THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠
Published Since 1993 Report #TCG2014018 October 9, 2014

When a Secure Mobile Host Platform is Required — Go with IBM zEnterprise

Analyst: Stephen D. Bartlett

Management Summary

It could be said that every technological innovation always presents new challenges. In the overarching context of this paper, this means that when an innovative technology is introduced within an enterprise, there is a ripple effect – a wave form that will pass through many within the organization. Some of those affected will have anticipated the "new" wave, but some will not. There is nothing more likely to stir the gut than getting hit with a new high-priority initiative as the first thing in your boss' Monday morning staff meeting. Therefore, the new wave can have a positive side, but also sometimes can be negative. **If there is essentially an irrevocable "will" within the enterprise to ensure the success of this new technology, then every part of the organization must address each new challenge successfully.**

Over the years, it could be said that the information technology (IT) industry frequently has been in the forefront of many technological innovations; innovations in IT probably have had the most profound and far reaching in terms of its effects on individuals throughout the world. The hottest "buzzwords" these days include innovations such as *predictive business analytics*, *integrated development operations*, and the less concrete, *cloud* and *big data*. There is the constant barrage from the technical media and the industry's "thought leaders" reminding us constantly and annoyingly that if your enterprise does not have a strategy for each of these, then you are near the front of the queue for planned obsolescence or failure. Drama aside, **there definitely is at least one new technology that all enterprises need to be addressing – mobile computing**, which is the focus of the paper. What is unique about this technology is that it hasn't been driven so much from within the confines of the enterprise, but from beyond its boundaries – by outside employees, business partners, and, most importantly, existing clients and potential customers.

The first efforts to address mobile users may have been throwing up a new colorful corporate website portal suitably streamlined to fit into the limited real estate of typical portable devices. But the opportunity to serve that audience with more content and timelier information is just too tempting and important not exploit. Besides, your competitors probably are doing it. But to do this, it was realized that you would have to let the uncontrolled masses look under the covers, so to speak, and allow them access to "real" data, the carefully protected corporate jewels, and thus the locations of those precious gems, the *systems of record*, where transactions are processed and records are kept.

The premise of this paper is that if your enterprise's primary systems of record reside on mainframes, specifically IBM's *System z*, only the most secure end-to-end solution will suffice to ensure the integrity of those systems; ergo, the core of that system should mainframe-based. If you are interested in how IBM's mainframe addresses this issue, please read on.

IN THIS ISSUE

You Need to be in Mobile

If your enterprise is not "on the Internet", for all intents and purposes it does not exist and is

irrelevant. Then consider that there are uncounted billions of these mobile or smart[1] devices *everywhere*. For the "millennial generation", these devices are likely to be their primary window to the Internet, if not their only one. And in emerging economies throughout the world, there never was nor will there ever be a "PC generation"; mobile devices are the rule. Sales of smartphone units are expected to exceed 1.2 billion units in 2014 and soon will soon outstrip desktops. If your enterprise is invisible to this huge audience through their smart devices, you probably have lost them; clearly, they are not inside your "opportunity set".

There is no need to wrestle with a business case on this issue. The pace of business and decision-making today is very close to being real-time. Stale data eventually will lead to failure in today's highly competitive world that appears to be "always on and always connected".[2] Even if there are doubts in your organization, at least accept as a given that little is more important to most businesses than having a positive, revenue-enhancing, mobile presence for it employees, partners, and customers.[3] **Today, mobile is a primary force and may become the primary outlet for your brand, if not a key to corporate survival.**

Mobile is Different, But in a Good Way

Many of the activities in the world of mobile are different from those of the desktop in a number of ways.

- Read while moving versus sitting and reading.
- Message-oriented versus document-oriented.
- Purpose-built mini-apps versus large, complex applications.
- Context-aware versus context-neutral.
- Notice-driven versus task-driven.
- Diversity of device types versus homogeneous device types.
- Unpredictable network response versus predictable network response.
- Multiple connection points versus single connection point.
- Frequent and quick application updates versus periodic and infrequent, often collective application updates.
- Battery power versus connected AC power.

