
OMTP
OPEN
MOBILE
TERMINAL
PLATFORM

What is OMTP?

Our community

- A group of around 40 companies with a proven track record of delivering on Terminal Requirements
- Operator Members define Goals and Direction
- Made "real" by a balanced community of Participants
- A permanent and dedicated Office Team

OMTP
OPEN MOBILE TERMINAL PLATFORM

Our mission...

OMTP MOTIVATION

- THE COMPLEXITY OF MOBILE SERVICE OFFERINGS IS INCREASING RAPIDLY
- THERE IS A NEED FOR SEAMLESS INTEGRATION OF THE MOBILE SERVICE AND THE DEVICE THAT DELIVERS IT
- MOBILE OPERATORS HAVE STARTED TO DEVELOP A SEAMLESS CUSTOMER EXPERIENCE ACROSS THEIR DEVICE
- PORTFOLIO VIA CUSTOMISED HANDSETS
- THE CONTINUOUSLY INCREASING FRAGMENTATION OF MOBILE DEVICES UNDERMINES THIS SEAMLESS CUSTOMER
- EXPERIENCE AND MIGHT BECOME A THREAT TO THE MOBILE SERVICES BUSINESS
- THE SECURITY THREATS ON MOBILE DEVICES ARE DEVELOPING RAPIDLY

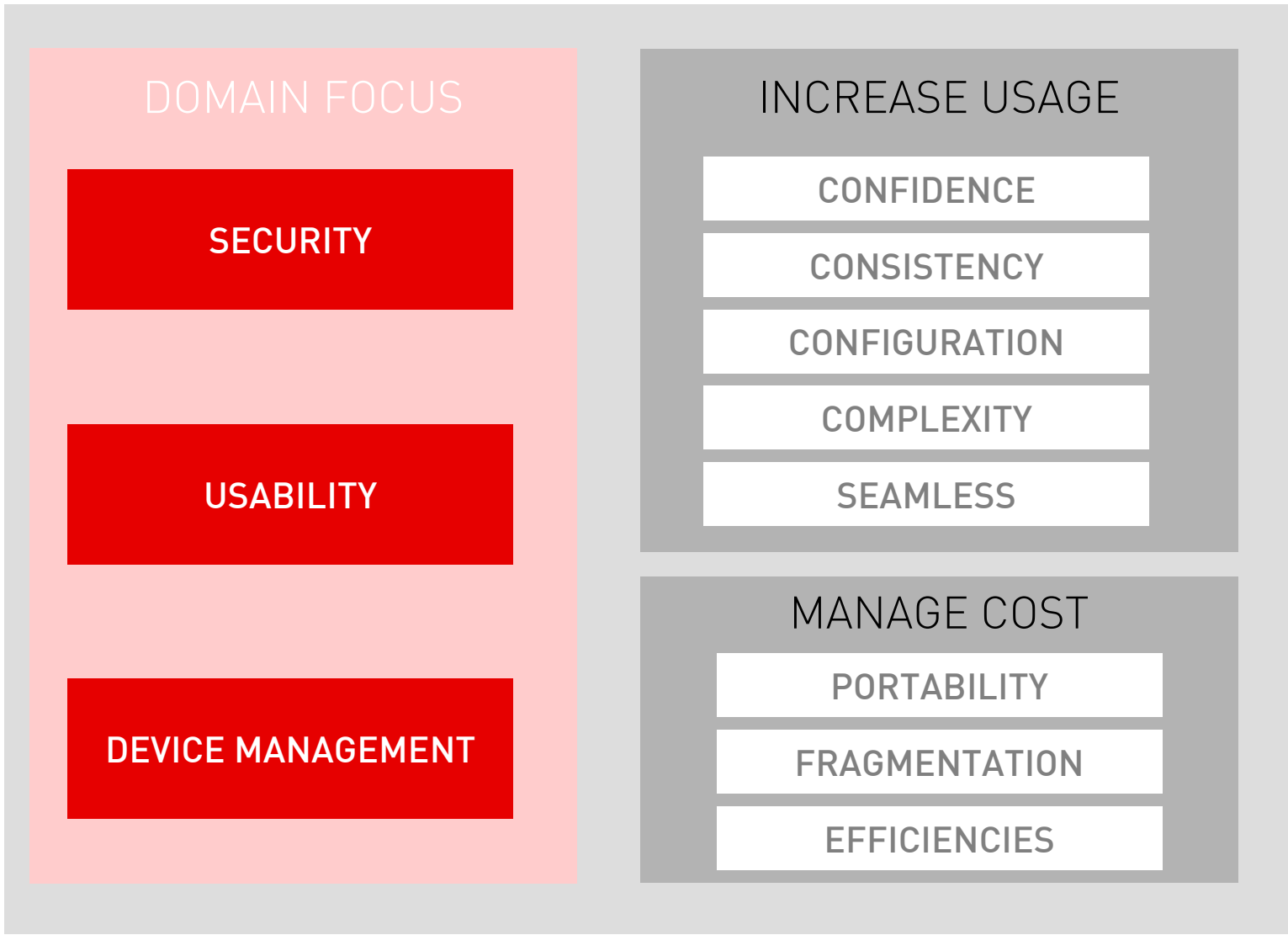
OMTP MISSION

"TO CREATE AN OPEN ECOSYSTEM FOR ADVANCED MOBILE PLATFORMS THAT SUPPORT ENHANCED AND CONSISTENT SUBSCRIBER EXPERIENCES ACROSS THE DEVICE PORTFOLIO, WHILE TAILORED TO BE ABLE TO MEET THE REQUIREMENTS OF EACH OPERATOR"

