21 June 2011

Interoperability for contactless services with mobile NFC

An introduction

Contents

Section One: Introduction and market overview

Projected to account for almost a third of mobile payments transactions by 2014 (source: Research and Markets, 2010), mobile Near Field Communication (NFC) promises to revolutionise both device to device communication, and the way consumers engage, interact and transact with brands. These contactless services present a host of opportunities in payment, transportation, access control and data exchange.

But addressing the challenges of the NFC world is critical to enable its success from a device, network and service perspective. Once again, the role of the 'Secure Element' within the device is paramount in managing authentication and certification; not only to ensure the integrity of financial transactions and data exchange throughout the NFC chain, but to deliver the required levels of interoperability as well.

The evolving market for NFC

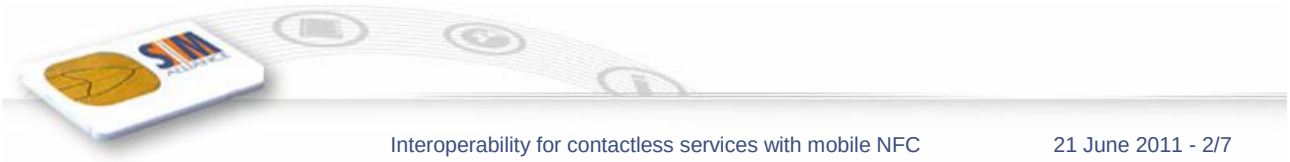
With the success of contactless trials across the world, mobile network operators, financial institutions and vendors are now coming together to deliver widespread commercial deployments of NFC. The hardware is becoming available – according to NXP Semiconductors we'll see between 40-50 million NFC-enabled mobile devices on the market by the end of the year, while Ingenico confirms over 1-in-5 payment terminals sold in 2010 were NFC-enabled - a figure that's set to rise again in 2011.

So, if the devices and technologies are ready, what about the applications? There's positive news here too. Since October 2008, the industry publication *NFC World* has reported on over 200 NFC trials, tests and commercial deployments in 48 counties. Globally, we're seeing major moves in the US, China, Japan and Turkey. Meanwhile, in Europe the market is hotting up as both pilots and the commercial adoption of a host of contactless payment, voucher and transport services take place across the continent - from Poland and the Czech Republic to Italy, Belgium, Netherlands and beyond.

In the UK the mass adoption of contactless payments is being championed by Barclays Bank, among others; services can be found on the high street in stores such as Pret A Manger (one of the earliest adopters) and increasingly in smaller independent outlets across the country. As we go to press, the coffee chain Starbucks has just announced an agreement with Barclaycard and Visa Europe to bring NFC contactless into its UK stores.

In France, a city-wide NFC trial is underway in Nice, offering payment, transport and loyalty programmes through the CITYZI SIM card. Such has been the success of this project that nine major French cities have announced plans to join it, with Bouygues Telecom, NRJ Mobile, Orange and SFR projecting to sell over 1 million CITYZI-enabled handsets in 2011.

But for all the apparent market optimism, there remains some doubt as to the pace of continued adoption without that most important of factors – security and interoperability.



Interoperability, NFC and the Secure Element

As in any emerging market that deals with financial transactions or manages personal data, the security issues of NFC must be addressed – and here standardization around the Secure Element within the device is paramount.

The Secure Element is the component within the connected mobile device that provides the application, the network, and the user, with the appropriate level of security and identity management to assure the safe delivery of a particular service.

It can be an embedded Secure Element or a Secure Memory Card – both of which can also be delivered simply and cost-effectively into the mobile environment. Indeed, the most common secure element within the mobile space, and the most widely used security platform in the world, is the SIM - or more accurately in today's world, the Universal Integrated Circuit Card (UICC).

Building on almost two decades of proven operational use, the UICC is an operator-owned connected cryptographic multi-application platform. It sits at the heart of the handset, managing and authenticating secure access between the connected device and host - to take full advantage of the increasing crop of IP and cloud-based services and applications, and helping to deliver on the promise of mass-market adoption of NFC technology.

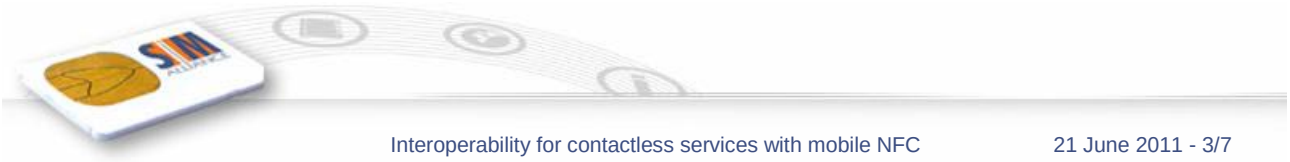
Interoperable and standards-based, the UICC is a combination of hardware and software, developed and delivered in controlled manufacturing environments to guarantee the highest levels of security certification for connected mobile devices in an IP world under attack from ever more sophisticated viruses, malware and phishing programmes.

