



The Role and Contribution of OMA in Service Delivery Platform Standardization

ITU-T SDP Workshop

17 October 2011



Musa Unmehopa

Technical Plenary Chairman, OMA

Senior Manager, Alcatel-Lucent

What I'll be Talking About

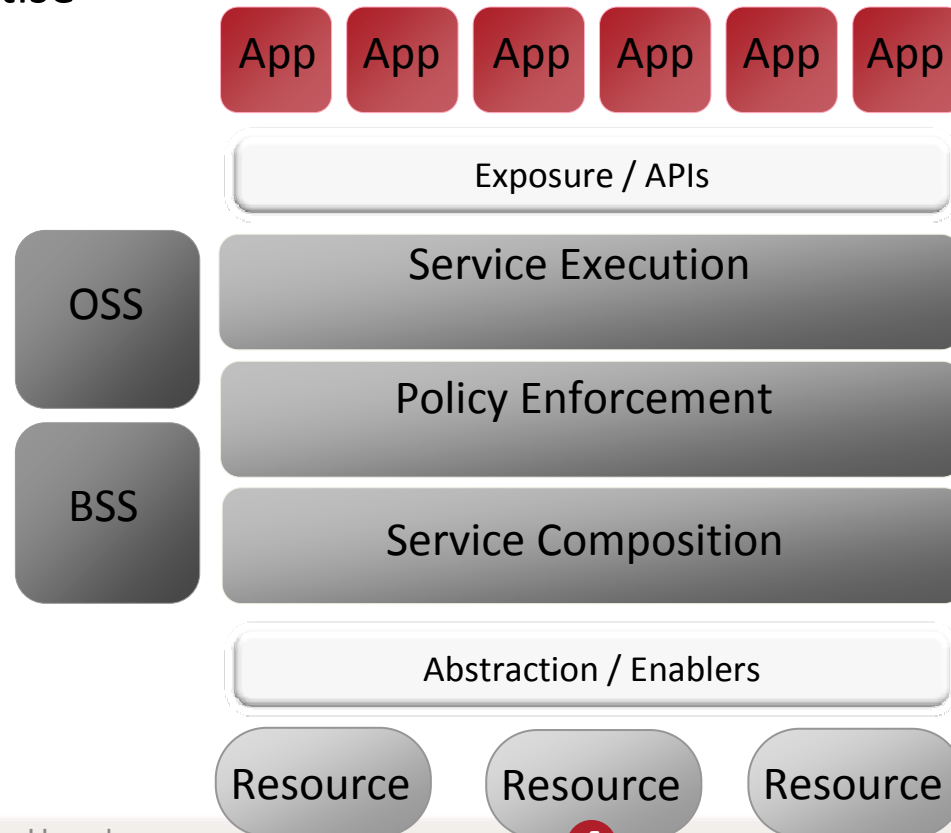




OMA STANDARDIZES KEY ASPECTS OF THE SDP

Generalized SDP Architecture

- There are many variants of an SDP architecture, with many components. Each of these architectures has common aspects and common components
- I will use the following **generic architecture** to superimpose OMA's areas of expertise



Resource Abstraction / Enablers

- OMA has published over 100 Enablers, for a wide range of capabilities, resources, and assets

Access to Content

- Digital Rights Management
- Browsing
- Push
- Broadcast
- Dynamic Content Delivery
- Mobile 2D Barcodes
- Mobile Search
- Mobile Advertising
- Download Over-the-Air
- MultiModal & MultiDevice

Person to Person

- Multimedia Messaging
- Instant Messaging
- Push to Talk over Cellular
- Mobile E-mail
- Spam Reporting
- Converged IP Messaging

Service Customization

- Mobile Location Protocol
- Mobile Location Service
- Secure User Plane Location
- Location in SIP/IP Core
- Presence
- XML Document Management
- Converged Address Book
- User Profile Management

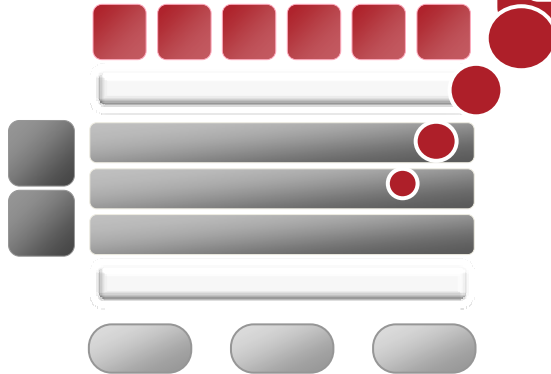
Devices

- Client Provisioning
- Device Management
- Firmware Update
- Data Synchronization
- Scheduling
- Diagnostics and Monitoring
- Software Component Update
- DM Smart Card
- User Agent Profile
- Look and Feel Customization
- Lock and Wipe Management
- Device Capabilities

