SIMalliance Open Mobile API

An Introduction v2.0

September 2015

Document History

Version	Date	Editor	Remarks
1.0	06/04/2011	OMAPI Working Group	Public release
2.0	27/09/2015	OMAPI Working Group	Public release

Table of Contents

1. Introduction

The ubiquity of IP/mobile broadband puts today's generation of connected mobile devices under constant threat of the same viruses and malicious attacks from hackers and cyber criminals that have challenged the fixed line internet for decades.

If not managed correctly, security challenges can cause reputational issues for brands, restrict the emergence of mobile services which would otherwise greatly enhance consumer choice and convenience, and as a result, limit potential revenue that can be generated for stakeholders across the mobile services value chain.

This paper presents a globally accepted and long established approach to ensuring security on connected mobile devices. It highlights the need to create security (and security policy) during the development stage, and reinforces the fact that the telecom industry already has a solution to the security challenges faced in today's mobile ecosystem.

It discusses why 'buy in' is needed from the application development and operating systems communities, and introduces SIMalliance's Open Mobile API (OMAPI) Work Group, together with its OMAPI Specification, which enables the application, operating system (OS) and the operator to connect with the Secure Element (SE) found in billions of connected devices across the world.

2. Open Mobile API Context

The emergence of smartphones and tablets has had a transformational effect on the creation and delivery of mobile services, resulting in millions of apps finding their way into the hands of device users worldwide. But this is not just a 'fun and games' revolution. Mobile connectivity has revolutionised the user's ability to not only communicate but to view the rapidly evolving digital world. The potential of the connected mobile device to shape consumer behaviour is massive and has become a major new channel through which brands can reach, influence and engage with their customers.

Mobile banking and transactions, for example, are just two areas where financial service organisations can create far stronger links with target audiences, affect real change in user behaviour and develop long-term strategies that will both restructure and drive out cost from their business. There are many examples of financial service organisations which have harnessed the power of mobile, particularly in conjunction with NFC contactless payment technologies, to revolutionise their service provision.

For detractors, the rise of the smartphone (or, more accurately, the delivery of IP-based services to the mobile) has opened the network – and its subscribers – to attack from fraudsters and malicious hackers. The threat of phishing, virus and sniffer attacks could become a barrier to adoption of, in particular, banking and transactional services on the mobile.

The proliferation of (increasingly open) OS, as well as the introduction of host card emulation (HCE) into the mobile NFC services ecosystem further complicates the security environment.

For these reasons, the SE continues to play a vital role in securing the future delivery of mobile services. As a well-established, globally implemented technology, it offers proven interoperability across devices and OS and the UICC/SIM/USIM is the most widely distributed secure application delivery platform in the world.

2.1 Security from the Operating System Upwards

The best way to curb any rise in security attacks is for the industry to recognise the value of a solution which addresses security from the OS up, and one that places the burden of responsibility firmly on both application developers and today's OS players. There are still many players within these communities who choose to ignore the potential of the SIM and other SEs within the connected mobile device, focusing security instead around single factor authentication methods such as passwords and log-ins.

Unfortunately, we have seen the results; attacks targeting security holes through which passwords can be intercepted. While OS developers and application providers have been quick to patch, such incidents will continue, causing damage to both reputation and revenues, unless security is taken further.

3. The Secure Element

The SE is a secure 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.

Going back almost three decades, the most common SE 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).

The SE, however, can also be an Embedded Secure Element (eSE) or a secure MicroSD Card – both of which can also be delivered simply and cost effectively into the mobile environment.

Today, the SE is a combination of dedicated tamper-resistant hardware and software, built to exacting standards and developed and delivered in controlled white room manufacturing environments.

The use of SEs within mobile security solutions eliminates the inherent insecurity of single factor authentication via password and adds another layer to create two factor authentication (enabled by the SE); which is nothing more than the use of two independent means of evidence to support authentication. PINsentry card reader devices are good examples from the banking sector while homeland security organisations are increasingly deploying biometric passports to authenticate people through fingerprinting or face recognition.

