Mobile Device Security Element

Key Findings from Technical Analysis v. 1.0

Edited By
Bishwajit Choudhary & Juha Risikko

Mobey Forum

Mobile Financial Services Ltd.

www.mobeyforum.org

Disclaimer:
This document is subject to change without notice.

Background

The Financial Industry is today issuing electronic payment products to its customers mainly in the format of plastic cards. Other key financial services, such as banking and brokerage, are now being increasingly handled through the Internet in most cases. Large-scale deployment of these services in the mobile channel is expected to bring numerous benefits, such as:

- Increased customer convenience and improved service levels
- Cost savings to the key stakeholders in mobile financial services (financial institutions, merchants) as part of cash payments become electronic
- Additional revenues to the operators as data traffic increases
- Benefits to the operators and handset vendors as the mobile handsets become the “trusted device” for enabling high value financial services such as payments, banking and trust services
- Further development of the user habits in “on-the-move” environments, leading to improved feasibility of new business propositions in the wireless mobile environment

However, the current payment and other financial service products do not easily fit in the mobile channel while keeping the user convenience at high levels.

For most financial services, security aspects such as authentication, authorisation, privacy and non-repudiation are critical factors. One of the most concrete symbols of security is a bank vault. For example, a wallet in the pocket is often allowed to contain similar contents to a vault, in smaller scale, not as securely but providing easier access and better usability in everyday situations. A vault is a centralised solution for security, allowing greater control on authentication, authorisation, privacy and non-repudiation. A wallet is a personal vault, made secure by the owner, who controls access to the content. As financial services increasingly become “online”, the physical wallet needs to have a trusted counterpart in the digital world.

Consequently, for quite some time now, the need to implement a Security Element (SE) in mobile handsets has been realized to store and process the required credentials, sensitive data and facilitate mobile financial services. While the handset technologies (TCP/IP, colour screens, etc.) and proximity transaction technologies (such as Near Field Communication (NFC)) have developed positively, the lack of success in implementing independent SE in the handset has probably become the final and most important challenge today.

According to Mobey Forum, the SE should not be narrowly used only for PKI type processing, but act as a modular element for storage and processing of the credentials, which are used for authentication or a payment. **The SE is a dynamic environment, where applications are downloaded, personalised, managed and removed independent of each other with varying life cycles.** The SE applications may come from different sources. The life cycle of SE includes re-initialisation (as mobile devices have a second-hand market). In some cases, the application in the SE can be used to provide security related services for a browser based or other remote online or local applications in the mobile device. The application itself within SE may be accessing facilities of the mobile device, such as local and remote communication capabilities, to provide the service.

Examples of applications where an SE is needed are mobile banking, remote payments, stored value local payments, authentication and card based local payments. Security element use case examples can also be found in JSR-177 Security and Trust API Specification Appendix F.

Methodology

During Q1-Q2 2005, Mobey Forum carried out in-depth technical analyses of the SE alternatives available and emerging as of today. The technical analyses report was completed in cooperation with Mobey Forum partner members. Existing and emerging SEs were compared and contrasted across a number of key business and functional parameters:

1. **Mandatory factors**
    - Performance
    - Security levels
    - Usability
    - Support needed
    - Technical feasibility
    - Commercial feasibility
    - Ease of large scale implementation
    - Business independence
    - Liability sharing
    - Life cycle cost

2. **Interoperability factors**
    - Network interoperability
    - IT & legacy systems

- Standards

3. Optional factors

- Customisability
- Vendor support

Potential SE alternatives can be broadly divided in the following categories (1) removable SEs (secure memory card, chip, (U)SIM, advanced secure USB), (2) non-removable SEs (embedded chip) and (3) software based solutions.

