CONTENTS

Near-field communications to go far in 2013

By Suzanne Deffree, EDN

This article is part of EDN's Hot Technologies: Looking ahead to 2013 feature, where EDN editors and guest contributors examine some of the hot trends and technologies in 2012 that promise to shape technology news in 2013 and beyond.

NFC, or near-field communications, has been around for 10 years, battling its own version of the chicken-and-egg question: Which comes first, the enabled devices or the applications?

The technology is there, yet there has been a major deterrent to NFC's market growth and consumer use: Why build into a device when no applications or services are available, and why offer applications or services when no devices have been built to utilize them?

In 2012, however, NFC started to break out of its shell. NFC-enabled devices rocketed up to 100 million shipped, a significant climb from 2010's 2 million devices sold. Estimates call for 300 million NFC-enabled devices to be sold in 2013 and for the billion-device mark to be reached in 2015.

To date, most such devices are smartphones. With many smartphone makers in the Android and now Windows camps getting on board with NFC, leading OEMs including LG, Nokia, and Samsung have begun designing NFC into products.

Notably, Apple left NFC out of its iPhone 5. As NFC Forum director Debbie Arnold observes, however, "Apple has about 15% global share of the market. With 85% leaning toward NFC … it's not something that keeps us up at night."

The NFC Forum formed in 2004, when the very short-range (5-cm) communications technology was in its infancy. Now,

the forum's more than 170 member companies showcase an extensive base of semiconductor industry players, including Broadcom, Intel, National Instruments, NXP, and Texas Instruments.

In November, the forum introduced the NFC Controller Interface specification, which defines a standard interface within an NFC device between an NFC controller and the device's main application processor. The group expects the specification will help broaden the availability and eventually encourage the price competitiveness of NFC.

Now that the devices and specifications are hatching, flocks of applications and services are on their way. In fact, more have arrived than many consumers realize. Beyond the mobile wallet (**Figure 1**), NFC is seeing use in Bluetooth pairing and applications in various transportation terminals, interactive signs and displays, identification, and peer-to-peer exchange.

Figure 1 A consumer pays using an NFC-enabled mobile wallet, by far the most talked-about application of NFC.

What remains an obstacle is educating consumers on yet another wireless communications technology that does not compete with but is complementary to Wi-Fi and Bluetooth. Samsung, for one, is playing up interactive displays and peer-to-peer sharing in advertisements for its Galaxy S III NFC-enabled phone by showing users scanning posters for free

songs or tapping phones together to share contact information, music, and files (**Figure 2**).

"Some of these things, in creating physical shortcuts and ways for mobile applications to interact with physical retail establishments, start to unlock the fact that there are hundreds of millions of customers who have these devices," says Jeff Miles, NXP's vice president of mobile transactions, which includes the company's identification business. "Tags and the different applications are an area that can explode. It's relatively simple to implement and is straightforward for consumers. Tap, and something magical happens."

Figure 2 NFC offers retail interaction by tapping a device to a sign or display, in this case to download a gaming demo.

Beyond smartphones, NFC is starting to be seen in other consumer goods such as tablets, PCs, printers, and even microwaves. Beyond the electronics vertical, sectors such as health care are starting to explore ways to utilize NFC.

"We often hear about the mobile wallet," says Arnold, "but NFC is going to go down so many different paths. Once we get over this hump, we are going to see this take off in a lot of different verticals."

Also watching:

• 3-D printing. This DIY maker technology has been around for some time, but now 3-D printers are becoming affordable for individuals, as well as lower-level educational institutions, to purchase for their workspaces (**Figure 3**). With everything from car parts to vital organs being talked about as possibilities for 3-D printing, we'll be seeing much more on this technology in 2013.

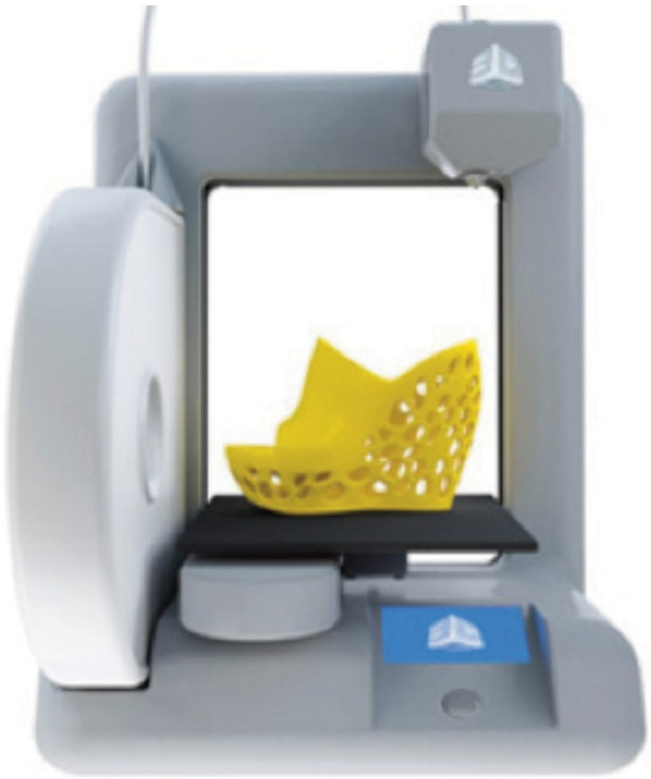
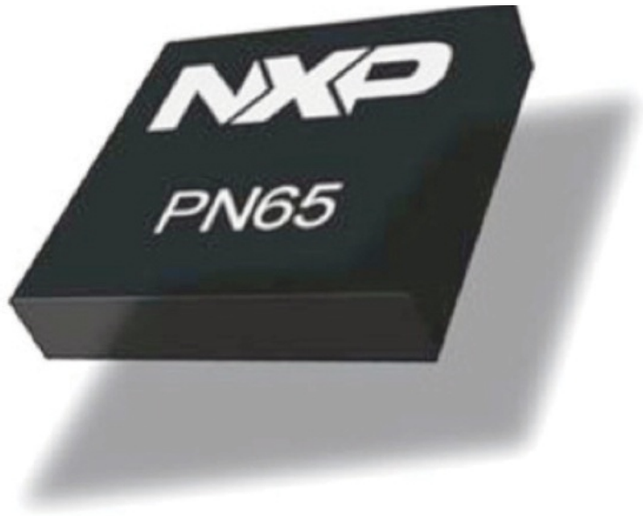


Figure 3 3-D printers such as the affordable, easy-to-use Cube home printer could allow consumers to print many household products less expensively than they could buy them.

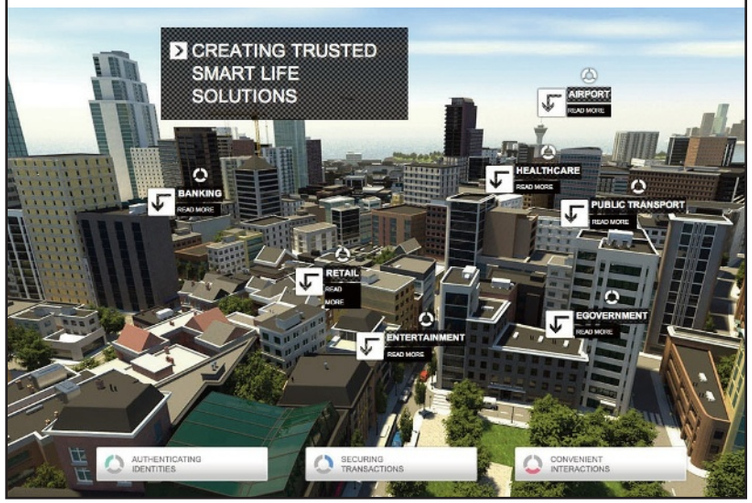
- Inexpensive tablets and e-readers.

The newest iPad may start at $500, but not every tablet needs the shine Apple puts on its products (Figure 4). Harking back to ideas pushed forth by the XO laptop—part of the One Laptop per Child effort, which sought to provide low-cost technology to the masses—sub-$100 tablets and e-readers will offer more alternatives to pricey iPads and even to less-expensive Kindles.



NXP

Creating Trusted Smart Life Solutions



Video: NFC technology, proliferation and challenges examined

By Sylvie Barak, EE Times - March 8, 2012

BRUSSELS—NFC (Near Field Communication) is a wireless connectivity technology that allows short-range radio communication between devices. Included in a small chip inside the device, NFC allows for mobile money transactions, data exchange, location tagging and wireless connections between two devices in very close proximity to one other, usually just a couple of centimeters apart.

Owing to the short-range nature of NFC, transfers are often completed by "tapping" devices either to another NFC-enabled device or a payment system.

Though the technology has been around for about seven years, NFC only seems to now be coming into its own, with a veritable explosion of NFC-powered devices and applications emerging over the course of the last couple of years alone. Indeed, according to a recent Juniper research report, by 2014, one in five smartphones will have NFC in them.

NFC services are set to proliferate rapidly over the next three years, with Juniper predicting almost 300 million NFC capable smartphones by the end of next year, more than half of which will be in North America, with Western Europe following closely behind.

The sudden growth spurt in the technology has much to do with its acceptance and adoption by many global mobile network operators, as well as giants like Google, RIM, Nokia, Samsung and more.

With more and more handset vendors integrating NFC chipsets, NFC payments, mobile coupons and smart posters are also slowly becoming more common amongst smartphone users in Western

Europe, North America, and other developed regions.

Last year Google announced its mobile Wallet initiative and partnered up with companies like MasterCard Inc and Citigroup Inc to embed technology into Android mobile phones that would allow customers to make purchases by tapping their phones over an NFC enabled point-of-sale system. Other companies have since followed suite, and the market for mobile payments is growing significantly, with numbers around $618 billion by 2016, according to an Edgar, Dunn & Co report.

Of course, before the technology truly takes off in a global and ubiquitous way, many believe firms will have to think seriously about the business model structures they plan to use. With banks, mobile operators, transport companies, and retailers all wanting a slice of the NFC pie, there's little doubt the technology will see its fair share of service complexity issues too.