It is also considered by the mobile networks operators as their preferred Secure Element within the handset, according to the Mobile NFC Services whitepaper from the GSMA.

The European Payments Council has also issued guidelines on contactless payment, and the UICC is clearly identified as one of the Secure Elements enabling interoperability and security here.

Key UICC features:

- Universal: UICCs present in all GSM / 3G / 4G handsets
- Portable: removable cards allows user to migrate credentials between handsets
- Accessible: fully manageable through secure Over-the-Air (OTA) protocols
- User-friendly: web 'look and feel' interface delivered through Smart Card Web Server
- Standardised: robust and interoperable, the result of two decades of continuous standardisation efforts by the UICC industry
- Secure: state-of-the-art security proven by accredited certification, verified by independent labs
- Multi-party services hosting: seamless integration and compatibility with all functional and security requirements of payment, access, and transport cards
- Multi-party services management: dedicated security domains allows individual service providers to manage contactless services within the UICC



Section Two: Addressing NFC interoperability with the UICC

The advent of mobile NFC and the undoubted opportunities the new technology affords has seen a host as new players enter the game, and that's changing the rules for the UICC. New end-users demand new types of applications and services, which in turn demands new levels of flexibility and interoperability from the UICC.

For example, payment applications require very high levels of transactional security, while the demand from transport applications is focused on the end-user experience to assure speed of operations at their logistics hubs.

And these demands create new challenges for application developers, device manufacturers and the Secure Elements sector. Interoperability is one of the most significant challenges here because without seamless (and secure) connectivity between a host of different devices and applications, implementation costs and user frustration will rocket – and adoption, and revenues, will fall.

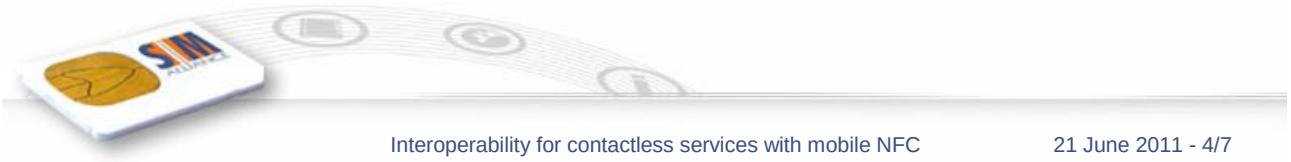
Guaranteeing interoperability between this increasingly expanding ecosystem of mobile operators, banks, payment organisations, transport operators and merchants through the UICC is therefore critical to the commercial success of an application or service. It also offers increased freedom (and an improved experience) as users easily migrate between services and devices.

Interoperability and more

In a similar way, NFC delivers remote access and management of the UICC to trusted third party service and application providers. This moves the game on from interoperability and into secure application and service lifecycle management. This allows mobile operators, through their trusted third party, to gain greater control of their contactless service portfolio – from activation and upgrade through to suspension – while the integrity of the service is reinforced by the fact that each relies on its own security domain on the UICC.

For example, a bank can remotely personalise its mobile payment application with its own security data secure, confident in the knowledge it is the only provider allowed to perform this task for the specific mobile payment application. This delivers greater security for the end user while also addressing the data compliance concerns of regulatory bodies.

Combining the interoperability functionality, OTA management and this 'secure channel', the UICC makes it possible to deploy volume contactless services involving multiple service providers, vendors and other ecosystem players in complete confidence.



Section Three: Interoperability and interfaces

As we've seen, the launch and success of an NFC contactless service requires a connected community of players - from mobile service providers through to banks, transport, and other end-user vertical organisations. And in the same way a typical service requires interaction with multiple technology elements, for example:

- the service is downloaded on the UICC via an OTA platform, and runs on the UICC virtual machine
- it requires connection to the user interaction components with the NFC extensions of the handset to deliver both user interface and contactless services
- it also requires a seamless interface with any existing contactless infrastructure – for example the access control systems of an underground train network.

This is a complex business, as each interface represents a potential barrier to interoperability. All of which is further confused by the fact that the service provider is rarely in control of these multiple products, services and devices to which their service must interact. And weak or unknown levels of interoperability in these environments increase cost across the board.

Today UICC interoperability has evolved from pure Java Card connectivity into a wider and more complex environment, and now offers open interfaces into OTA platforms, handsets and contactless infrastructures. By placing the UICC at the very centre of the NFC ecosystem – with all interfaces connecting into it – issues are eliminated and interoperability guaranteed. And that's good news for service creation and deployment as the market races towards an NFC future.