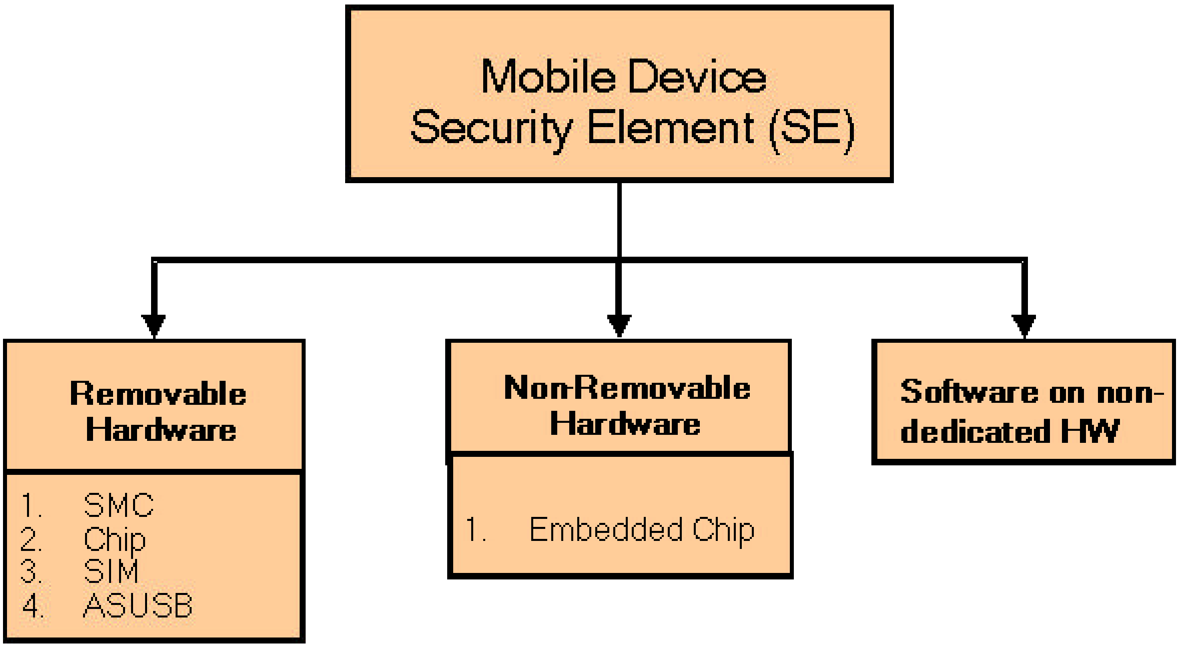

Figure 1: Security Element Classification

Key findings

In terms of the knowledge and experience that the industry has with various SE alternatives, they can be divided into two main categories: the current ones, of which we have experience and the potential (future) SE alternatives. Hence, drawing objective comparisons between these two categories is challenging.

Software and SIM based SEs are the two currently available and technically feasible alternatives, though both options face challenges in meeting all the key SE-requirements of the financial institutions. Thus, there is a need to look more closely at the options beyond those already known to us.

In the near future, the mobile handset SE will be widely used for several purposes including: debit, credit, mass transit ticketing, access control, loyalty etc. The concept will be modular and transparent to the user so that the user does not (need to) see which technical alternative is being used.

It is important to note that the use of security element always involves a trusted application (outside of the SE), the SE authorized user, and the security of the full chain is dependent on the security of these parties as well.

We now summarize selected conclusions from the SE analyses:

- **Software based SE and Advanced Secure USB** token do not qualify as a general multi-purpose SE that could be used both in remote and proximity transaction environments. Usually a "multi-environment and multi-functional" SE would store and securely process the credentials with high performance in both the remote and proximity environments. The need to use SE both in the remote and local environments implies that the mobile device vendors should implement suitable interfaces towards SE and hence have a central role in defining the SEs and their roles in both these environments. This, in turn, may be dependent on mobile handset models and their manufacturers. Local payments products require tamper proof SEs, ruling out pure software based solutions. Local payments need to be more convenient than the existing alternatives available and in the case of Advanced Secure USB token this requirement is hard to achieve. Both software based SE and ASUSB[1] may well be used for remote mobile financial services such as, authentication.

- **From the "Usability" point of view**, USB hardware token SE alternative is cumbersome to use (as it needs the simultaneous use of both hands) when compared with mobile phones with integrated SE solutions. In the remote services, customers may find it logical to use advanced secure USB as SE if the same USB token is (already being) used as authentication token with PCs in fixed Internet environment.

- **SIM as SE** implies a long-term banks' dependence on the telecom sector and operator proprietary SIM Application Toolkit. Clearly, a long-term dependence on a sector as telecom (which has great interest in mobile payments and mobile trust services) can challenge the business independence that the banking sector would usually like to keep.

[1] USB and ASUSB are used interchangeably

Further, the banks will need to establish one-to-one agreements with the telecom operators and this would potentially fragment the creation of a seamless Pan European Mobile Financial Services (MFS) marketplace. However, the control and role of the banks in using SIM as an SE will depend much on their negotiations with the telecom sector both at national and international levels.

- **From "business independence" point of view**, Software SE, Secure Memory Card, Advanced Secure USB token and Embedded Chip are the optimal options.