For example, if phones are now also wallets, who would one call to report a theft? One's bank or the mobile operator?

With many opportunities but also still many questions about NFC and its growing role, *EE Times* took to the MWC show floor last week to get a bigger picture of what the technology could do. *Check out the video here.*

Digital Identity White Paper

Introduction

Username and password have been used for the last 40 years as the basis for authentication to computer based services, and are still broadly used in most online services today. However, although this still could be seen as practical and secure enough for closed system access, the evolution that we have seen during the last years make it more and more obsolete.

A study realized by Microsoft back in 2007 has shown that in average, an American user had 25 online accounts secured using 6.5 passwords . This has likely worsened with the time, leading to serious password quality issue and associated risks. The recent hack of 6.5M Linkedin user passwords illustrates the limits of username/password authentication technique to secure today services and transactions of increasing value.

Recent initiatives, such as US National Strategy for Trusted Identity in Cyberspace show government commitment to enforce cyber security: “The Internet and e-commerce are keys to our economic competitiveness”, as stated in the National Security Strategy in 2010.

This white paper will introduce the concerns behind user authentication to online services. It will describe various concepts and solutions around digital identity, high security authentication methods and digital signature.

Problems to solve

To start with, let’s go through a simple example, where we will identify the various steps that must be taken to initiate and utilize online service and the risks that apply to these steps.

Bob wish to join a club that will provide him with a wealth of online services,

chat room, online storage and sharing, instant messaging, mail, localized information and booking services… Bob has many friends already members of the club and he looks forward dating, sharing messages, information and pictures with them.

The first step Bob will go through is the online registration to the club. He will need providing his name or pseudo, probably his age (or an information that he his older than 18 or another minimum age) and other attributes required by the service provider to fulfill service provision and legal obligations.

Based on the information and attribute that Bob provided, the service provider will issue a token and a credential binding the token to Bob's identity.

Then, as soon as the registration process is completed, Bob will start using the service. He will securely authenticate presenting his token, which will be used together with the credential to verify his identity. Once the authentication process will be completed, the service provider will grant the access to Bob who can then enjoy the services he subscribed too.

Say now that the service provider has implemented a directory search possibility, that any user can call to discover if their friends are connected to the service. One of Bob's first actions will be to look for his friends, try to connect with them, and as Bob is a fan of Alice, the famous actress, he will subscribe to get updates on Alice daily life.

Here we could the major threat, related to Bob's and friends' real identity. As Bob and his friends will share secrets, they better be sure that they are the one they pretend to be. As well, the famous Alice wants to protect her image and as such wants to protect someone stealing her identity.

This threat can occur at the registration process if the subscriber does not have to prove his real identity and at the authentication process if the token or secret is stolen or if the credential is hacked at the service provider server.

Then, Bob will invite his closest friends in a restaurant to celebrate his membership to the club. He will use one of the services that utilize Bob's and friends' localization to find a suitable place and will book a table in the restaurant. As the club has a solid reputation, he guarantees the booking to the restaurant and must make sure that Bob understands that he is accountable for the booking. The club asks Bob to "sign" his reservation in such way that he can't pretend at a later stage that he was not aware of the responsibility nor deny he conveyed the transaction.

We will describe in the next sections solutions to decrease the likeliness of

the identity stealth threat to materialize in issues, as well as the signature process that could be used for non-repudiation feature when conducting online transactions.

Registration

The registration process covers the user identification, the formal service subscription and the credential issuance. It is a very crucial step for the service provider, and should follow ad-hoc security and background checks.

No strong user authentication can happen if the registration process is not appropriately controlled. On another hand, the user shall have to provide only the identity attributes or traits required for the service provision, and these shall be treated confidentially to protect his privacy.

In most of the cases, when the service access is not anonymous, the registration process shall involve an identity verification mechanism.

In a pure online process, this can be done using credentials guaranteed by a third party, so called credential-broker. For instance, the user could prove his identity using his electronic national identity card and a secret, or his banking card hosting a special application. The service provider would then use a third party for the identity check, and issue his own credentials based on this trusted verification.

In our example, Bob will fill all the details and identity attributes and traits using a secured session on the service provider web site, and prove his real identity using his identity card and PIN. Once Bob's genuine identity will have been confirmed, the service provider will proceed to the credential issuance.

Obviously the security checks on the registration step have to be balanced with the user perceived security requirement (the user may not accept going through intensive background checks to register a social network), the legal requirements (the minimum set of attributes that may be required to collect by the local laws) and the service requirements. As well, a seamless pure electronic registration will be judged more convenient by the user and will demonstrate a higher registration completion rate than a system using paper mail exchange.

Authentication

Once the service registration step is completed, the user can claim for service access.

The authentication step allows the service provider to assert that the user is the one he pretends to be, and as such to grant or deny the access to the service under his identity. As well, the strength of the authentication process

increases the confidence that the user will have in the service. Bob will be keener using and promoting the club if he is confident in the way his personal details, data and the services he gained access are well protected.

The user authentication process involves presenting an identity (name, pseudo, certificate…), and a proof that a secret is shared between the user and the service provider.

The authentication may be more or less secure depending on how the secret is protected. As well, the proof exchanged between the parties may not be the secret (a password), but the result of a mathematical operation using the secret (in this case the secret may be called a key). For instance, the proof exchanged could be a password (the secret information) or the result of an operation on this "secret" (or the "key")

In addition, the secret can be complemented by other factors, such as something that the user must have in his possession or something that indubitably defines or belongs to the user (an identity trait).

The authentication strength, e.g. the confidence level that the user is the one he pretends to be, grows with the number of used factors.

Single factor vs. multi-factor

As introduced in the previous paragraph, we may consider several authentication factors:

- What the user knows: the secret, e.g. password, passphrase, PIN code…
- What the user owns: a token, a PC, a smartphone,…
- What the user is: his identity traits, e.g. fingerprints, voice, DNA, face, iris, vein network…

The very basic username/password authentication method uses only a "what the user knows" factor: it is a single-factor authentication method.

A method based on a certificate (stored in a USB key or in the PC for instance) and no password uses only a "what the user owns" factor: it is also a single-factor authentication method.

A method based on a certificate but requires a password or a PIN code from the user is based on "what the user owns" and "what the user knows" factors: it is called a multi-factor authentication method.

Multi-factor authentication is also called "strong authentication".

"Strong authentication" does not preclude on the resistance or strength of the factors:

- A password may be weak, when susceptible to attacks using dictionary or publicly known information on the user
- Or could be stronger when based on

a “long” character suite that includes uppercase, lowercase, numeric and symbol characters
- A key could be of different length, the longer it is the more secure it is
- A proof of ownership could use smartcard hardware security, and as such be tamper protected
- Or a may be a simple file stored on a PC or a USB key and susceptible to duplication or tampering

However, the overall security and access protection depends of the factor strength and this point shall be taken into consideration when designing the system.

Ownership factor

The ownership (“what the user has”) factor shall be deemed as genuine by the service provider. Therefore, it is usually issued by the service provider at the registration step and consists of a “certificate”, comprising at a minimum a user identifier digitally signed.

When logging in to the service, the certificate will be presented and the provider will verify the signature to assess its authenticity.

In addition to being genuine, the ownership factor should be copy protected, to avoid duplication without the user knowledge.

Knowledge factors

As mentioned earlier, these are passwords, PIN codes or other secrets that the user shall present to prove his identity. As they are secret, they should obviously not be exposed in any way. As such it makes sense to implement mechanisms where the secret is either verified locally in the terminal or at least used in such a way that it is not transferred as is to the service provider.

Inherence factors

These “who the user is” factors are unambiguous and/or immutable data who identify a person. Biometrics data are among the inherence factors.

Regardless the location where these data are stored, they should be protected against modification –to insure they describe the right individual- and against unauthorized access –as they contain privacy critical information.

Privacy

Privacy of the user identification data, as well as non-traceability of the services he used is a key feature of the authentication service.

To benefit from a promotional offer, Bob decided to use his club’s credential to subscribe another service. However, Bob does not want that this service utilizes non required identity attributes to profile him. Nor does he want to be

traced when browsing through the various services he subscribed.

Some countries have regulatory bodies entitled to verify that user privacy is well implemented and respected prior to authorize a service deployment. For instance, the default behavior of a system should not give it the ability to monitor user behavior at atomic level. As a result minimal disclosure policy should be the rule, which does only provide information required to exercise the service. For example, full name, or national ID number shall not be used unless accessing a service that requires these information.

Software vs. hardware (authentication)

Software may be opposed to hardware with regards to the following topics:

- Where the security credentials (the factor elements) are stored
- Where the authentication algorithm is executed

"Software authentication" would apply for implementations where there is no dedicated secure element to store the credentials and run the security algorithm, whereas "hardware authentication" describes cases where a dedicated element using secured smartcard technology hosts the critical items.

"Software authentication" may also apply to implementations that use server storage and checking of credentials.

Hardware tokens no longer take the only form of removable token –smartcard or USB key- as there are more and more equipments with embedded secure element. Smartphone, tablet PC and PC which includes Near Field Communication (NFC) option may open the secure element to authentication applications.

Software and hardware have respective advantages and disadvantages, summarized in below table.

	Software	Hardware
Issuance	Easy, possibly online	More complex
Security	Low	High
Security portability	Low	High
Privacy (by design)	Low	High

Issuance

Software has an advantage here as being purely dematerialized. The "token" is installed online and may comprise a certificate, key(s), algorithm…

Hardware is obviously more complex to handle from an issuance perspective as involving personalization and shipment of tokens. However, there are examples of secured hardware token that the user can purchase in stores

that could be “personalized” or “bind” to his account online.

Security

Software tokens are intrinsically easier to tamper or duplicate. As residing on equipments connected to the internet, they are more subject to attacks by malware. Moreover, they are not protected by hardware firewall and therefore are exposed to reverse engineering attacks.

