Workplace as a Service (WPaaS) White Paper

January 2013

Creating a secure cloud services delivery framework that is needed to support Bring Your Own Device applications

By Enterprise Cloud Leadership Council

List of Figures and Tables

Executive Summary

Enterprises face a challenge in providing ways for employees to use Bring Your Own Device (BYOD). Current solutions provide a means for many companies to tie such devices to Virtualized Desktop Infrastructure (VDI). This approach, however, leaves both the device and the corporate desktop vulnerable to intrusions. A better approach is to create an ecosystem that treats the BYOD as vulnerable until it is approved by a multi-part sign-on procedure and that lends itself to embedding enterprise applications in a separate partition of a BYOD.

In the first part of the White Paper, we explain the forces driving large enterprises to view solutions to Workplace as a Service (WPaaS) as part of a larger effort to transform the enterprise, in particular, enterprise IT. Enterprises view BYOD as a way to:

1. Reduce costs by altering the use of software, computing resources, and staff.
2. Use BYOD solutions provide new ways to support important customer groups.
3. These solutions are innovative because they transfer legacy and new apps to iPads and other intelligent devices, making applications more ubiquitous and easier to use as well as contributing to cost reductions.

The second part of the White Paper explores what enterprise applications need in order to be WPaaS enabled. It identifies the requirements, i.e., what needs to be included in the systems that large firms want to implement to solve the BYOD challenge. For the most part, these firms need a flexible, secure, cloud services delivery framework for edge applications. The solution described here delivers end-user computing, communications and collaboration capabilities. We call that set of world-class services WPaaS.

The final part of the White Paper explores WPaaS architectures, implementations and APIs.

This White Paper offers an innovative conceptual approach to WPaaS. This is built upon a reference architecture that facilitates interacting with and providing access to legacy and new applications on a mobile device. Through a shell on the mobile, users can navigate through older generation as well as new generation applications, creating needed reports and information for users, accessing web sites, and connecting to enterprise data centers. In the case of UBS, a legacy wealth management application on a mobile device lets account representatives present recent results and performance, create graphs or spreadsheets that can be provided to investors and their financial advisors, and transmit data and graphical results to investors and their advisors. It also provides control technology from the device through to the enterprise data center. The overall approach creates a more trusted environment on the mobile device since data are wiped off the device once any interaction with data is complete. In addition, geo-positioning data and identification and authorization through an enterprise data center add to the trusted nature of the solution.

This WPaaS solution merges cloud computing, big data and mobility. It creates an IT computing environment that uses service brokers with a wide range of applications and an accompanying consumption model. This is important because the solution can be vendor neutral, i.e., the hope is that a number of different vendors' products can be swapped in and out of the solution. The solution leverages applications as a service, a characteristic that clearly differentiates it from virtual desktop infrastructure (VDI) which is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server.

In addition, this WPaaS solution points to an ecosystem where any channel, offering a set of applications and data sources, can be accessed by any device. It uses Open Source business elements and is highly scalable. It is inherently secure and works on any HTML 5 device.

This White Paper's Reference Architecture defines ways to incorporate contributions from different vendors and developers in the basic WPaaS model. The Reference Architecture provides a way for vendors to provide alternative solutions that achieve the same end goals and performance. It serves as a plan for further development and elaboration of the main design. In addition, it points the way to the future evolution of the current approach.

The White Paper also identifies a series of application protocol interfaces (APIs) that provide for a wide range of functions in the WPaaS, from Authentication and Authorization to Resource Management. Once these APIs have been developed and/or contributed, they will broaden the TM Forum's Frameworx model for the enterprise and communications.

In addition, Workplace as a Service (WPaaS), Compute Infrastructure as a Service (CIaaS) and Virtual Private Cloud (VPC), when linked together, serve as reference architectures that can potentially meet the unique needs of enterprise-grade customers. Enterprise customers have a greater need to place legacy applications on mobile devices and have them interact with newer applications, such as Outlook and Windows applications. They also require a higher level of security than many applications providers. The broad outlines of this are described in the Reference Architecture at the end of this White Paper. A fully implemented VPC implies WPaaS and CIaaS development for enterprise-grade operations, where "enterprise-grade" is the ability to deploy business critical services that match or exceed the level of security, quality, reliability, and availability found in internal corporate data centers.

The TM Forum's Enterprise Cloud Leadership Council envisions this White Paper as a vehicle to explain the value of WPaaS.

1. BYOD and Creating Applications as a Service for the Enterprise

This White Paper presents a new vision for IT infrastructure that centers on applications as a service for BYOD (Bring Your Own Device) solutions. A ubiquitous consumption model obtains a wide range of applications from service brokers. WPaaS enterprises take a completely different approach to supporting their mobile workforce, for improved performance, efficiency, and security. Furthermore, as this White Paper highlights in its example implementations and reference architecture, enterprises now have access to a wide range of novel applications never feasible before the advent of WPaaS.

Big data, cloud computing and mobile applications are combined for a BYOD solution that is significantly different than the VDI solutions most vendors offer today. A primary benefit for the enterprise is that the solution is vendor neutral, so applications can be swapped in or out to provide functionality needed to support business users. For instance, an investment bank can use this framework to put wealth management applications on an iPad, while a pharmaceutical firm might run analytic programs for molecular structure from an IPAD with the same architecture.

In addition to employing different applications, the WPaaS BYOD solution with applications in the cloud provides ways for enterprises to establish a detailed, multi-layered approach to security. This means that the WPaaS solution discussed here is a more secure, flexible and fully functional approach to bringing mobility into the enterprise.

This White Paper explains why this approach is important to the TM Forum’s Enterprise Cloud Leadership Council (ECLC), and its members. It draws upon several “best of breed” approaches to IT transformations, some of which highlight innovations from TM Forum members and present a high level conceptual argument about why enterprise users prefer the approach outlined here.

1.1. The Enterprise Cloud Leadership Council’s Workplace as a Service Approach

The ECLC has proposed a new approach to WPaaS as is described in this White Paper. It differs from the traditional VDI approach in the following ways:

1. A cloud operating model stands at the center of enterprise IT. It must have an architecture that is based on an Open Source architecture that can be modified and altered as new products become available to support this solution. This condition is required in order for the ecosystem to support legacy and new applications for BYOD users. In this cloud operating model, the enterprise relies upon a service broker that it runs or that an external entity operates. The service broker offers a wide range of applications and permits different patterns of consumption.

This model integrates cloud computing, big data and mobility.

2. BYOD devices must be secured and partitioned to access sufficient information for legacy and new types of applications that run in a cloud ecosystem. The applications they carry should be seamlessly connected to enterprise data centers that are part of such a cloud ecosystem that provide the data for the BYOD. For security reasons, the BYOD is wiped clean of any data after every transaction, so that there is no data lost if the BYOD is stolen.

1.2. Workplace as a Service is Part of Workplace Transformation

The WPaaS project is part of an extensive transformation in the use of information technology (IT) that will create a mobile workforce.

The key change in the move to cloud computing is that enterprise or corporate resources are delivered as standardized services. As a consequence, IT is no longer a provider of services to the enterprise. It is extended by a cloud services provider that delivers a wide range of applications as a service.

Under this new regime, success is measured by the business value that each IT service delivers.

The WPaaS project has several aspects:

- It is “challenging the traditional notion of a "desktop" and the delivery of productivity applications to end users…
- Exploring the potential cost savings and agility of "as-a-service operating models".
- Incorporating the need to accommodate both new and legacy applications, and the proliferation of new devices into the enterprise.”[1]

1.2.1. Workplace as a Service and Workplace Transformation: The Commonwealth Bank of Australia Case

Commonwealth Bank of Australia has large-scale, private, cloud architecture. Its IT group is using it to deliver everything-as-a-service (see Figure 1). As part of this transformation, it has virtualized existing resources, developed a standard set of well-defined IT services based on those resources, and made these services portable. The mobilized services can be run from the most cost-effective location, either in-house or at a managed-services provider in the public cloud.

[1] Tim Whiteley, “Leveraging the Cloud to Drive Standardisation in the Enterprise,” presentation at Cloud Computing Forum 2012, Canberra, Australia, 22 February 2012, p. 11. http://www.cloudforum.com.au/presentations/2012

The bank has become a cloud service integrator. The IT team defines services and decides the performance requirements they should meet. It also maintains end-to-end service management and orchestration functions.

