Barnes INTERNATIONAL

CLOUDING THE ISSUE:
CONTACTLESS PAYMENT CARDS, MOBILE PHONES AND "THE CLOUD"

Barnes International Ltd
Cedar Court, 5 College Street, Petersfield, Hampshire,GU31 4AE,UK
Tel: +44 (0)1730 231313 **Fax:** +44 (0)1730 265353
Email: sales@barnestest.com **Web:** www.barnestest.com

We've been hearing a lot recently about Host Card Emulation (HCE), Tokenisation, and Cloud Based Payments, as if it's all new technology that's going to revolutionise the payment world. Well, like most much-hyped new developments, the technology is an evolution of what's been around for some time and whether it revolutionises anything depends to a large extent on public acceptance. So maybe it would be good to reflect on the technology involved, how we arrived here, and what it really means to players in the payment business.

EARLY DEVELOPMENTS IN CONTACTLESS PAYMENT CARDS

When chip and PIN was introduced around the turn of the century there were already global interoperability standards in place. EMV was well established before significant numbers of cards and terminals were in use, so that all the cards and terminals worked together from day one with relatively little drama. However, the introduction of contactless payment cards happened suddenly and there was no time to produce a global specification like EMV. As a result each payment scheme has adopted its own unique approach.

The suddenness with which contactless burst upon the payment community can be explained by the fact that the technology was already well established in other spheres. There were many highly successful closed systems in use, mostly for access control. In a closed system, where one manufacturer supplies all the cards and all the terminals, there is no pressure to ensure widespread interoperability. When the technology was adapted for use in payment systems it took some time to iron out all the interoperability issues so that the majority of cards would communicate effectively with the majority of terminals.

As the payment community picked up contactless technology, the focus of the interoperability effort was on the low level parameters, the hardware and RF characteristics. At the payment application level, so closely controlled by EMV in the contact cards, each payment scheme went its own way. The result was that a variety of contactless payment applications appeared, all based on EMV, but some rather more loosely than others.

SPEED VERSUS SECURITY

Conceived to replace low value cash transactions, the main advantage of a contactless card is speed. TV commercials emphasise this by the use of roller coasters, athletes, or other high speed icons to advertise how quickly a payment can be made. The downside is security. The contact card is very secure, and the communications between it and the payment terminal are difficult to eavesdrop without introducing cumbersome and highly visible hardware. Contactless cards are powered by a high frequency electromagnetic field and communicate with the terminal by radio. This means that the possibility exists of fraudulent terminals accessing the card's data while it's tucked away inside the cardholder's wallet or purse, or of hidden eavesdropping devices listening in on the communications of a genuine transaction. As a result of this the data exchanged between a contactless card and terminal has to be limited, for instance contactless cards can never use plaintext offline PIN and have to be confined to low value transactions. The world is getting used to these limitations and as acceptance grows the use of contactless technology is spreading.

MOBILE PAYMENTS

A useful spin-off of contactless technology is that because there are no electrical connections to be made, it's no longer necessary for the device to be a standard shape to fit the slot in the reader. It doesn't even have to be a card. Contactless chips have been embedded into watches, key fobs, adhesive labels, in fact anything big enough to contain an adequate antenna will do the job. Which brings us to the mobile phone, or cell phone, or smart phone, call it what you will.

We now have a device which can appear to a contactless terminal exactly like a card but which has its own screen, keyboard, sophisticated processor and large memory. On the face of it this offers a number of advantages, not the least of which is the ability to enter a PIN using the device's own keypad without the need to transmit it by radio. However, the handset, with its open operating system and various alternative communications interfaces, is continuously connected to the internet and thus open to malicious attack, which brings us back to the problem of security.

THE SECURE ELEMENT

The concept of the "Secure Element", or SE, was developed as a means to keep sensitive data safe within the mobile handset. A secure element can exist either as dedicated hardware within the handset, as an application in a secure partition on the SIM, or as an external peripheral such as an SD card or a sleeve. It has the means to communicate with the device's main processor so that a dedicated app can provide access to the keypad, and it can also use the telephone's other connectivity options (e.g. WiFi or the phone network) to exchange encrypted messages with the payment system issuer. It also has a private connection to the NFC hardware for direct communication with the contactless payment terminal.

In spite of a huge investment of money and time there are currently only a small number of handsets available which support an internal or SIM based SE, and the performance of some of the peripheral devices is marginal. A further complication is the fact that the SIM and mobile data connections are under the control of the Mobile Network Operator (MNO), which introduces another large organisation into the equation.

But more concerning than the organisational complexities and lack of suitable hardware is the question over the security of the dedicated app running in the smart phone's open OS. Even though the SE itself is secure, it still has to communicate with the handset's main processor, and that is the weak link.

TOKENISED PAYMENT SYSTEM, HOST CARD EMULATION (HCE), OR CLOUD BASED PAYMENT

An alternative approach would be to devise a system that will operate in an insecure environment without compromising too much sensitive information. The result is variously known as a Tokenised Payment system, Host Card Emulation, or Cloud Based Payment.

Host Card Emulation is an app running on a smart phone. It needs no Secure Element, or any special hardware, just access to the NFC interface which is now standard equipment on most devices. The HCE app, when activated, uses the NFC interface to emulate a contactless card so that the phone can be used as a payment device. Simple, but on the face of it not very secure. The security comes from the fact that the personalisation data used by this virtual payment card is not the cardholder's real account data, but a token which is only linked to the cardholder's account via a database held securely by the token issuer.

In order to use the HCE app as a payment device the cardholder must obtain a token, or tokens. Normally these will be issued by the bank who issued the payment card they are linked to, but they could just as easily be bought from another provider, such as a transit system operator or online merchant. Tokens can be downloaded to the handset via any convenient means, WiFi is likely to be the most commonly used, which is where the "Cloud Based" nomenclature comes from, but SMS or a hardware memory device would
To the contactless payment
terminal the HCE/token combination just looks like any contactless card, and as such must obey the rules of the payment scheme under which it is issued.
the equivalent actual

There are a couple of important differences between the token and the cardholder's real contactless card.

- The account number in the token is a dummy. It can only be linked to the real card account when the transaction data gets back to the token issuer.
- It has a very limited life, a short expiry date, a limited number of transactions and/or a limited total spend.

The token can be thought of in the same way as cash. Your wallet or purse is much less secure than the vault at your bank, but this is acceptable because it contains only a small percentage of your worldly wealth. If it is lost or stolen the damage is limited. Similarly, the token in your smart phone, if compromised, can only be used to steal a small proportion of the wealth your card account represents.

HARDWARE UPGRADES NOT NECESSARY

The most attractive advantage of the HCE/Token/Cloud based payment system is that it works on existing hardware. There is no need to modify any terminals, and the purely software product can be installed on a wide variety of existing handsets without the expense and complexity of providing and programming a Secure Element and doesn't require any action or permission from the MNO.

QUALITY AND INTEROPERABILITY TESTING

However, it is still necessary to ensure the quality and interoperability of the app and the tokens. And since these are likely to be supplied by software providers new to the payment industry token issuers will need to provide themselves with the means to ensure their tokens will work.

Fortunately the tools needed are already available. Because the handset with its app and token must appear to the payment terminal just like a real contactless card, the test tools that already exist for testing contactless cards can be used with only minor modifications. Card issuers who have already equipped themselves with such tools to ensure the quality of their chip based payment cards will be able to easily validate the quality and interoperability of the app and tokens. It would be a wise move for other organisations wishing to issue tokens to similarly equip themselves so that tokens issued on their behalf can be tested.

ABOUT BARNES

Barnes International is the world leader in the development and supply of Chip Card Test Tools and Magnetic Stripe Analysers. Barnes world class Test Tools enable the manufacture and issue of valid magnetic stripe, contact and contactless EMV chip cards, ensuring quicker approval by Payment Schemes and minimising pre-issue costs. Its Test Tools for Laboratory, Manufacturing and Bureau include QC testing to ISO, EMV, Amex, JCB, MasterCard, Visa, CUP, Discover, Interac, SPAN, GlobalPlatform and GSM specifications. Barnes also offers EMV Consultancy and Card Testing. For further information on Barnes' products and services go to www.barnestest.com