Hardware tokens are based on smartcard technology, known for its tamper resistance. Information stored on the smartcard are protected by strong hardware firewalls and controlled by password or PIN code. The keys or credentials used by the authentication algorithms never leave the protected environment. Last, they are ideal for biometrics based authentication, for security –the user details are neither exposed, and privacy –nor stored outside of his token.

Smartcard technology implements secure memories to store the critical data (PINs and keys) such that they cannot be easily readout. It further implements countermeasures against various attacks on the cryptographic algorithms. For software implementations using standard controllers and memories the keys and PINs have to be stored in an unsecured external memory. Furthermore secure implementations of cryptographic algorithms are a huge challenge; in practice it is often not possible to implement those securely.

The advantages to hardware tokens for security are acknowledged by the US National Institute of Standards and Technology (NIST) in their Electronic Authentication Guideline where it is stated that “hard” cryptographic token are the only applicable technology for the highest authentication assurance level.

Security portability

Hardware token insures intrinsic security portability. A token can be used on any equipment providing this equipment can access it. Nowadays tokens with USB/contactless or smartcard ISO/contactless interfaces are available to secure PC, NFC devices, and potentially smartTV and game console devices.

Privacy (by design)

Hardware token securely store the user credentials and attributes, which are verified locally without any unnecessary exposure. Software authentication usually stores the user attributes in a server belonging to the service provider, an identity provider or the service provider acting as identity provider for a third party application. Storing the attributes in the hardware token allows a straightforward “minimum disclosure” implementation keeping all credentials under

user's direct control and insuring that unnecessary details are kept hidden in the token and that only the required information are disclosed during the transaction. For instance, a service that only requires the user to be older than 18 will be provided with an "older than 18" flag rather than with the user birth date.

Signature

Beside authentication, signature is an equally important step for electronic transactions security.

In the real world, hand written signatures are used to stipulate that all parties agree for a transaction. In case of dispute at a later stage, the signed contract will recall the parties the rights and duties they formally agreed. Hand written signatures are also used by people to testify and guarantee the validity of the information they provide, to engage in a business proposition, or to acknowledge the reception of goods or information.

Use cases for digital signature

Online signature generation and verification respond the same use cases as real world hand written signature.

Bob, friendly tax-payer, has decided this year to fill his tax declaration online, through his government web-portal. He authenticates to the portal using his National electronic ID card and a secure session is initiated over the internet connection.

Once Bob has finished filling his tax declaration, he confirms that the editing session is complete. The tax declaration is then compiled in a document that Bob will sign if he agrees with it after a quick proof recheck, as he would have done with the former paper based declaration. For the "virtual" digital signature process, Bob will re-use his National electronic ID card and confirm he agrees with the document content with a formal signature generation that will require a specific validation, likely based on a new PIN code presentation. Once generated, the signature is sent to Bob's government portal and is appended to the declaration for future reference. It is likely that Bob will receive from his government portal a dated certificate of deposit, also built using a similar signature process.

Generally speaking, signature generation – the proper document signing process- is used when the user needs to provide to the other party a proof of acceptance or authenticity of a document.

In the previous example, signing the online tax declaration engage the responsibility of the signing party regarding the information provided. As well, signing a mail will prove the receiver that the sender is the one he pretends to be. Digitally signing a contract document

proves that the signing party received and accepted the contract as is.

Requirements and features

The signature generation algorithm must guarantee that the signature is bind to the document it was generated with and only that document: If the document is modified, the algorithm shall produce a different signature regardless of the importance of the modification. As well, the signature process dates the signature with a timestamp.

The signature verification process checks the signature against the related document and the signing party, and therefore controls both the authenticity of the document presented and the identity of the signer.

Signature algorithms rely on so called public key cryptography. This technology utilize a public key, bind to the user identity and a private key. The signing operation consist in running the algorithm on the document to sign (or a digest of the document) using the user's private key; the signature verification consists in applying another operation to the signed document using this time the user's public key: if the operation results in the document or its digest, then the signature is verified. The basic principle is that only the private key holder can create a signature but everyone else can verify the signature using the public key. From this description it becomes obvious that the signature can only be trusted if the user's private key is kept in a much secured area and never exposed, e.g. in a hardware token.

The same generation and verification algorithms are often used by secured authentication processes. If a user wishes authenticating to a service, he signs a "piece" of document (a "challenge") randomly issued by the service provider. The provider then verifies the signature and authenticates the user if correct. Again, only the holder of the private key – typically buried in a smartcard – can generate the signature and therefore successfully authenticate.

Data encryption

Another main challenge is the data confidentiality especially when the data is transferred in the internet. As illustrated in the previous example, the hardware token is a highly secured place holder for cryptographic keys. With the advent of portable data storage and cloud storage, user data privacy is at risk, which can be circumvented by data encryption. Hardware token could possibly be used to encrypt/decrypt user locally or remotely stored data, the challenge in this case being the performance of the interface and the encryption/decryption engine that may decrease significantly the

data bandwidth.

Of course it is also for a hardware token based encryption essential that the token is not accessible by an attacker. So some additional access protection to the token (e.g. via a PIN) is always recommended to achieve also Multi-Factor Authentication.

Conclusion

Username and password authentication method is obsolete whenever strong authentication is required. Using a strong password brings a significant security improvement, however we deal with too many online services to remember a different strong password for each.

Multi-factor authentication brings much stronger and convenient security, distributed over the several factors.

Software tokens such as certificates stored in a PC enhance the authentication strength. However, no software solution exists today which could reach the level tampered resistance enabled by secured silicon technology.

Most of us use smartcards in their daily life. This technology – the first widely deployed multi-factor authentication enabler- has proven its efficiency in reducing offline payment fraud and has taken part in the success of GSM and most of 3G and 4G telephony services as an essential brick in the security architecture.

Many cases of identity theft and fraud on internet are reported daily, no doubt that secured silicon technology can sort some of the issues, and enable additional services to the users.

NXP solutions

Genuine reference in security, NXP owns an astonishing number of 74 common criteria certificates for its security devices to date .

#1 supplier to the high security eGovernment market, NXP technology is used in more than 80% of the ePassport projects in the world.

Co-inventor of the NFC and inventor of the Mifare contactless technologies, NXP is at the forefront of the market convergence to contactless security, with an offer combining secured and reader interface devices. Our NFC technology is today in 200 devices, bringing contactless and security to millions of mobile users.

Reference

1. A Large Scale Study of Web Password Habits, WWW 2007, May 8–12, 2007, Banff, Alberta, Canada.

2. National Security Strategy, May 2010, The White House

3. “Electronic Authentication Guideline, NIST Special Publication 800-63-1”, December 2011. www.nist.org

Smaller Diagnostics and Changes in Materials Drive Medical Market

By Charles J. Murray, Senior Technical Editor, Electronics & Test and **Doug Smock,** Contributing Editor, Materials & Assembly

Imagine a new kind of electrocardiogram (ECG) without the typical jumble of crisscrossed wires, gels and electrodes. Instead of all that, this new-age ECG would use an adhesive patch, about the size of a Band-Aid, to extract performance data from the heart. It might also measure respiration, blood pressure and body temperature, and then store all that data in memory for days before being disposed of.

Sound too good to be true? Maybe so, but many such devices are already reaching the prototype stage, and could hit the market as soon as the next 12 to 18 months. The key is the development of a new breed of electronic components that dramatically reduce size and current consumption.

"These very small form factors have enabled creation of new products that could never have existed in the past," says Robert Burnham, marketing manager for biopotential analog front ends at Texas Instruments. "To create such feature-rich

products in the past, the electronics would have been too big and the battery life would have been too short."

Indeed, one of the keys to this diagnostic revolution is the development of analog front ends (AFEs) that pack dozens of discrete components - amplifiers, filters, attenuators and converters - into electronic packages measuring less than 10 mm on a side. Component suppliers Texas Instruments and Analog Devices have both announced AFEs that incorporate ECG and respiration monitoring capabilities onboard. In April, Texas Instruments rolled out a chip with ECG, EEG (electroencephalograph) and respiration impedance measurement. Measuring 8 x 8 mm, the 24-bit ADS1298R device packs 40 analog components and is said to be 97 percent smaller and use 95 percent less power than discrete implementations.

Similarly, Analog Devices announced in February that it is introducing the ADAS1000 ECG analog front end, which incorporates pacemaker pulse detection and respiration measurement. The new device, which incorporates 50 analog parts, reduces a conventional 4 x 6 inch printed circuit board down to a single silicon chip.

Such parts enable the construction of smaller diagnostic systems for two reasons: first, the chips themselves are vastly smaller than their predecessors; second, the AFEs enable engineers to use much smaller batteries.

"Our device, at only 750 µW per channel, uses only about 6 mW in an eight-channel part," Burnham says. "It really moves the bar for portable devices." Burnham says that with the new breed of analog front ends, many applications will be able to replace AAA or AA batteries with so-called "button cell" batteries.

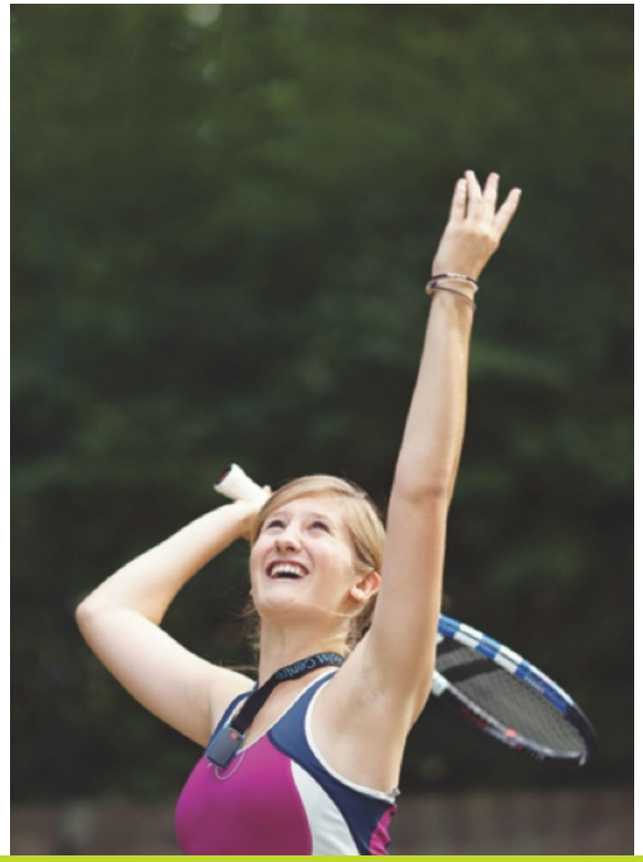
Analog Devices engineers say their AFEs will be able to record electrical activity of a heart in detail, enabling accurate analysis of numerous heart conditions, ranging from birth defects to arrhythmias to lack of blood flow. While all of those capabilities are commonplace today, they are generally done by cart-based instruments.