Vendors are now invited to compete to provide these services. To comply, vendors had to adjust their own commercial terms to meet the bank's business requirements, not the other way around.

BYOD extends this approach to create a refined way to further transform the relationship of IT vendors to enterprises. It builds upon the same core tenets that CBA identified in its IT transformation efforts.

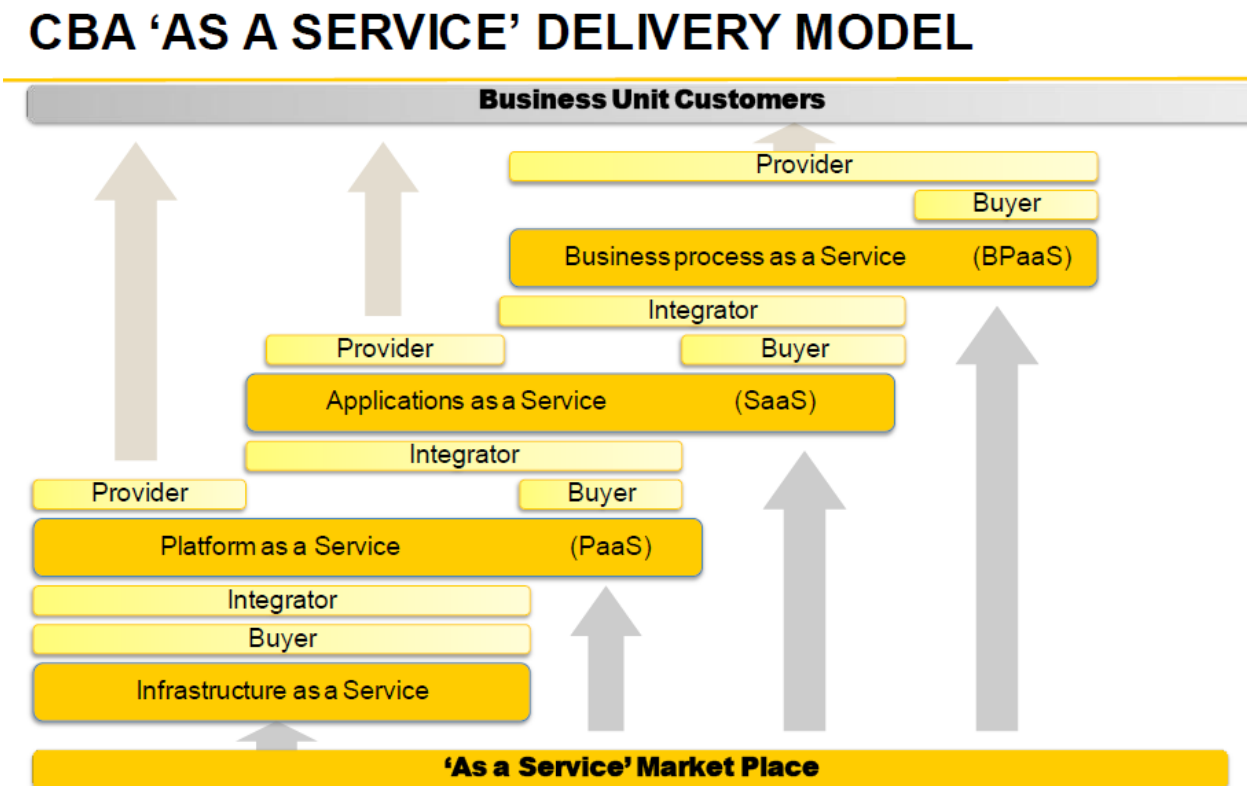

CBA 'AS A SERVICE' DELIVERY MODEL
Business Unit Customers
Provider
Buyer
Business process as a Service (BPaaS)
Integrator
Provider
Buyer
Applications as a Service (SaaS)
Integrator
Provider
Buyer
Platform as a Service (PaaS)
Integrator
Buyer
Infrastructure as a Service
'As a Service' Market Place

Figure 1: The CBA 'As a Service' Delivery Model

1.2.2. Core Tenets of the CBA Transformation

CBA built a cloud operating model and reference architecture to align with six core tenets, the fundamental principles that underpin its everything-as-a-service vision:

- Pay-as-you-go. Business customers only pay for products and services actually used on a metered, chargeback basis under flexible service agreements, as opposed to fixed-term contracts.

- Contestability. Every IT service is offered for bid to multiple vendors (internal or external) to encourage competitive pricing and eliminate lock-in to any one exclusive provider.
- On demand. Requests for IT services should be delivered immediately as requested, supported by real-time processing to cut the time required to begin the fulfillment process.
- Automation. Business customers must be able to request services from a catalog via self-service interfaces. Fulfillment is then executed by governance policies, fully automated approvals, and on-demand provisioning processes.
- Standardization. The IT organization defines and enforces the use of a set of standard services articulated in a comprehensive service catalog to encourage reuse and cost predictability.
- Workload portability. IT services are designed to be fully portable between infrastructures and vendors, letting the bank easily move workloads to the most cost-effective location.

1.2.3. Best Practices

In order to implement the core tenets and ensure the persistence of their benefits, a holistic approach involving people and processes was used. The team built the organization and processes required to deliver infrastructure-as-a-service (IaaS) first, then went to work transforming the existing IT infrastructure to support the new capabilities. Four years in, several best practices have emerged:

- Strong leadership eases the transition to a service-led organization. Drive organizational change from the top down, but develop clear cloud service quality objectives and metrics to motivate changes to improve performance.

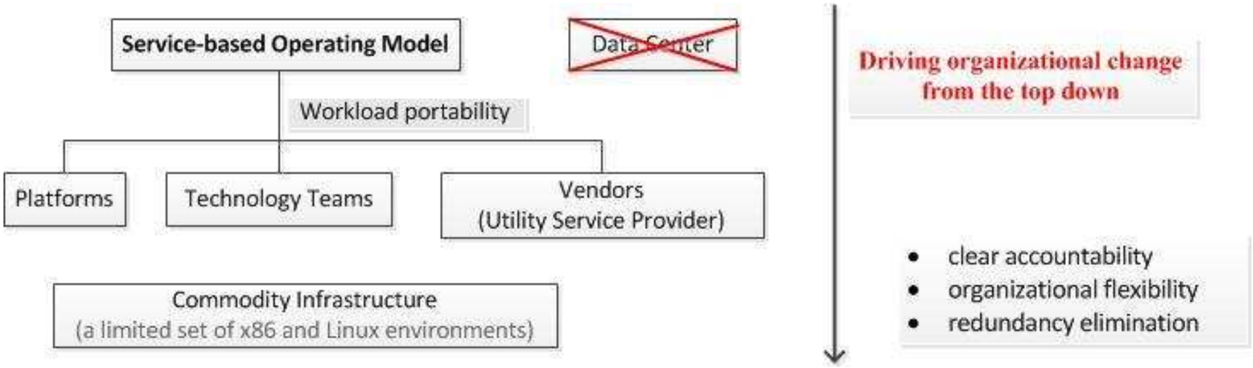
Traditional IT organizations are typically structured around technology silos, special skills, or team allocated to specific business units. Service-led organizations use a leaner and more efficient infrastructure technology and operations (IT&O) team.

- Get your cloud service catalog and operations processes in place first. Build a holistic cloud operating model first. Look holistically at processes and elevate IT resources to strategic assets.

The bank developed a target state automation model which included the service catalog, billing and recharge, orchestration, and provisioning and governance domains. Enforce standardization to take advantage of cloud economics. Build and own your own processes, and focus energy on standardization. Cloud economics work best with a limited set of well-defined services, and this becomes more difficult the further you move up the stack from IaaS to providing higher-order IT services such as (development) platforms- and databases-as-a-service (PaaS and DBaaS).

