THE BEST OF
BOTH WORLDS

Dual-frequency RAIN RFID cards add flexibility
while increasing smarts and security

By Mahdi Mekic, NXP Semiconductors

NXP

A new generation of **contactless smartcards**, built to support **short-range HF** as well as **long-range UHF technology**, deliver the advanced security, performance, and privacy needed to support valuable new uses cases, while maintaining multi-application functionality and compatibility with the existing infrastructure.

CONTENTS

RAIN RFID is a global alliance promoting the universal adoption of UHF RFID technology.

INTRODUCTION

Contactless RFID smartcards that use **High Frequency (HF)** technology, including **MIFARE®**, have been in widespread use worldwide for more than 20 years. In that time, they've found their way into dozens of complex applications, such as secure building access, ticketing for public transport, loyalty programs, micropayment, bank cards, and more.

HF-based cards are recognized for their high security and their ability to support multiple applications on a single card. That is, instead of carrying separate cards for three separate use cases – such as public transport, access to an office building, and membership to a local gym – you can carry just one card that supports all three. This multi-application functionality is the newest and the most advanced feature of the HF format.

Given their long history and widespread use, HF-based smartcards are supported by an exceptionally broad reader infrastructure. However, because they can only operate over short distances (under 10 cm), there are limits to how HF-based smartcards can be used.

There have been attempts, over the years, to change this. Developers have created dual-frequency cards, with support for short-range HF as well as long-range Ultra High Frequency (UHF). However, certain shortcomings in the UHF technology, regarding security, privacy, and reliable performance in challenging environments, have proved to be limiting factors. Since so many of the most desirable long-range use cases – such as hands-free access, easy visitor registration, crowd control, and location services – require levels of performance and protection not obtainable with conventional UHF formats, dual-frequency cards haven't really caught on.

That is, until now. With the arrival of improved UHF, which supports cryptographic authentication for security and privacy protection, dual-frequency cards are ready to go mainstream, with a new set of compelling applications. This paper summarizes the new features of this UHF with cryptographic security, and looks at the potential for using it in dual-frequency formats to create smart, scalable deployments with backward compatibility.

THE NEW RAIN RFID UHF: SECURITY AND PRIVACY OVER A LONGER DISTANCE

UHF tags have traditionally been used in manufacturing, industrial, and retail environments to identify and track items as they move through production facilities, supply chains, warehouses, and stores. The technology is relatively inexpensive to implement, can identify many items at once, doesn't need line of sight to read a tag, and has an operatingrange of several meters. What's been missing, however, is the right level of security.

Until only very recently, UHF tags have not offered the advanced security mechanisms needed to ensure tag authentication, protection of data, and the prevention of unauthorized reads.

But that's changing. A new version of UHF, known as UCODE® DNA, is the first to combine best-in-class read range with cutting-edge security, in the form of cryptographic authentication. Cryptographic authentication offers protection against fraud or misuse, since each UHF tag now not only has a unique ID but can also use secret cryptographic keys to confirm the originality of that unique ID. These secret crypto keys, which are used to authenticate a tag's identity, are securely stored in a heavily guarded vault inside the microelectronic memory. The hidden crypto keys never leave the tag, thereby ensuring the identity of the tag is protected from theft or copying.

Support for cryptographic authentication also protects against data emulation and can ensure privacy protection, since each time a tag responds it can send a reply that's different from the one before. The use of randomized responses strictly limits the

impact of eavesdropping, since any data obtained by an unauthorized read is essentially worthless. Also, the ability to encrypt data at the point of issue means that only authorized readers, equipped with the keys needed to read the encrypted data, can access private information. This adds to the eavesdropping protection.

Along with cryptographic authentication, UCODE DNA also supports longer read ranges and faster performance. The combination of security, privacy, speed, and accuracy mean UCODE DNA is letting UHF expand into new areas. For example, UCODE DNA is being used in Automatic Vehicle Identification (AVI) schemes, which use automated systems, based on UHF, to identify and authenticate motorcycles, cars, trucks, and service vehicles, even when driving on open roads at highway speeds. A subset of AVI applications involves automatic fee collection, with things like road tolling, collection of parking fees, traffic citations, and more. The security and privacy features of UCODE DNA ensure proper billing and protect the identities of the people making the payments.

Table 1 - UCODE DNA takes UHF to new levels

Security	Crypto authentication means **UCODE® DNA** ensures tags originality and protects against eavesdropping, emulation, and reverse engineering.
Privacy	Sensitive data can be hidden and accessible only via secret crypto keys assigned at the point of issue; furthermore, the responses to reader inquiries can be randomized to prevent tracking even of unknown identities.
Speed	Hundreds of objects can be securely and accurately identified and authenticated within seconds, even when the objects are moving at very high speeds.
Distance	Superior chip sensitivity enables best-in-class read ranges, even when there's no line of sight.