But by combining the new AFEs with a small processor, a memory device and a tiny battery, engineers say they can bring the size of an ECG monitor down to an adhesive patch measuring just 3 x ¾ x ¼ inch.

"Tiny is what people are looking for, says Patrick O'Doherty, vice president of the Healthcare Segment for Analog Devices. "This technology will be clipped on people's belts and go inside Band-Aids."

Many engineers say the obvious first step for the technology is to serve as a decidedly smaller replacement to the well-known Holter monitor, an ECG device

that is strapped onto patients for days at a time to check their hearts for abnormalities. In those applications, the new AFEs could offer a significant cost advantage. Because the new devices could potentially be disposable, they would eliminate the cost associated with collecting data, cleaning and re-packaging the monitor each time it's used by another patient. Those steps are now said to cost between $27 and $44.



"So the threshold for a disposable monitor doesn't have to be $1 or $2; it just needs to be less than $27," Burnham says. "That's not tough to achieve."

Some medical suppliers are already building medical products that use variations of the new technology. Imec, a Belgium-based nanoelectronics company, has already built a smart ECG necklace that can be worn around a person's neck like an ID badge. The smart ECG necklace, which works with two electrodes attached to the body, embeds a beat detection algorithm and is already being employed for ambulatory cardiac monitoring.

The Holy Grail, however, is still the creation of ECG systems in a small stickable bandage. By rolling the AFE chips together with a wireless transceiver and four or five small electrodes inside the bandage, engineers could eliminate the jumble of crisscrossed wires that's normally associated with ECGs.

"People who get an electrocardiogram won't need to be wrapped up in leads anymore," O'Doherty says.

If the technology receives widespread adoption, it could also open the door to a multitude of other possibilities. Temperatures, blood pressure measurements and respiration, along with ECGs, could all be done by a stickable bandage.

"I know many customers who are well along in their approval process," Burnham says. "Those products are definitely on their way."

Health Reform Drives Material Changes

Just as new technologies are changing

the way designers develop products for the medical industry, so too are regulations - particularly in the area of materials selection.

Industry experts interviewed by Design News see these specific trends in materials' selection:

- A major escalation in the battle to fight the spread of infectious diseases in hospitals through use of antimicrobial compounds and materials that can better tolerate demanding cleaning processes;
- Investigation of increased home-based health care; and
- More efficient use of operating room resources through better identification of instruments.

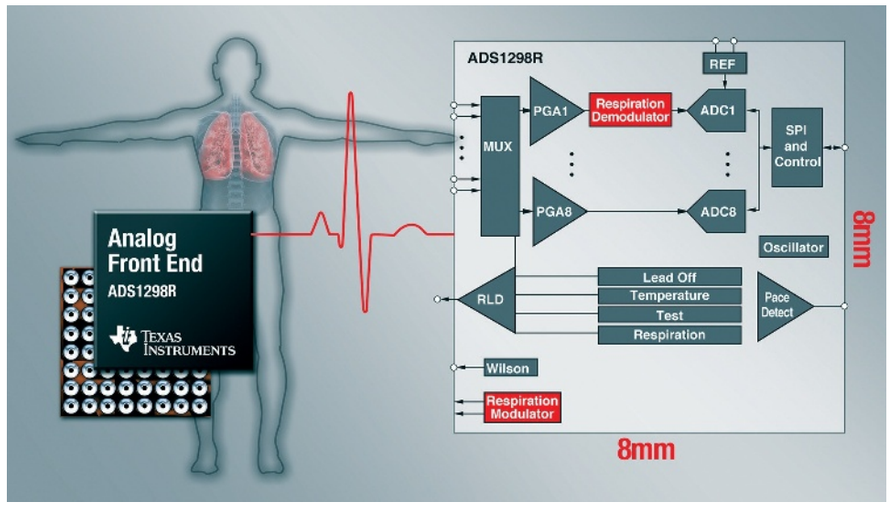
"The health care industry is in a period of dramatic change due to urgent calls for quality improvements and cost reduction," says Thomas O'Brien, global product marketing director, health care, Sabic Innovative Plastics. "Medical device manufacturers are right in the middle of this process and are looking for answers from suppliers - including new ways to design and manufacture to achieve the highest quality, meet new regulatory requirements, support new care approaches and drive down costs."

Fighting infections in hospitals may be the top immediate priority. In 2009, Medicare said it would no longer pay hospitals for additional costs to treat hospital-acquired infections. As a result, hospitals are declaring an all-out war on germs.

Two major producers of transparent plastics are rolling out new tougher grades.

"We understand that this market is changing," says Carmen Rodriguez, business manager, resin products at Altuglas International Resin, part of the Arkema group. "New developments dictate that we take a different approach."

Altuglas International has developed what it describes as the next generation of impact acrylic polymers for use in transparent disposable medical devices. They are said to offer improved resistance to environmental stress cracking



(ESC), excellent gamma sterilization resistance and good melt processability. Target applications include drug delivery applications as infusion systems, stopcocks, manifolds, luers, and intravenous (IV) and syringe components.

Arkema says the polymers' superior resistance to isopropyl alcohol (IPA) is particularly important because of patient safety guidelines aimed at preventing catheter-related blood stream infections that require new disinfecting techniques. One of those techniques is rigorous cleaning of intravenous lines.

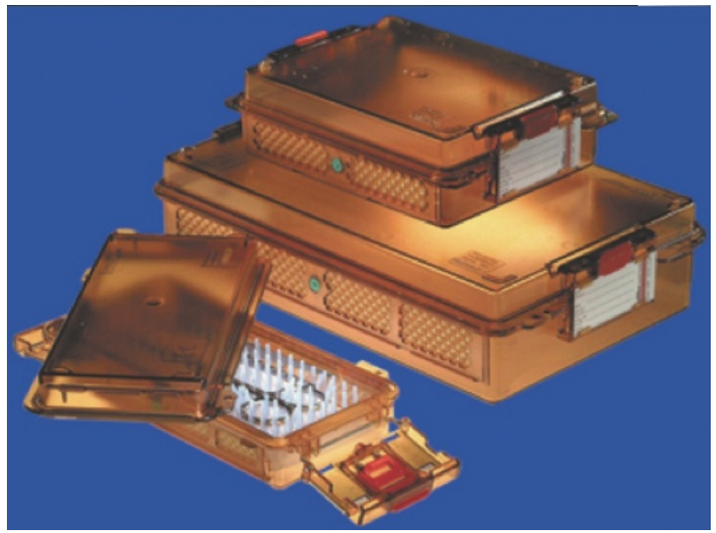
Evonik Cyro is now marketing an acrylic-based multipolymer compound that uses a proprietary silver-based antimicrobial agent to kill germs on the surface of medical equipment. The compound targets FDA-regulated Class I or Class II medical devices covered by 501(k) submission. Evonik Cyro expects the materials to be used in place of existing acrylic compounds, polycarbonate or polyvinyl chloride (PVC).

George Pape, head of medical and pharma in North America for the Clariant Masterbatch Business, says he also sees renewed interest in antimicrobial compounds for medical applications. "Everything is pretty much done on a custom basis," says Pape. Some applications require maximum protection, and others may be less critical. He sees a trend in particular to the silver-based antimicrobials.

Efficiency is also an important trend affecting materials selection in the medical market.

"More efficient use of operating room resources requires quick visual confirmation and improved inventory tracking and management" says Judy Melville, industry manager at Solvay Advanced Plastics.

One method for quick visual confirmation is using colors to distinguish different medical instruments or components. That can be tricky for medical applications because many plastics are colored with dyes, which can migrate to the surface of molded products.



Clariant is introducing Mevopur color concentrates and pre-color compounds, whose ingredients have been biologically evaluated against USP parts 87 and 88 (Class VI devices). Clariant also recently launched a new range of globally harmo-

nized standard colors for polypropylene and polyethylene, as well as other materials such as polyether block amide plastic, where ingredients have been biologically evaluated according to ISO10993 and USP parts 87 and 88 (Class VI).

Wavemark Inc. is putting radio frequency identification (RFID) tags on the packages of expensive medical devices to monitor inventories of such items. The company estimates that supply chain expenses as a percentage of cost of goods is 39 percent for medical devices, compared to 3 to 6 percent for retail stores.

One technology on display at MD&M West that has significant potential to boost RFID use in medical devices is called 3D-MID. Harting Mitronics is producing three-dimensional injection-molded RFID tags based on 3D-MID (MID is an acronym for molded interconnect device). A laser activates the surface of a plastic part made with specially engineered plastics. Then, the activated surface area is chemically plated to create the antenna. The process is called LPKF LDS (laser direct structuring).

Another megatrend in the medical market is at-home care. Moving patients out of the hospital, when possible, reduces costs and decreases risks of infection. Several exhibitors at MD&M West showed portable medical devices for home or field use that employ lightweight plastics for housings and other components that previously have been made from metals.

One example is the Inogen One G2 System, a second-generation portable oxygen concentrator. Compared to its predecessor, it's 40 percent smaller, 25 percent lighter, with 20 percent more oxygen and a longer battery life.

