

**The company hopes its proprietary solution will gain acceptance as a way to secure tag data, as well as authenticate tags and the products to which they are attached.**

By Claire Swedberg

Dec. 8, 2010—[Adasa](#), a Eugene, Ore., provider of mobile EPC Gen 2 RFID tag encoders designed to facilitate in-process RFID tagging in remote or non-centralized locations, is preparing to commercially launch an encryption solution that it says can be used for existing EPC Gen 2 RFID inlays.

The [U.S. Patent and Trademark Office](#) recently granted Adasa [a patent for its EPC tag-encryption solution](#), which the company hopes to make commercially available by January 2011. The commercial product is intended to combat both privacy concerns and counterfeiting, the firm reports, by ensuring that a tag can not be read or killed by an unauthorized interrogator, nor cloned by a counterfeiter.



*Clarke McAllister,  
ADASA's president and  
founder*

The system enables users to encode each RFID inlay with access and kill passwords, encrypted and hidden within the publicly readable EPC tag data, using a periodically changing encryption key. Downstream in the supply chain, in order to authenticate, kill or alter the inlays' password, or to read an EPC number or other data encoded to those inlays, the users would query an encryption module—a device the size of hockey puck, embedded or plugged into an EPC reader.

A tag's encryption key is used to generate a password necessary either to read the data encoded to that tag, or to kill that tag. To prevent unauthorized individuals from identifying the password and using it to access information on RFID tags, the encryption keys are designed to be changed by the encryption module at periodic intervals. Therefore, says Clarke McAllister, Adasa's president and founder, users of the company's inlay-encryption system can provide security and anticounterfeiting protection to their customers—such as brand owners and retailers—by ensuring that the tags can not be read or altered by clandestine readers, as well as proof that a product and its RFID inlay has not been counterfeited. The inlays could be utilized by retailers and brand owners, as well as by government customs and border patrol, to protect personal data encoded to tags embedded in identity documents.

Typically, EPC tag users either do not implement the password-protection function to deny access to data for those lacking the proper password, or have passwords that are encrypted on the tag and must be verified at the time of an RFID read—in some cases, with information on a remote server, which would require accessing the Internet. However, McAllister says, there are potential security risks inherent to the Internet, since data can be captured or diverted by individuals. "EPC chips work fine as they are," he states. "The tag has some security [assuming its built-in password feature is activated], but it can be cracked with brute force (such as by using a computer to search for passwords until the correct one is randomly produced), or by eavesdropping on transmissions." In that case, he says, an

individual could use the Internet to capture transmission data. Internet transmission can be encrypted as well, he notes, and there are many commercial solutions for this, but "we adopted our techniques from former NSA [National Security Agency] cryptographers that design and audit bank-security systems," that he says make Internet connection with the encryption module safer than most commercial encryption solutions.

There are already security options in place for some EPC tags. In February of this year, [Impinj](#) announced its Monza 4QT chip, which has a public and private data mode controlling the amount of data that can be read (see [Impinj Launches New High-Performance RFID Chips](#)). And in April, [NXP Semiconductors](#) unveiled its G2iL series of RFID chips, featuring an on/off mode (see [New NXP RFID Chips Bring Multiple Functions to Item-Level Tagging](#)), which have been selling well, the company reports. "We see good traction from brand owners to use security features in RFID tags to protect their products from being counterfeited," says Heinze Elzinga, NXP's director of product management.

Adasa's solution aims to add an additional layer of security to either of these companies' chips, or to any other make and model of EPC chip with its own offline, changing encryption key. The firm has spent several years developing this system in anticipation of security problems, as RFID tags become more ubiquitous. To date, McAllister says, there have been few cases of EPC tag cloning or clandestine access of tag data. However, he notes, the need for security solutions will grow with the expected rise in tag volume.

In 2006, the company introduced its PAD3500 line of mobile EPC Gen 2 RFID tag encoders, for use in such remote locations as manufacturing plants and distribution centers, and for exception handling within retail stores (see [Adasa Developing Wearable Tag Encoder](#)). Those encoders do not support encryption of tag data, however, so the company began developing its encryption technology to solve a challenge that it predicts will grow: namely, protecting information on RFID tags in all parts of the supply chain, in order to thwart the potential proliferation of EPC tags for false IDs or counterfeit products.

The company then developed a device capable of encoding the tag in such a way that the encryption key would periodically change the password. In addition, it developed the module to store those keys for offline users, thereby reducing the need for Internet data traffic for such applications as transmitting unique ID numbers to a back-end server to verify passwords at a store's point of sale for each RFID tag read. Only when cryptographic keys are periodically changed, McAllister says, does the module go online, download replacement keys and provide them to the interrogator. This, he indicates, vastly reduces the amount of time vulnerable data is being transmitted on the Internet, and that users await responses from globally remote servers. Encryption of the Internet communication between the module and the remote server reduces vulnerability, he says, though he notes that the need for Internet transactions can still slow the process of reading tags. "Variable network delays are unavoidable," he states.

