As markets converge to deliver real convenience and innovation to end-users through chip-based technology, the ability of an issuer or service provider to secure their application from malicious attacks or unintentional corruption is essential. In this article, we explore the importance of security across the chip landscape and consider how security can be achieved on a multiapplication, cross-sector basis through the development and deployment of industry standards, and the ongoing commitment to compliance schemes and security certification bodies.

Market Expectations
As chip-based applications become more prevalent in everyday life, the security surrounding the technology has become increasingly important to all stakeholders.

- **End-users demand security** - consumers must be confident that a product is secure before they will purchase and use it. This is particularly important when engaging end-users in a new concept such as NFC technology. Security at this level is emotive, and users will either consider a product is trustworthy or not.

- **Issuers and service providers aim to mitigate risk** - the issuer recognises that no technology is 100% secure, but needs to invest in delivering the appropriate level of security for their product or service. Obviously, the more sensitive the information stored on or handled by the application, the more important security becomes. Bringing a product to market that lacks the suitable security standards is not only detrimental for that product, but can also have long-lasting consequences for the company behind the solution and its reputation. These consequences could be the cost of relaunching an unsuccessful product or potentially legal consequences for issuers that could be held liable for security problems.

- **Vendors need to ensure credibility** - vendors delivering the technology infrastructure – hardware and software – are responsible for ensuring that an application is being managed securely and as intended. This is important to satisfy both end-user and issuer expectations. Developing and providing products that meet and exceed expectations can significantly strengthen a vendor’s credibility and offer it a competitive advantage within the marketplace.

With so many different players contributing to such a dynamic landscape, each with different security needs, an independent and neutral party – a testing laboratory – is required. Its role is to objectively evaluate that the vendor’s solution will perform as advertised and delivers both the security and functionality promised.

Industry Standards
Behind every secure product or application should be a carefully planned infrastructure and system, which accommodates all the security requirements from each and every stakeholder contributing to the ecosystem. This is of increased importance in today’s multiapplication environment where many markets – that have never worked together before – aim to develop and implement sustainable solutions for the first time.

The convergence of the mobile sector and payment market is particularly interesting as both have such opposing business models. For example, a mobile handset manufacturer will develop a new handset model, undertake the required testing and launch to market within 6 months. In contrast, a new payment application to be delivered on a mobile phone must undergo detailed and complex security evaluations to ensure the financial and confidential information it stores is protected; a process which may far exceed the mobile handset manufacturers six-month turnaround depending on the scheme. Another issue is that there is currently no certification scheme for mobiles. This offers an opportunity to potentially develop one which meets the short-term evaluation requirements of the telecom sector’s specific needs and is independent from any market, most specifically the payment sector.

To manage such contrasting priorities, and as multiple application chips come to market, the cross-industry work of standards bodies and industry associations has become interestingly important to balance technical security requirements with commercial considerations. These standards and the ability to acknowledge products that align with them, provides issuers and service providers with a way of verifying genuine technology that will perform appropriately today and in the future.

In addition, due to the evolving nature of this ecosystem, post-issuance updates will continually need to be made to enhance functionality. This means that a range of different applications must be able to securely reside on the same mobile phone without complication or corruption. Currently, the security evaluation process is not adapted to the unpredictable nature of the content in the mobile. As this is an emerging technology, there are a lot of unknowns and ensuring security is not an easy task. Beyond the standardisation, it is critical to also streamline the evaluation process. There are ongoing efforts in this direction such as the Composition Model provided by GlobalPlatform and already endorsed at a certain level by EMVCo.

Once standards are created, it is equally important that compliance and certification programmes are founded to support market stability and demonstrate the market’s commitment to the long-term evolution of the environment. The testing and evaluation stage, therefore, builds confidence in the qualified solution and infrastructure; providing much needed guarantees.

Keeping Ahead Of Security Breaches
Although nothing is 100% secure, security provision should always aim to be one step ahead of the hackers 100% of the time and should be approached as a long-term investment. Even when a system is deployed, security measures must continue to be assessed and additional security elements added where necessary to protect against fraudulent activity.

Key to success in this dynamic landscape is the ability to quickly bring convenient and secure products to market. To make multiple application technology commercially feasible, standards bodies must aim to streamline compliance programmes and evaluation requirements to align with the fast-pace advancement of this market.

At the same time, technology developers should engage testing and evaluation consultancies such as FIME during the R&D stage. This will ensure from the start that solutions are aligning to the latest requirements, saving significant time and money.

---

**Vendor Views - Testing**

**Understanding Security Expectations**

**Greg Zheng**

*Business Development Manager*

*FIME Asia*