4. The Secure Element & Application

Connecting the application to the SE within the device is the only way to guarantee the highest levels of security for connected mobile devices in an IP world. It is for this reason that SIMalliance encourages OS and application developers, alongside the mobile community at large, to come together to utilise the SE, an essential security feature that in many cases is already available on mobile devices through the UICC.

5. SIMalliance Open Mobile API (OMAPI)

SIMalliance established its OMAPI initiative to allow OS and application developers to realise the benefits of the SE. It was widely acknowledged that the creation of an open API between the SIM (or any other SE) and the application will decrease the threat of attack.

Today, in 2015, SIMalliance's OMAPI Specification is implemented in nearly 250 models of Android (NFC) smartphone and is globally recognised by the industry as a standardised way to connect mobile applications with all SEs on a device. It provides an intuitive interface and increasingly powerful functionality and enables the delivery of highly secure business and consumer mobile applications across all SE form factors.

The core OMAPI Specification is referenced by the GSMA in its TS 26 NFC Handset Requirements.

The OMAPI Test Specification is referenced by the GSMA in its TS 27 NFC Handset Test Book.

GlobalPlatform, the association which standardises the management of applications on secure chip technology, has also adopted the SIMalliance OMAPI Specifications. It has implemented an OMAPI test suite based on the SIMalliance OMAPI Test Specification and has referenced the core OMAPI Specification within its device compliance programme.

The Global Certification Forum is currently certifying devices with OMAPI as part of its NFC related work activities. Today more than 80 models have been certified and this number is rapidly growing.

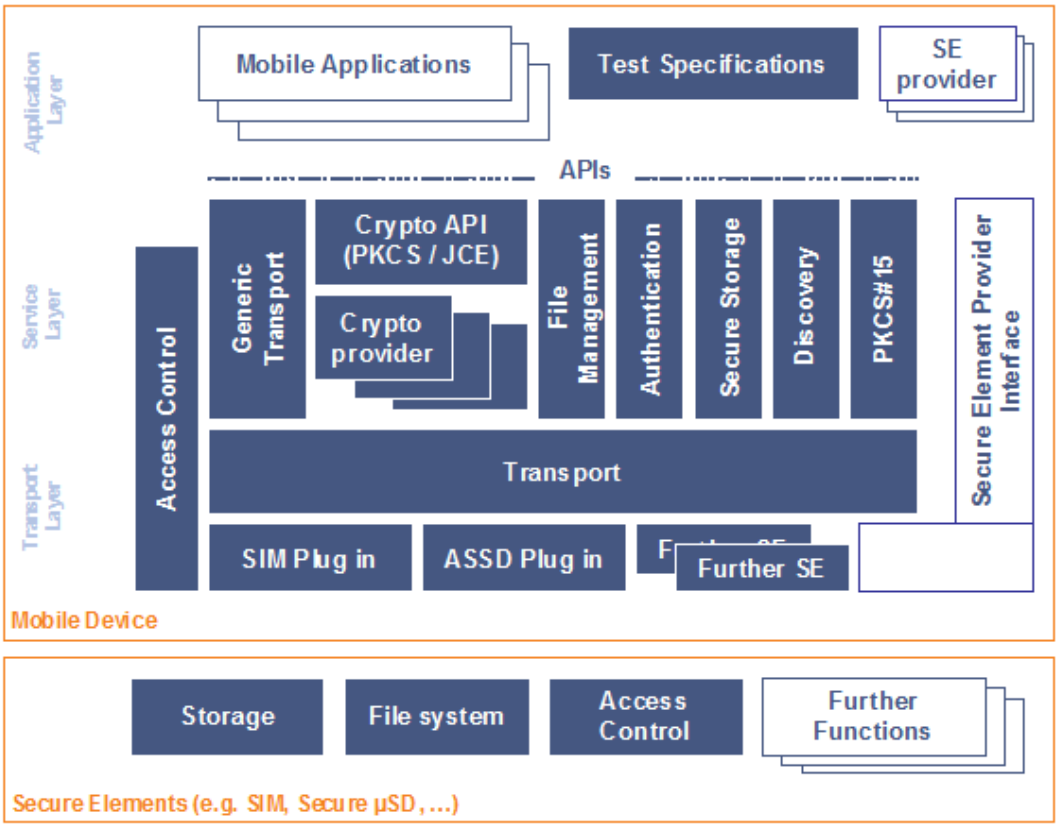
The North American certification scheme PTCRB will soon start certifying devices with OMAPI implementation as part of its NFC programme.