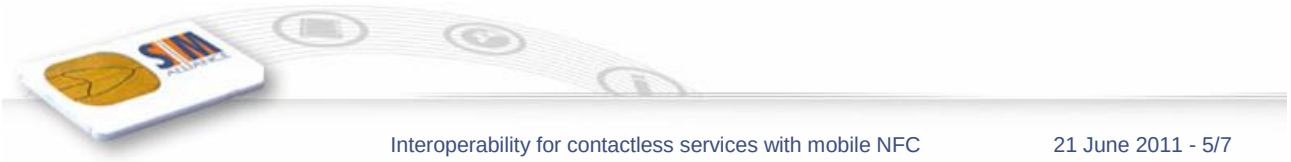
Section Four: SIMalliance Work Group solution

The SIMalliance has led this move towards interoperability for over a decade, having established its Interoperability Working Group more than ten years ago to look specifically at Java Card implementations. Having recognised the growing complexity of the mobile ecosystem and its need for seamless service delivery across multiple networks and devices in previous years, the SIMalliance extended the objectives and scope of the Group to create specifications that take interoperability further.

Stepping Stones

The Work Group has produced and maintained a set of industry leading 'Interoperability Stepping Stones' collaterals, from the early Java focus through to new technologies such as Smart Card Web Server (available since 2009), including a new set of documentation addressing today's challenges of NFC technology.

Each of these latter documents - containing detailed specifications, standardisation considerations and pragmatic tips - aim to simplify the development, implementation and support of new NFC contactless services and applications.



CAT Loader for contactless

In addition to the Stepping Stones programme, dedicated software tools to confirm interoperability levels are provided by the Working Group. In 2011 the Group is focusing particular attention on developing the CAT Loader - the only existing card management tools to have been verified with UICC from all the SIMalliance members – to enable on-card management of contactless services. The Group will also work to enable application personalisation via the CAT to bridge the existing gap between mobile and banking services.

The CAT loader is available for free download by going to www.simalliance.org/interop

Section Five: Audience benefits

For the mobile network operator

Interoperability offers significant advantages for the operator. Chief among these is the ability to select multiple UICC providers and then deploy the same services across all their UICC estates in a seamless manner. Multiple UICC suppliers are common, so ensuring interoperability across all will reduce the cost of bringing services to market through more efficient testing programmes leading to faster deployment timescales. And once in the field, management, support and replacement costs are reduced.

Crucially, a developing NFC market offers opportunities to extend the ecosystem to deliver new applications and services. The presence of a centrally managed and interoperable UICC allows these applications (and providers) to utilise the single Secure Element while controlling and securing access.

And finally, mobile operators are able to take advantage of the free tools provided by SIMalliance to test and manage UICC based services.

For the standardisation community

Development of the Stepping Stones collateral packages begins with current card specifications. This includes analysis of existing specifications from the perspective of o/s developers and typically results in a series of corrections and modifications that are passed to the community.

Also, because interoperability is a key end-game for the standardisation community, SIMalliance is working with ETSI to prove and improve interoperability (the "*plugTest" events*) where developers from across the sector have been able to verify the interoperability of their own solutions.

For the mobile application provider

Interoperability means the maximum number of devices can deliver the maximum number of services into market, and that means application providers have access to an ever expanding addressable

market. Assuring application interoperable with the SIMalliance specified UICC opens up around 90 per cent of all existing UICCs across the world. And that results in greater service adoption, usage and revenue.

Moreover, applications developed according the Stepping Stones programme are typically more reliable and efficient, while application developers can take advantage of the free tools provided by SIMalliance to develop and debug services (such as the CAT Loader).

○ For the mobile user

Interoperable interfaces – the ability to guarantee a consistent user interface even if the UICC is moved between devices – offer mobile subscribers the freedom they desire. They are able to upgrade their UICC products or even to migrate from one operator to another, while maintaining the same looks and feel, user experience and quality of service. And with Stepping Stones-developed applications offering more reliability and security, the customer experience will be maximised.

Section Six: Reaffirming the proposition

There is little doubt that NFC offers a host of opportunities for mobile network operators, ecosystem players and the end user. However, the potential service delivery, revenue generation, differentiation and loyalty benefits of mobile NFC will remain unrealised without a concerted push towards standardisation and interoperability – with inherent security built in - somewhere within the device.

The UICC is that 'somewhere', and as the most widely used security platform in the world the mass market and expansion opportunities are significant. The 3GPP has already defined the UICC within its own specifications, and the European Payments Council has done likewise with NFC.

But while the UICC is now the mandated standard, there remain interoperability challenges even here. That is why the SIMalliance has built a programme, a set of detailed documents and specifications, and downloadable tools to encourage standardisation. And with it, guaranteed interoperability for services and applications across the mobile device spectrum can be delivered.

Adoption of this specification is a significant step forward in enabling interoperability and opens up a host of existing and emerging market opportunities for brands right across the mobile spectrum.

For more details on the Interoperability Work Group, and to download the specifications and Stepping Stone deliverables, go to www.simalliance.org/interop