CHAMPIONING CONSISTENCY ACROSS DIFFERENT ADVANCED SERVICES AND DEVICES

MAKING LIFE EASIER, LESS COMPLICATED AND LESS CONFUSING FOR CUSTOMERS

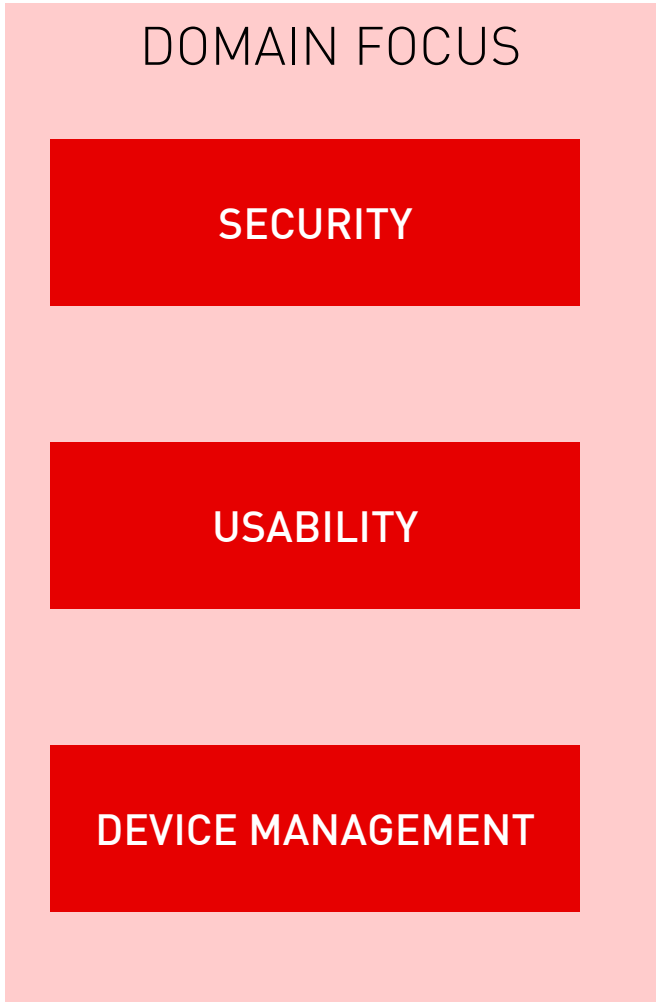
Our focus...



OMTP
OPEN MOBILE TERMINAL PLATFORM

Our focus

- Terminal-centric
- Customer driven
- Produce targeted Recommendation Documents:
  - Endorsed by ALL Operator Members
  - Not in conflict with primary Standards Bodies
  - Adds industry value
- Define functional equivalence not "bit exact" protocols and API's
- Platform Agnostic: encourage multiple solutions
- Use Case not Technology driven
- Requirement Defragmentation

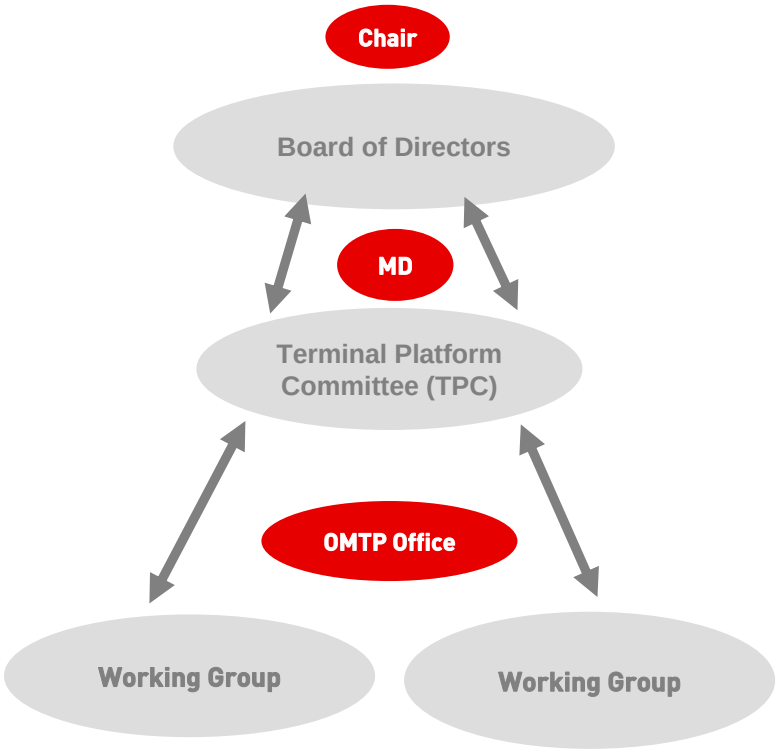


OMTP
OPEN MOBILE TERMINAL PLATFORM

What we are?