From these we can infer that there are similarities, but some uses will be dramatically different. Several of these have implications to the security of the infrastructure, the primary focus of this paper, which will be discussed in detail later.

In addition, with mobile enabled, information may need to flow in both directions – from the central data store, the mainframe's systems of record, to the user's smart mobile device *and* vice versa. The real-time information from mobile devices, including passive activity, may be very valuable to business processes. For example, an application or smart device that has built-in GPS (location-aware) capabilities (almost all do) would locate the user geographically and supplement/direct interaction with the user – in near real times.

The Mainframe as the Linchpin to Successful Mobile Enablement

When *Apple* revealed its first *iPhone* in June 2007,[4] Apple developers, marketers, and certainly Steve Jobs, probably had nothing further from their very creative minds than enterprise computing or mainframes. And why should they have been? They had just launched what would become an inflection point in the computing and communications industries and consequently almost every other human enterprise.

But this was certainly not the case for enterprise CIOs who sensed the pressure of the users of smart devices (as they evolved) to want to reach deeper into the enterprise information structure. Distributed web services satisfied these needs initially but, for many, that has become only a short-term solution. Likewise, it became evident that information about this audience could be useful to the enterprise as well, so there has become a certain amount of *kismet* connected with these two forces.

But why the mainframe? The simplest response is – that's where the data is, the systems of record that are key to the operation of many enterprises, including most of them in financial markets. Mainframes are the repositories to the

[1] In this paper, the phrase *mobile devices* is used interchangeably with *smart devices*, but the latter may be more descriptive, mostly because it is their local intelligence that makes them an interesting IT endpoint. Of course, being mobile is an assumed characteristic of many smart devices, i.e., smartphones and tablets, but there are other smart endpoints, such as remote data capture devices, not considered here. Both terms refer to the same devices.

[2] Enterprises not only have to deal with their "traditional" competitors, but must always be looking "over their shoulder" for the new guy on the block who could seemingly appear from anywhere at any time.

[3] These arguments, though couched in business terms, are no less significant to non-profit or governmental organizations, where the focus is to maximize its services scope and depth at the highest level of efficiency.

[4] See http://en.wikipedia.org/wiki/IPhone.

CICS and *WebSphere* application transactions, the *DB2* and *IMS* databases, and *VSAM* files.[5] As suggested earlier, the initial approach taken by many enterprises was to make a copy or an extract of the core data and host it on a set of distributed servers along with complementary set of storage devices and networking. This appeared to be less expensive and more efficient (because it was supposed to save expensive mainframe cycles) but really wasn't, because the mainframe was needed to extract and export this data, often many times per day.

Mainframe Qualities of Service are Essential to an Enterprise-Scale Mobile Solution

The *mobile world* is always "on", especially if your enterprise reaches beyond regional geographic boundaries or, for that matter, desires to do so. What are the implications of that reality? In the mainframe world, we call it *RASS* (taking some liberties with the traditional "RAS" acronym), which now stands for *reliability*, *availability*, *scalability*, and *security*. **If a mobile solution is to be resilient and persistent, it should exhibit these qualities at the highest levels. The IBM mainframe, *System z*, is unchallenged in delivering these qualities.**

The mainframe's *reliability* is the result of a half-century of research, development, and refinement of an architecture that is designed from the ground up to minimize failures, and if one should occur, to recover or work around it without a noticeable interruption. There are a number of mainframe customers who will testify that their mainframe systems have run continuously in time frames measured in *years*.

In parallel with that are the *availability* characteristics of the platform. Essential elements are hardware redundancy, elimination of single-points-of-failure, multiple layers of resource virtualization across several dimensions, and system management and diagnostic tools that anticipate potential issues with the platform as well as its sub-systems.[6]

As suggested above, if there is one thing we know for sure about mobile workloads is that they likely are going to be unpredictable in both volume and randomness. The inherent mobility of users and their smart devices results in a high degree of variability of the traffic that they will spawn. Some of these requests may be simple and straightforward – therefore the incremental load will be trivial – but many will be much more complex requiring more platform and subsystem resources, particularly when mobile-based transactions arrive in volumes of the thousands per second or higher. Under these unpredictable high loads, your systems, no doubt, will be tested at the extreme.[7] Not only will these workloads arrive randomly, but if *Murphy's Law*[8] prevails, the heaviest demands will occur at the worst possible time, when many (other) things also are happening.