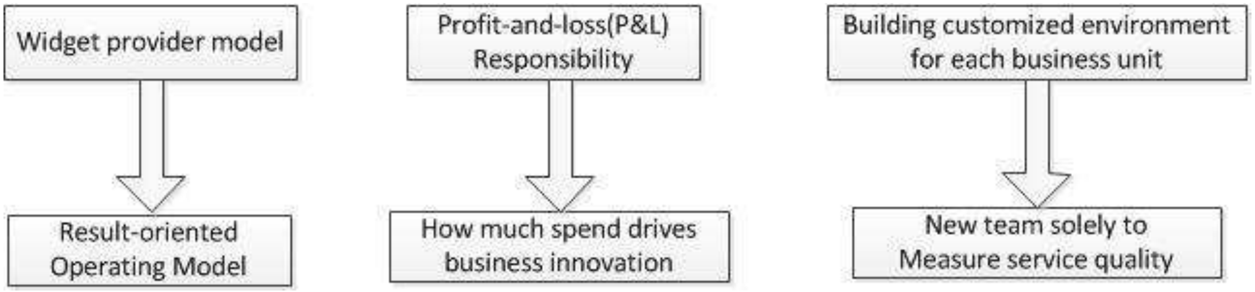
- Define clear vendor roles and implement policy-based governance.

The goal was to transition from high-cost, low-flexibility agreements into arrangements on the bank's as-a-service terms (short term, no exit fees, low transition costs) with vendors that understood that they would have to compete regularly to continue to provide IT services.


Service-based Operating Model
~~Data Center~~
Workload portability
Platforms
Technology Teams
Vendors
(Utility Service Provider)
Commodity Infrastructure
(a limited set of x86 and Linux environments)
Driving organizational change from the top down
clear accountability
organizational flexibility
redundancy elimination

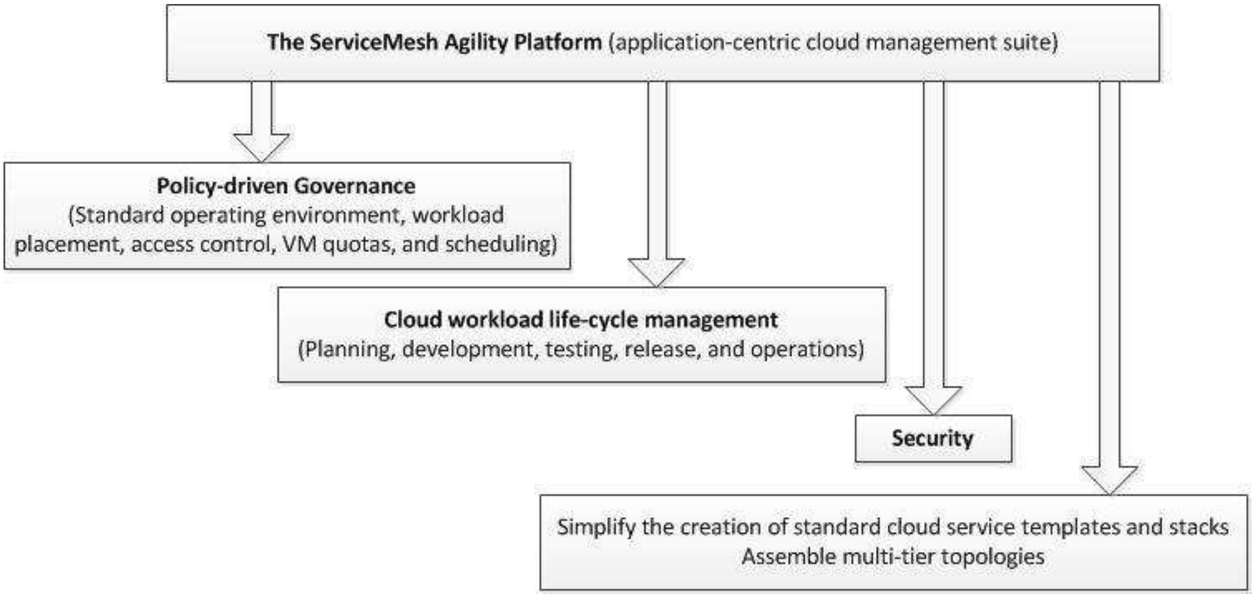
Instead of building custom systems for each business unit, cloud services are horizontally integrated. Service quality is measured against a results oriented model.

Figure 2: Driving Organizational Change from the Top Down


Widget provider model
Result-oriented Operating Model
Profit-and-loss(P&L) Responsibility
How much spend drives business innovation
Building customized environment for each business unit
New team solely to Measure service quality

(Source: Commonwealth Bank of Australia)

Figure 3: Developing clear cloud service quality objectives and metrics


The ServiceMesh Agility Platform (application-centric cloud management suite)
Policy-driven Governance (Standard operating environment, workload placement, access control, VM quotas, and scheduling)
Cloud workload life-cycle management (Planning, development, testing, release, and operations)
Security
Simplify the creation of standard cloud service templates and stacks
Assemble multi-tier topologies

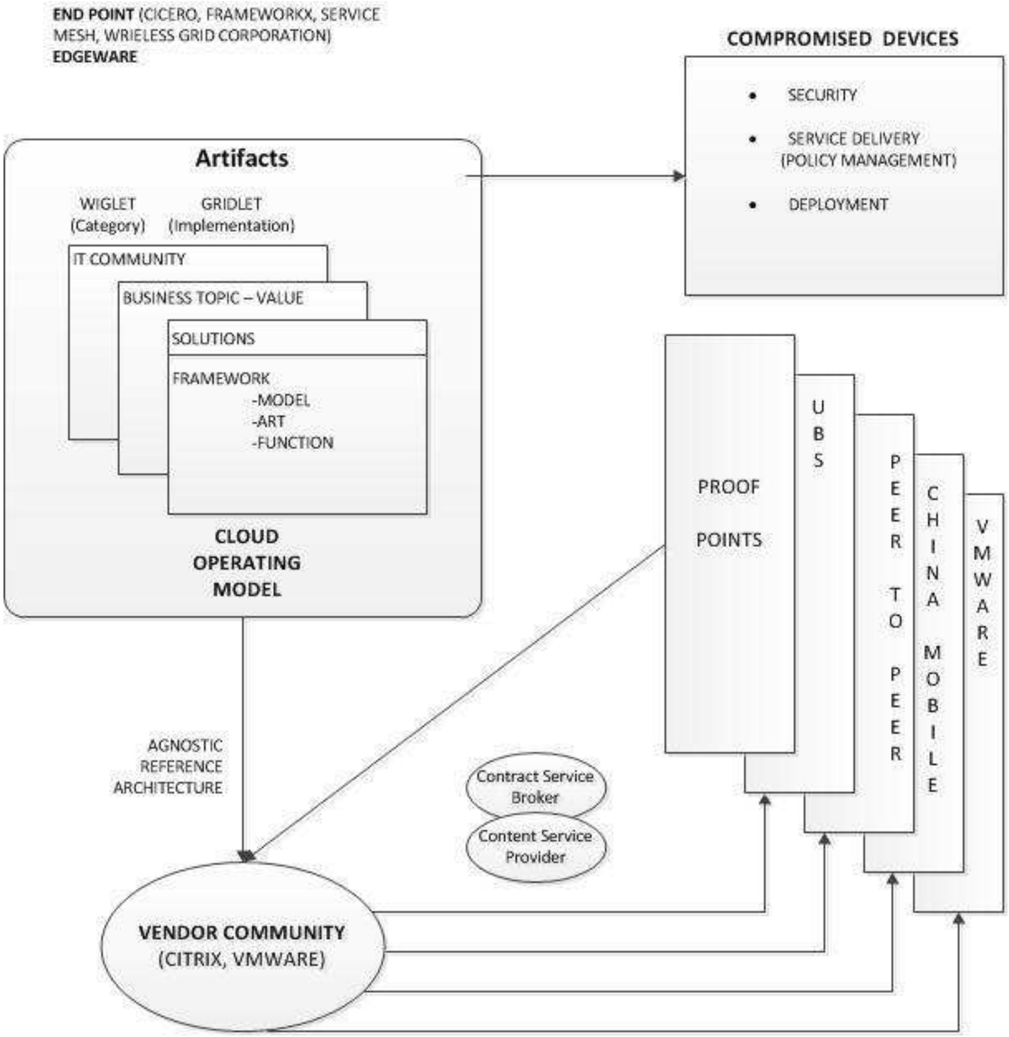
(Source: ServiceMesh)

Figure 4: Develop clear cloud service quality objectives and metrics

1.3. Implementing the ECLC Vision of WPaaS

TM Forum's Enterprise Cloud Leadership Council decided to describe its WPaaS vision (see Figure 5). The vendor and user names in the figure illustrate the role of different parties in using a cloud operating model to create ways of proving why a new approach to WPaaS and BYOD is needed. The ECLC is implementing a series of "proof points" to validate the idea that a cloud operating model can be linked to compromised, insecure, mobile devices once features to support security, service delivery, and deployment are added.

