



Near Field Communication spells plastic card decline

Near Field Communications (NFC) technology removes the need for a payment instrument to make contact with a payment device to initiate a payment request. Removing this physical contact means the chip can be supported from a variety of form factors (devices), making the plastic card redundant, writes Peter Goldfinch – GFG Group’s General Manager for South East Asia. In this issue of the monthly Goldfinch Report, Peter considers what NFC means for the payments industry. Peter’s credentials have been earned over 23 years experience in electronic payments, including pioneering work on ATMs and EFTPOS, and the introduction of credit and debit cards in Russia.

NFC is a connectivity standard designed to support the two-way communications between various devices such as PDAs, mobile handsets, cameras etc. Within the context of payments, NFC is likely to take on a meaning beyond the original intent as has happened with EMV. Even today, many see NFC as a payment method and not a communications protocol.

“THE REAL POTENTIAL OF NFC IS WHEN THE FORM FACTOR IS A MOBILE DEVICE.”

“THE ABILITY TO COMMUNICATE BACK TO THE CARDHOLDER’S ISSUING BANK INTRODUCES THE ABILITY FOR BOTH CARDHOLDERS AND ISSUERS TO COMMUNICATE UNOBTRUSIVELY WITH EACH OTHER ON AN EVENT-BY-EVENT BASIS, IN REAL TIME.”

The issue with device-to-device communications is security, especially over extended ranges. NFC has been designed for communications within a close range: ten or less centimeters. Holding the device (of whatever form factor) containing the payment details close to the reader addresses the security concern. The possibility of any person or device coming within range to eavesdrop on the messaging traffic is minimized.

NFC works by magnetic field induction and operates within the globally available and unregulated RF band of 13.56 MHz. Development of NFC is being driven by the NFC Forum, which is a body of organizations cooperating to develop this communications standard. NFC Forum members include MasterCard, Visa, Sony, Panasonic, Microsoft, Texas Instruments, NEC, Nokia and others.

Although many see NFC as a payments standard this is not the case. Payment is only one use of the technology. NFC can be used to configure and initiate other wireless network connections such as Bluetooth and WiFi. In the payment context NFC is starting to be considered more than a communications protocol. It is being seen more as a proximity payment method, bundled with ISO14443, the proximity standard and EMV.

So what does this bundled NFC mean to the payments industry? What does it promise? In the passive mode it is always the NFC capable device, (with a power supply) to communicate, (two-way) with a contactless chip. The contactless chip may support the EMV security standard, or the chip may just hold a magnetic strip image. This enables proximity payments where the card and device generates a standard purchase transaction under the request and response payment model.

The advantages of this technology are reflected in the MasterCard Paypass and Visa Wave solutions. These two payment methods are based on lower value proximity payments without the need for either signature or PIN.

The business justification is based on increasing the customer throughput per cashier, resulting in a higher retail sale volume at a lower cost for merchants while improving the consumer experience. Removing cash reduces handling costs and shrinkage.

The EMV application of Wave and Paypass does perform two-way card-to-device authentication. But obviously the cardholder is not authenticated. It will be interesting to see if the business case stacks up once a high market penetration rate of Wave and Paypass capable cards is reached and the merchant acceptance base expands.

From a payment perspective, unauthenticated transactions represent a payment risk. Keeping proximity fraud levels within budgeted limits is the key. The risk is intended to be carried by the issuer, although merchants will inevitably pay indirectly through the interchange rates.

More importantly NFC technology removes the need for a payment instrument to make contact with a payment device to initiate a payment request. Removing this physical contact means the chip can be supported from a variety of form factors. The plastic card becomes redundant.

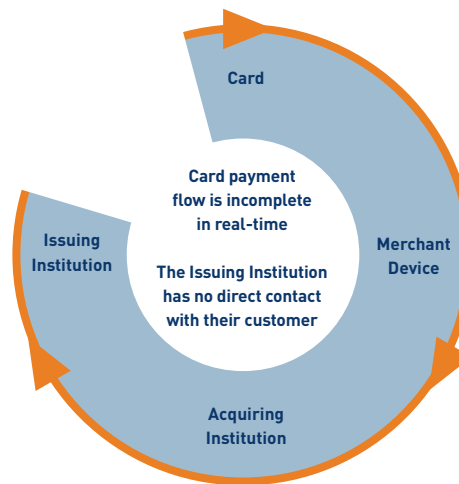
The real potential of NFC is when the form factor is a mobile device. The card is limited by an inability to communicate neither back to the issuer or to the cardholder. It can only communicate with the merchant’s device. The mobile as a form factor is a three-way communications device, merchant, cardholder and issuer.

The ability to communicate back to the cardholder’s issuing bank introduces the ability for both cardholders and issuers to communicate unobtrusively with each other on an event-by-event basis, in real time. This completes the communications link in a way that is impossible for payment cards.

“USING A MOBILE TO CHANGE THE WAY TRANSACTIONS ARE PROCESSED MEANS AUTHORIZATIONS CAN BE ROUTED OVER THE MOBILE NETWORK TO THE ISSUERS DIRECTLY.”

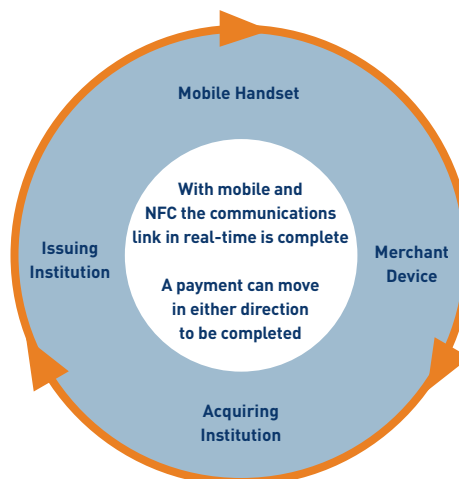
“ACQUIRING COSTS ARE REDUCED AS THERE’S NO NEED TO SUPPORT REAL-TIME SWITCHES.”

The Current Card Present



The transaction originates with the swipe of the card and passes to the issuer through the merchant and acquirer. It never passes back to the cardholder except as a paper receipt.

The Handset, (Virtual Card Present)



This closed communications loop will drive personalization. This process is likely to cover:

1. The downloading of the wallet to the handset. Note these payment instruments are most likely to be multi-institutional.
2. The initialization of a wallet stored value repository on the handset. Multiple applications will access a single repository.
3. The establishment of the payment security closely relates to the downloading of the wallet. This involves the downloading of security keys, which should be unique for the handset. They may be DES keys, (triple) or PKI, (handset) private key pair and the public key of the scheme operator or financial institution.
4. As the wallet is expected to hold payment instruments issued by multiple financial institutions, multiple key sets are a potential requirement, especially as payment messages will contain PIN blocks.
5. An over the air data encryption key will also be required. This does not need to be an institution-specific key.

About Peter

Peter Goldfinch, GFG Group's General Manager South East Asia, is a respected analyst and commentator on global trends in payment technology.

One of the original founders and shareholders in GFG Group, Peter has a background of more than 23 years in the information technology industry, most of which has been involved with consulting and systems development for banking and finance customers in 25 countries.

He has particular expertise and experience in payment systems, including mobile payment systems. His career highlights include pioneering work on the first ATM and EFTPOS networks.

In the mid-1990s, he played a key role in the introduction of credit and debit cards into the Russian market, working with GFG's customer SBRF.

About GFG

Accredited by the World Bank, GFG Group is a company of banking experts specialising in payments. More than 20 years of payments experience stands behind the company's worldwide leadership in integrated Card and Mobile-based payment products.

GFG's solutions are based on a single, integrated architecture comprising two key products:

Simfonie™ A proven, market-leading product which enables a mobile phone to operate as a fully mobile payment device.

Cadencie™ - a full-function, real-time, credit, debit and charge card management system.

GFG Group operates from offices in Auckland and Wellington New Zealand, Melbourne Australia, Manila in the Philippines, Singapore and Toronto. The company's core research and development team is based in Auckland, with consultants and technical staff located in the international offices to provide front line 24/7 support for customers in multiple geographies.

GFG Group Ltd
Level 10
Qantas House
191 Queen Street
Auckland
P O Box 5825 Wellesley Street
Auckland 1141

Telephone: +64 9 966 7041
Facsimile: +64 9 966 7070
E-mail: info@gfg-group.com

6. For downloads the handset must be able to validate the source. This may be done with a digital signature.
7. Potentially there is also the option to use PKI and have transactions digitally signed rather than use the traditional DES algorithm. A single handset could use either method based on financial institution or transaction type.
8. These processes may also require that handsets are 'sold' with a preloaded master key or a key is derived from a unique handset identifier to protect the transportation of the keys.

Dynamic Risk Management

1. A feature of low value proximity payments is the support of off-line, non-validated transactions. After a certain number of such transactions an online transaction would be forced. This is a very simple example of a parameter that could be changed over the air by the issuing institution without the knowledge of the cardholder.
2. The range of parameters can be extended to cover off-line or non-validated transactions by merchant category code.
3. If a cardholder is uncharacteristically increasing their plastic usage, or if the account is reaching its credit limit, the parameters on the handset could be automatically reduced, and expanded when a deposit is made.
4. Similarly a single payment instrument or all instruments could be blocked as in the case of a handset being lost or stolen.

Changing the Transaction Path and Authorization Method

1. The authorization process can be managed by the handset and mobile network. The handset can request an authorization directly from the issuing institution and deliver an approved payment to the merchant's terminal. Potentially - based on the risk profile - the handset can approve payments itself.
2. The merchant terminal then can act in a purely EDC mode and does not need to be online.
3. The issuer then carries the payment risk.
4. For card-not-present transactions, the card issuer has the ability to send a confirmation request to the cardholder's handset.

The key advantage of using mobile to change the way transactions are processed is that time dependent network connections are removed from the typical on-us transaction flow, with authorization being routed over the mobile network to the issuers directly.

For the customer they have a single device that will hold multiple payment instruments. Initiating a payment is easier and quicker. It is lower risk, as the handset can be protected with a password.

The cynic may say the problem has just been transferred to the mobile operator. If there are network capacity issues the operator is better equipped to resolve these than a financial institution. Financial institutions are only in real-time dealing with their on-us traffic. The acquiring institutions should concentrate on settlement related payment tasks.

What is outlined in this paper may take 10 to 15 years to eventuate. It will be rolled out by merchant category based on where the greatest benefit can be realized. Also expect the champions of this not to be the financial institutions but those merchants who today have a heavy dependency on cash or stored value. The plastic card will remain long into the future with the numbers on issue declining gradually over 20 to 30 years.