"Durability is one of the most critical factors of our device," says John Stump, mechanical design engineer, Inogen. "We have experimented with many different grades of resin to find the best quality molded parts for our application." The portable device's shell is constructed of six separate components molded from Bayer MaterialScience LLC's Bayblend FR 3010 polycarbonate/ acrylonitrile-butadiene-styrene (PC/ABS) plastic. The external battery housing is also made of three components molded from the same polycarbonate blend.

Look for challenges on materials' technology to escalate as the effort to improve health care and reduce costs intensifies. ■

PUF – Physical Unclonable Functions

Protecting next-generation Smart Card ICs with SRAM-based PUFs

The use of Smart Card ICs has become more widespread, having expanded from historical banking and telecommunication applications to electronic passports, electronic IDs, anti-counterfeiting devices, smartgrid applications, and more. The security requirements for most of these applications are crucial and evolving. In addition, more and more sophisticated attacks are being developed every day. As a result, design of Smart Card ICs is a growing challenge.

This paper summarizes the present-day security challenges for Smart Card ICs and describes how a special technology, called Physical Unclonable Functions (PUF), delivers comprehensive protection in today's applications. PUF technology provides a secure method for storing a key, withstanding today's attacks, and even protecting against future potential attacks.

Note: For the purposes of this document, the term "Smart Card ICs" refers to microcontrollers based on smart-card secured technologies in traditional smart-card applications and in the secure elements of NFC-enabled devices, authentication tokens, and other high-security modules.

Types of attacks

The Smart Card industry typically places attacks in one of three categories:

- Side channel attacks (non-invasive attacks) – such as using information out of the power profile or the electromagnetic emanation
- Fault attacks (semi-invasive attacks) – such as disturbing the IC by applying laser light or a voltage glitch
- Reverse engineering (invasive attacks) – reverse engineering parts of the IC, possibly combined with probing signals

There has been important progress in all of these attack categories during the last few years. Smart Cards have to use sophisticated countermeasures to withstand these new attacks. In some markets, such as electronic passports, Smart Card ICs have to withstand attacks in the field for the ten years they are valid.

Reverse engineering attacks are back in focus, especially after recent attacks on some widely used Smart Card ICs. These attacks often have a much higher impact than side channel and fault attacks because there are essentially no ways compensate for them with additional software countermeasures. Fault and side channel attacks are often carried out on a limited basis, on specific modules or portions of the device, and can be addressed with additional software countermeasures.

There are several countermeasures available today that hinder reverse engineering and prevent attacks, and new technology nodes and more sophisticated techniques continue to improve security. But, in the end, given unlimited effort, there is an attack path for every chip. The reality is that there is no such thing as guaranteed protection.

Typical reverse engineering attacks on Smart Card ICs include the following:

- Reverse engineering of a functional block
- Reverse engineering of parts of the IC as preparation for a subsequent probing attack
- Extracting memory content

The standard countermeasures taken against reverse engineering attacks include the following:

- Memory encryption
- Encryption of data
- Scrambled logic (especially no hard macros)
- No logic relevant to security in top metal layers

The problem of storing a key

The standard countermeasures used against reverse engineering today are unlikely to be able to protect against future challenges. The memories of a Smart Card device (ROM, EEPROM, Flash, RAM) are usually protected by memory encryption. These memories contain security-relevant assets which need to be protected. The Flash or ROM also contains the Smart Card Operating System (OS) code, which is critical intellectual property (IP) and essential to protect.

There is, of course, some basic physical protection for the different memories. But attackers have been able to extract some (even if only a little) data from these kinds of memories. It is expected that these attack techniques will

improve significantly in coming years. At that point, the protection of the assets is down to the memory encryption being used. A fundamental issue which still remains – even with a theoretically unbreakable memory encryption – is the protection of the key. Storing the key in one of these memory areas is not an option if this area can be read out .

An alternative approach is needed. One such alternative is Physical Unclonable Function (PUF) technology.

Physical Unclonable Function (PUF)

Physical Unclonable Functions (PUFs) are defined as functions based on physical characteristics which are unique for each chip, difficult to predict, easy to evaluate and reliable. These functions should also be individual and practically impossible to duplicate. PUFs can serve as a root of trust and can provide a key which cannot be easily reverse engineered.

In principle, any physical device characteristic that fluctuates can be turned into a PUF. Two prominent examples of PUFs in Smart Card applications (and other secure applications) are arbiter PUFs and SRAM-based PUFs. Arbiter PUFs rely on race signal conditions, and are not the focus of this paper. SRAM-based PUFs work with the SmartCard IC's internal memory, and are described in more detail below.

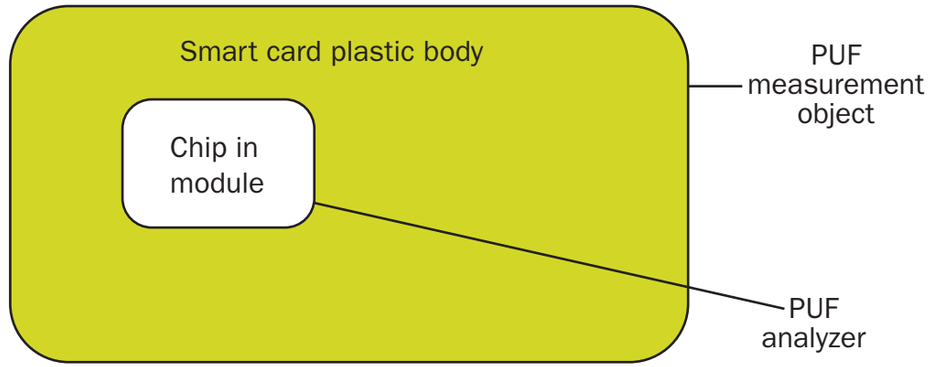
PUF and environment monitoring

In addition to SRAM-based and arbiter PUFs, there are other PUF technologies that can be used to help monitor the surrounding environment of the Smart Card IC, including the card body.

The IC itself can check whether the environment is intact. During production or personalization, the IC measures its PUF environment and stores this unique measurement. From then on, the IC can repeat the measurement (preferably during startup), and check if the environment has changed, which would indicate an alteration in the card body. This protects against many kinds of invasive attacks.

PUF technology in NXP's next-generation Smart Card ICs

SRAM PUFs rely on physical characteristics of SRAM technology. These types of PUFs are currently being integrated into NXP's next-generation Smart Card ICs. After powering the Smart Card IC



(and as a result the embedded SRAM), the cells are initialized with a pattern randomly made of zero and one logical values. This startup behavior – each specific bit in SRAM getting zero or one as an initial value- is different for every individual chip. But, looking at an individual Smart Card IC, this random initialization of SRAM content is very similar from one startup to another (for a single device). Small deviations in processing inside a SRAM cell lead to variants of electrical characteristics for each transistor. The SRAM cell design is symmetrical but the deviations lead to a small asymmetry resulting in a preferred state (0 or 1) during startup. The SRAM content after startup can serve as a unique fingerprint of the Smart Card IC. As the behavior is not completely the same for every startup, and some of the SRAM cells show different initialization after startup, error correction is necessary. Typically, codes for error correction (such as Reed-Solomon codes) are used to derive a unique device fingerprint. The derived fingerprint can then be used as a key, to protect a cryptographic key, or to protect a memory. The physical behavior over the device lifetime, as well as the error probabilities, make it essential to evaluate the reliability in a typical Smart Card environment together with a suitable post processing function (i.e. error correction).

SRAM PUF implementation

The SRAM PUF generates a device-individual fingerprint using the startup behavior of SRAM cells. The generated SRAM PUF fingerprint can be used for various use cases. It can be used directly as a key or indirectly to protect sensitive data (e.g. application keys).

The SRAM PUF typically consists of the following components:

1. SRAM area used as PUF source
2. Measurement circuit and error correction used to derive an individual IC fingerprint (hardware)
3. PUF IP (Activation Code Constructor and Key Extractor), which adds functionality to protect keys or memories (hardware)

The PUF IP adds functionality to protect application keys with the IC individual fingerprint. It acts as an internal key vault and therefore solves the problem of storing a key. The OS has to provide the application keys to the PUF IP. The PUF IP then uses the IC fingerprint to protect these values. The PUF IP needs to store an activation code, which can be public related to the respective application key, and stored in non-volatile (NV) memory such as EEPROM or Flash. The key is essentially split into two parts – the SRAM PUF fingerprint and the activation code. The attacker must know both

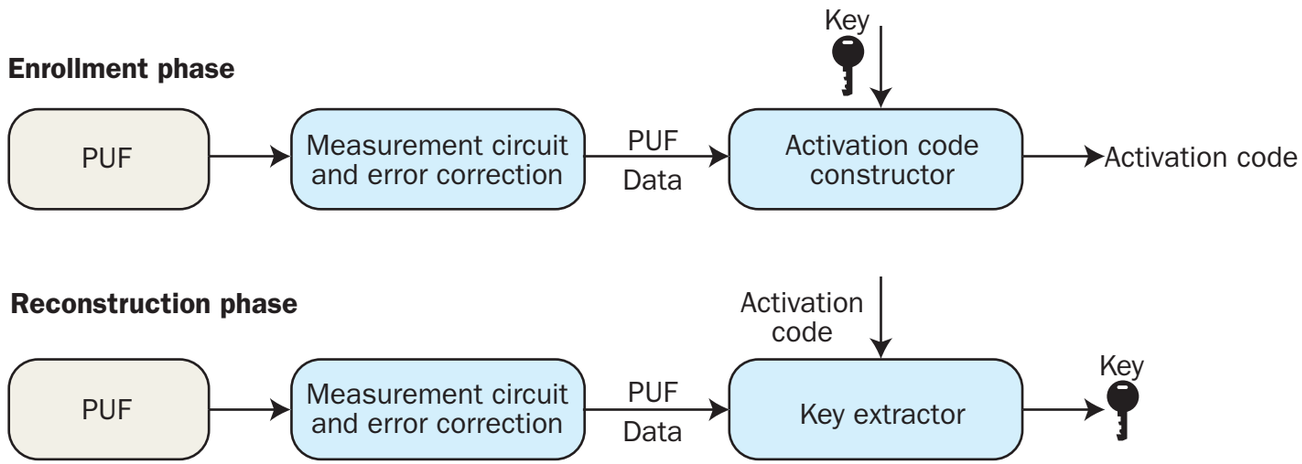
values to reconstruct the application key.