Once they are added, "proof points" from different users and vendors can show vendors how they can proceed to replicate these approaches in a commercial product.



(Source: TM Forum, Enterprise Cloud Leadership Council, Workshop at TM Forum Action Week, July 17, 2012.)

Figure 5: WPaaS Vision Implementation: TM Forum Management World Americas, Orlando, Dec. 3-6, 2012

Edge devices such as iPADs may always be in the Grid, or Enterprise and Service Broker network. Therefore, they are always available to monitor and authenticate specific applications and services that run in the Cloud. Cloud Services may then extend well beyond the physical boundaries of a Cloud. They can interact with confidence with known and trusted users, devices, resources, and applications. For sensitive financial services such as wealth management, this capability of ensuring that an iPad is a known resource in the virtual grid and is independent of the specific application running on it, can add several additional degrees of security and confidence. This is helpful when the iPad can authorize large financial purchases that need to operate across heterogeneous edge devices.

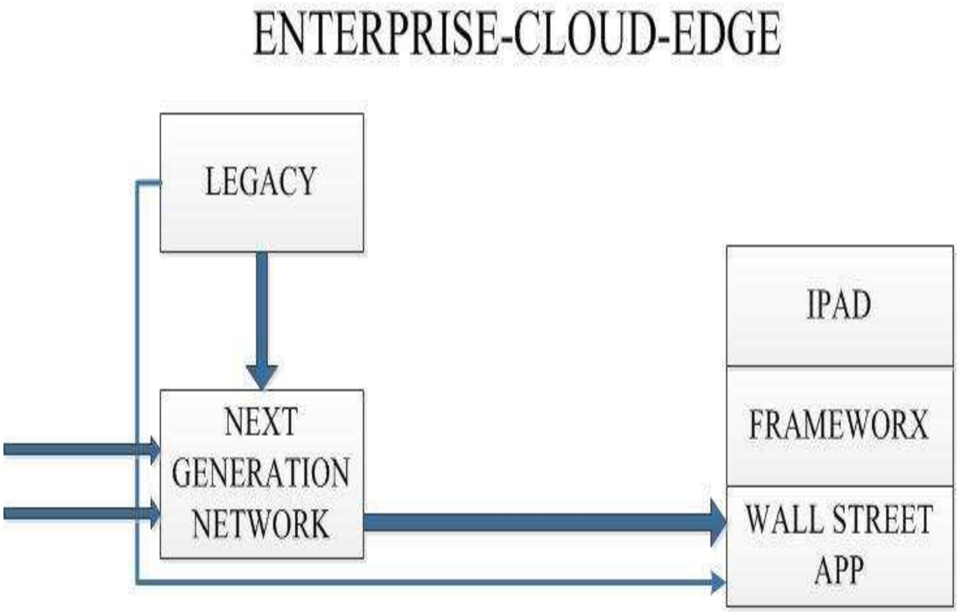


Figure 6: WPaaS Architecture to Unite the Cloud with Edge Resources

2. The Enterprise Cloud Leadership Council's Assumptions and Principles Concerning Workplace as a Service: A Summary

Key assumptions:

1) Legacy lives where there is business rationale and value

2) All devices (glass and Non Person Entities (NPE)) are compromised[2]

3) All workloads need to be as secure as possible[3]

Seven WPaaS Principles:

1) Employees are consumers and producers of WPaaS.

2) Employee-owned devices are first class citizens in our environments.

3) Native capabilities of mobile and new form factor devices should simplify the user experience while maintaining consistent functionality.

4) Identities (both human and Non Person Entities (NPE): machine to machine, sensors, agents, applications, content, etc.) need levels of access to our applications and data.

5) Collaboration and unified communications need to extend across flexible work patterns, loosely-connected virtual teams, and increasingly diverse combinations of customers, partners, contractors, consultants and NPEs. We provide a wide range of ways for employees and customers to collaborate. We expect that users will be able to choose and move between collaboration tools as their immediate needs for collaboration change.

6) Data held internally and externally will be classified according to risk and accessed based on context.

7) Open standards and APIs are the enabler of our WPaaS vision.

[2] Regarded as insecure unless their status is secured by various measures taken by the enterprise to secure them.

[3] All data used on the device is expunged after use, so the device never carries any sensitive data except when interacting with a client. The main data is kept in enterprise repositories.

2.1. The Enterprise Cloud Leadership Council's Assumptions and Principles Concerning Workplace as a Service: Details

2.1.1. Key Assumptions

1) Legacy lives where there is business rationale and value

   Legacy systems are valuable assets and knowledge repositories, to be utilized by our employees when there is business rationale. Therefore, future services and systems must easily and transparently bring these assets to our employees and customers, anytime, anywhere.

2) All devices (glass and Non Person Entities (NPE)) are compromised

   The range of security threats to our systems and our employees' devices is long and daily getting longer. Therefore, it is best to assume all devices (whether glass and Non Person Entities (NPE)) are compromised, and deliver trusted applications and services even in that user environment.

3) All workloads need to be as secure as possible

   Based on assumption 2) above, all workflows and processes will be designed with attention to risk assessment and cost-effective risk management. Applications and data must be as secure as they need to be.

2.1.2. Seven WPaaS Principles

The seven principles that define and guide WPaaS service oriented architecture are discussed in greater detail below.

1. **Employees are consumers and producers of WPaaS:**

   - Our employees should be able to choose the services that most improve their productivity.

   - We should enable and encourage the consumption of an increasing spectrum of third-party services as components of WPaaS.

   - We will enforce or restrict components of WPaaS where third-party services do not meet specific security, regulatory or governance requirements.

- We should only engineer components of WPaaS where there is a tangible user or business benefit in integrating one service with another or with our legacy systems.

- We should only engineer world-class services that our employees will want to consume.

  Given a wide variety of legacy systems within and across our enterprises, we anticipate unlocking tremendous value for our firms and customers through WPaaS. User benefits should be readily apparent as well. All WPaaS service offerings must be above a critical world-class services bar, for the term to have meaning and market value. Our own employees are the best judges of which of those above the bar service offerings meet their needs.

  Advances in network architecture and proliferation of bandwidth are driving our rethinking and redesign of the way applications and services are delivered. Until now applications have been bundles loaded on PCs, individual servers, and websites.

  Sensor networks and nodes are growing rapidly. They are capable of relaying information about their environment, to support business needs. Machine to machine communication across a variety of Non-Person Entities is already occurring within our enterprises. Applying Cloud principles to these new power-constrained devices can greatly enhance their capabilities through ad-hoc aggregation of available resources, where network links between nodes are based on physical proximity and dynamic network configurations at any given point in time. Furthermore there are opportunities to make a wider array of services available to mobile devices and the advanced data gathering abilities of sensor networks available to the wider enterprise. This vision raises significant challenges not the least of which is ensuring that the networks are trustworthy despite the limited capabilities, in both processing and battery power of mobile devices. When cloud services, grid computing and wireless networking are combined, trustworthiness and feasibility challenges increase exponentially. However, the integration of these wireless devices into Enterprise Clouds result in benefits with increased resources extensibility such as increased network bandwidth and demand for new and better ways for computation. Crucially, continuing to benefit from our legacy IT investments is also greatly enhanced by following WPaaS principles.

  Challenges include resource discovery and sharing in dynamic ad-hoc cloud environments, power and bandwidth management for power constrained devices, mobile user interface design, business models, and critically for our businesses, policy infrastructure.

2. Employees' Devices are Citizens in Our WPaaS Environments

- Secure and managed channels for accessing enterprise applications and data should be provided for these devices.

- Application and data access should depend on trusted connections and context rather than trusted networks or trusted endpoints (in contrast to prior paradigm).