5.1 OMAPI Workgroup Objectives:

- To maintain an industry agreed API specification for all kind of SEs, SIM cards and SIM card extensions.
- To contribute specifications and documentations to the community and application developers.
- To promote the integration of SIMalliance-provided APIs and drivers by the various handset manufacturers.
- To facilitate interoperability between SEs, devices and APIs.

5.2 Overview

The diagram below shows the architecture covered by the SIMalliance Open Mobile API.



6. Use Cases

By providing a specific API for accessing the SIM and other SEs, the OMAPI Specification enhances the usability and opportunities for the platform to support the following types of services:

- NFC services
- Payment services (e.g. mobile wallet)
- Ticketing services and public transport
- Access control
- ID services
- Identity management (e.g. Liberty Alliance, Kantara)
- Loyalty services

Since the API recommendations are based on existing, standardised and security approved technology, the highest levels of compliance and security is assured.

7. Benefits for the Application Provider

By delivering a single, consistent specification and interface, the OMAPI Specification eliminates the need to reengineer applications for different devices and OS. This results in reduced application development costs, and improved time-to-market and time-to-revenue.

Since the release of OMAPI v3.0, the OMAPI can be implemented in both object oriented and non-object oriented OS.

The OMAPI Specification includes a set of service layer APIs which streamline development time and cost, by defining a common set of reusable high level services, such as secure storage.

8. Benefits for the End User

The end user can trust the application provider to effectively manage and protect their identity and eliminate fraud. This is critical to encourage wide adoption and frequent usage of secure mobile services. With maximum security assured, brands will also be more willing to develop their own applications, which will increase the number and availability of service offerings in the market, to increase consumer choice, convenience and satisfaction.

9. Benefits for the Mobile Network Operator

By providing a greater range of customer focused applications, the mobile network operator (MNO) can enjoy greater differentiation within the market and increase their incremental revenues. Critically, operators will also be able to fully leverage service usage data to increase personalisation and offer yet more targeted and relevant services to the end user.

In addition, by demanding application compliance to strict levels of security the MNO is able to build its own reputation as a security leader and further extend its trust relationships with subscribers.

MNOs can also position themselves as identity providers, protecting users against identity fraud. There is also the potential to create new business models by offering third party access to the UICC which would allow that MNO to build and deliver its own identity service.

10. Benefit for the Platform

The existence of a SE to store certificates and other confidential information, will allow the platform to be enriched with a host of additional applications. These applications include (but are not limited to) enterprise grade security applications including VPN access, SMIME and SSL authentication.

11. SIMalliance's Position and Conclusion

The development of an open API is a major step forward in enabling the delivery of an increasing number of business and consumer applications that demand the very highest levels of security and information assurance.

The SE protects sensitive data, the user and the mobile network from IP-borne malware attacks, and shields brands from financial and reputational issues which are still so common today.

Only the UICC, or any other hardware-based SE, can afford the highest levels of security for secure mobile services. Through the creation and provision of the OMAPI Specifications, SIMalliance offers a standardised solution which allows the industry to maximise opportunities and reduce the security risks of today's IP world.