PUF usage is typically divided into two phases, Enrollment and Reconstruction.

The figure shows the PUF and Error Correction post-processing that produces the PUF data, which is the IC's individual fingerprint.

The Enrollment Phase occurs just once, when a new key is generated or being stored. The key is put into the Activation Code Constructor, which produces the activation code to be stored in NV memory.

In the Reconstruction Phase, the activation code is used in the Key Extractor to reconstruct the key. The actual key is not stored in NV memory. The key cannot be derived with the activation code alone; the code and the PUF data must both be available to reconstruct the key.



PUF reliability and limitations

To evaluate the reliability of SRAM PUFs, researchers have analyzed the physical characteristics of SRAM startup behavior under various operation conditions. Temperature and aging have been given special attention. The results have shown that SRAM PUFs are suitable for use in Smart Card ICs with a lifetime of more than 10 years.

It's also important to understand the limitation of a countermeasure based on PUF technology. PUF is primarily used to protect critical data, such as keys or complete memories, from offline attacks. Offline attacks are attacks mounted when the device is powered off. There might be further attack paths on the critical data when it is being used (the device is “online”). For instance, PUF can’t provide additional protection when a key is being used for a cryptographic operation. This still needs to be covered by other measures.

A PUF implementation also has to be carefully designed and security tested such that the PUF implementation itself

is not opening other security attack paths, such as some weaknesses with respect to side channel or fault attacks.

SRAM PUF use cases

Key protection

As described above, SRAM PUFs can protect application keys or other critical user assets in a way that is more secure than just storing the key in NV memory. The following table compares the two methods: The traditional method, where the application key is stored in NV memory, and the PUF-based one, where PUF is added to protect the application key. The table provides an overview of the different attack categories together with an assessment whether the attacks are applicable, now and in the future, without and with PUF technology.

Attacks on Smart Card ICs without and with PUF technology (Key protection)

Type of Attack	Traditional technology, application key stored in NV		Application key stored with PUF technology	
	Today	Tomorrow	Today	Tomorrow
Copying NV memory contents from one device to another (offline)	Difficult to impossible	May be possible	Impossible	Impossible
Extract application key (offline)	Difficult to impossible	May be possible	Impossible	Impossible
Extract application key with fault attack (by distributing I/O function)	Difficult (normally secured by software and hardware firewalls)	May be possible (depends on software implementation)	Impossible (only additional data in NV memory can be read out)	Impossible (only additional data in NV memory can be read out)

Reading out Non-Volatile (NV) memories (i.e. EEPROM or Flash) is mostly impossible, but reading out ROM contents may be easier. Thus far, only a few bytes have been successfully read out of EEPROM or Flash. But even if this is not feasible today, attacks are likely to improve significantly in future. If at some point it is possible to read out larger parts of the memories, or even the complete memory, the protection for the application key is gone.

PUF technology also protects against fault attacks in this use case. With standard approaches (where the application key is stored in NV), there might be ways to manipulate an I/O function such that the application key is compromised. A key protected with PUF technology cannot be extracted with this attack. Only the (non-sensitive) activation code can be extracted.

Memory protection, countermeasure against cloning

Another important use case for PUF technology within Smart Card ICs is the encryption of memories. Nowadays, the encryption keys for ROM, EEPROM and Flash memories have to be stored in the memory areas as well. If – at some point in the future – it becomes possible to read out complete memory contents, there is no secure place to store the encryption key. In this case not even the strongest memory encryptions will prevent successful attacks.

PUFs can play a crucial role in future resistance to reverse engineering attacks on memory. Offline attacks on memory content (such as applications keys or critical IP) become impossible when using PUF technology for memory encryption.

External memory protection, countermeasure against cloning

In some applications, a Smart Card might also be connected to an external (unprotected) memory. Standard external memories (such as Flash memories in USB sticks) are easy to read. PUF technology can be used to protect these kinds of insecure external memories. PUF technology can serve as a root of trust, implementing the source for the memory encryption.

Fingerprinting

Another use case of PUF technology within the Smart Card IC area is fingerprinting.

Attacks on Smart Card ICs with and without PUF technology (Cloning)

Type of Attack	Standard Memory encryption		Memory encryption using PUF technology	
	Today	Tomorrow	Today	Tomorow
Copying NV memory from one device to another (offline)	Difficult to impossible	May be possible	Impossible	Impossible
Extract memory contents (offline)	Difficult to impossible	May be possible	Impossible	Impossible

Attacks on external memories with and without PUF technology

Type of Attack	External Memories (unprotected)	External Memories protected by PUF technology
Extracting (sensitive) data (offline)	Easy	Impossible
Cloning / copy data from one device to another (by reverse engineering memory contents offline)	Easy	Impossible

The PUF is used to provide every device with an individual fingerprint, which is characterized and stored in a data base during the production phase. At a later stage, every device can be identified in the field using this PUF fingerprint information.

PUFs in different applications

Although Smart Card ICs are used in a variety of different application scenarios, the applications have several things in common. The Smart Card IC usually protects sensitive user data (such as private keys for electronic signatures), and the OS source code is often seen as a critical asset that needs to be protected. If attackers gain access to the source code, it's easier to identify areas of vulnerability, and source code is typically a crucial piece of intellectual property for the OS provider. This next section looks at specific requirements for today's most popular applications for Smart Card ICs.

eGovernment

Electronic passports (ePassports) and electronic ID cards (eIDs) are the leading Smart Card applications in eGovernment. Passports equipped with Smart Card ICs were introduced in 2005. The Smart Card ICs typically store personal information that is also printed on the document – such as name and photo – along with optional data such as fingerprints. ePassports also usually include a mechanism for authentication, called chip or active authentication, that prevents the document from being copied and provides proof that the document is valid. Authentication relies on a private key hidden in the Smart Card IC's secure memory. PUF technology can protect the key and prevent reverse engineering.

Using PUF technology, the private key used in a passport (which prevents the cloning of the document) is more strongly protected against (memory) reverse engineering attacks than with standard methods.

With eID applications, the situation is similar. The document typically uses an au-

Type of Attack	Private Chip/Active Authentication key stored in NV memory		Private Chip/Active Authentication stored with PUF technology	
	Today	Tomorrow	Today	Tomorrow
Extracting Private key material (offline)	Difficut to impossible	May be possible	Impossible	Impossible
Clone a passport (by reverse engineering memory contents offline	Hard to Not possible	May be possible	Impossible	Impossible

thentication method based on a private key stored in NV memory. PUF technology can be used for added protection against future attacks. The eID may also use an electronic signature, based on a private key.

Some eID cards use a private authentication key, called a group key, that is shared among a set of cards. The idea is that a group key does a better job of masking the identity of each individual in the group, making it harder for thieves to track a given user. The security requirements for this kind of key are especially high, because anyone successfully extracting the key ID has access to more information. PUF technology can protect authentication keys or the memory that contains the key.

Type of Attack	Private key for SDA/Online Authentication or DDA stored in NV memory		Private key for SDA/Online Authentication or DDA stored with PUF technology	
	Today	Tomorrow	Today	Tomorrow
Extracting Private key material (offline)	Difficult to impossible	May be possible	Impossible	Impossible
Cloning device (by reverse engineering memory contents, offline)	Difficult to impossible	May be possible	Impossible	Impossible

Payment

In the payment market, MasterCard, VISA and other large players are defining the standards and the usage of Smart Card ICs. The cryptographic protocols used within Smart Card ICs are defined by the EMVCo standard. This standard comes with a set of protocols that serve different application scenarios and provide different security levels.

There are two main EMVCo protocol branches: Static Data Authentication (SDA), which may include an Online Authentication procedure, and Dynamic Data Authentication (DDA). Both protocols rely on a private key which is buried in the Smart Card IC's memory. Keeping the key private prevents the payment card from being copied.

Mobile devices

Smart Card ICs are now in widespread use in mobile phones and tablets. A common use case is the electronic wallet, where the Smart Card IC acts as a secure element to emulate a bank card in a mobile phone. The Smart Card IC,

equipped with data similar to that of a bank card, works with a contactless interface to let the phone serve as a contactless payment card. In this case the threats and attacks are the same as for a standard payment card.

In future, PUF technology might be used to protect external memories. The secret key used for encrypting external memories (partly or just some application keys) could be provided by PUF technology.

Type ofAttack	Private key for Device Authentication stored in NV memory		Private key for Device Authentication-stored with PUF technology	
	Today	Tomorrow	Today	Tomorrow
Extracting Private key material (offline)	Hard to impossible	May be possible	Impossible	Impossible
Cloning of a Device (by reverse engineering the memory content)	Hard to impossible	May be possible	Impossible	Impossible

Authentication

In the consumer segment, which includes mobile phones and tablets, manufacturers need to protect against the copying of accessories. In the case of printers, for example, copying or cloning printer cartridges is a serious threat. Some manufacturers are integrating Smart Card ICs into their accessories to prevent cloning and unauthorized access. Because this is a new trend, formal standards for cryptographic protocols have yet to be developed, but most are based on a symmetric or asymmetric cryptography. The security relies on a private key buried in the Smart Card IC. PUF technology can, again, be used to increase security of the key.

Conclusion

Reverse engineering has emerged as one of the most dangerous kinds of attacks for Smart Card ICs. Unlike other attacks on Smart Card ICs, including side channel or fault attacks, reverse engineering attacks are difficult to protect against using additional software countermeasures.

Partial reads of NV memory are already possible, and full reads are likely to be possible sometime in the future. This means that even the strongest memory encryption methods won't be able to protect stored assets over the longer term.

SRAM PUFs, with their ability to pro-

tect against offline attacks, are an especially useful tool in the fight against reverse engineering. By generating a unique IC fingerprint, SRAM PUFs make it much harder to attack memories and other sensitive data when the device is powered off. With SRAM PUFs, it's possible to implement a secure mechanism for key reconstruction without storing the key. In this way, PUF technology effectively addresses the issues of reverse engineering and NV memory readouts.

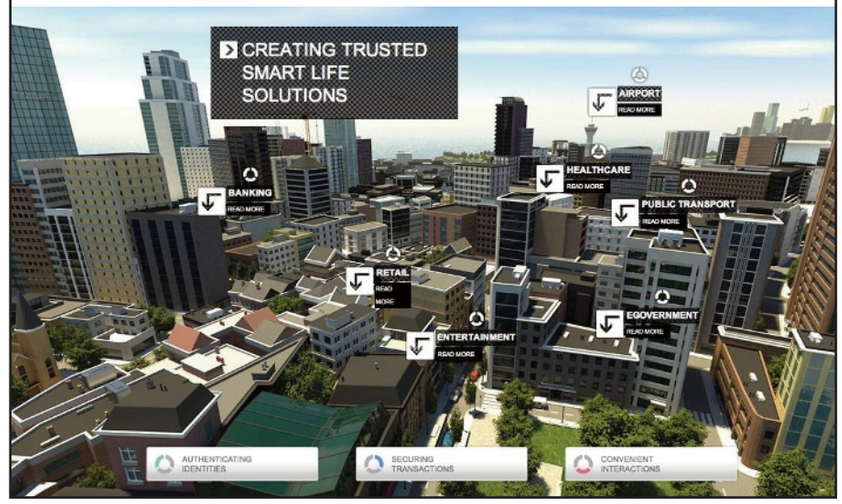
SRAM PUFs will be a key element of the “Integral Security Concept” used in NXP’s Smart Card ICs. NXP is also investigating on future PUFs to be used for other security countermeasures. One idea is a PUF which enables the Smart Card IC to check if the surrounding environment is still intact. The chip measures the environment (the surrounding card body) in the production and personalization stages and rechecks the measurement regularly when the IC is in use (preferably at every startup). Such PUF technology could serve as a highly effective protection against many types of reverse engineering and fault attacks.

About NXP

Building on trusted security, a complete product portfolio and the best contactless performance, NXP is the leader in the overall ID market and in key market segments such as transport ticketing, eGovernment, access, infrastructure, RFID/Authentication, payments and NFC. NXP provides the entire ID market with end-to-end solutions, enabling customers to create trusted solutions for a smarter life. ■

NXP

Creating Trusted Smart Life Solutions



NFC Tags: A technical introduction, applications and products

By Francesco Gallo, NXP Semiconductors

The NFC Data Exchange Format (NDEF) is a data format to encapsulate and identify application data exchanged between NFC-enabled devices. One such device is the NFC Forum Type Tag. The NFC Type Tags are contactless cards based on currently available products capable of storing NDEF formatted data. NDEF and NFC Tags allow new kinds of touch-based applications such as Smart Poster, automatic wireless communication configuration, and electronic business card exchange. Such applications can be implemented using NFC-enabled Tag products already available in the market. This white paper describes NDEF, NFC Forum Type Tag Operations, NFC-enabled Tag products, and several related use cases. ■

Protect Your Electronic Wallet Against Hackers

By Craig Zajac, Synopsys

The capability to protect personal information from hackers through a secure element is critical to the continued development of the NFC ecosystem. SoC designers who most effectively implement data security from the start will have a competitive advantage in the marketplace. There are two technologies in use today for NVM IP in SoC applications, antifuse for OTP and floating gate for MTP. Understanding the impact that they have on which reverse engineering techniques is critical to making the right NVM IP choice. After reviewing three reverse engineering techniques, the conclusion is that while both technologies are secure, floating gate is more resistant to reverse engineering. ■

Bridging the gap for new applications in electronics with interactive Gen2 RFID

From adding visibility to the production process, through work-in-process manufacturing techniques, to adding accountability and speed to the movement of finished products through the supply chain, RFID has already changed the way manufacturers of electronics operate. But a number of challenges and shortcomings have limited the benefits the technology delivered.

Often, product housings made of metallic or other types of conductive materials, present an obstacle when using off-the-shelf RFID labels, because the surfaces block the RF signal transmitted by readers, making the tags difficult

NXP's new UCODE I2C integrated circuit (IC) is transforming EPC Gen 2 UHF RFID tags into interactive tools for electronics.

to read. Additionally, an RFID label attached to the exterior surface of a product can easily be found and removed—a weakness that a nefarious party could exploit in order to divert goods to the grey market or disassociate a product from its warranty records.

Moreover, applying RFID tags to the exterior surface of electronic products, after they've already been manufactured, robs the manufacturer of the added visibility and control the technology could provide throughout the entire manufacturing process.

NXP has introduced a new IC platform designed to enhance RFID beyond the traditional track and trace applications. This new product, known as the UCODE I2C boasts a slew of features tailored specifically for the electronics market. The chip provides high memory, security features, and a variety of packaging options that make it highly versatile. By enabling a bidirectional communication bridge between products' electronic circuitry and a wireless

Gen 2 infrastructure, this new introduction offers features never before seen in standard passive UHF RFID tags and opens doors to new applications for wireless sensors, product security, customization and authentication features. NXP's UCODE I 2C is a game-changer for RFID and the electronics industry.

Key to these benefits is the addition of NXP's inter-integrated circuit, or I 2C, which is a technology that NXP (formerly Phillips) developed more than 30 years ago and which is used widely in electronics today. The UCODE I 2C RFID chip comes with a high speed I2C serial bus that enables a wireless link between an RFID reader and the electronic device's microprocessor. Through this interface, users can turn basic EPC Gen 2 tags into communication portals that will allow for unprecedented levels of product interaction, configuration, security and product interactivity for manufacturers, retailers and consumers, alike.

Case in Point: A Smarter, More Secure Laptop

There are numerous use cases for which using RFID tags based on the UCODE I 2C chip would help ensure optimal performance while enhancing tag customization and consumer convenience.

Let's take a laptop as an example where a manufacturer integrates an NXP UCODE I 2C RFID chip right into the device's electronics.

Reliable Track and Trace

The UCODE I2C chip may be integrated

within the product's printed circuit board (PCB) usingthe traces to function as the tag's antenna. The chip may also be coupled to the product chassis to further enhance the tag's performance.

This solves two potential dilemmas. For one, it removes the burden of finding a way to apply an RFID tag to the exterior of the computer while ensuring that the tag doesn't change the laptop's aesthetics. Plus, it protects the tag from damage or tampering. Product aesthetics is a growing concern among manufacturers, as many newer devices, such as smart phones or tablets, are becoming as much a statement of art as of technology. We're seeing this through increasingly streamlined designs that do away with conventional bar-coded labels or printed or etched serial numbers. To accommodate this style, sometimes bar codes are placed inside electronic devices, which means they can only be accessed by opening up the device. An internal, integrated RFID tag removes this hurdle.

The second benefit of an integrated RFI D tag is that using the device itself to act as the tag's antenna helps ensure that the tag will be read-in fact it can even increase a tag's read range because integration may help make the antenna relatively large, compared to an off-the-shelf tag. For devices with conductive enclosures, placing a conventional RFID tag inside the laptop often restricts the tag's functionality.

Once the tag is integrated into the device, it can be used to track the laptop throughout the manufacturing process. RFID readers mounted along the production line will collect the unique tag ID encoded within the chip's memory, enabling a work-in-process tracking system that ensures fast, error-free assembly.

Bi-directional Communication

Integrating the UCODE I 2C chip into a laptop opens the doors to many new and exciting applications. By tapping directly into the RFID chip via the I 2C serial bus, the electronics manufacturer can establish a link from RFID chip to the laptop's microprocessor. This not only integrates the RFID tag into the device itself-providing the basic tracking benefits described above-but it takes this integration an important step forward, because it paves the way to interactive Gen 2 RFID functionality. It establishes a bidirectional wireless bridge between the electronic device and the manufacturer, the retailer and the consumer.

Securing Shipments

Integrating the tag into the laptop's main processing unit gives the manufacturer and retailer the power to wirelessly control the device through the RF interface.

For example, once the laptop passes its final inspections and is ready for shipment, the manufacturer can disable the unit, th rough its RFID interface, as a disincentive from theft until ready for purchase. This way, once the laptop is placed into the supply chain, it would be of no use to any nefarious party that might want to divert shipments of the laptops to unintended grey markets.

To disable each laptop, the manufacturer would simply use an RFID reader to send a command, through the laptop's RFI D IC, that renders the laptop locked.

Because the embedded RFID tag could still transmit its unique identification number through backscatter, the disabled laptops could still be traced as they move through the supply chain.

Later, once a retailer or distributor receives the laptops, an RFID reader would again be used, this time to send an authentication code, also through the RFID interface, which would unlock the laptops and make them operable again.

And at the retail store, the RFID tag continues its work as a unique identifier, enabling fast, accurate inventory cycles. But its usefulness is far from over.

Upgraded, Customized Products

At the point of purchase, the integrated, bi-directional RFID tag becomes a tool for product customization. Say, for example,

that the laptop is a gift. Upon the consumer's request, the retailer can use the RFID reader to upload, through the IC's I 2C bridge, a customized wallpaper backdrop (e.g. a birthday or holiday theme) with a personalized message for the recipient. Using this same technique, the retailer can also preload the laptop with an online gift certificate, encouraging the recipient to return to the retailer for additional products or services. Plus, the RFID gateway would even allow the retailer to set up the laptop with the user's wireless account credentials or set up an account for downloading music or eBooks for an extra special touch.

Or, say a customer was given a base model laptop as a gift and was interested in upgrading its video graphics quality or increasing its processing speed. If these improvements could be made through software upgrades, a provisioning key may be uploaded through the IC's 1 2 C bridge. The retailer could make the upgrades without having to swap out any hardware, and the con-

sumer would pay only an upgrade fee.

Through RFID-enabled product customization and software-enabled upgrades, retailers could provide more value to-and earn more loyalty from-their consumers, while also creating new revenue streams through upgrading services.