- Solutions that enable non-intrusive, secure connectivity between employee-owned devices and our environments will be broadly deployed.

Scalability is critical especially for collaboration in large enterprise workplaces. Wireless grids edgeware represents a collection of sub-systems that comprises an infrastructure upon which "Grid-enabled" applications for the Workplace as a Service can be built. At the "core" of the edgeware resides a substantial library of intellectual property that enables the wireless grid. Open interfaces and specifications can provide support for an array of new industry standards as well as for open APIs and WPaaS-compliant freeware.

The ultimate vision of the ECLC Workplace as a Service is development of an adaptive enterprise cloud services offering secure, inexpensive, and coordinated real-time access to dynamic, heterogeneous resources, potentially traversing geographic, political and cultural boundaries but still able to maintain the desirable characteristics of a simple distributed system, such as stability, transparency, scalability and flexibility including for our employees mobile devices.

3. WPaaS leverages its citizens' native capabilities

- We want our suppliers to build applications and services that take advantage of new device capabilities.

- We also have a need for solutions to support our legacy platforms.

Different network architectures for WPaaS should be evaluated in order to identify the optimal levels of uninterrupted transmission of data and services, security and privacy, cryptographic primitives and protocols for authentication, digital signatures, anonymous payments, and micropayments. In addition, network architectures need to be evaluated for the usual tradeoffs between efficiency, security, robustness, collection of data that may make the grid more useful or efficient, and protection of the privacy of users.

4. WPaaS Identities

- Externally managed identities are valid for certain levels of collaboration and communications within the enterprise.

- Externally managed identities include known and unknown aliases of our own employees as well as the identities of customers, partners, suppliers and vendors.

- Third-party services and applications that enable federation with corporate identity through authentication and integration standards will have the deepest and broadest penetration into our environments.

Both human and Non Person Entities (NPE): machine to machine, sensors, agents, applications, content, etc. need levels of access to our applications and data. Because the boundaries of the physical organization become ephemeral, organizations built around distributed computing or working in a distributed computing environment exist virtually [Foster, Kesselman, and Teuke, 2001]. Business partners can be incorporated into a virtual organization at will; users of like interests can form into their own virtual organizations. The mobility of small, wireless devices creates tremendous opportunities to grow the diversity of devices and users that utilize the grid, and enhance the services available on the grid. These mobile devices have very different constraints than typical grid servers and clients. Their communication and computation abilities are limited because of power constraints, small screen real estate, and the transitive nature of their connection to network infrastructures. Once integrated into the grid, we expect that this new generation of small, mobile devices will enhance the benefits of belonging to a virtual organization.

5. WPaaS provides maximum service capability and flexibility for virtual teams, and Non-Person Entities

- Collaboration and unified communications need to extend across flexible work patterns, loosely-connected virtual teams, and increasingly diverse combinations of customers, partners, contractors, consultants and NPEs.

- We provide a wide range of ways for employees and customers to collaborate. We expect that users will be able to choose and move between collaboration tools as their immediate needs for collaboration change.

    - Collaboration and communication services should allow flexible movement between services while maintaining context such as participants, artifacts, media and their interactions.

- Collaboration and communication services should be fully functional across mobile and new form factor devices and based on trusted connections and context.

- Collaboration and communication services need to intelligently extend across unmanaged identities and/or devices to enable rich collaboration and communication channels between employees, customers, partners, suppliers and BPI systems.

- Systems that enable integration with our collaboration & communication services will have the deepest and broadest penetration into our environments.

6. **WPaaS classifies data appropriately and provides protections at all levels**

   - Classifications of internal and external data stores should be provided based on risk and access levels.

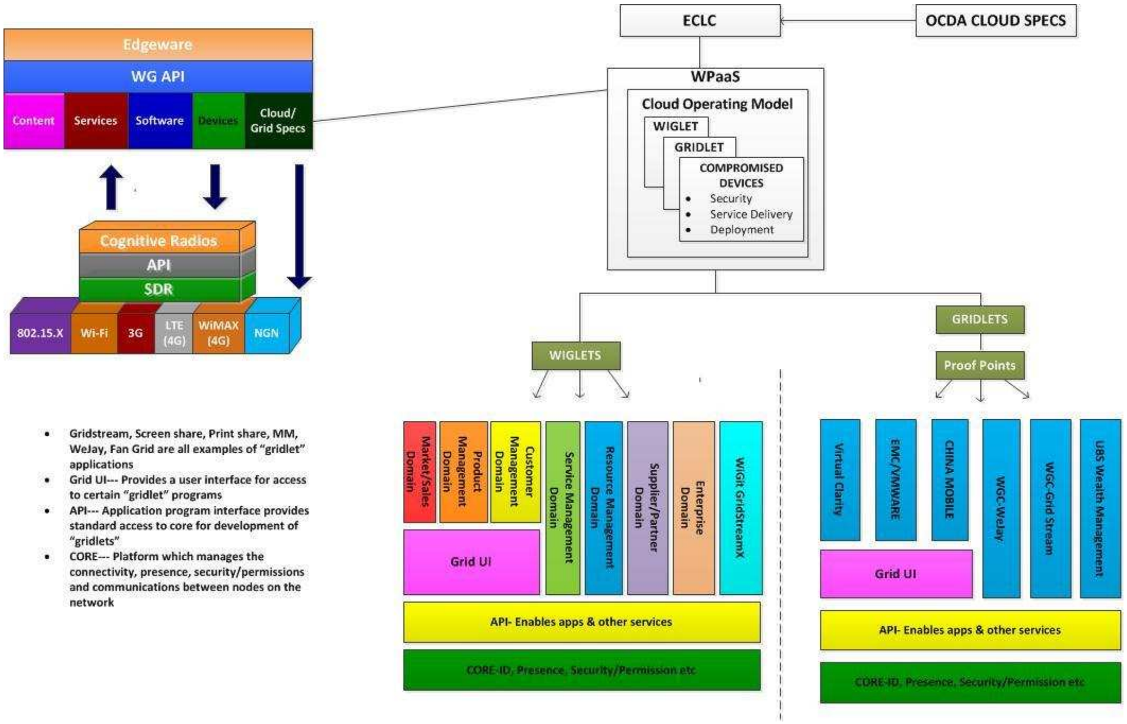
   - Access to classified data stores should be evaluated at connection- or run-time and based on identity, location, device and other context parameters.

   - Data will be made available to user applications transparently, to the user, providing the above requirements are met. The user should not need to understand where data is stored

Under emerging wireless grid architectures, network-based security models are far from adequate. These new systems will be about net-centric information sharing and collaborating business functionality which will become service-enabled and exposed to external wireless clients via standard web services type protocols. These wireless clients, which themselves may be applications, will dynamically discover services and make real time use of their code and data. Their services will be inherently location independent, not necessarily bound to a physical location, which can change over time as services are relocated or for fail-over reasons. Since wireless grid clients and service providers may belong to different physical networks or even different service providers, these networks and/or organizations may be governed by entirely different security policies.

Therefore, in a wireless cloud environment, organizations will need to shift their focus from perimeter-based security models to a service-level view of security. Emphasis should be placed on network identities, trust, and authorization of both users and applications rather than on ownership and control.

Figure 7 represents an architectural model of a wireless cloud computing environment. Research has identified the wireless cloud as a natural extension of the wireless grid. It provides seamless access to the internet, networked devices and computing capabilities. (Brooks, Robinson, McKnight, 2012)



- Gridstream, Screen share, Print share, MM, WeJay, Fan Grid are all examples of "gridlet" applications
- Grid UI--- Provides a user interface for access to certain "gridlet" programs
- API--- Application program interface provides standard access to core for development of "gridlets"
- CORE--- Platform which manages the connectivity, presence, security/permissions and communications between nodes on the network

(Source: McKnight, ed. WiGiT v0.2 in process.)

Figure 7: An Open Edgeware-Enabled Approach to WPaaS

7. WPaaS is enabled by open standards and APIs

- Application and Service Providers must provide API access to their application stacks to enable integration with applications, services and data hosted by other providers or internally.

- Open standards for identity management, collaboration and communications services enable us to integrate components of WPaaS.

- Applications and services with rich APIs and based on open standards will have the greatest penetration into our environments.

