

**The Dynamic Authentication feature verifies the authenticity of a Higgs 3 EPC Gen 2 UHF passive tag, to provide an additional layer of security.**

By Mary Catherine O'Connor

Sept. 18, 2009—Morgan Hill, Calif. RFID hardware manufacturer [Alien Technology](#) has announced a new security application designed to make RFID tags made with its Higgs 3 chip impossible to clone. The feature, known as Dynamic Authentication, relies on a challenge/response algorithm to verify that a tag is authentic, explains Victor Vega, Alien's marketing director.

Alien began producing the Higgs 3 chip in April 2008 (see [Alien Technology Announces New EPC Gen 2 Chip](#)), and while the chip has had the dynamic authentication capability since then, the company is now making available the reader software needed to unlock the functionality. "We designed the Higgs 3 chip with layered security features," Vega says. The firm's intention was to make the features available in a staggered manner. "Rather than add all the security features to the chip at once, we layered them. The idea is that when it comes to security, we always want to stay one step ahead [of the fraudsters]."

The algorithm is a custom command that verifies the authenticity of a Higgs 3 EPC Gen 2 UHF passive tag by querying the chip. It is referred to as a dynamic authentication, because in response to a query from the interrogator, the chip will change select different bits within its response each time it is verified. Only an authentic Higgs 3 chip will respond to the query this way, Vega explains. End users who have tags with Higgs 3 chips—even if those tags are already encoded and deployed in, say, a closed-loop asset-tracking application—can begin using the custom command by requesting a special application protocol interface (API) from Alien. Today, that API is available only for Alien's EPC Gen 2 RFID readers, but Vega says Alien will share that API work with other EPC Gen 2 reader manufacturers so that end users can deploy the command on those devices.

According to Vega, the dynamic authentication is the most robust custom command for the Higgs 3 chip, building on the already-available Higgs 3 security. These include the use of a 96-bit tag identification number (TID) that is factory-programmed into the chip when it is fabricated. This number consists of 32 bits of data indicating the chip's maker and model (as required by the Gen 2 standard), and 64 bits for a unique ID number.

Alien Technology is not the first EPC Gen 2 chipmaker to program unique chip IDs—designed to be used in combination with an EPC or another unique number that the end user encodes to the tag memory in order to authenticate a tag—into its products. But the Higgs 3, Vega says, is the first Gen 2 chip to use a 96-bit TID containing a 64-bit unique ID number (other makers have utilized up to 32 bits for this identifier).

End users, such as Italian garment manufacturer G&P Net, plan to employ the Higgs 3 chip's unique TID in order to bolster the authentication of tagged apparel shipped from its distribution centers to retail outlets. The retailer already pairs the unique serial number encoded to each tag with information stored

in its warehouse management system, such as the time and location at which the tag has already been read. In this way, the company can trace any gray-market items introduced to the supply chain by a third party (see [RFID Targets Gray Market in Europe](#)). But soon, Vega says, the retailer will also begin storing the 96-bit TID encoded to the Higgs 3 tags it attaches to clothing items, and associating that with the tag serial number and ancillary data (size and style) for each apparel item, in order to add an anticounterfeiting measure to the system.

Since the tag ID is factory-programmed, it won't appear on more than one tag—whereas if users read only the serial number they encode to the tag, there's no way to ensure that the tag is not a clone that was encoded with the same serial number.

[Pfizer](#) started using this method for fighting counterfeit Viagra utilizing high-frequency (HF) tags in 2006 (see [Pfizer Using RFID to Fight Fake Viagra](#)).

If someone wanted to clone an EPC tag carrying a Higgs 3 chip, Vega indicates, he or she would need to be "very rich and have tremendous resources" in order to copy not just an EPC or other unique serial number encoded to the chip, but also that chip's unique TID, and encode both to a new chip. Nonetheless, he says, Alien's Higgs 3 strategy has been to layer security functions into the product in order to build up an arsenal of security tools. "Counterfeiters will generally try to find a way around the latest security measure," he notes, "so the industry always needs to be ready to pull out a new tool from its tool chest to throw the frauds off guard."

Another custom security feature on the Higgs 3 chip is called ReadLock. With this feature, users can parse the 512 bits of user memory on the Higgs 3 chip into eight separate 64-bit blocks. An end user can permanently lock any of these blocks, so that the information cannot be altered. It can also prohibit third parties from reading any of these blocks by protecting them with a password that a third party needs in order to read the data.