

OMA and Smart Card Technology

SIMposium 2011

28 June 2011

Patrice Beaudou, OMA ARC-SCT SWG Chair



Agenda

OMA Overview

OMA Organizational Structure

OMA Recent Work

APIs in OMA

OMA ARC-SCT SWG Current Work Program



OMA – Overview

Over 135 members from across the mobile value chain

- Founded June 2002
- Operators, terminal and software vendors, content and entertainment providers

Interoperable service enablers across multiple domains

- Architecture, Security, Charging and Network APIs
- Person-to-Person Communications
- Device Capabilities
- Access to Content
- Services Access Interface
- Service Customization

Current and Ongoing Technical Deliverables – more detail in presentation

- 44 service enablers delivered in 2010 with 80 planned for 2011
- Ongoing refinement of interoperability testing program with Test on Demand in Q3 2011
- API Framework—building on success of GSMA OneAPI and Parlay affiliation
- M2M Communications—enabling terminals as gateways and converged personal networks

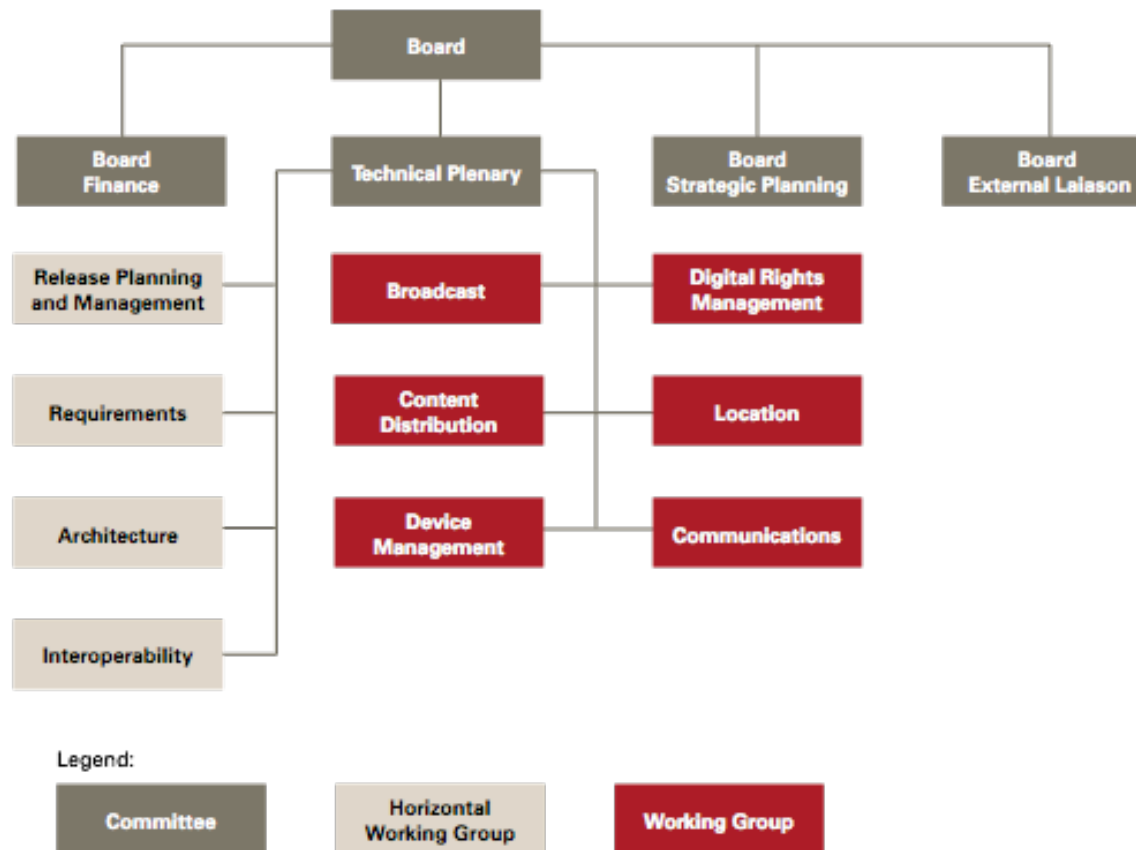
New and improved organizational structures and efficiencies