Transforming an enterprise's business processes to services using standards-based communication protocols opens new avenues to strategic partnerships with suppliers, partners, and customers. In turn, a new business model emerges based on re-bundling intra- and inter-enterprise business processes as seamless services.

A service-based approach to system design allows existing and proven legacy system functions to be encapsulated as services on a new standards-based integration platform. The services can encapsulate single functions or combine and integrate several smaller services that represent legacy functions on diverse hardware and software platforms.

Over time, developed services become an organization’s core asset — a library of tested, ready-to-use, compatible components. This potentially reduces the time to pull well-tested functionality together to meet new market needs. Potential reductions in development and testing costs can increase service modularity and potential reuse. In addition to offering cost efficiencies, reusing existing components also reduces risk by limiting the introduction of new potential points of failure. (H. Luthria and F.A. Rabhi, 2012)

3. Reference Architecture

ECLC is recommending the Reference Architecture developed by Visual Clarity (Figure 9 below) as a basic WPaaS reference architecture. It identifies the key components of the WPaaS environment. The reference architecture can enable and support diverse applications and uses in mobile clouds. Following this, the paper discusses the APIs used for WPaaS and compares several reference architectures.

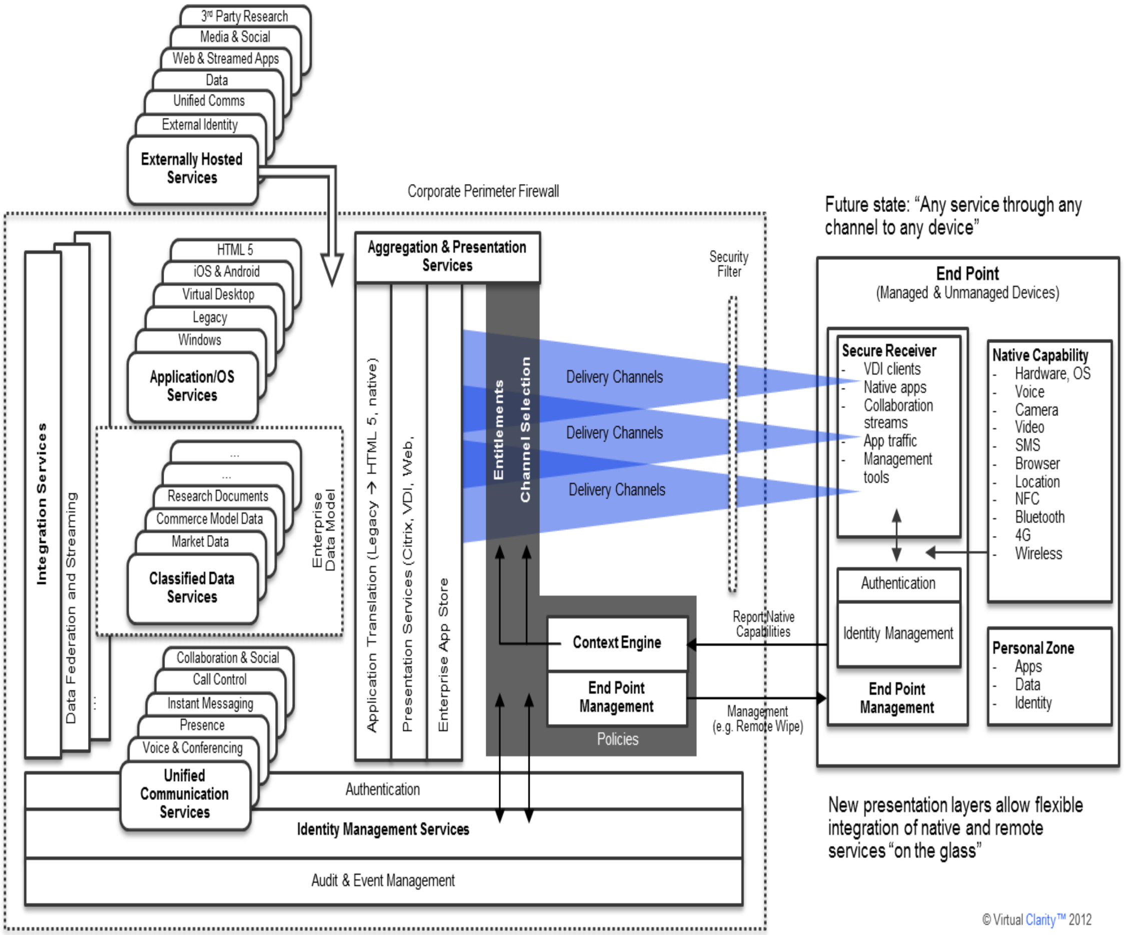
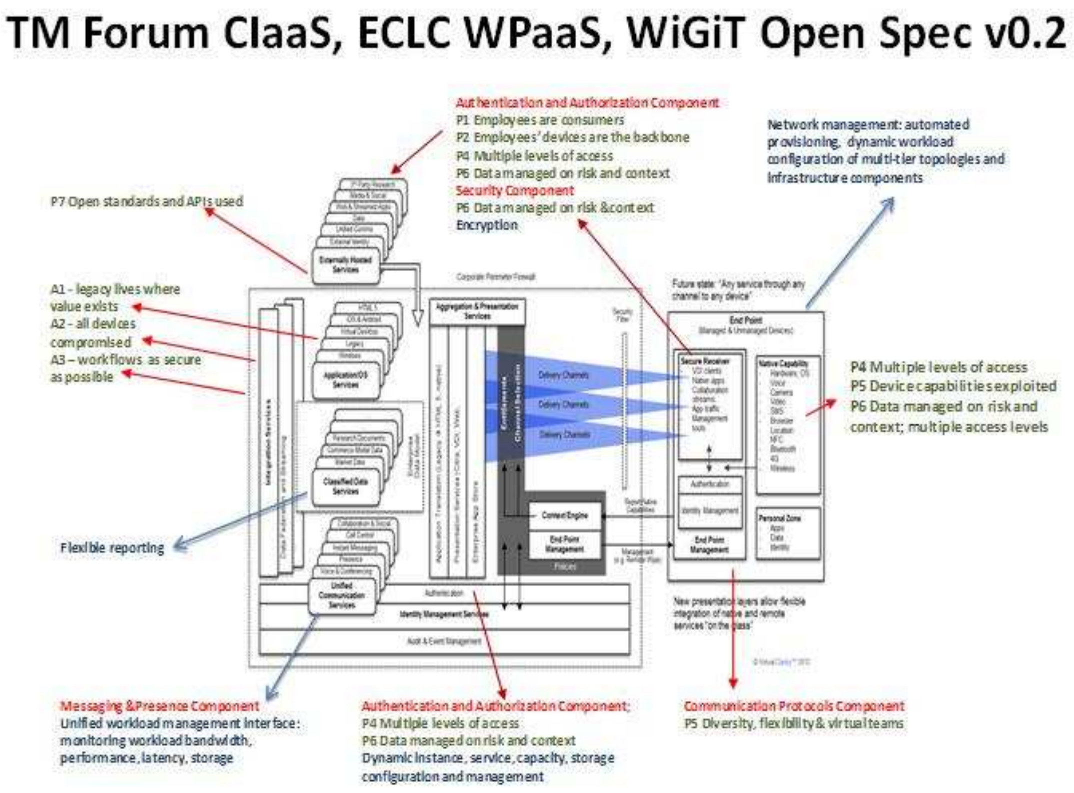


Figure 8: Proposed Reference Architecture for Workplace as a Service—Describes the Key Flows and Functions in the Design of the WPaaS



TM Forum ClaaS, ECLC WPaaS, WiGiT Open Spec v0.2

Authentication and Authorization Component
P1 Employees are consumers
P2 Employees' devices are the backbone
P4 Multiple levels of access
P6 Data managed on risk and context
Security Component
P6 Data managed on risk &context
Encryption

Network management: automated provisioning, dynamic workload configuration of multi-tier topologies and infrastructure components

P7 Open standards and APIs used

A1 - legacy lives where value exists
A2 - all devices compromised
A3 – workflows as secure as possible

P4 Multiple levels of access
P5 Device capabilities exploited
P6 Data managed on risk and context; multiple access levels