- Terminal Focused
- Time to Market Focused
- Not an SDO
- OMTP was created to complement SDOs:
  - Requirements based
  - Co-ordinated input
  - Multi SDO Liaison
- Look at 'Why?' and 'What?' first… then 'How?'
  - Always based on Use Cases
  - Not "bit exact" specifications
- Service Viability vs. Technical Interoperability

OMTP management structure



Board

- Provides strategic direction makes key business decisions
- Operator Members - not open to Vendors

TPC

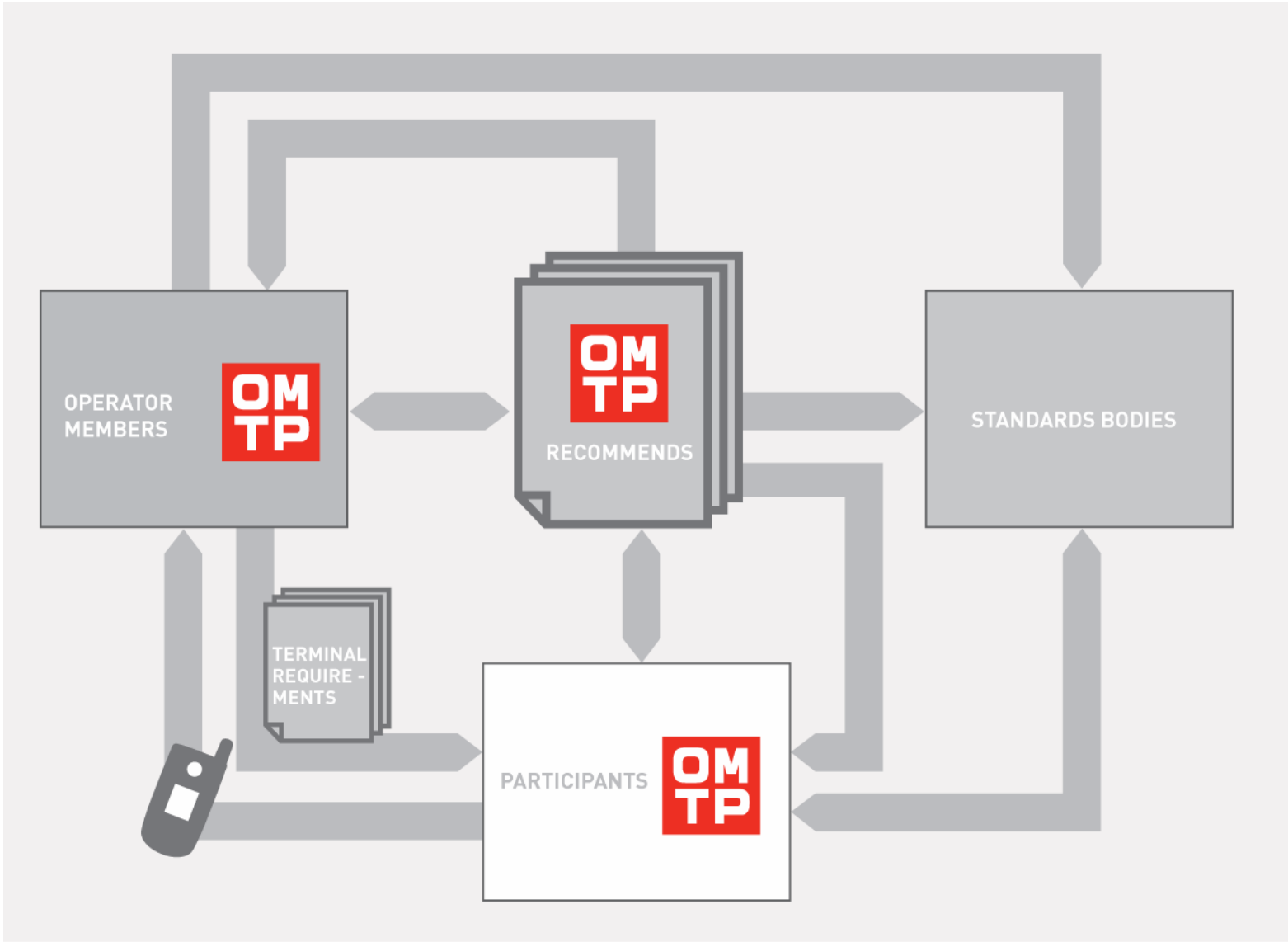
- Main executive function
- Operator Members and six Vendor representatives elected by OMTP Sponsors
- Advises/recommends to board
- Escalation route/arbitration for Working Groups

Working Groups

- Community of experts in a given area of OMTP focus
- Produce the Specifications