- Fast track process for omitting or combining steps and deliverables in OMA Process
- Min Max procedure for an alternative path to traditional testing of every OMA enabler

Collaboration with other bodies—including GSMA, ETSI & 3GPP/3GPP2

- Reduce duplication and fragmentation
- New strategic program of liaisons with appointed Board level champions to other bodies
- OMA maintains formal cooperation agreements or frameworks with nearly 50 industry bodies

OMA – Organizational Structure





Highlights of OMA Service Enablers

Over 50 Candidate and Approved Enablers Published in the Last 18 Months

Candidate Enabler Releases

- OMA Device Management Smart Card V1_0
- OMA Lock and Wipe Management Object V1_0
- OMA Converged Address Book V1_0
- OMA XML Document Management V2_1
- OMA Secure Content Identification Mechanism V1_0
- OMA SIP Push V1_0
- OMA Location in SIP/IP Core V1_0
- OMA Secure User Plane Location V2_0
- OMA Mobile Search Framework V1_0
- OMA Mobile Codes V1_0
- OMA Mobile Advertising V1_0
- OMA Mobile Spam Reporting V1_0
- OMA Customized Multimedia Ringing 1.0
- OMA Presence Access Layer V 1.0
- OMA Mobile Spam Reporting V1.0
- OMA Application Layer Security Common Functions V1.1
- OMA Next Generation Service Interfaces V1.0
- OMA Digital Rights Management V2.2
- OAM Key Performance Indicators in OMA V1.0
- OMA Smart Card Web Server V1_2
- OMA Mobile SMIL V 1.0 (Reference Release)

A Candidate Enabler Release (CER) delivers an approved set of open technical specifications that can be implemented in products and solutions, and then tested for interoperability.

An Approved Enabler Release (AER) represents Candidate Enabler Releases that have gone through the Interoperability Program (IOP) of OMA. The IOP tests interoperability between different member company's implementations—either within the OMA or through other means



Highlights of OMA Service Enablers

Approved Enabler Releases

- OMA EFI V1.1
- OMA Browser Protocol Stack V1.2
- OMA Push V2.1
- OMA User Agent Profile V1.1
- OMA Rich-media Environment V 1.0
- OMA Games Services Client/Server Interface V1.0
- OMA DownLoad Over The Air V2.0
- OMA Browsing V2.4 (enhancements ph 2)
- OMA Look and Feel Customization
- OMA On Board key Generation / Wireless Public Key Infrastructure V1.0
- OMA Device Management V1_2
- OMA Smart Card Web Server V1_1
- OMA Presence SIMPLE V1_1
- OMA Global Service Architecture V1_0 (Reference Release)
- OMA IMPS Implementation Guidelines V1_3 (Reference Release)

A Candidate Enabler Release (CER) delivers an approved set of open technical specifications that can be implemented in products and solutions, and then tested for interoperability.

