TRUSTED
CONNECTIVITY
ALLIANCE

Open Mobile API Specification - An Introduction

Published by simalliance now Trusted Connectivity Alliance

April 2011

Table of Contents

1. Introduction

You don't have to look too hard to find a newspaper article highlighting yet another mobile application security breach. In contrast, as little as three years ago you would have been hard pushed to find the merest suggestion of successful virus or other malicious attack that had any sort of negative impact on the mobile ecosystem.

Today, that has now changed. IP/mobile broadband has meant that the connected mobile device is, for almost the very first time, as fair game to hackers and cyber criminals as the fixed line internet has been for the past decade.

The security challenges we'll see in this second decade of the 21st Century, will directly impact mobile's ability to structurally change consumer's lifestyles, will cause reputational issues for brands and perhaps more crucially, will mean that fewer services are used…and that means less money to go around the value chain.

This paper highlights the need for a change in how security is approached on the connected mobile device. It focuses on the need to create security (and security policy) at the development stage, and highlights the telecoms industry's unique position of already having a solution to the problem.

It discusses why 'buy in' is needed from the application development and operating systems communities, and introduces the SIMalliance's new Open Mobile API workgroup whose task it is to connect the application, operating system and the operator with the Secure Element found in billions of connected devices right across the world.

2. Open Mobile API context

According to even the most conservative of estimates the smartphone is stealing market share away from so-called feature handsets at an incredible, or alarming, rate – depending on your perspective. For supporters, this is a positive step and has been the catalyst for the creation and delivery of tens of thousands of internet-enabled applications on the handset.

But this is not just a 'fun and games' applications revolution. True internet on the mobile will revolutionise user's ability to not only communicate, but increasingly it becomes the portal through which we view the world. The potential of the connected mobile device– be that the smartphone or the tablet – to shape consumer behaviour is massive and has rightly attracted attention from brands right across the world.

Mobile banking and transactions, for example, are just two areas of opportunity where financial services organizations can create 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. This is particularly clear when used in conjunction with NFC contactless payment technologies.

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 is a serious barrier to adoption of, in particular, banking and transactional services on the mobile.

The proliferation of (increasingly open) operating systems further complicates the security environment.

However, the genie won't go back in the bottle; the market share of smartphones will continue to rise apace and that means we can expect more 'hacker' stories in the media.

2.1 Security from the Operating System Upwards

That is, of course, unless the industry comes together to develop a solution from the operating system up – and that places the burden of responsibility firmly on both application developers and today's operating system players. Until now these communities have largely ignored the potential of the SIM and other Secure Elements within the connected mobile device and instead focused security around single factor authentication methods such as passwords and log-ins.

And we have seen the results – attacks to security holes through which passwords can be intercepted. While the o/s and applications providers have been quick to patch, such incidents will continue unless security is taken further. And that will damage both reputation and revenues.

3. The Secure Element

The Secure Element is the 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 secure element 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).

But the Secure Element can also be an Embedded Secure Element or a Secure Memory Card – both of which can also be delivered simply and cost effectively into the mobile environment.

Today, the Secure Element is a combination of hardware and software, built to exacting standards and developed and delivered in controlled white room manufacturing environments.

Use of such available solutions eliminates the inherent insecurity of single factor authentication via password and adds another layer to create two factor authentication (enabled by the Secure Element); 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 organizations are increasingly looking to biometric passports, authenticating the person through fingerprinting or face recognition.

4. The Secure Element & application

Connecting the application to the Secure Element within the device is the only way to guarantee the highest levels of security for connected mobile devices in an IP world. And it is for this reason that the SIMalliance is encouraging the o/s, application developer and mobile community at large to come together to utilise these essential security features that in many case are already available on the mobile device through the UICC.

5. SIMalliance Open Mobile API

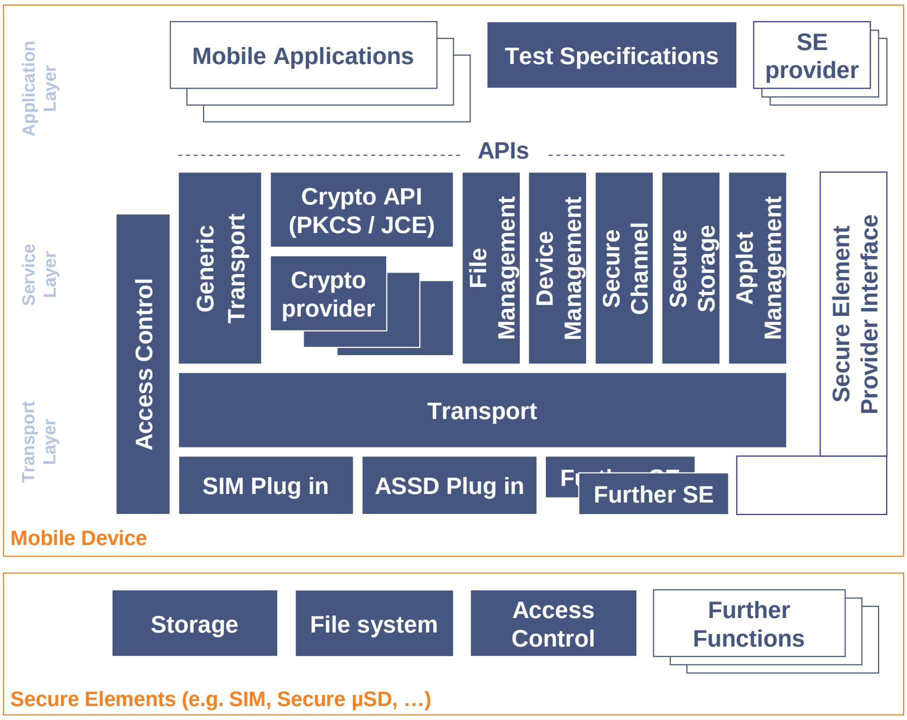
SIMalliance has established its Open Mobile API initiative to do so. Allowing o/s and application developers to realize the benefits of the Secure Element through the creation of an open API between the SIM (or any other Secure Element) and the application, will decrease the threat of attack.

5.1 Workgroup Objectives:

- To create an industry agreed API specification for all kind of Secure Elements, 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 ensure interoperability between Secure Elements, devices and APIs

5.2 Overview

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



6. Use cases

Having a specific API for accessing the SIM and other Secure Elements enhances the overall usability and opportunities for the platform for using services, including:

- 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

And because the API recommendations will be based on existing, standardized and security approved technology, the highest levels of compliance and security will be assured.

7. Benefits for the application provider

The creation of a common API – delivering a single, consistent specification and interface across multiple operating systems – eliminates the need to reengineer applications to each specific Operating System; resulting in reduced application development costs, time to market and time to revenue.

While release v.1.01 of the Open Mobile API deals with the transport layer, future versions will further streamline development time and cost by defining a common set of reusable high level services such as file encryption.

8. Benefits for the end-user

The end user can trust the application provider to effectively manage and protect their identity and eliminate fraud – both absolutely critical in encouraging wide adoption and frequent usage. 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 operator

By providing a greater range of customer focused applications, the operator 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 personalization and offer yet more targeted and relevant services to the end-user.

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

Operators 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 provider to build and deliver its own identity service.

10. Benefit for the platform

The platform itself will be enriched with a host of additional applications – something only made possible by having a Secure Element available to store certificates and other confidential information. These applications include (but are not limited to) enterprise grade security applications including VPN access, SMIME, SSL authentication.

11. SIMalliance's position and conclusion

We believe 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 Secure Element protects the application, the user and the mobile network from IP-borne malware attacks, and shields brands from the financial and reputational issues they are experiencing today.

Allowing controlled access via the open API will stimulate growth within the application provider community by addressing the costs of application development and delivery in a multi-device, multi-operating system world.

There is little doubt that the UICC or any other Secure Element affords the kind of protection that the market and its consumers need. Through the creation of the Open Mobile API workgroup the SIMalliance is offering a standardized solution to allow the industry to maximize the opportunities and reduce the security risks of today's IP world.