How OMTP operates

OMTP role

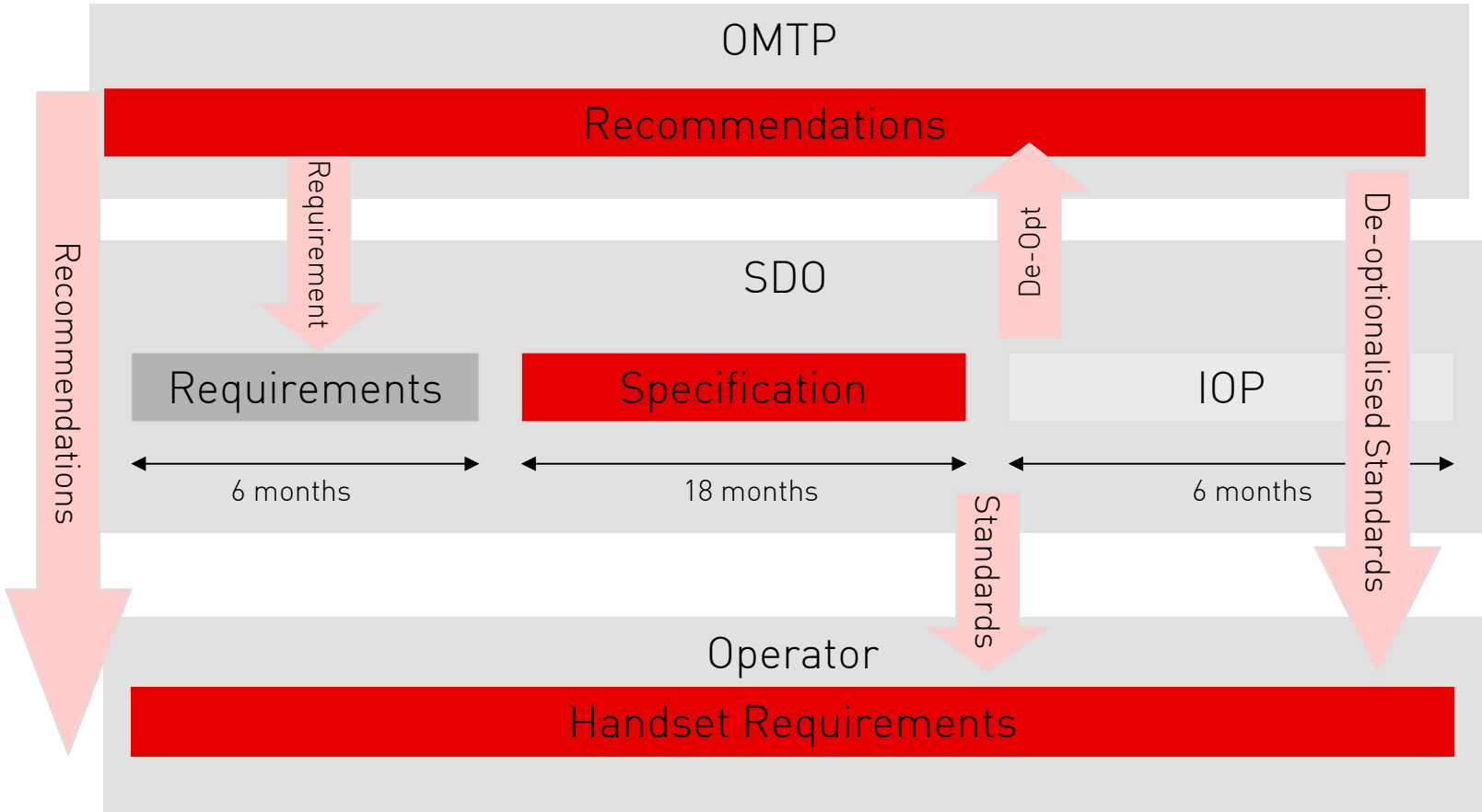


OPEN MOBILE TERMINAL PLATFORM

Level of detail

1	Use Cases, Business Drivers	Direction	OMTP
2	Functional Requirements, UE Requirements	Functional Equivalence	OMTP
3	Technical specifications	Theoretical Interoperability	Others
4	Interoperability Tests	Practical Interoperability	

Route to market



Overview of deliverables

COMPLETED IN 2006	COMPLETED IN 2007	IN PROGRESS/SCOPE
CUSTOMISATION ENABLER	DATA TRANSFER	RECOMMENDED PRACTICES FOR CONNECTED APPLICATIONS
BASIC TRUSTED ENVIRONMENT	LOCAL AUDIO CONNECTIVITY	INCIDENT HANDLING
JAVA WITH FOCUS ON CDC	IMS FRAMEWORK	ADVANCED DEVICE MANAGEMENT
SEAMLESS BROWSER	ADVANCED TRUSTED ENVIRONMENT	LOCAL DATA CONNECTIVITY
SIGNING SCHEME REQUIREMENTS	INSTANT MESSAGING	POSITIONING ENABLERS
UICC/USIM	VoIP DEVICE MANAGEMENT	LOCAL WIRELESS CONNECTIVITY
APPLICATION SECURITY FRAMEWORK		

OMTP OPEN MOBILE TERMINAL PLATFORM

EXPERT GROUPS

Software | User Experience | Security | Hardware

Resident Applications
Seamless Browser
Instant Messaging
VOIP
Data Transfer
Customisation
Application Security Framework
Downloaded or other post factory Application installations
Application Management
Certify
Test
Develop
Signing Scheme Requirements
App Mngnt
OMTP
OPEN MOBILE TERMINAL PLATFORM
Enablers
IMS
Device Management
Foundations
Codecs
Cameras
Displays
Trusted Env
Connectors
USIM
Dev Mngnt

Detail on past/present projects

Basic Trusted Environment - TR0

Problem Statement

- The problem of non-standardized security requirements and implementations results in:
  - High development costs and complexity for operators and manufacturers
  - Increased security risks - cost of abuse – cost of lack of trust

Scope

- To formalize the security needs of sensitive assets and enablers, such as
  - Debug Port protection
  - Secure Boot
  - Secure Binding and Secure Flash update
  - Mobile Device Id protection
  - SIM Lock protection
  - DRM application
  - General
- The document currently defines one security profile, TR0

