simalliance

Bringing Security & Interoperability to Mobile Transactions

Critical Considerations

April 2012

Table of Contents

1. Introduction

From m-commerce, through m-banking to couponing services, the level of mobile industry enthusiasm for using the mobile as a transactional device is understandably high.

Scratch the service of potential mobile transaction portfolios and it is easy to see why. Whether enabling instant international payments, credit and loan applications, stock trading, NFC retail goods payments or a host of marketing-led loyalty point collection and usage services, the opportunities appear endless.

But while market projections and developing service suites point to an industry worth in excess of $670 billion by 2015 (Juniper Research), translating this from a slideware to the balance sheet is no small task.

The likelihood of success, of course, cannot be questioned; not least because of the commitment (and investment) of the mobile industry to making it happen, or indeed the growing consumer acceptance of the mobile as a payment mechanism - which is as high as 70 percent in some markets. The associated rampant adoption of iOS and Android smartphones in developed markets, the functional possibilities they offer and the increasing market penetration of NFC-enabled handsets are also driving the market.

Consumers love their mobile devices; and there is ample evidence that should transaction services be mobilized in such a way as to offer some kind of differentiation, then consumers will adopt - whether that value is in increasing convenience for the consumer, giving them back more time, offering free 'stuff' or reducing the costs of goods and services. Ideally, it will be a combination of all. But the beauty of the mobile device is that it enables impulse online purchasing – from an advert seen in a train carriage or passing billboard. This will, of course, drive data traffic but also increase revenue-share returns between all the members of the mobile value chain – from the retailer right through to the mobile operator.

There are, of course, concerns. These range from the rapid ROI for mobile transaction services, how to assure the consumer adoption above, and how to build the right business models to get the money flowing through the value chain. But perhaps before all of these, we need to look to two key elements without which it will be impossible to build a platform for success; security and interoperability.

2. Section 1: Facing up the challenges of a connected mobile world

The aforementioned consumer love affair with the smartphone (and tablet) is combining with faster mobile broadband speeds to encourage an increasingly rapid migration away from traditional PC application and boost mobile transaction service consumption.

In doing, it is bringing a host of pressures to bear on developers, brands and mobile network operators that must be addressed if mass adoption and ubiquitous access to mobile transaction services are to be delivered.

The first pressure is of course on security. Once confined to the wired internet, malware, virus and hacking threats have now migrated to the mobile. And these threats range from denial of service, through fraud to identity theft.

Similarly, the complexities of developing and deploying services in this increasingly dangerous world are rising. The vast majority of transactional services will involve some form of financial agreement; which in turn makes them subject to a multitude of tightly managed and geographically different certifications and regulations.

This picture is further complicated by the existence of multiple payments schemes, from JCB and AMEX, to EMV and numerous domestic systems – not to mention multiple payment providers; from Apple, Google and PayPal to name just three.

Success here means being in a position to rationalise and solve all these issues, to offer the highest levels of identity protection and assurance, alongside a fully open and interoperable service portfolio to deliver the ubiquity of access and seamless user experience that are critical factors in driving the market forward. But more, enabling complete data confidentiality between service providers will be key.

2.1 Managing security through authentication and access

Remote mobile transactions require some form of authentication that assures the adequate level of security - both for the integrity of the transaction and to avoid scaring away security conscious consumers. This requires we bring authentication and identity up the agenda, and demands a closer investigation into protection mechanisms currently employed to assure security.

2.1.1 Log-in password

Traditional mobile security is most often based on a very conventional log-in and password authentication - on 'something you know' such as a password or PIN number. This is single factor authentication and it's easy to deploy and great for offering secure email access on the move. However, with 'known' password or PIN information able to be stolen at the client side – either through user-error or keylogging spyware – further steps must be taken to assure transactional security.

Similarly, with the password and username stored in the server, a successful breach would expose all users' details to the attacking code. And because single authentication lacks point to point encryption, data can be attacked in transit…over the wired or wireless internet.