Architecture

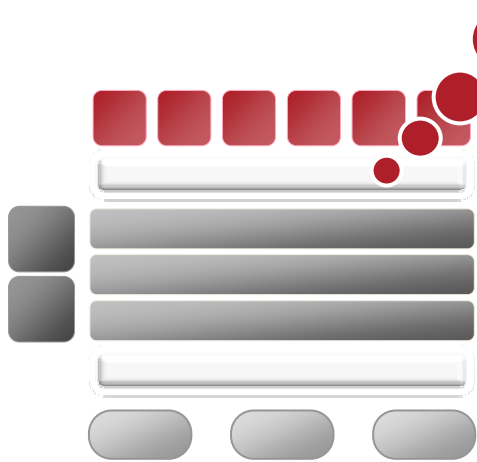
- Mobile Commerce & Charging
- Online Certificates
- On-Board Key Generation
- Common Security Functions
- Payment
- Smart Card Web Server
- Content Screening
- Permissions Management
- Subscription Management
- Policy Enforcement
- Privacy
- Secure Content Identity

Policy Enforcement



- The OMA Service Environment (OSE) is a layered architecture blueprint for the SDP. This architecture defines the components, but not their relationships, interactions, or governance
- The Policy Enforcer is a logical component responsible for the evaluation and enforcement of service provider policies (e.g. SLA, privacy, user preferences)
- In OMA, the PEEM enabler (Policy Evaluation, Enforcement and Management) realizes the PE concept
- PEEM has two operational models
 - Ruleset-based: IETF Common Policy framework
 - Workflow-based: Business Process Execution Language (BPEL)

Exposure Layer Application Programming Interfaces



- OMA APIs Standardize Access to Unique Resources within Operator Networks
- Standardized APIs are necessary to help realize the tremendous growth potential for the Applications Market
- OMA APIs expose the network assets that developers need - no matter what signaling protocols, platforms or other APIs they use
- Core network assets and device capabilities must be made available in order to deploy the wide variety of new applications and services that enter the market every day
- Includes both **Device APIs** as well as **Network APIs**

Network APIs, a big list and growing

Abstract APIs

- Call Control
- Call Notification
- Call Handling
- Context Entity Discovery
- Context Information
- Generic Data Change Notification
- Generic Data Management
- Identity Management
- Identity Resolution
- Multimedia Conference
- Multimedia List Handling
- Service Discovery
- Service Registration

RESTful APIs

- Address List Management
- Audio Call
- Call Control
- Call Notification
- Device Capabilities
- Multimedia Messaging
- Payment
- Presence
- Service User Profile Management
- Short Messaging
- Terminal Location
- Terminal Status
- Third Party Call

SOAP/WSDL APIs

- Account Management
- Audio Call
- Application Driven QoS
- Call Notification
- Call Handling
- Content Management
- Device Capabilities
- Geocoding
- Multimedia Conference
- Multimedia Messaging
- Multimedia Multicast Session mgt
- Multimedia Streaming Control
- Payment
- Policy
- Presence
- Short Messaging
- Terminal Location
- Terminal Status
- Third Party Call



OMA FUTURE REQUIREMENTS FOR SDP STANDARDS

Future Requirements for SDP Standardization

- OMA recognizes two deployment models for OMA enablers
 - Composited services, running on application servers in the operator domain
 - Mash-ups, running in the 3rd party, Internet domain
- This leads to the following future SDP requirements
 - SDP to support service components and 3rd party applications **running in the users' devices**
 - SDP to support **dynamic offering, negotiation and subscription** for accessing the exposed service components
 - an open service marketplace requires high level of flexibility and automation
 - SDP to support **dynamic update of policies** for protecting the exposed service components (e.g., policies on load control), according to the changes to the active subscriptions;
 - SDP to support **dynamic mechanisms for optimizing the allocation of resources** according to the requests of the applications, and for guaranteeing a fair usage of them in the open marketplace.
 - SDP to support **flexible payment model**, e.g. when a service component is executed “on behalf of a specific user”
 - This payment model must consider the involvement of at least three actors: the provider of the composite service, the provider of the service component and the end-users involved in a service session