Status Published March '06

Advanced Trusted Environment - TR1

Problem Statement

- As per TR0 – with scope increase

Scope

- Market Feedback
  - How existing hardware security platforms resist attack in the field
- New Areas
  - Inclusion of downloaded applications in boot time checks
  - Run time integrity checks of ME hardware and software
  - Secure USIM/UICC to ME and other involvement of USIM
  - Secure access to User Interface (i.e. keyboard, screen, touchpad, LED...)
  - Hardware security support for Device Management, service protection (e.g. Mobile TV) and mobile payments
  - Trusted execution environment (interpreter, hardware and middleware)
- Liaison
  - Global Platform Device specifications (GPD)
  - Trusted Computing Group (TCG) Mobile Phone Working Group (MPWG) specifications

Status 3 phases – 3rd phase to be published February '08

Application Security Framework (ASF)

Problem Statement

- Malware threatens usability and consumer trust, and consequently future operator revenues
- Lack of consistency in the security user experience is a potential barrier to uptake of new application based services

Scope

- Develop abuse cases detailing threats
- Develop application security framework to prevent applications from accessing particular functional capabilities when they have no need to do so.
- Develop recommendations for user experience and prompting to aid user understanding and allow users to informed decisions to control their security environment

Status Published February '07

Signing Scheme Requirements

Problem Statement

- For the application security framework to be useful, it is necessary to have schemes which can check developer identity and an application for possible malware. This process is not foolproof, but can significantly reduce the numbers of malware applications becoming freely available to subscribers if the schemes are well managed.

Scope

- The OMTP Application Security Working Group seeks to define a set of requirements for 3rd party signing schemes to meet, such that applications signed by these schemes can be considered as TRUSTED.
- These requirements to include items such as:
  - Authentication
  - Legal Assurance
  - Application Validation
  - Revocation
  - Key Management + Certificate Processing
  - General

Status Published October '06 & updated February '07

UICC/USIM

Problem Statement

- The different MEs have different support for the variety of features provided by the UICC.
- Also, the wide optional parts within UICC/(U)SIM related standards make the interoperability tests between ME and UICC/(U)SIM a huge and costly issue for the operators.

Scope

- To gather and de-fragment operator/technical requirements on UICC / USIM
- The task will address gap analysis towards ongoing standards in order to define the areas of enhancement related to UICC / USIM and ME support
- Includes
  - Application Protocol
  - Physical Interface
  - ISIM Configuration
  - Remote Management
  - Application Requirements
  - AT Commands/SAT Commands
  - UE Requirements

Status Published October '06

Data Transfer

Problem Statement

- Handsets do not offer a consistent experience for data backup and synchronization
  - Can form a barrier to handset upgrade
  - User dissatisfaction in case of lost and stolen phones

Scope

- Definition of common requirements for the supply, preservation, restoration, synchronization and transfer of a user's data throughout the lifecycle of a terminal.
  - Back-up and restoration of user's data
  - Transfer of data from old to new terminals
  - Synchronization of a user's personal data with a remote server or PC.

Status To be published September '07 (TBC)

Customisation

Problem Statement

- Operators need to extent their brand onto the UI of the handset in order to provide a compelling and differentiated experience to their customers (mainly subsidized handset)
- Current attempts at customization have proved enormously expensive, prone to error and inconsistently achievable across the handset portfolio

Scope

- Definition of UI elements and configuration parameters that can be customized, OTA provisioned and locked by operators
- Requirements for simple integration of operator services and applications, either via the idle screen or via the configuration of the cache for off-line operator services
- Customization to be enabled OTA, SIM card, removable storage

Status Published March '06

Device Management

Problem Statement

- Misconfiguration leads to:
  - Lack of service uptake
  - Poor user experience
  - Increased support costs

Scope

- Operators wish to be able to configure handsets in a consistent, easy and secure way post-sales.
- To define clear and agreed operator requirements for device management with particular attention to gap analysis with existing OMA DM work
  - Specifically de-optionalises OMA DM work to give a common base upon which operators can plan services

Status Published March '06

Codecs

Problem Statement

- Fragmentation within codec support across handsets, both
  - Creates interoperability problems with peer to peer messaging services , and/or places significant demand on server based transcoder services in order to enable
  - Creates significant overhead on client server content application which have to deal with each device type independently

Scope

- To define a fixed number of device classes which will in turn support pre-identified sets of codecs to maximized interoperability

Status Published July '05

Java with CDC focus

Problem Statement

- To assist operators in technology selection needed to create consistent looks and feel
- Reduce fragmentation in the Java space and prevent technology lock in, reduce cost and time to market for Java content

Scope

- Perform technology assessment on available Java UI technologies
- Identify Gaps and feed operator requirements to the appropriate JSRs

Status Published March '06

Seamless Browser

Problem Statement

- The lack of consistency in the manner in which the browser integrates with other application on the phone is a barrier to usage and a barrier to the development of truly useful and usable browser based applications

Scope

- To define both functional and User Experience requirements which will determine the minimal level of browser experience. Specifically this task is tiered at two level to address mass market an mid tier handsets over time.