2.1.2 One-time passwords

A move into two factor authentication would seem to solve this problem – with One Time Password (OTP) solutions offering a more stringent authentication process by creating a single time-bound password and adding a second level of security.

For instance, an OPT secured service will request a PIN code or password and then require an additional 'something you have' which may be a token, a device or channel that provides this one time password. In the case of online banking that 'token' will be a code from a card reader, while gaining password reminders online may involve keying in a code received by SMS after providing a user name online.

This achieves a higher level of security than standard password authentication because of the use of this second channel of communication – meaning the potential attacker will have to gain access to both channels to log in. However, in a smartphone environment where users grant some applications access to their messages, the additional security benefit of the second channel disappears as both now converge on the same device.

And then there's the user experience. It is rather impractical in many situations to retrieve a passcode with an application and then copy it into another application on the device. Similarly, having to carry round multiple devices to access key services seems a little excessive. And this is an important point because in creating a challenging user experience security becomes a compromise, with consumers more likely to choose convenience over assurance – and that's when they are most at risk.

2.1.3 Electronic Signature

Secure online services based on (Wireless) Public Key Encryption or (W)PKI provide a more secure framework. They are not, however, very popular today as they are rather more complex in design. While supporting user identification, authorization and transport channel encryption - and of course the exchange of digital certificate or keys - certificates can be manipulated on the server and on the client side if they are not properly protected.

3. Section 2: Introducing the Secure Element

So, what is the best way forward for service providers and brands?

For the SIMalliance the most effective route to securing today's generation of smart open devices is through the adoption of a (SE) within mobile security architectures.

Quite simply, the SE is as secure as a credit card. It is fully certified – EMVCO, CC, EAL5 and CAST – offers a highly customizable platform on standardized Java technologies and can be remotely managed through the contactless interface or over the air. It also offers the platform to host multi-party services in secure, defined domains.

Crucially perhaps, the SE can also work in tandem with the existing mechanisms we have already discussed. Both the OTP password and the PKI certificate can be stored on the SE to enhance levels of security within these existing mechanisms. Such flexibility also helps to protect investments already made by providers in security policy.

The most common Security Element, and indeed the most widely used secure platform in the world, is the UICC. It delivers precisely the levels of assurance needed in transactional security – from crypto processor, countermeasures, and security certifications. However, with deployment flexibility and choice now key in today's market, the same level of functionality and security can be delivered through other Secure Element form factors – and this unique combination of hardware and software can be hardwired directly into the handset or added through a secure Micro SD card.

The Secure Element is essentially 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 is a combination of hardware and software, built to exacting standards and developed and delivered in controlled white room manufacturing environments.

Going back almost three decades, the most common secure element within the mobile space, and indeed 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). But as above, the SE can also be delivered as an embedded chip in the handset (eUICC) or external MicroSD card.

Crucially, when discussing mobile transactions, the SE can be securely managed remotely. This is a critical feature when one considers the potential number of devices in the field today and the regularity of update.

The chief benefits of the SE in this environment are:

- Highly secure (OS Certifications: EMVCO, CC EAL4+, CAST)
- Highly customizable (dynamic security domains creation, embedding unique credentials and certificates)
- Multi-party services: secured domains and applets inside managed independently by each entity
- Connected: remotely manageable (OTA & OTI)
- Standardized and interoperable for mobile devices, services hosting & management (TSM compliant)
- Proven and mature technology

But, security is nothing without functionality. Here too the SE delivers, playing a key role in enabling the following mobile transactions:

3.1 Benefits of the Secure Element

3.1.1 End user benefits

As discussed in the introduction, encouraging consumer adoption must be of primary concern across the mobile value. Much of this responsibility lies with the marketing departments of brands and operators across the world. However, understanding the key benefits above and beyond the convenience factor (no.1 below) is critical:

3.1.1.1. Convenience

- Physical wallet replacement / less plastic cards in wallet
- Speed of transaction (reduced queuing at the point of sale)