CONCLUSION

**OMA STANDARDIZES KEY ASPECTS OF THE SDP
OMA FUTURE REQUIREMENTS FOR SDP STANDARDS**



REFERENCES AND BACKUP

OMA – Overview

More than 150 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

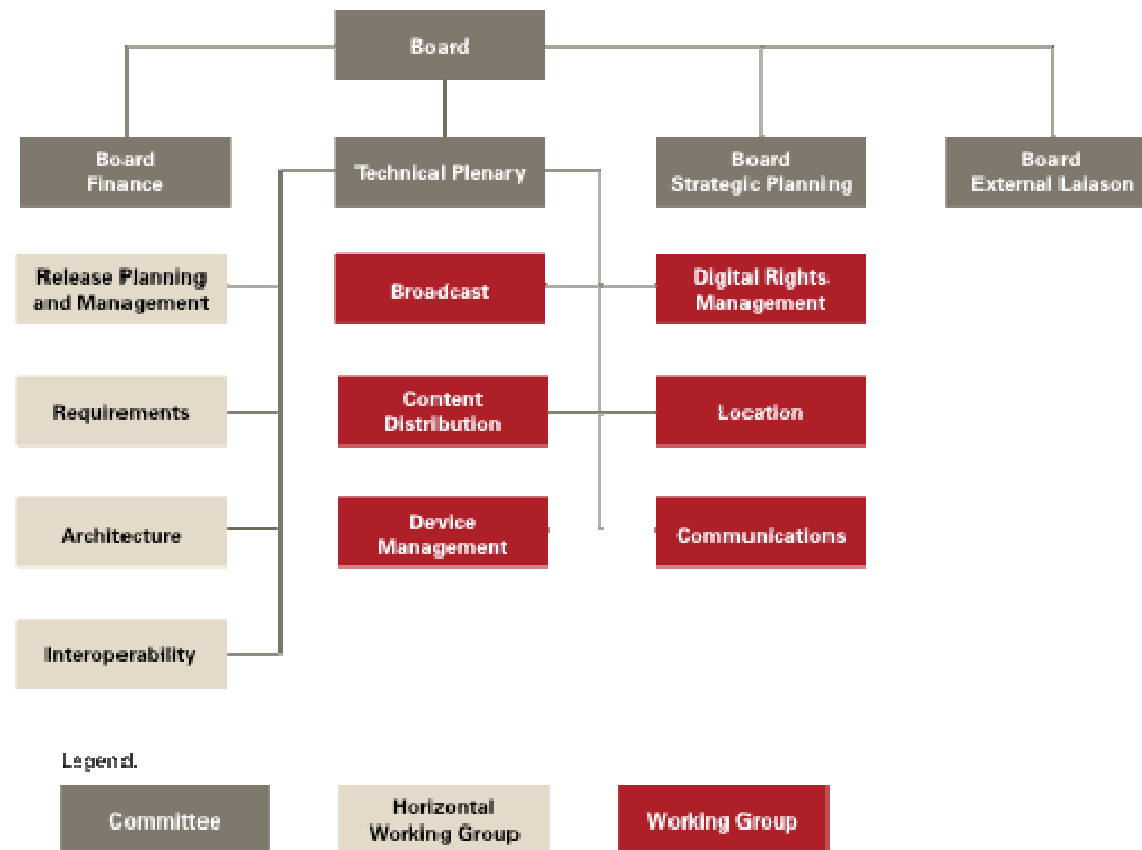
New and improved organizational structures and efficiencies

- 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 WAC, GSMA, W3C & ETSI

- 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.

More Information

- OMA Communications Contact
Bobby Fraher, External Communications Manager
bobby@agilis-communications.com
- 2011 Q2 OMA Quarterly Newsletter
http://www.openmobilealliance.org/comms/pages/OMA_quarterly_2011_vol_2.htm
- Full list of OMA Mobile Service Enablers
<http://www.openmobilealliance.org/Technical/releaseprogram.aspx>
- OMA API Program
<http://www.openmobilealliance.org/API>
- Interested in joining the OMA
<http://www.openmobilealliance.org/Membership/default.aspx>