Status Published March '06 & September '06

IMS Functional Requirements

Problem Statement

- If minimal IMS requirements are not defined this will lead to significant fragmentation in implementation, significantly hampering service development and successful service launch
- Further, if terminal requirements are not identified which address the functionality to distribute, provision and enable IMS compliant applications on the handset then there will be no route to easily and consistently launch the revenue driving IMS applications

Scope

- This task will define the minimal set of requirements for IMS functions on a mobile platform and define which of the functions shall be available for developing new IMS capable applications in the mobile terminal

Status Due to be published April '07

VOIP Device Management

Problem Statement

This task will ensure that terminal platforms have the capability to offer mobile operators the opportunity to uphold current business practice in the mobile ecosystem, at the same time as offering enhanced, easy-to-setup and easy-to-use customer experiences associated with the use of voice applications (VOIP) on wireless bearers, e.g. UMTS WIFI etc

Scope

- The task is to define requirements for a mechanism for controlling the VOIP settings in phones that are subsidized by the operators (to be enabled by the vendors depending on sales channel). It should be possible for the operator to allow trusted corporate or SME customer to manage the VOIP settings for the mobile phones of their employees.

Status Due to be published May '07

Local Connectivity

Problem Statement

- Reaching industry agreement on standard connectivity solutions - without restricting the freedom of innovation - would streamline the whole value chain and provide end users with a larger choice of peripherals including legacy home entertainment systems and PC equipment. This would also create a new market for peripheral vendors with no expertise in the mobile space which would clearly benefit the end users and support convergence related operator business cases such as operator delivery.

Scope

- This task references existing and approved industry standards to de-fragment local connectivity offering implemented by device manufacturing.
- The following use cases will be covered over three phases
  - Audio input and output e.g. headsets (April '07)
  - Charging and data connection (July '07)
  - Wireless connectivity (Autumn '07 TBC)

Status Due to be published from April '07

Instant Messaging

Problem Statement

Currently many operators are working with numerous terminal manufacturers and 3rd party vendors to ensure that there is a seeded market of capable devices to satisfy the basic IM requirement. These parallel activities are causing considerable deavelopment and supply congestion – many players are all asking for very similar solutions

Scope

- The task will address the issue of generic IM Client requirements ONLY. The goal of the task is to reference existing standards (IMPS1.2 & 1.3), remove specification ambiguities, ensure support for legacy messaging services, define service provisioning and subscription mechanisms and share best market practice.
- Specifically Phase 1 will address
  - Indication of legacy customers
  - Service provisioning mechanism

Status Due to be published April '07

Advanced Device Management

Problem Statement

If a user has a problem with their device, the first point of contact is generally with the operator. The operator offers the main customer services to users. Whether the problem has been caused by the users own actions on the device or by the installation of applications onto that device it is very important to be able to correct problems efficiently and effectively without the need for the customer to return the handset to the operator or a service centre. There will be significant cost savings in proactively monitoring the users' device and enabling capabilities which allow the operator to react quickly to customer problems (which may be complex and difficult to deal with in conversation with a user).

Scope

- Derive agreed use cases for the protection of the user from the problems described above
- Compare use cases with the capabilities in existing specifications and specifications under development
- Derive appropriate input into standards groups to enable the operator to substantially manage the agreed use cases
- Produce requirements for devices to enable operators to manage the agreed use cases
- Understand the needs of the virus protection, software firewall industries and of the developers of utility software.

Status

Due to be published February '08

Incident Handling

Problem Statement

Malware on devices has the capability of creating billing events for customers, spying on their personal information or simply vandalism. The mobile industry's duty of care means it is essential to develop mechanisms to identified malware, protect the customer from any ill-effects and communicate any required actions throughout the value chain. Existing work by the OMTP Application Security Framework team addresses requirements for devices and signing schemes; however, more needs to be done to ensure end-to-end handling in case where malicious applications have been installed.

Scope

This task will address the following issues:

- Who are the stakeholders across the industry, which processes are established to date and how can these be aligned?
- How to identify (precisely) a security vulnerability or malicious application (and anything it may have spawned)
- How to report potential issues to stakeholders
- How to "revoke" the application (both for signed and unsigned applications)
- How to correct vulnerabilities and manage security policies based upon threat levels
- How to patch bugs in existing devices and correct new software releases

Status

Due to be published February '08 (TBC)

Requirements for OMA DRM V2 Enabled Devices

Problem Statement

Operator and vendor alignment regarding the implementation of DRM shall be beneficial and vital to the whole mobile industry. Widespread adoption by mobile users, vendors and content providers can only be achieved by

- Ensuring functionality where this is not captured by the OMA DRM specifications (e.g. handling of error cases)
- Ensuring interoperability between terminals and terminals and servers to facilitate legal content sharing
- Ensuring usability. This should be as limited, user friendly and consistent as possible)

Scope

Includes:

- Download, installation, rendering and storage of protected content
- Content differentiation
- Forwarding or receiving protected content
- Security and revocation

Status Due to be published May '07

Recommended Practices for Connected Applications

Problem Statement

- Connected applications (such as push email) have already proven that they are a compelling mobile service and the market for Connected Applications has plenty of scope to grow.
- To enable the next tranche of Connected Applications, user experience barriers and infrastructure limitations need to be addressed

Scope

Define a common approach and recommendations for the design and configuration of Connected Application solutions for mobile terminals, including:

- Defining the priority areas of concern
- Recommendations on how Connected Applications should behave on mobile terminals
- Specification of a common approach with the configuration of a Connected Applications connection settings
- Specification of a mechanism to allow operator configuration of Connected Applications both prior to and post distribution (inc. OTA)

Status Due to be published July '07

Displays

Problem Statement

- Fragmentation within display support across handsets, both
  - Creates interoperability problems with peer to peer messaging services , and/or places significant demand on server based transcoder services in order to enable
  - Creates significant overhead on client server content application which have to deal with each device type independently

Scope

- To define a fixed number of device classes which will in turn support pre-identified sets of displays to maximized interoperability

Status Published June '05

Cameras

Problem Statement

- To increase and consolidate camera dependent service experience and reduce the cost and time to develop camera dependent applications.