To create the keys, the encoder employs the industry-standard AES-128 encryption algorithm. The amount of memory necessary on the inlay to support the encryption key varies, depending on the

desired security strength. Adasa's solution supports keys up to 512 bits in length, with the key stored in the tag's user memory. (In comparison, NXP's SmartMX HF RFID chip supports a key up to 256 bits in length.) The transmission of data from reader to tag, and vice versa, is made more secure by the cover-coding technology to obscure the data during transmission.

The encoder has another feature as well, one intended to reduce the cost of its technology: the ability to support unconverted inlays, rather than RFID labels. By enabling users to encode an unconverted inlay—simply an RFID chip and antenna embedded on a plastic substrate with an adhesive backing—the company was able to eliminate the need for label manufacturers to get involved in the tag manufacturing and encoding processes, McAllister says, thereby potentially saving up to 5 cents per inlay. Here's how the system works: The cartridge in the encoder holds unconverted EPC inlays from any inlay manufacturer, encoding each inlay with an encrypted unique ID number, as well as encrypted passwords and data. During the encoding process, Clarke explains, near-field magnetic induction is used to reduce the transmission distance by forming inductive loops around the inlay's immediate vicinity. A worker in a product manufacturer's factory or warehouse then removes each inlay and attaches it directly to a product, or to its packaging or hangtag.

When the item arrives at a store, the interrogators operated by the store's staff utilize Adasa software to link the ID numbers and encryption keys they read (for example, at the point of sale) with those on the module plugged into a computer or network device via an Ethernet cable. The module either approves or rejects the password sent by the inlay, and the point-of-sale transaction is then complete. This is faster and more secure, McAllister says, than sending the ID and password back to a server with each read of an inlay. The module connects to the Internet only to download new encryption keys at the times at which they change, greatly reducing the time and risk of sending sensitive data over the Internet.

All encryption keys will be stored on a hosted server, to be managed by an IT partner not yet selected by Adasa. Once the IT company is chosen, the technology will be ready to be offered commercially—as early as January 2011, McAllister hopes. The full system consists of server access, an encoder for commissioning the tags, an encryption module and associated software, and the inlays themselves. The encoder can also support converted RFID labels; however, those labels must meet the size requirements of the cartridge form factor. Because unconverted RFID inlays are cheaper than RFID labels, McAllister says, the solution will be less expensive than existing EPC labeling systems. Any make or model of ultrahigh-frequency (UHF) Gen 2 RFID reader, with the encryption module and required software, could operate with the Adasa system.

Another company that offers technology designed to address either counterfeiting or data security is [Verayo](#), which sells its Physical Unclonable Functions (PUF) technology. PUF technology is designed to provide security functionality on existing RFID chips, most commonly for high-frequency (HF) 13.56 MHz RFID inlays used for NFC systems, by establishing an expected response from each RFID chip to a transmitted "challenge," based on its own unique physical characteristics during manufacture. "NFC is becoming a very interesting space for Verayo," says Vivek Khandelwal, the firm's VP of marketing and business development. "Most of the attention we are getting is from NFC applications." In that case, he

explains, the rollout of NFC-enabled mobile phones will increase the demand for the PUF product. In September 2010, Verayo announced that Nigeria's [National Agency for Food and Drug Administration and Control](#) (NAFDAC) had approved the use of an RFID system employing its PUF technology to authenticate pharmaceutical products sold in that country (see [Nigerian Drug Agency Opts for RFID Anticounterfeiting Technology](#))

Currently, there is no internationally accepted specification for data-encryption technology for EPC Gen 2 tags, thus posing a challenge for RFID security providers. "Interest in encryption-based security in UHF Gen 2 applications is simmering, but not active," says Scot Stelter, Impinj's senior director of product marketing. "The reason is that there is no industry standard for security as yet." Impinj, he says, is involved in standards-setting groups working to develop an encryption standard for EPC Gen 2 UHF tags. The establishment of such a standard would provide a common approach to technology that could include tag and reader security, and target both privacy protection and anticounterfeiting (anti-tag-cloning) applications. What's more, he says, it would also reduce cost and enable rapid adoption.

Thus far, Stelter says, "there have been a few attempts to implement non-standard subsets of security in Gen 2 systems." However, he notes, "None have stuck."

McAllister does not disagree with Stelter's assessment. "Adasa is about three years ahead of the standards process," he says. "That is why it's critical that we select the right 'pedigreed' IT partner to license our technology, so that they can deploy a proprietary system in the absence of a standard." He adds that, "as this proprietary solution gains adoption... then it can become part of future standards on a RAND [Reasonable and Non-Discriminatory] licensing basis."

Another important key to the adoption of security systems, Elzinga says, is their ease of use. "Customers don't like to be bothered with implementing complex security features," he states, "and therefore, the technology providers must look at security implementations from an end-to-end perspective, and make the components available for customers."