Managing the UICC Certification Lifecycle

An SPA Position Paper

November 2013

Dr. Andreas Strobel, President of the Smart Payment Association (SPA) examines the challenges inherent in managing mobile payment applications deployed on the UICC. He argues the Mobile Network Operator (MNO) community must be prepared to deal with emerging lifecycle challenges – and calls for greater cooperation between the mobile and payment communities in addressing this up-and-coming issue.

Growing consumer familiarity with mobile payment, greater penetration of NFC capable smartphones, and the rise of superfast 4G networks is ushering in a wave of innovative mobile payment services.

Mobile payments are already predicted to hit $1 billion in the US this year, reaching $58 billion by 2017. But as mobile payment technology becomes mainstream and global consumer uptake increases, payment scheme operators and MNOs need to consider the repercussions in relation to longer term UICC lifecycle management.

The root of the challenge lies in the certification process: how to make sure that payment applications executed on mobile platforms offer the same level of trust as a bank issued payment card. Yet the mobile UICC/SIM is managed using different business rules than those utilized for payment cards. This variation in business practice, and the fact that different independent applications, each with its own lifecycle, have to coexist on the same platform, makes the product certification policy and its management highly complex.

Given this new context MasterCard and Visa, through EMVCo, have extended the EMVCo Security Evaluation process to include mobile platform products. Yet this is a new world for MNOs, who may not be familiar with incorporating EMVCo processes into business planning and card replacement strategies. But if these processes are not properly managed, a number of problems are likely to occur – extending from the failure to trigger in-time product re-certification requests, through to the management of multiple applications (both payment and non-payment) on the MNO's UICC real estate.

In this paper the SPA identifies the main issues for the application of the EMVCo certification framework to mobile platforms and explains the initiatives we have undertaken to facilitate its implementation.

1. The current certification approach and challenge

EMVCo specifies a three-step certification process for mobile payment platforms, resulting in the issue of three different but mutually dependent certificates: one for the integrated circuit, one for the platform and a third for the payment product itself.

- Firstly, the Integrated Circuit Card (ICC) – the chip - is certified by EMVCo for one year and granted a certificate - the ICCN (Integrated Circuit Card Number). This original certificate for the chip can be renewed annually for a maximum of six years, after which it expires.
- Secondly, based on the certified chip a platform will be developed by vendors: a computing stack made up of an operating system and other software modules designed to host and execute one or more payment applications. This platform is granted a certificate - the PCN (Platform Certificate Number) – which is valid for one year. The original PCN can be renewed annually for up to a maximum of six years after which it definitively expires. It should be noted that EMVCo requires that, for a platform to be eligible for the certification process, the ICC certificate must be no older than one year.
- Thirdly, the mobile payment platform - made up of a certified platform and at least one resident payment application - is certified by the payment scheme whose specification was used to develop the application. This product certificate is granted for an initial period of three years and may be renewed annually for an additional three years, after which it definitively expires. It should be noted that EMVCo requires that, for a payment product to be eligible for the certification process, the platform certificate must be no older than one year.

Given this inter-related certification framework, it is important to understand the resulting constraints and management complexities for both MNOs and vendors.

For comparison, let's first take a look at a typical payment card model, in which a vendor usually provides an issuer bank with a certified card. The bank then independently determines the lifetime of the card, according to its own risk policy. All of which makes it easy for a renewal card policy to be planned for and scheduled well in advance of the point in time at which the card is issued.

The scenario for mobile platforms, however, is substantially more complex to manage and it is important to understand why.