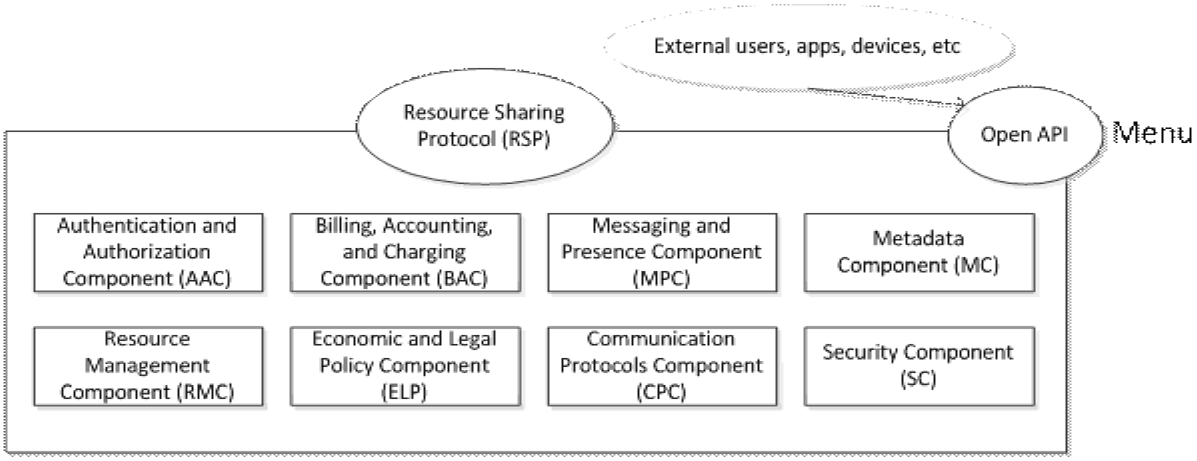
Flexible reporting

Messaging &Presence Component
Unified workload management interface: monitoring workload bandwidth, performance, latency, storage

Authentication and Authorization Component;
P4 Multiple levels of access
P6 Data managed on risk and context
Dynamic instance, service, capacity, storage configuration and management

Communication Protocols Component
P5 Diversity, flexibility & virtual teams

Externally Hosted Services
Corporate Perimeter Firewall
Future state: "Any service through any channel to any device"
Application/OS Services
Aggregation & Presentation Services
End Point
(Managed & Unmanaged Devices)
Secure Receiver
Native Capability
Delivery Channels
Delivery Channels
Delivery Channels
Entitlements
Channel Selection
Integration Services
Classified Data Services
Context Engine
End Point Management
Authentication
Identity Management
Personal Zone
Unified Communication Services
Authentication
Identity Management Services
Audit & Event Management
New presentation layers allow flexible integration of native and remote services "on the glass"



External users, apps, devices, etc
Resource Sharing Protocol (RSP)
Open API
Menu
Authentication and Authorization Component (AAC)
Billing, Accounting, and Charging Component (BAC)
Messaging and Presence Component (MPC)
Metadata Component (MC)
Resource Management Component (RMC)
Economic and Legal Policy Component (ELP)
Communication Protocols Component (CPC)
Security Component (SC)

Figure 9: Reference Architecture Showing an Open API Requirement Map – This Iteration Identifies the APIs that need to be supported in the WPaaS Solution. The Charts below add greater detail to the APIs

Main APIs from the WPaaS Project
1. Authentication and Authorization API (AAA)
2. Billing, Accounting, and Charging API (BAA)
3. Messaging and Presence API (MPA)
4. Metadata API (MA)
5. Resource Management API (RMA)
6. Economic and Legal Policy API (ELA)
7. Communication Protocols API (CPA)
8. Security API (SA)

Source: WiGiT v0.1 open spec, at: http://wigit.ischool.syr.edu

Table 1: Main APIs that are Part of WPaaS Project

Compute Infrastructure As A Service (CIaaS)[1,2,3] Requirements	**Workplace as a Service (WPaaS) Assumptions & Principles**		**Virtual Private Cloud (VPC) Requirements[2]**
Capability to scale up or down on demand	P-3 Device capabilities are exploited. P-4 Multiple levels of access. P-7 Open standards and APIs are used.		Stateless computing architectures enabling dynamic instance, service and capacity level, and storage configuration and management
Pay per use pricing	P-1 Employees are WPaaS consumers. P-6 Data managed on risk and context.		Support for billing and accounting processes; integrated monitoring and metering of workloads
Virtualization enabling hardware/driver independence	Integration Services (Ref Arch for WPaaS) P-3 Device capabilities are exploited. P-5 Diversity, flexibility & virtual teams. P-7 Open standards and APIs are used.		Vendor agnostic solution not locked into a hardware vendor, software vendor, or service provider. Unified workload management interface across all internal and external providers.
Image-based workload instantiation	Integration Services (Ref Arch for WPaaS) A-1 Legacy lives where business value exists.		Portability to move running workloads from one physical host to another in an automated manner.
Ability to store images	Integration Services (Ref Arch for WPaaS)		Flexible reporting including the capture of historical data for

			predictive usage models and analytical efforts.
Management interface: basic, admin & service functions, SLA monitoring, reporting, console access	P-4 Multiple levels of access. P-7 Open standards and APIs are used.		Integrated monitoring and metering of workloads, including monitoring of bandwidth, performance, latency,storage, etc., which can be provided through a portal or an API
Baseline security: encryption & isolation	A-2 All devices are compromised.		Encryption services for data in transit and at rest; user account management (e.g. authentication and authorization); secure management of encryption keys
Baseline network control: VLAN mapping, firewalls, intrusion detection/prevent ion	A-2 All devices are compromised P-2 Employees' devices are the backbone. P-4 Multiple levels of access. P-7 Open standards and APIs are used.		Network configuration and management; automated provisioning and dynamic configuration of diverse workloads, multi-tier topologies and infrastructure components

1 TM Forum/ECLC and ODCA, Joint Statement on Compute Infrastructure as a Service: Findings from the ODCA^{SM} Usage Model and TM Forum's Enterprise-Grade External Compute Iaas White Paper
2 TM Forum, TR174 Addendum C V0.1 Enterprise-Grade Virtual Private Cloud from a State-of-the-Art Implementation
3 TM Forum, RN330 V1.1 Enterprise Grade External CIaaS Requirements Solution Suite

Key:
Assumptions
A-1 Legacy lives where business value exists.
A-2 All devices are compromised.
Principles
P-1 Employees are consumers.
P-2 Employees' devices are the backbone.
P-3 Device capabilities are exploited.
P-4 Multiple levels of access.
P-5 Diversity, flexibility & virtual teams.
P-6 Data managed on risk and context.
P-7 Open standards and APIs are used.

Table 2: Comparison of CIaaS, WPaaS, and VPC

3.1. A Reference Architecture Comparison: VPC/WPaaS/CIaaS

Workplace as A Service (WPaaS), Compute Infrastructure as a Service (CIaaS) and Virtual Private Cloud (VPC) are reference architectures that potentially can meet the unique requirements to satisfy enterprise-grade customers. VPC fully implemented implies WPaaS and CIaaS development for enterprise-grade operations. We define “enterprise-grade” as the ability to deploy business critical services that match or exceed the level of security, quality, reliability, and availability found in internal corporate data centers. VPC enterprise level requirements are typically not cost effective or practical to implement for external public clouds and a general purpose customer base. VPC requirements include:

- High levels of automation, including automated provisioning and dynamic configuration of diverse workloads and multi-tier application topologies including web servers, application servers, database servers, security components (e.g. firewalls) and infrastructure components (e.g. DHCP).
- Unified workload management interface across all internal and external cloud providers.
- A vendor agnostic solution that is not locked into a hardware vendor, software vendor, or service provider.
- Portability to move running workloads from one physical host to another in an automated manner.
- The ability to create and enforce automated workload management policies for stateless computing architectures including:
  - Instance management (e.g. creating and deleting VMs, starting and stopping VMs, etc.)
  - Storage configuration and management (e.g. creating and deleting storage volumes, attaching volumes to VMs, initiating backups/snapshots, etc.)
  - Network configuration and management (e.g. VPN, NAT, VLANs, IP address overlays, etc.)
  - Security configuration and management (e.g. creating and deleting security zones, dynamically configuring firewalls in accordance with security zones, etc.)
  - User account management (e.g. authentication and authorization)
  - Service level management (e.g. instance scalability limitations, automated recovery, etc.)
  - Capacity management (e.g. auto-scaling, cloud-bursting, etc.)
- Encryption services for data in transit and for data at rest.
- Secure management of encryption keys (including private key certificates or pre-shared keys).
- Flexible reporting including support for billing and accounting processes and the capture of historical data for predictive usage models and analytical efforts.
- Integrated monitoring and metering of workloads, including monitoring of bandwidth, performance, latency, storage, etc., provided through a portal or an AP.