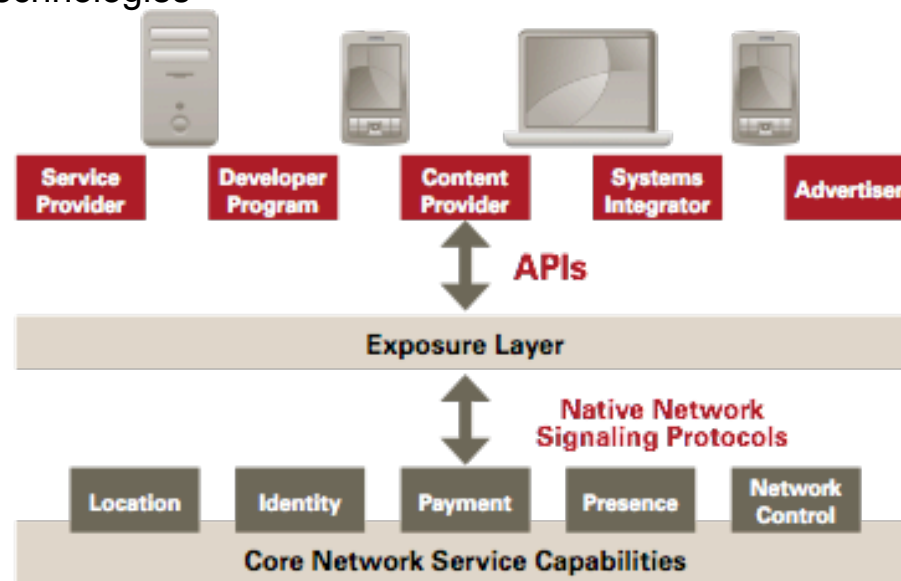
An Approved Enabler Release (AER) represents Candidate Enabler Releases that have gone through the Interoperability Program (IOP) of OMA. The IOP tests interoperability between different member company's implementations—either within the OMA or through other means.

APIs: What, Why, Who, Where?

Use Application Programming Interfaces (APIs) to open up service capabilities and assets in the core network to application developers

OMA APIs provide an abstracted view of these capabilities

- Application developers do not require comprehensive knowledge of arcane telecommunication signaling protocols and call state models
- Applications built towards the API can be ported across network types and access technologies