Scope

- To define a fixed number of camera resolutions

Status Published June '05

Terminal Requirement Consolidation

Problem Statement

Operators current terminal requirements consistent of a significant proportion of non differentiating and largely identical requirements in terms of intent. The format, structure and wording of these requirements can be quite different. This adds significant unnecessary cost to the industry both from vendor and operator side

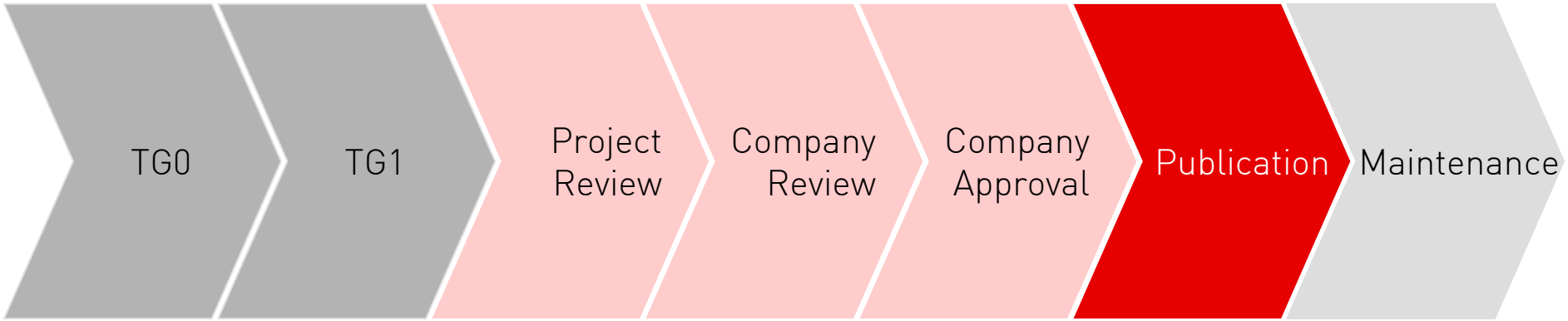
Scope

- By examining existing contributed “non-differentiating” requirements attempt to consolidate identifiers, format, structure and wording of requirements, across operators

