

# SkyeTek Adding Security Support into Passive Platforms

The firm's ReaderWare software can be used to add data security to HF tags now, and to UHF Gen 2 tags once they become available with extended memory.

By Mary Catherine O'Connor

July 11, 2006—[SkyeTek](#), a Boulder, Colo., designer of RFID hardware and software systems for original equipment manufacturers (OEMs) and technology integrators, says it is adding support for standards-based data encryption and hashing algorithms to ReaderWare software. ReaderWare is part of SkyeTek's Advanced Universal Reader Architecture (AURA).

The company is supporting the security tools so manufacturers or integrators of RFID systems can enable end users to protect data encoded to tags used for payments, electronic pedigrees and other applications in which sensitive information, such as account information or personally identifiable data, is encoded to tags.

Specifically, ReaderWare now supports both Advanced Encryption Standard (AES), the data encryption algorithm standard ratified by the [National Security Agency](#) (NSA), and Secure Hash Algorithm (SHA), the [Federal Information Processing Standards](#) (FIPS) algorithm standard for hashing.

In cryptology, a hash algorithm creates a digital fingerprint used to authenticate communication between a tag and reader. It also supports the Digital Encryption Standard (DES) and Triple DES standards, as well as [Philips'](#) MiFare and DESFire and [Texas Instruments'](#) HFI tags, which all use proprietary algorithms.

ReaderWare runs the algorithms and stores the required "handshake" between tags and interrogators, enabling the reading and encoding of tags to use the algorithms. ReaderWare runs on the M2 HF SkyeModule and M9 UHF SkyeModule (EPC Gen 2-compliant) interrogator modules, both of which SkyeTek offers in its new item-level developer's kit (see [SkyeTek HF/UHF Development Kit](#)).

None of the EPC UHF Gen 2 tags, or any of the legacy Gen 1 tag formats, currently on the market have enough memory to run the data security standards SkyeTek is supporting. So while ReaderWare runs on both HF and UHF interrogators, only the data encoded to HF tags—and only those compliant with ISO's 14443 A/B and ISO 15693 standards—can be secured utilizing ReaderWare.

However, the EPC UHF Gen 2 protocol does support more memory than Gen 2 chipmakers have built into the chip to date, and SkyeTek says it has spoken with Gen 2 silicon providers who, according to Martin Payne, SkyeTek's vice president of marketing and strategy, "have indicated that extended memory is in their plans to provide functionality such as encryption."

To license the ReaderWare software, customers must first either purchase one of the reader modules or license the reference design to create their own.

Rob Balgley, SkyeTek's CEO, says that by building data encryption and hashing support into its RFID platform, the company is putting RFID "on par with banking services and Internet-based security." Furthermore, he adds, by offering it as a non-proprietary platform his company is able to make the software less expensive for OEMs and other RFID systems designers or integrators to add data security to their products. This should make deploying secure RFID systems more affordable to end users, as well.

Companies such as Philips and Texas Instruments already offer RFID data encryption, but their systems are proprietary and require the use of tags made with Philips or TI chips. SkyeTek estimates that its OEMs and other customers can embed data security into their offerings using SkyeTek's platform at a savings of 70 percent by using generic tags rather than proprietary ones. "Potentially," says Balgley, the Pfizers and the Wal-Marts of the world could save money [on secure RFID systems] if their OEMs use the SkyeTek format."

Industry analysts and pundits have been calling attention to the need for greater data security for passive RFID systems. At data security specialists RSA Security's annual conference this year, Adi Shamir, one of the company's founders, raised concerns over the data security—or lack thereof—for passive UHF tags by announcing that he and a colleague had easily determined the password needed to kill a EPC Class 1 Gen 1 UHF passive tag. Shamir and his partner indicated they might also be able to use a similar hacking method on more advanced generations of the protocol, such as EPC Class 1 Gen 2 (see EPC Tags Subject to Phone Attacks).

SkyeTek reports that it will begin shipping the M2 HF interrogator module with ReaderWare in July.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved