NFC: BRIDGING TECHNOLOGIES

BY DAVE BIRCH

With a lack of handsets in the market, organisations are looking to other NFC implementations

What are bridging technologies? They are the technologies for adding NFC capabilities to consumer equipment without having NFC chipsets integrated into that equipment. The general term has taken on a very specific meaning in the context of mobile proximity applications, where it means technologies other than the SWP/UICC combination set out by the GSMA (since so few handsets are available and the ecosystem is still forming) for adding NFC interfaces plus SEs to devices that lack them. The Mobey Forum (an industry association that includes banks, device manufacturers and mobile service providers) recently published a very detailed White Paper on this topic[1], recognising that many financial institutions and other service providers had become frustrated with the slow progress towards mass-market handsets incorporating NFC in the face of clear consumer demand.

We will use a similar categorisation to the Mobey Forum to explore the technologies, which they divide into stickers (active and passive), secure Micro SD (µSD) cards, embedded secure elements (eSEs) and what they call the "trusted mobile base" but what we will call the Trusted Processor (TP).

Stickers

The idea of taking chips with contactless interfaces and simply sticking them to other objects goes back some time (certainly to experiments with the Dexit payment system in Canada some years ago), and it has always been clear that when it comes to consumer payments, the mobile phone has already been the preferred object. The most straighforward implementation is to simply take the NFC chip and its antenna and combine them in a self-adhesive sticker, as shown in the photograph below.

[1] *Alternatives for Banks to Offer Secure Mobile Payments*, Mobey Forum (March 2010).



David Birch from Consult Hyperion shows us the MasterCard sticker on the back of his phone.

Such stickers are produced in the millions and place no demands on the MNO so they are easy to deploy. They are called “passive” because they have no power source. Nor do they have any connection to the phone processor, the UICC or the network. Therefore their functionality is limited: there is no way for the service provider to access their applications over-the-air and applications on the phone cannot access the applications in the sticker (so, for example, if the sticker contains a prepaid payment card, there is no way for a phone application to interrogate this “card” to find the remaining balance: this must be done OTA).

Passive stickers are already mass market. First Data shipped half-a-million "Go-Tag" pre-paid stickers last year. Their average user is paying with the sticker 2.5 times per month and the average reload is $93. In addition, Bling as been shipping stickers to community banks for local payment schemes (and recently hooked up with PayPal) and Citi has just announced a large scale launch of stickers as well. Customers clearly like waving and paying with their phones, and stickers are an easy way to help them to do this. The market is not only about payments. Stickers are already being used by merchants, an indication of their acceptability, for value-added services such as loyalty schemes. *Business Week* highlighted one example in Indiana: at the Rochester *Dairy Queen*, more than 350 customers can wave stickers fixed to the backs of their phones at a scanner in the store, thereby banking loyalty points and qualifying for free cones and Blizzard sundaes. Customers have come back to the store more frequently as a result, helping sale rise more than 3% in the past year (the only thing that retailers care about!). On a larger

scale, the French children's clothing retailer Tape à l'oeil has rolled out a 300,000 sticker loyalty programme across all its stores.

Other companies are working on types of active sticker. An active sticker has power and can connect with the UICC either through the phone using Bluetooth or wifi. This connection means that the SE can be reached OTA, but it also means that (since the SE is now in a powered environment) phone applications can use the full range of NFC interface possibilities (including peer-to-peer).

Active stickers are in limited trials right now, although there are as yet no large-scale commercial deployments.

Micro SD Cards

Mobile users are generally familiar with SD Cards in mobile phones. 40% of all mobile device holders are active SD Card users. In 2009, 90% of all shipped Handsets that included memory cards had SD Cards slots, and these are increasingly slots for µSD cards (these were in two-thirds of all mobile devices shipped last year). Since 2000, 2.5 billion SD cards have been shipped making it the *de facto* standard for removable media. Thus, µSD card with an embedded chip for the SE are a potential way to extend the security level and service offerings on mobile devices.

It has to be said that financial services are well-suited to this packaging, because it means that the service providers can use the MNOs as a pipe to communicate with the SE but do not need to deal with the MNOs. And consumers can use the same SD card when they swap handsets or even when they swap devices. This kind of implementation opens up a variety of business models, ranging from banks perhaps giving SD SE cards to their customers, or the SD SE cards coming bundled with devices or perhaps even third-party specialists distributing and managing the SD SEs on behalf of banks and retailers.

Visa has just announced a large-scale pilot of the technology with Bank of America but it is fair to note that another service provider (RFinity, which focuses on campus solutions) has just abandoned its µSD pilot to use passive stickers instead.