VPC is a modular, flexible design with minimal complexity. The VPC reference architecture has four major components: workload lifecycle management, automated infrastructure as a service, zoned security model, and optimized physical infrastructure.

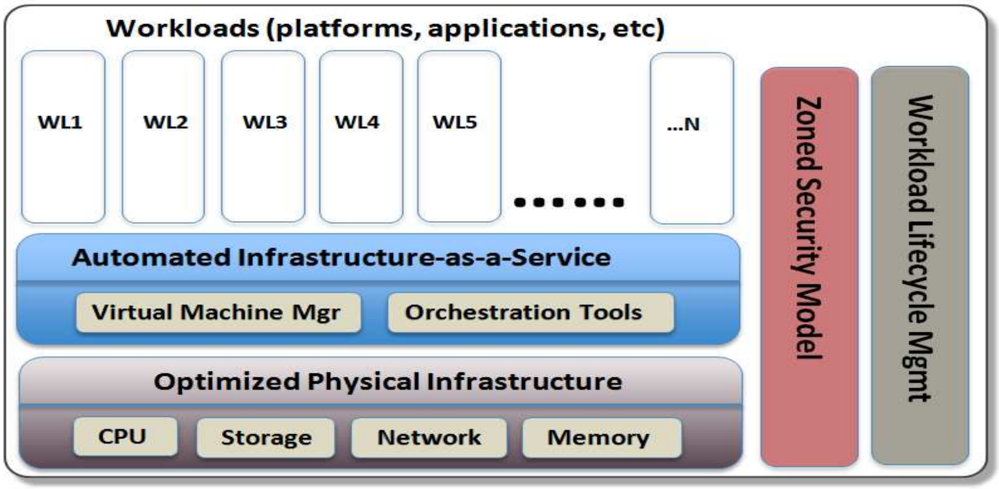
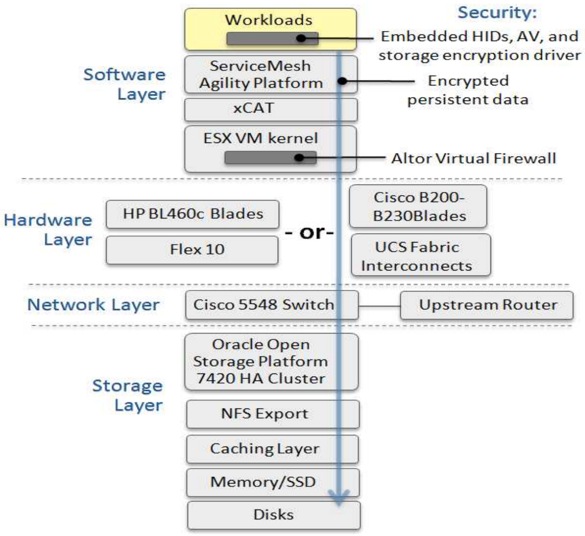


Figure 10: VPC Reference Architecture Overview

Based on results which were tested and validated in a lab environment, VPCs offer an agile and less costly IT operating model for enterprise customers. These results show that VPCs can be implemented rapidly and that they deliver high levels of automation and time savings. They also operate VMs at costs up to 75% less than comparable public cloud offering.



*Summarized from TR174 Addendum C V0.1 Enterprise-Grade Virtual Private Cloud from a State-of-the-Art Implementation

Figure 11: VPC Reference Implementation Topology

4. References

Tyson Brooks, Jerry Robinson, Lee McKnight, “Conceptualizing a Secure Wireless Cloud,” *International Journal of Cloud Computing and Services Science* (IJ-CLOSER) Vol.1, No.3, August 2012, pp. 89-114. *Journal homepage: http://iaesjournal.com/online/index.php/IJ-CLOSER*

Ian Foster, Carl Kesselman, and Steve Teuke, “The Anatomy of the Grid: Enabling Scalable Virtual Organizations,” *International Journal of High Performance Computing Applications,* Volume 15 Issue 3, August 2001, Pages 200 – 222. http://dl.acm.org/citation.cfm?id=1080667

H. Luthria and F.A. Rabhi. “Service-Oriented Architectures: Myth or Reality?” IEEE Software, volume 29, issue 4, July/August 2012, pages 46-52. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6086531&contentType=Journals+%26+Magazines&sortType%3Dasc_p_Sequence%26filter%3DAND%28p_IS_Number%3A6265068%29

Dr. Lee W. McKnight, Editor, “Open Specifications for Wireless Grids: Technical Requirements,” Version 0.2 in process. To appear on http://wigit.ischool.syr.edu/index.php/news/96-wigits-idawg-communications-elements-progressing-to-field-test-

TM Forum, Enterprise Cloud Leadership Council, Workshop at TM Forum Action Week, July 17, 2012.

Dave Bartoletti, James Staten and Heather Belanger, “Case Study: Commonwealth Bank of Australia Gets Service-Oriented Via Cloud Computing,” FOR CIO PROFESSIONS, Forrester Research, Inc., OCT 1 2012.

Enterprise Cloud Leadership Council Partners

Bank of America

School of Information Studies
SYRACUSE UNIVERSITY

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS
北京邮电大学

BOEING

CommonwealthBank

Curtin
University of Technology

CREDIT SUISSE

DASSAULT SYSTEMES

MOTOROLA

NORTHROP GRUMMAN

ServiceMesh.

THALES

SWIFT

SAUGATUCK
TECHNOLOGY

Carnegie Mellon
SILICON VALLEY

UBS

PEARSON

virtual
clarity.
clear thinking, straight talking.

WEST AVENUE
CAPITAL • MANAGEMENT PARTNERS

Table of Contents

5. Acknowledgments

This draft was prepared by an ECLC working group that included representatives from Commonwealth Bank of Australia, UBS, ServiceMesh, Virtual Clarity, Cisco, EMC, Northrop-Grumman, China Mobile, Huawei, and Syracuse University. Special thanks are due to Tommy Armstrong of Virtual Clarity who drafted the initial Manifesto that identified the main requirements. Special acknowledgement is also due to team members from Syracuse University who provided additional information based on the initial draft. These included Prof. Lee W. McKnight, Janet Marsden, Joe Treglia, and Ed Nanno plus a number of graduate students.

5.1 Company Contact Details

Company	Team Member Representative
UBS Financial Services	*Name: Tony Pizi* *Title: CTO, UBS Investment Bank's Wealth Management America* *Email: tony.pizi@ubs.com* *Phone: 201-352-5548*
Cisco Systems	*Name: Aron Dutta* *Title: Managing Director Financial Markets Strategy* *Email: ardutta@cisco.com* *Phone: 973-464-1107*
Syracuse University	*Name: Lee W. McKnight* *Title: Director, WiGiT; Associate Professor* *Email: lmcknigh@syr.edu* *Phone: 315- 278-4392*
ServiceMesh, Inc.	*Name: Jim Houghton* *Title: Managing Director, VP Global Client Services* *Email: Jim.Houghton@servicemesh.com* *Phone: 845-494-9419*
Syracuse University	*Name: Janet Marsden* *Title: PhD Student* *Email: jamarsde@syr.edu* *Phone: 315-447-9551*
Syracuse University	*Name: Joe Treglia* *Title: Assistant Director, WiGiT* *Email: jvtregli@syr.edu* *Phone: 315-382-1614*
Syracuse University	*Name: Ed Nanno* *Title: Executive Director, WiGiT* *Email: elnanno@syr.edu* *Phone: 315-443-1332*
TM Forum	*Name: Robert Cohen* *Title: Director, Enterprise Cloud Program* *Email: bcohen@tmforum.org* *Phone: 917 705 6524*