Plus, all of the wireless services that the 1 2C bridge enables-from uploading minor firmware patches, configuring language settings or customizing a laptop for a specific customer-can be done without even removing the laptop from its original packaging.

All of these benefits add up to opportunities for boosting sales, offering customization services and enhancing the customer experience.

Positive Identity

In addition to all these possibilities, this new chip, through its anti-tampering features, can also be used as a tool for authenticating products, as long as the retailer chooses to keep the embedded RFI D tag intact after the point of purchase (rather than decommissioning the tag). Retailers can, thanks to another UCODE 1^2C feature, decrease the RFID tag's read range at the point of sale, as a means of addressing privacy concerns the consumer might have a bout the tag embedded in his new product.

The UCODE 1^2C can be configured such that if the device into which it is embedded-say, a motherboard-is tampered with, the chip can report a breach, along with its unique identification during its next RF transmission. This feature would help root out criminal activity such as the practice of purchasing high-value electronics, swapping out the original components for lower-grade versions-or even replacing them with weights rather than electronics-then returning the product while it's under warranty and selling the original, high-value components on the black market. An embedded UCODE 1^2C RFID tag would stymie attempts to do this by alerting the retailer to the tampering.

Outside of stemming illegal activities, the technology can also help retailers authenticate legitimate returns, making warranty processing and product returns easier and more accurate. In these scenarios, the retailer would use the embedded RFID tag to identify a product that is returned, either for repair or as a product return or exchange. Once the tag number is captured, the retailer can use it to access the original sales record and warranty, in its back-end records, erasing any doubt as to whether the product was legitimately obtained.

Diagnostics Duty

In the case of a repair, the bi-directional

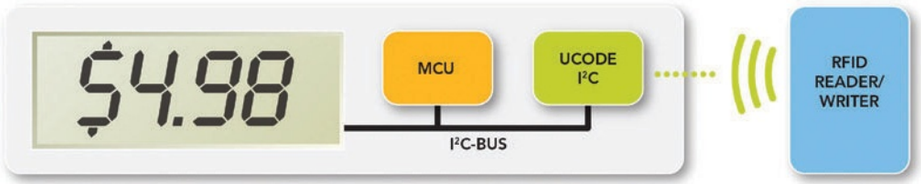
functionality of the wireless bridge can be used to collect any error logs that the computer saved to its memory. This enables access even if the computer ceases to ope rate.

The 3,328-bit user memory within the UCODE I 2C allows adequate space for error logs or other data the stakeholders might want to save to the tag's memory. And embedding the RFID tag into the manufacturing process saves money and time compared to tagging goods as a secondary operation later in the supply chain, where the benefits are less attractive.

All of the above scenarios also play out with a tablet, smart phone or other consumer electronics, as well. In all cases, this new integrated and interactive approach to RFID in electronics opens up many new applications for stakeholders across the consumer electronics industry-from manufacturers to consumers.

Case in Point: Electronic Shelf Displays

Tagging electronics at the item level using the UCODE I 2C chip offers manufacturers and retailers many clear advantages, as we've already outlined. But this chip also opens doors to novel cost-effective applications in the retail environment that can improve inventory controland boost sales.



Printed shelf labels have long been the main medium that retailers use to convey special offers inside stores. But managing these labels, and ensuring that they are placed and removed in accordance to a strict time table, can pull e mployees away from se rving custom ers. Plus, poorly-managed shelf labels can lead to customer disputes; customers often demand that retailers honor the lower prices if sale prices are not removed from sales in a timely manner.

Smarter Shelves

But wh at if switching shelf l a bels was no longe r a con ce rn? What if th ey ch a nged a utomatica lly, always reflecting the accurate prices and terms? The UCODE 1 2C chip, joined with an inexpensive e-pa per display solution, can make this a cost effective reality.

A RFID-enabled dynamic price label can be controlled wirelesslythrough a nearby RFID reader that is co ncealed fro m view-perhaps mounted above ceiling tiles.

Not only does this reduce the labor requirement and complexity of managing

shelf tags,it allows retailers to offer many more dynamic sales than they could with paper labels. For example, a retailer might want to dabble with a very short, hour-long sale-perhaps one timed w ith a special tel evision or rad i o ad, or to reward sh oppe rs f or gettin g to the store early on a holiday weekend. With a few keystrokes, a store manager can lower the price of specific items, based on their shelf location, with the UCODE-based electronic shelf labels. As soon as the sale window closes, the labels will automatically revert back to the original retail price. All this would be done using a common, off-the-shelf Gen 2 reader infrastructure.

Electronic shelf displays also help protect revenue by eliminating the need to manually alter the price tags attached to the products—a practice that leads many retailers to having to honor sale prices even after a sale has ended.

And unlike an LCD or LED display, the ePaper can be activated when the tag receives new pricing information from the reader, but does not require energy to sustain the information after the content is adjusted, thereby conserving power.

In instances where batteries are used and where battery life starts to wane, the UCODE I²C may alert the reader of a low power indicator along with its unique ID number, so the retailer can look up its location. Then, the next time the tag is read, the reader detects the status and alerts staff to recharge or replace the battery. Alternatively, power for displays or microprocessors may also be feasible with energy harvesting techniques using the RFID signal, WiFi signals or light, and therefore never need battery replacement.

In Summary

Aside from all of the features and functions listed here, the UCODE I²C offers all basic EPC Gen 2 capabilities, including password protection and cloaked viewing for instances where data is not intended for public viewing. In addition, it offers added features such as a status flag bit, which can be used in combination with an RFID security system to trigger an item to sound an alarm if it is removed from a store without being purchased.

Best of all, the UCODE I2C chip is the foundation of an EPC Gen 2/ISO 18000-6c tag, and accepted worldwide, so you'll realize the new benefits that NXP's I²C platform offers by using your existing Gen 2 infrastructure, without having to sacrifice your adherence to industry standards. That's NXP's approach to RFID: Multi-application, without compromise.

So, what's your next step? NXP's RFID Application and System Center and our qualified partners are ready to help you determine the optimal methods for em-

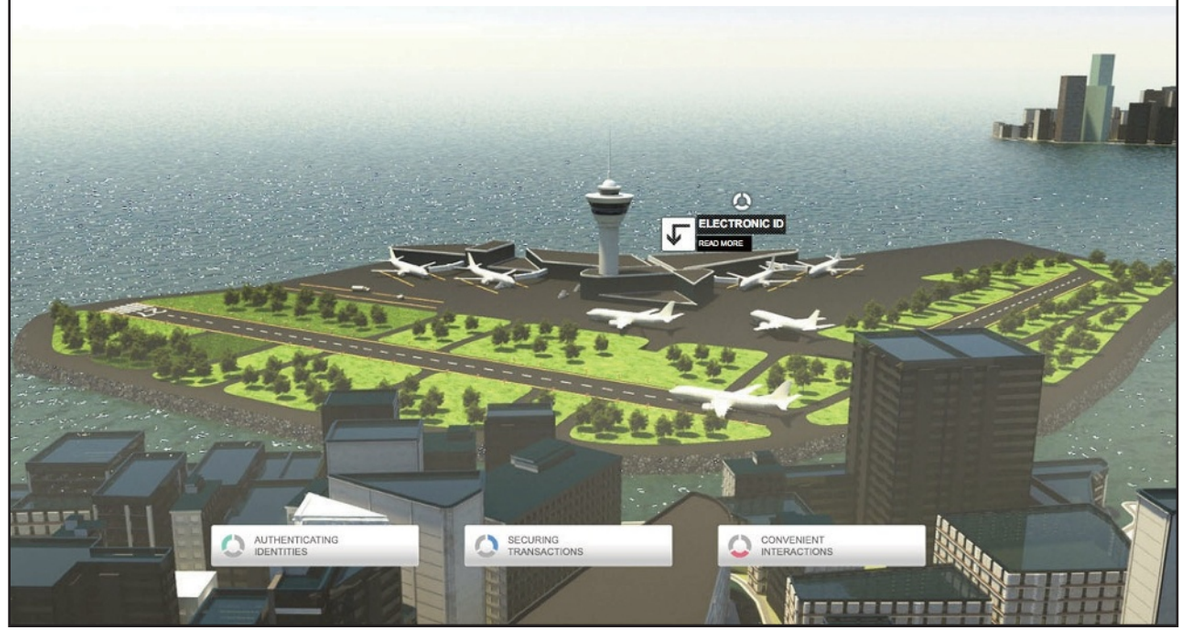
bedding UCODE I2C products into your consumer products. NXP provides assistance from concept and design to compliance and production, insuring quick and trouble free implementations to maximize your ROI and time to market. Let us know how we can help.

About NXP

NXP Semiconductors (Nasdaq: NXPI) is the leading global provider of RFID ICs. NXP creates semiconductors, system solutions and software that deliver better sensory experiences in RFID identification applications, eDocuments, mobile phones, TVs, set-top boxes, automobiles and a wide range of other electronic devices. A global semiconductor company with operations in more than 25 countries, NXP posted revenue of $4.4 billion in 2010. For additional information, please visit www.NXP.com or our RFID specific website at www.NXP-RFID.com.

NXP

Do you have an innovative application idea?



VIDEO VAULT

Industry Executive Confirms NFC's Massive Growth Opportunity

Executive Editor Justin Fritz interviews Steve Owen, VP of Sales and Marketing Identification at NXP Semiconductors (NXPI).

Rudy Stroh

Secure Multi-applications without compromise - Identification systems that support multi-applications are the new reality. NXP is leading the way in this new era, with technologies that let you deliver multi-function systems without forcing you to sacrifice on security, convenience, or design productivity.

NFC with NXP - Mobbb.TV investigates

We caught up with NFC pioneer NXP Semiconductors to find out the latest applications for this exciting technology

NXP Wins 2 SESAMES Awards @ CARTES 2011

NXP was awarded two SESAMES awards this year: Best Mobility Application: PN65 Secure NFC Module and Best Software: Android NFC Software Stack

Sponsored by NXP