- Portability between mobile devices

3.1.1.2. Enhanced security

- Protection against theft and fraud (though enhanced state-of-the-art counter-measures)
- Remote service lockdown

3.1.1.3. Improved customer experience

- Purchase history
- Instant rebate
- Relevant coupons and deals
- Enhanced product information

3.1.2 Service provider and merchant benefits

At the same time, understanding the hard and soft benefits to the service provider is vitally important:

- Improve customer satisfaction
- Reassure on the security
- Reduce costs (cash and checks handling, equipment maintenance, ticket issuance…)
- Reduce risks of fraud and thefts
- Increase revenue for merchant acquiring banks
- Improved marketing (customer location, communication channel)
- Increase usage of retailer store cards

4. Section 3: The importance of interoperability

But security is only part of the equation. Seamless communication between below are all required:

- the application and the SE
- the Graphical User Interface (GUI) in mobile device and the application on the SE
- The Trusted Service Manager (TSM) servers, SE and its installed applications

It is this demand complete interoperability throughout the application development, delivery and remote service management lifecycle that led the SIMalliance to develop its Open Mobile API initiative. And in doing so, SIMalliance is offering that missing link between the Secure Element and the secure mobile applications nested on the device.

From a business perspective the creation of this common API is a very positive step forward. It delivers a single, consistent specification and interface across multiple operating systems of mobile devices – eliminating the need to reengineer applications to each specific operating system. This of course then results in reduced application development costs, time-to-market and time-to-revenue.

From a security perspective, connecting the applications to the Secure Element delivers a higher security while the credentials (passwords, codes, license keys, certificates etc.) are stored in a secure environment and the access to it is regulated. In this ideal scenario (system setup) the credentials are never exposed to the outside world in plain text.

Launched in 2011, the SIMalliance Open Mobile API Specification describes how a mobile application running on an open smartphone operating system can access a Secure Element. In Release 1.2, the specification describes the process of managing the transport layer to allow applications to transmit messages to the SE. The format of those messages is called APDU (Application Protocol Data Unit).

Open Mobile API Release 2 enhances the current transport API to provide a more intuitive interface and increasingly powerful functionality to make it easier for feature phone and smartphone application developers to connect their applications to the Secure Element. A common set of reusable high level services as crypto, file management, discovery, PKCS#15 and secure storage allows developers to allocate time and resource to developing the functionality of their application rather than focusing on the complexities of integration with the device's Secure Element.

4.1 Interoperability beyond the Open Mobile API

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.

4.1.1 Stepping Stones

The Workgroup 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.

In addressing the evolving NFC ecosystem, in 2011 the SIMalliance introduced its Stepping Stones for NFC. This defines a clear path for NFC integration into the UICC, and interoperability across the device, OTA platform and UICC operating system.

In 2012, the NFC Stepping Stones will also address the two other Secure Elements form factor: embedded and secure MicroSD.

4.1.2 CAT Loader for contactless

In addition to the Stepping Stones programme, dedicated software tools to confirm interoperability levels are offered by the Working Group. The Group is working on updating the CAT Loader - the only existing card management tool to have been verified with UICC by 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

4.1.3 Cooperation with other industry organizations

In 2011 the SIMalliance established a formal partnership with GlobalPlatform; committing to work together to develop an end-to-end solution that will allow a mobile device application to communicate with an application loaded in the Secure Element. The two associations will combine the filtering technology of GlobalPlatform (known as SE access control) with the Open API to deliver a complete solution for handset manufacturers.

5. Conclusion

For the SIMalliance, the introduction and wide scale adoption of the Secure Element as the de facto security for mobile devices and applications will significantly increase levels of assurance for mobile transactions. It will combat the ever-growing sophistication and volume of attacks and guarantee the highest levels of security for connected mobile devices in an IP world.

But as we have discussed, security is nothing without interoperability. It is for this reason that the SIMalliance is encouraging the o/s, application developer and mobile community at large to utilize these essential security features which, together with the Open Mobile API, will enable the industry to turn predictions into profitable, ubiquitous mobile services.