- **Businesses intending to make fast in-roads in (limited) national markets** may find SIM as SE to be reasonable for mobile authentication solution. The business processes supporting SIM lifecycle are stable and mature in the telecom world. Much of these business processes can be reused by the banking industry, depending on negotiations with the operators. However, it will take time to rollout suitable SIMs for the end-users which would be necessary in most markets. Software SE alternative is also very good as the banks have flexibility with respect to pricing and vendor relations.

- **Life Cycle Costs** of the Software SE alternative are potentially the lowest. SIM cost should also be manageable and this may be the "second best solution" from cost perspective as banking and telecom industry will share some of the costs, while reusing existing business and support processes for enabling and using SIM for new (financial) services.

- **From Vendor support point of view,** software-based solution is the simplest and most well developed in the banking sector. The SIM alternative also is well supported by the telecom industry. However the banks' experience on using SIM as SE for high value mobile services and the consequences of dependence on operators are largely unknown.

- **Of all the SE alternatives,** SIM is and can be the most widely deployed SE in the short term. However, the deployed SIMs "out there" are not used as SEs the way financial institutions would prefer. On the other hand, cooperation between the banking and telecom sector could lead to harnessing a widely distributed and used platform for implementing financial services. Further, it will take a few years to replace the existing SIM-base with suitable (secure) SIMs if a natural SIM life cycle is followed. Furthermore, new standardization is required in order to use SIM as SE in the proximity environment.

Conclusions

Software SE

The merits of a software SE are evident in many areas and it is the only operator independent alternative available today and also allows smooth transition to hardware-based security in the future. Many local applications require hardware-based tamper-proof SE, implying that software based solutions cannot be used as multipurpose SE covering all the mobile financial service areas. Among many requirements, “tamper proof solution” requires that the SE cannot be modified and its contents cannot be copied/ used / reproduced through unauthorized processes and that the content may be automatically destroyed or otherwise become inaccessible if certain number of unauthorized attempts are made to ”open up the SE”.

Advanced Secure USB

In “on-the-move-environment” as is the case with MFS, removable / separate token SE as ASUSB are more cumbersome to use than the embedded or other removable SEs that remains attached to the mobile device most of the time. The usability dimension is a key success factor in making a mass-market use of the SE for mobile financial services.

(U)SIM

(U)SIM as SE is also viable as it has currently the widest market acceptance and usage experience, sometimes even as SE for low value financial and non-financial services. The main challenges are related to business models and the choice of suitable (U)SIMs. Some standardization work is needed to enable the use of (U)SIM as SE in the local environment. (U)SIM has the potential to be used as SE in the whole range of mobile financial services.

Secure Memory Card

Secure Memory Card as SE provides high usability as it is expected to remain inside the handset “in its default position”. Greater storage and processing power compared to chip and U(SIM) may also imply higher performance and its greater use by the end user as a mobile storage platform (for music, video, messages etc.). Any stakeholder in MFS can issue SMCs and therefore SMCs can enable completely independent business processes of different players from different industries. Business issues related to the cost of SMCs, handset support / compatibility towards the SMCs and establishing standard interface towards local applications remain the key challenges. SMC has the potential to be used as SE in the whole range of mobile financial services.

Removable Chip

The characteristics of the removable chip SE solution are similar to the SMC SE solution. Chips can be issued with significantly lower cost than SMCs, but at the same time, their performance is relatively weaker. However, there are currently no mobile devices available with a slot for the second chip and there are no indications (from the mobile handset vendors) that such developments would take place in the near future.

Embedded chip

Embedded chip as SE is an extremely interesting and cost-efficient solution for all the parties in MFS. Embedded chips require post-personalization processes as mobile devices cannot be personalized in the manufacturing process. It remains to be seen how widely mobile devices with embedded chips will be launched in the market. Embedded chip has the potential to be used as SE in the whole range of mobile financial services.

In conclusion, we find that all of the SE alternatives have several challenges on their way to becoming widely accepted by all the mobile financial services stakeholders. It is very likely that the market will adopt several SEs, which are supported in different market-segments and in different handset models. Mobey Forum foresees the highest potential for general purpose SE to be in the following 3 alternatives

- (U)SIM as SE platform is interesting and may reflect pragmatism from industry partners, especially in (and starting from) a national market. However, its acceptance as multi-purpose SE through inter-sector accreditation may be complex.
- Embedded chip seems a promising cost efficient solution.
- SMC allows for business independence and multi-issuer environments with large storage and processing power.

The mobile financial service business ecosystem built on the above-mentioned SE alternatives will be studied at Mobey Forum during rest of the year 2005. The successful SE alternative(s) will be the one(s) that can create and sustain commercially viable business models and attract the interest, not only of financial institutions, but other key stakeholders as well.