API Dimensions in OMA

Abstract APIs

- Focus on functional aspects
- Protocol independent

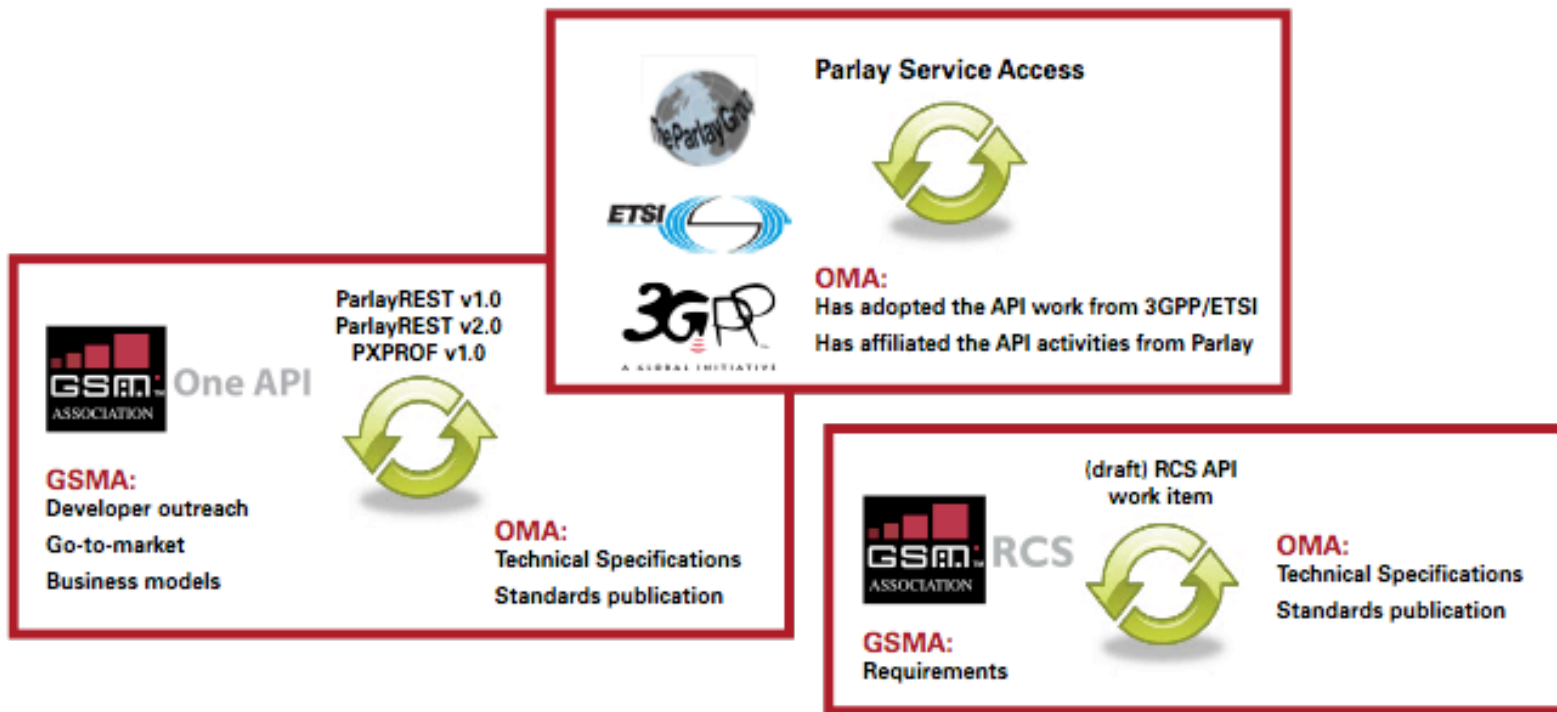
API Binding Technologies

- SOAP/WSDL Web Services
- HTTP protocol binding using REST architectural style

Network APIs & Device APIs

- Network API—exposed by a resource residing in the Network
- Device API—exposed by a resource residing/running on a Device

OMA APIs and the Rest of the Industry



OMA Current and Future API Work

Ratified APIs

1. Next Generation Service Interfaces
2. SOAP for Next Generation Service Interfaces
3. Client Side Enabler API
4. RESTful Bindings for Web Services
5. Parlay Service Access
6. ParlayREST (OMA PXPREF) and its GSMA OneAPI Profile

Pipeline APIs

1. Web Runtime API
2. APIs for Rich Communications
3. Converged Address Book APIs
4. Open Connection Manager API
5. RESTful Bindings for OMA Push Access Protocol

Others under consideration...

OMA Architecture/Smart Card Technology Working Group (ARC-SCT SWG)

OMA ARC-SCT SWG is the primary source of expertise for the OMA on issues related to smart cards and other secure hardware tokens using similar technology (e.g. smart card technology on different form factors).

• OMA ARC-SCT SWG current activities include:

- OMA On-Board Key Generation v1.0 (OMA OBKG)
 - OMA OBKG reached Approved Enabler status in March 2011.
http://www.openmobilealliance.org/Technical/release_program/obkg-v1_0.aspx
- OMA Smart Card Web Server (OMA SCWS)
 - OMA SCWS allows local communication between the Smart Card Web Server and an HTTP application (e.g. Web browser) running in the handset. This facilitates the implementation of a mobile operator's services making them portable across handsets.
 - OMA SCWS 1.1 reached Approved Enabler status in May 2009.
http://www.openmobilealliance.org/Technical/release_program/scws_v1_1.aspx
 - OMA SCWS 1.2 reached Candidate Enabler in April 2011.
http://www.openmobilealliance.org/Technical/release_program/scws_v1_2.aspx



OMA SCWS v1.2 Enabler

OMA SCWS v1.2 Enabler introduces additional features to SCWS v1.1. These features include:

- An additional requirement for the SCWS to allow for the possibility of several removable web servers operating in the terminal.
- The addition of optional support for TLS 1.1 and TLS 1.2.
- An additional feature that allows the smart card issuer to allocate a certain amount of memory for a specific 3rd party.
- The Access Control Policy mechanism becomes mandatory for the device.
- The addition of an alternative solution (the current solution is SMS) to send the push message to the SCWS on a SIP network re-using the OMA SIP Push Enabler.

Some clarifications are also provided among these additional features. They include:

- The use of the Ethernet Emulation Model (EEM) over the USB-IC interface when using the TCP/IP interface between the device and the Smart Card.
- The clarification of the Smart Card definition.
- The clarification of the commands available for remote administration.

OMA SCWS V1.2 Architecture Diagram