UCODE® DNA is already transforming Automatic Vehicle Identification (AVI)

ELECTRONIC TOLL COLLECTION

INTELLIGENT TRAFFIC LIGHTS & ROAD SIGNS

GREEN ZONES THAT LIMIT VEHICLE ACCESS

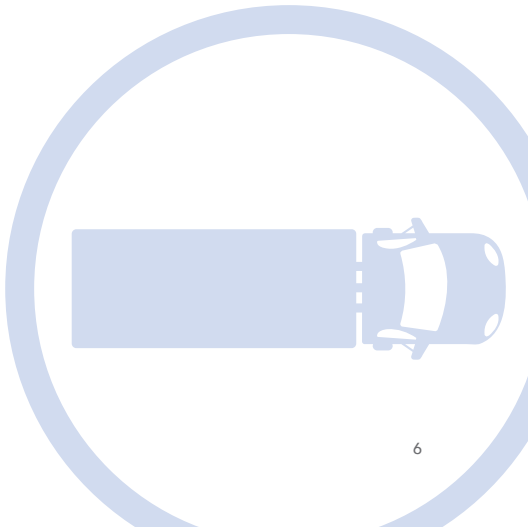**AUTOMATED BORDER CHECKPOINTS**

VEHICLE REGISTRATION ENFORCEMENT

PARKING ACCESS & PAYMENT

STOLEN VEHICLE TRACKING

A BETTER DUAL-FREQUENCY ARCHITECTURE

Using **UCODE DNA** to create a dual-frequency card makes it possible to introduce compelling applications that benefit from the technology's advanced security, privacy, and performance.

The short-range HF portion of the card offers the same secure, multi-application functionality associated with the best of today's smartcards, and is fully compatible with the existing card-reader infrastructure. The multi-factor authentication function, which is made possible by the dual-frequency solution, can be used to enable the cardholder's eligibility for privileged and/or limited services.

Namely, a high-security, short-range interaction with the HF portion of the card can pre-approve the user, and then the secure long-range UHF can be used for final approval before assigning certain privileges.

The UHF portion of the card can also be used to do things like manage crowds and enable hands-free access, and can also be used to compile usage statistics and gather business intelligence – all while maintaining the cardholder's privacy.

SOME SAMPLE USE CASES

A **dual-frequency card** can operate in all the ways a regular smartcard does – as a ticket, a payment card, an access pass – and can serve as an entry point for new services that are only possible with long-range UHF. A look at some sample use cases give an idea of how dual-frequency cards will work in the real world, with applications in public transport, building access, event planning, and more.
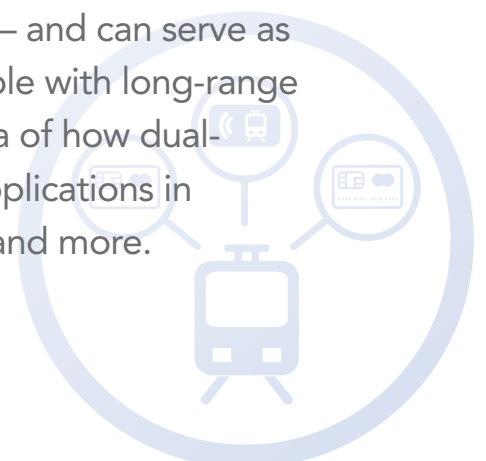
PUBLIC TRANSPORT:

Reduce Rush-Hour Congestion at Turnstiles

With an HF smartcard for public transport, you present your card at the turnstile, wait for the reader to confirm your card validity and open the gate, and then you walk through. It's not a long process, but when hundreds of people are trying to use the system at once, turnstiles can quickly back up and cause frustrating delays. With a dual-frequency card, there can be special "hands-free" lanes that operate on long-range UHF technology. You don't need to present your card – the reader recognizes the valid credential in the UHF portion of your card, and you just walk through. Entry points can even remain open, and only close if the system can't detect a valid credential. To use the hands-free system, passengers can present their dual-frequency card at a reader posted outside a designated "express area," and receive a period of hands-free access, limited to a day, a week, or a month, depending on their subscription.

BUILDING ACCESS:

Authorize Hands-Free Zones for Qualified Personnel

Having to present a badge at every doorway while navigating a large building can be cumbersome and time-consuming. That's especially true if you're hands are already doing something else, like carrying progress materials in a factory, or guiding a patient on a gurney through a hospital. A dual-frequency card can be used to designate hands-free access to pre-defined zones while personnel are onsite. When you first enter the building, you present your dual-frequency card to the reader. The reader authenticates your card and then grants you hands-free access for as long as you're inside. As you approach a door, a long-range reader detects a valid credential and lets you in. Doors operate in response to your access privileges, and certain areas can be made off-limits. If you leave the building and re-enter, you present the card once more to regain hands-free access to your designated areas.

