Certification on Mobile Payment Platforms

The SPA Position

April 2013

1. Introduction

The issuance of new card payment instruments, such as mobile platforms, requires payment card vendors to manage an ever-greater volume of EMVCo certification, and certification renewal, processes.

Such processes are time consuming and increasingly costly for the vendor community.

The SPA believes it is time for EMVCo certification processes to be reviewed; with new, more optimized processes agreed and standardized for mobile payment platforms.

While such an evolution will not be without its challenges, and trust in the certification process cannot be undermined, action must be taken to make the processes more workable. To achieve this goal, the SPA strongly believes a common and collaborative effort between all the different stakeholders is required.

This document offers some suggestions on how to achieve this goal.

2. Certifying a Mobile Payments Platform

The mobile payments platform we will be specifically referencing in this document is the SIM/UICC.

Issued by a Mobile Network Operator (MNO), the SIM/UICC hosts the payment application - possibly alongside other card-hosted applications that may or may not have security certification requirements themselves. In either scenario the SIM/UICC provides authentication and secure access to the mobile network for the payment application it carries. At present, that authentication is typically evaluated by the proprietary processes of the MNO.

The secure management and execution of the application itself is typically covered by a security certification process specified by the industry payment schemes, who certify the SIM/UICC as a traditional card product.

Herein lies the challenge. The SIM/UICC is not a traditional payment card – being much more dynamic in nature than a conventional payment card. Yet, under current rules, any changes to the SIM/UICC requires a recertification of the application itself.

Recertification in the real world

In practice this means that every time a SIM/UICC is customized for a specific MNO (which happens often), a 'new' product is created which must then be recertified by the payment scheme. This is deemed necessary despite the fact that the MNO customization typically only impacts the card's operating system, and has no impact on the management or execution of the payment application itself. So, a minor change to the SIM/UICC currently results in a major recertification of the application (despite the fact the latter has not changed). Inevitably this pushes up costs to the point where managing and maintaining a mobile payments platform is artificially, and unnecessarily, high.

Managing the payment application lifecycle

Of course, it is important to be aware of, and make provision for, potential changes in the payment application itself during the product's lifecycle - after the SIM/UICC has been issued to the end user. It may, for example, require a version update in the field via over-the-air distribution.

Should such an event be necessary it will be important to take into account both functional and security considerations. The application would have to be backwards compatible with the payment platform in the field, while it remains paramount that the new 'packaged' application and mobile payment platform is fully secure.

As mobile payment application versions change frequently, managing such changes in the field is likely to be a challenging activity. In scenarios where SIM/UICC substitution is not possible – such as for embedded Secure Elements – the impact of change will be ever greater.

The answer is to develop clear policies of how to manage such changes in the most efficient way. Such policies must be discussed and agreed with all stakeholders involved; the industry payment schemes, MNOs and vendors.

Duplicating cost and effort

It is the SPA's position, supported by a wealth of evidence from its members, that vendors are duplicating their security evaluation efforts due to these minor modifications of the underlying platforms as a result of SIM/UICC customization. So while redundant evaluations on already certified platforms fail to increase security, they significantly increase the final cost and lead times of end-user mobile payments solutions – overheads that are difficult to pass to the final customer.

While the SPA welcomes the greater number of payment platforms and new form factors now marketed as payment products, it believes there is a high price to pay – both in terms of the sharp rise in the number of required certifications and recertifications, and in the delays caused by these long and complex procedures.

There's little doubt then that improvements in the current certification methodologies for mobile payment platforms are much needed, and we are keen to explore new rules to improve the competitiveness in the security certification market for mobile payment platforms.

3. Optimizing existing certification methodologies

Identifying the ideal certification process

SPA considers that characterizing the "ideal" certification features could provide a sound base from which to move ahead; to improve current practices and avoid serious issues in the future. SPA is well aware that this initial list of suitable characteristics is not exhaustive, and the degree of relevance may differ depending on the stakeholder. However, as a starting point, we believe that the "ideal" process for the certification of a mobile payments platform is as follows:

1. That the certification process is based on the principle of justified administrative and operational process, with the permanent objective of shortening certification time frames. For example, the establishment of a periodic revision process by all the stakeholders in support of continuous process improvement. This would take into account shared in-field experiences, potential new threats, new mobile platform technology and results from laboratory tests
2. That the process should meet the vendor's business needs in terms of time to market, delivering an appropriate balance between technology evolution and certification renewal policies
3. That the process meets the vendor's business needs in terms of harmonized common test practices and the high level of technical skills of accredited laboratories
4. That the process enables maximum reusability of existing security evaluation reports and tests, while generating trust and maintaining collaboration between all the stakeholders involved
5. That the process is fully documented and traceable, including reference to the product operating guides to ensure all the users of the certificate (issuer MNO, payment schemes, payment application owners, retailers) are clear on what the security evaluation has targeted
6. That the evaluation methodologies are transparent, and based on vulnerability assessments as defined by JHAS.

Redefining evaluation and certification practices

The SPA believes that the final implemented certification process should be able to address the needs of the market in terms of cost and lead times, and should accommodate future technology evolution.

Furthermore, recertification of an existing, but slightly modified, certified mobile payment platform should only be performed after careful evaluation of the interactions between the operating system and the payment application. If the modifications of the platform do not impact the execution environment of the payment application, recertification processes should be minimized.

Similarly, the criteria for the recertification process should be agreed and harmonized between certification bodies and published - with a strong focus on reusing existing evaluations.

At present, different laboratories apply different ways to implement tests. This makes it difficult to compare evaluation reports and to draw accurate conclusions as to which product is safer. It is the

SPA's recommendation that security certification bodies should clarify a minimum set of common requirements for the evaluation laboratories when performing security testing.

Improving the management of the certification process

The SPA believes a specific process could be developed for the recertification of a mobile payment platform.

- **Shortening the time frame** required to grant a certificate. SPA members have often experienced long certification time periods - from the initial product submission to the laboratory for the security evaluation, right through to final certification. In particular, shortening the review period needed for the report produced by the laboratory will be important.
- **Increase cooperation and process responsiveness**. SPA members recommend certification bodies appoint an expert project manager to be assigned to each individual submitted product. The PMs role would be oversee the evaluation and certification process. In particular, the PM would respond to vendor and laboratory operational queries, and facilitate dispute resolution during the entire certification process.
- **Improve and harmonize accredited laboratory competence**. SPA members believe that all security evaluations be conducted with consistently high technical standards, and that test cases should be implemented in the same way, using top of the range technical tools.
- **Extra resources to be assigned:** SPA members recognize that ensuring high levels of responsiveness from certification bodies will require the allocation of additional resources – and that the extra burden imposed by this proposal should be shared between all the stakeholders.

Towards a Service Level Agreement for card payment certification

SPA is evaluating the possibility of defining a Service Level Agreement (SLA) concept based on compliance by certification bodies and laboratories to a common set of requirements (e.g., appointment of a contact person during the certification process, availability, time required for the certification, etc.). The SLA is intended to recognize that all processes applied by stakeholders are demonstrably cost efficient and support the high level of assurance required.

4. SPA and continual improvement

SPA has already established a program to identify the bottlenecks that are the source of extra costs and greater inefficiencies. It is looking at ways to address these bottlenecks in the existing mobile platform certification methodologies.

Our conclusions and proposals will be shared with the payments industry, and particularly with the security evaluation laboratories, certification and type approval bodies.

SPA will be submitting a proposal to optimize the certification for mobile payment platforms in bodies such as EMVCo, EPC-CSG and GSMA.