a network appliance situated between the reader and the middleware.

The tag and secure reader host each use their private keys to read the public key and the data it protects.

RELATED_ARTICLES According to Louis Parks, SecureRF's president and CEO, his company plans to work with pharmaceutical companies and other end users over the next six months to perform pilot tests using the tag. It will then create its final specifications for the tag, based on user feedback, and begin manufacturing an integrated version in which the separate chips and other components will be built into a single IC. Parks says the fully integrated version of the LIME tag should measure 3 cm square. Once the pilot tests are complete and SecureRF has a final design ready, he estimates it will be roughly a year before the integrated version of the tag will be available.

In addition to space savings, Parks notes, the integrated chip will also offer performance improvements over the current discrete-component version. While the discrete-component LIME tag can be read from up to 15 meters away, the integrated version should be readable from up to 50 meters. The cost savings will also be significant once the tag is fully integrated, he adds, from the tag's current price of \$50 apiece to possibly as low as \$2.50 each.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved