Input Paper for the W3C Workshop on Authentication, Hardware Tokens and Beyond

Submitter: SIMalliance Open Mobile API Working Group

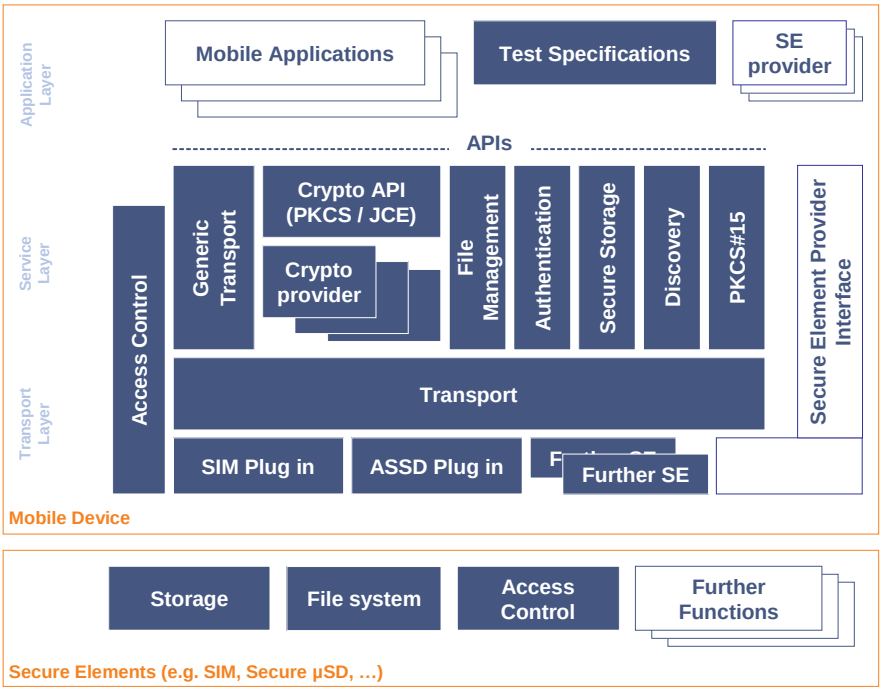
SIMalliance is a global, non-profit industry association which simplifies secure element (SE) implementation to drive the creation, deployment and management of secure mobile services. The organisation promotes the essential role of the SE in delivering secure mobile applications and services across all devices that can access wireless networks.

SIMalliance has a strong interest in the work undertaken within the W3C around web browsers, specifically the possibility to provide enhanced security services based on an SE.

SIMalliance has created, and maintains, the Open Mobile API (OMAPI) Specification, which is free-to-download from the SIMalliance website. The OMAPI specifies how mobile applications may access different SEs in a mobile device, such as a UICC or an embedded SE. SIMalliance's OMAPI has been referenced by the GSMA and is currently implemented in over 150 models of Android NFC smartphones and by several tablet manufacturers. As a complement to the OMAPI, SIMalliance has also developed a test specification and will soon be launching a test application (also both free to download). These make it easier to implement and verify the use of OMAPI in handsets, encouraging greater standardisation in SE access management across devices.

Within the scope of this paper, SIMalliance will provide a view of market trends relative to the implementation of OMAPI and will share information on which devices already support it.

The OMAPI is based on two main layers: 'transport' and 'services' (see below)



The OMAPI Specification is platform agnostic and is designed to provide access to different SEs including UICC, embedded SE and micro-SD. Together with GlobalPlatform's Secure Element Access Control Specification, the API provides an efficient solution for mobile applications willing to leverage on SEs. This

presentation will address the architecture of the OMAPI, as well as the benefits of the architecture and the access control mechanism. The presentation will also aim to generate further discussion among delegates attending the workshop, to clarify understanding of current industry requirements.

Finally, SIMalliance will provide examples of use cases and services, focusing on identity services that can be built on top of the API, and explain why it will be beneficial for all parties to have such an API available in the browser.

SIMalliance aims to engage in a productive collaboration with W3C on this topic and would be interested to attend and contribute to the W3C Workshop on Authentication, Hardware Tokens and Beyond in September 2014.