Embedded Secure Elements

The first NFC mobile phones (such as the Nokia 3220) used embedded SEs. That is, the handset contained two smart card chips: the removable UICC (the SIM) and an additional one built-in to the handset and controlling the NFC interface. eSEs add a small premium to the Bill of Material (BOM) of the handsets, depending on the technical capabilities of the eSE and whether they are purely payment focused or offer a greater multi-application support and provided they are standard Multos or JavaCard chips they are straightforward to access.

The concept of eSEs is very close to the UICC SE model as can use a TSM (although one of the joys of the 3220 was that you could use applications through the NFC interface as well) and leverages the same core provisioning technology. The integration of eSEs has limited or no impact at all on the phone design in terms of hard- and software.

There is a subclass of eSEs that are not built in to the handset but are added to the handset with an interface that sits between the handset and the UICC: these are known as "SIM overlay" eSEs. They generally comprise a thin connector that fits between the handset and the SIM contacts, attached to an SE. The idea is that the consumer removes the SIM, adds the SIM overlay and then replaces the SIM.

Whether consumers want their "cards" tied to their SIM or to their handset remains to be seen. The idea of shipping handsets with "open" eSEs (ie, eSEs that allow anyone to create new secure partitions within the SE) is certainly appealing and might well provide a better platform for innovation.

Trusted Processor

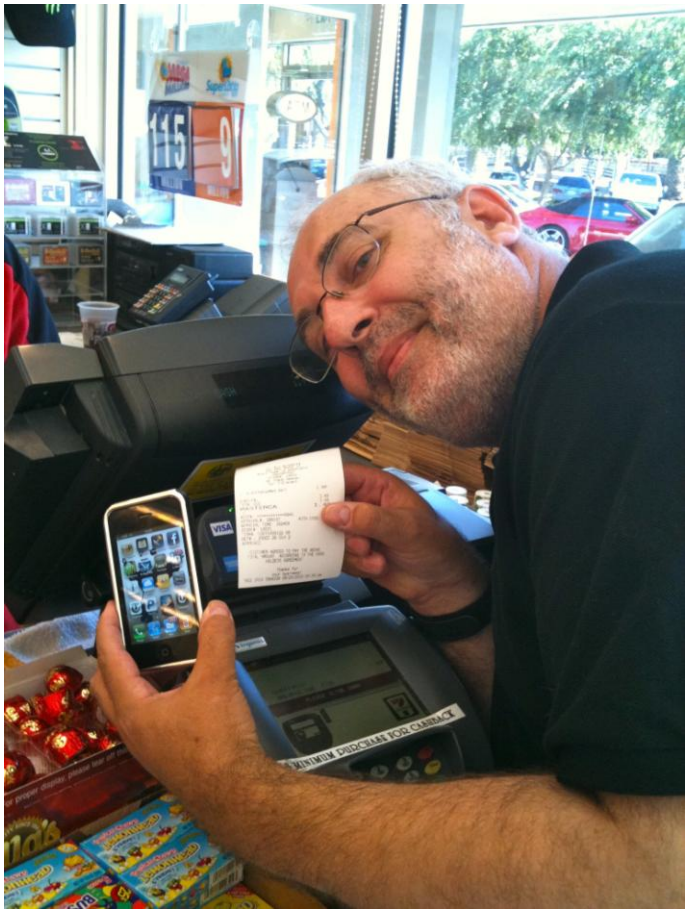
Trusted Processors (TPs) are promising upcoming solutions which may help take the fragmentation out of the mobile ecosystem through an integrative solution. The TP is designed into the Central Processing Unit (CPU) of the mobile devices. Being part of the CPU means natural distribution to a wide consumer base. TPs are not mutually exclusive to other SEs. A key role of the TP is to add security. Current mobile phones run in untrusted modes, so it is possible for malware to sit between the SE and the elements of the phone that it needs to connect to: the keyboard, the screen and perhaps other interfaces. The TP means that when customers enter their

PIN into their mobile phone, they can be sure it is the payment application that reads it and not a hacker. Similarly, customers can trust what they see on the phone display when they run their payment application.

Even if the TP does not contain its own eSE, they can support and enhance UICC SEs, active stickers and eSEs cand ombine these into integrated solutions with much higher levels of security than might be obtained with SEs alone.

Technology Trajectory

It is simply not possible to identify a clear trajectory for these bridging technologies, but it does seem as if one reasonable approximation might be the use of stickers with handsets to introduce consumers to both mobile proximity “tap and go” functionality for payments, ticketing, events and perhaps access control as well. As these users groups scale, they will become a factor in the potential business model for operators, who will then be incentivized into ordering NFC handsets from the manufacturers.



Using bridging technologies in the real world to pay for things with iPhone sticker