1. When the mobile payment platform is implemented in a UICC/SIM, the owner is a Mobile Operator. But payment applications resident on the card are owned by a third party - usually a bank. The bank must trust the platform on which its application will be executed, and must therefore negotiate the certification policy with the MNO.
2. Mobile payment platforms are intended to be multi-application, but not all applications have the same requirements in terms of security. The certification policy of the overall product is, therefore, partially determined by the application having the strongest security requirements.
3. The same certified platform may be sold to a client MNO, resulting in two different payment products: one cobranded with Payment Scheme 1 and a second cobranded with Payment Scheme 2. However, the common PCN lifetime is bound to six years and the certification dates for the individual payment products may be different. For example, one may have been certified just after PCN first certification, while the other may have been certified closer to the end-of-life of the PCN. As a result, the re-certification effort and cost will not be the same. Furthermore, the certification policies of the individual payment schemes with respect to the payment products may differ.
4. Platforms are often tailored to the needs of a particular client MNO; very often these modifications have no impact on the security robustness of the platform. The reuse of a previous evaluation report of a base platform for the certification of a related new platform is a key consideration. A flexible policy for the re-certification of a family of platform products will reduce time-to-market - a key concern for the highly competitive MNO business.

5. Payment systems can revoke their approval if a security breach is discovered in the platform or the payment application whilst the UICC/SIM is in the market.
6. The mobile payment platform may be implemented using secure elements other than the UICC/SIM, introducing additional issuance constraints.

The SPA is well aware of the complexities of this mobile certification scenario, and has taken the initiative to start discussions in this area with the EMVCo Security Evaluation WG. The objective is to streamline the certification framework to enable MNOs to better plan and execute UICC delivery dates whilst ensuring the highest level of security for the resident payment applications.

1.1. Further considerations

Cost-effective and highly secure payment application management in UICC/SIM is not the only challenge facing MNOs and payment application issuers.

Other in-field scenarios related to the multi-application nature of the mobile platform include:

- updates/changes to payment applications once the UICC is already issued
- the reissue of a new UICC/SIM form factor to an existing customer
- the reissue of a new UICC/SIM card in the event of loss/theft/handset damage
- firmware updates to the handset/user changes to handset with new OS.

These and other scenarios create logistical challenges for all parties. And while MNOs may issue the UICC, once in the field they may not have knowledge which – or how many - payment applications have been downloaded by end users.

2. The need for action

With consumer interest in mobile payment growing, the SPA believes that industry players urgently need to address potential post-issuance certification to ensure the end-user experience is optimized and end-of-life scenarios managed in a standardized and effective manner to the mutual satisfaction of all the stakeholders.

The SPA therefore proposes that discussions need to take place between MNO, EMVCo, Payment Application Issuers and Vendors to explore common streamlined procedures to reduce operational complexity, risks and logistics costs.

The SPA proposes that dialogue needs to take place in three key areas:

- Streamline the certification process: further dialogue is needed to review how current certification processes could be adapted and refined.

  Harmonization of UICC/SIM Lifecycle practices by payment schemes: while the freedom of banks and payments systems to establish their risk policies should be preserved, some alignment would

ease the management of the product lifecycle by MNOs and vendors. This harmonization could address the following primary areas:

1. Expiry dates for payment applications after the expiry date of the ICCN/PCN certificates.
2. A common approach for the activation of pre-loaded but not yet activated applications when the UICC is issued.
3. Best practices in terms of UICC/SIM replacement policies, enabling both the protection of the resident payment applications and easier planning for MNOs and vendors.

- Improvement of the user experience: it is in no one's best interest for consumers to have to manage the logistics of their own UICC and applications. Consumers want a seamless experience, and for someone – the MNO, or payment service provider – to invisibly manage the process for them.

About the Smart Payment Association:

The Smart Payment Association addresses the challenges of the evolving payment ecosystem, offering leadership and expert guidance to help its members and their financial institution customers realize the opportunities of smart, secure and personalised payment systems & services both now and for the future.
For more information on the SPA, visit our website: www.smartpaymentassociation.com or contact us by email: info@smartpaymentassociation.com.

Press Contact:
Stéphanie de Labriolle
+33 6 85 91 19 94
Stephanie.delabriolle@smartpaymentassociation.com