Status DRM task being launched as a result of this work

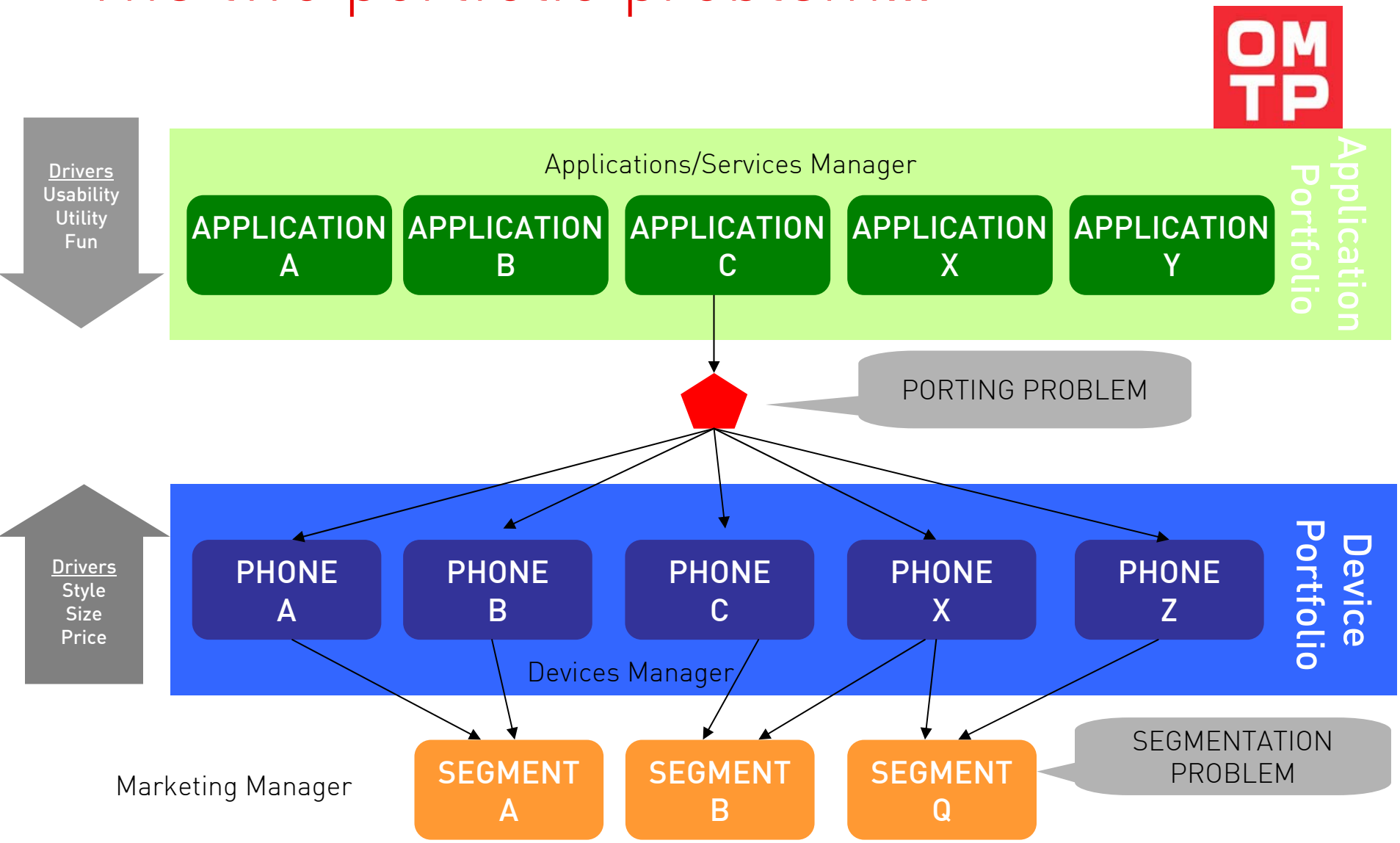
Backup slides

Document Lifecycle

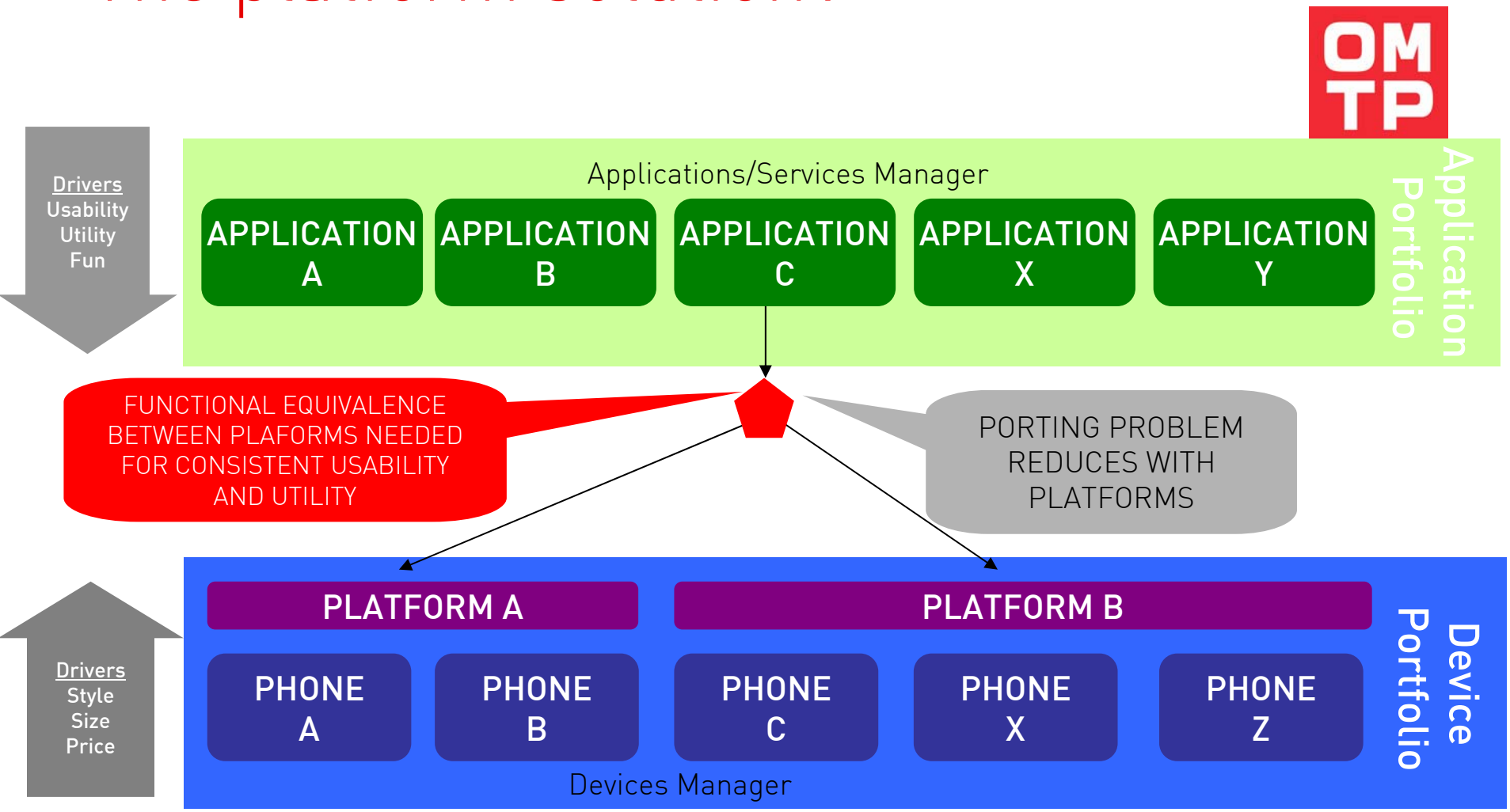


Another look at the problem

The two portfolio problem…



The platform solution?




OMTP
OPEN
MOBILE
TERMINAL
PLATFORM