VEHICLE PARKING:
Save Time and Carry Fewer Cards

A dual-frequency card can be configured to let you drive into a parking area and even pay for your space, without getting out of your car or stopping to open a window and insert a card into a machine. When you approach the entry point, the reader at the gate can validate your credential, using long-range UHF, and open the gate. If it's a paid parking area, the system can also initiate a payment or log the visit in your account records. The short-range HF portion can take on any of many tasks a smartcard can perform, working as an access pass to your workplace, a loyalty card at a shopping mall, an event ticket, a payment card, and so on.
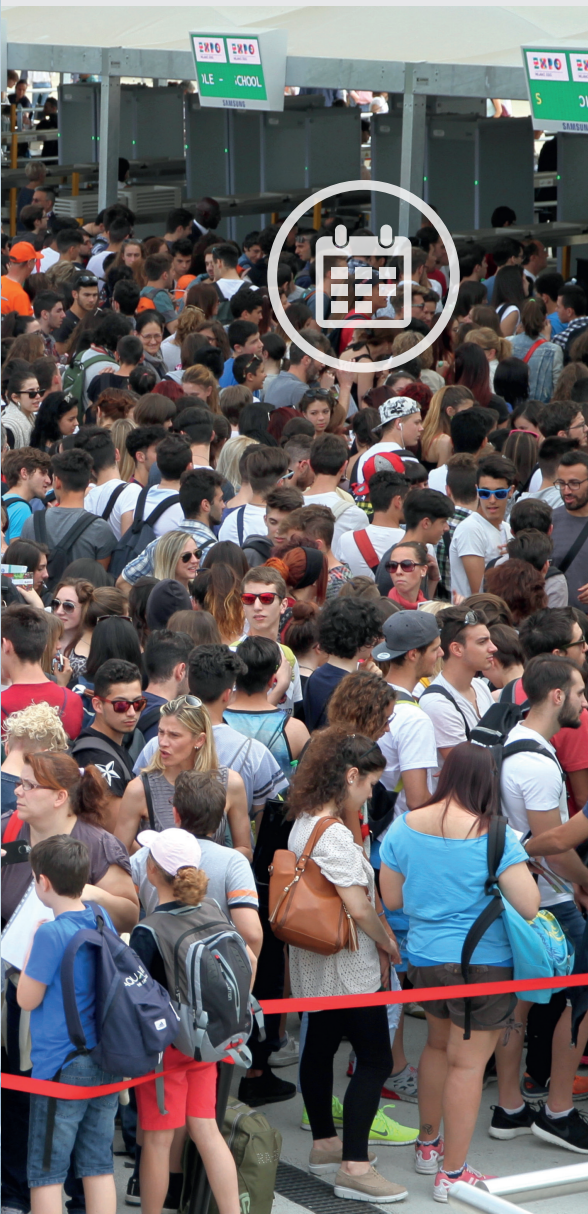
EVENT ACCESS:
Gain Insights While Protecting Privacy

Issuing dual-frequency cards as access passes can help you understand how people spend their time while at your event. The HF portion of the card acts as a ticket that enables entry into your venue, whether it's a conference, a stadium, a concert hall, a theme park, or an open-air festival. The HF technology enables secure, multi-factor authentication, and then initiates UHF capabilities for logging where the card is used or where the card carrier spends their time. At the end of the event, you can review patterns, with reports that tell you, for example, the average amount of time people spent in the arena gift shop. You can evaluate activities, too, using pre-defined categories. With a tradeshow, for instance, you can learn how many visitors to a booth were show attendees or delegates, understand what items attracted people from different geographic regions, and learn that 10% of your visitors were hardware providers, 20% were software providers, and 70% were service providers. It's important to note that all these reports can be generated using pre-assigned categories or Class IDs, and not people's actual identities. The UHF system only compiles statistics based on Class ID, and doesn't track individuals or record private information. Class IDs let you know more about what's happening, while letting people maintain their anonymity.

EASIER DEPLOYMENTS

Dual-frequency cards offer several advantages when it comes to deployment. The HF portion of the card works with the existing infrastructure, while allowing for development of new use cases, so there's less pressure to have **UHF functions** ready at the same time as HF functions. Deployments can be rolled out in stages, or scaled as needed, since a single card works in any installation, old or new. There's also no rush to replace HF cards that are already in place, since dual-frequency cards can be part of a heterogeneous system that supports single- and dual-frequency cards.

Dual-frequency cards can be seen as a premium item, offering special extras or VIP privileges, and as a result can attract participation in a given program and even be offered at a higher price. Dual-frequency cards can also reduce risk, because HF authentication can be used to pre-approve UHF services that are only issued on a time-limited basis. Program operators have more control over the provision of temporary features, so there's less chance of misuse or fraud.

CONCLUSION

Dual-frequency smartcards have, until now, been held back by the need for enhanced security, improved privacy protection, and better long-range performance. The recent arrival of **UHF** with **cryptographic authentication** means credentials can be verified using multi-factor authentication, private information stays private, and cards can be operated quickly and accurately over longer distances.

As a result, it's now possible to add long-range capabilities to smartcards while offering the security, privacy, and performance necessary to deliver compelling new features. Dual-frequency cards now offer the best of both worlds, providing short- and long-range functionality with security, smarts, and more meaningful applications.

To learn more about NXP's work on dual-frequency applications based on MIFARE® DESFire® and UCODE® DNA, visit www.nxp.com or contact your local sales office.