Thus, solutions to meet these needs must be able to demonstrate rapid and easily managed horizontal and vertical scalability. *Need and additional set of cores or memory?* Dial them up from resources in a standby mode (*capacity on demand*) which, by the way, you don't pay for unless you use them.[9] *Need another instance of an application that is peaking?* Mainframe virtualization capabilities are unmatched by any other platform and can deliver a new set of resources that will be integrated seamlessly into the total pool.[10]

Accepting these requirements premises does not lead automatically to the implementation of a mainframe-based mobile solution, because the platform needs to have the software tools and business services that can support mobile solutions capably. However, the mainframe does not let you down and offers robust mobile solutions appropriate for accessing the critical and sensitive data stored on most mainframes.

Leading the Way to a Robust Mobile Solution

IBM's response to these enterprise-class mobile requirements is engendered in an

[5] ***CICS*** = *IBM Customer Information Control System*, initially implemented to support the utility and communications industries; ***IMS*** = *Information Management System*, a hierarchical data management system initially enabled for the manufacturing industry; ***DB2*** = *IBM Data Base 2*, a relational data management system, initially enabled to facilitate complex queries, all enabled for IBM's mainframes in the late 1960s and early 1970s; ***VSAM*** = *Virtual Storage Access Method*; ***WebSphere*** is a family of JAVA-based products and system services for enabling service-oriented architectures (SOA), including the *WebSphere Application Server (WAS)*.

[6] When a *zEnterprise* mainframe system senses errors above a threshold where a failure is likely to occur, the system will automatically place a call (controlled by customer specific policies) to IBM Dispatch for onsite maintenance.

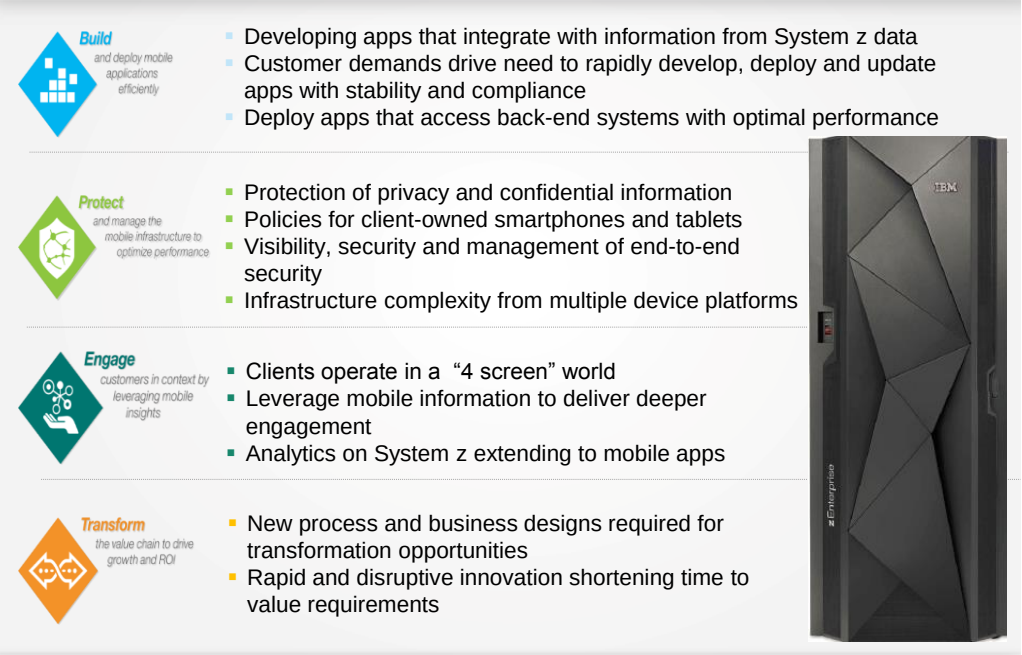
[7] IBM has documented a number of CICS and IMS workloads well in excess of 100 million transactions per day.

[8] "Anything that can go wrong will go wrong." See http://en.wikipedia.org/wiki/Murphy's_law.

[9] Modest fees for maintaining this capability will apply.

[10] For more detail on IBM's mainframe technology and how it enables enterprise-scale cloud and mobile solutions see *IBM zEnterprise is Enterprise Cloud Infrastructure* in **The Clipper Group Navigator** dated April 8, 2014 and available at http://www.clipper.com/research/TCG2014008.pdf.

Exhibit 1 — Solving Key Business and IT Challenges with System z



Source: IBM

overarching solution portfolio known as *IBM MobileFirst.*[11] The portfolio includes a number of elements that offer a comprehensive and cohesive structure to support all the enterprise-class needs for a mobile solution, especially for enterprise data already residing on System z.[12] It has been designed to meet the four key challenges to a successful mobile solution for System z.[13]

- **Build** – Quickly develop, test, and deploy quality mobile applications across multiple mainframe applications; seamlessly integrate rich mobile apps; and leverage existing z/OS transactions and data into new mobile applications.
- **Protect** – Instrument applications with security protection from mobile to back-end systems'; secure mobile transactions from customers, partners, and suppliers; preserve native device experience without compromising security; separate personal and business data; and provide intelligent access based on risk and location.
- **Engage** – Quickly create and deploy personalized mobile campaigns and gain insights with analytic information from System z; maximize brand value by integration the physical and digital experiences of mobile customers; and receive timely, informative, and interactive information to support decision making, regardless of location.
- **Transform** – Design new engagement models placing the customer first; use cost-effective workload mobile pricing on System z (more about this shortly) for competitive advantage; and use Linux on System z solution to build new business models that drive revenue. This is an invitation to reinvent your business with mobile applications as the driver. (See Exhibit 1, above.)

It is within these themes and overall context that this paper focuses on the requirements and the implementation of a secure, enterprise-class mobile solution.

Securing Every Transaction – the Second "S" in RASS

A number of studies, including those conducted IBM, clearly indicate that "mobility solutions" are a top target for IT investment increases over the next few years. However the barriers to implementation are led by the concerns

[11] See *IBM MobileFirst Solution Brief* at http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=SP&htmlfid=WSS14156USEN#loaded.

[12] For a comprehensive analysis of mainframe-based mobile solutions, see *Enabling Your Mainframe Data on Mobile Devices* in **The Clipper Group Navigator** dated April 23, 2013 and available at http://www.clipper.com/research/TCG2013008.pdf.

[13] MobileFirst is agnostic in that it designed to operate in each of the IBM's three server architectures: *System x, Power Systems,* and System z (the mainframe). (Portions of IBM's System x server business have been sold to Lenovo.)

for assuring a secure implementation encompassing smart devices (phones and tablets), management of confidential data, and integration with the existing infrastructure and data.

The top concerns relative to smart devices are:

- The risk of device theft or loss or misuse.
- Data leakage – unauthorized copies being distributed and/or retained outside those who have an approved need.
- Data interception by a "man in the middle", e.g., those snooping on Internet traffic.
- Malware incursions that put the data and/or its veracity at risk.

Security concerns for mobile solutions are not dramatically different from those of any other application accessed remotely, but they do have characteristics that are unique to mobile. For instance mobile devices:

- **Have a wide range of capabilities** – The combinations of device manufacturer (and smart device models), OS provider (and release version), and common carrier (or network) are manifold; and they may change frequently and somewhat unpredictably.
- **Have multiple personas** – A smart device can be used as a work tool, entertainment medium, access device, and an organizer interchangeably (and, sometime concurrently). Ease-of-use and near-universal accessibility facilitates large volumes of low-value transactions (and inquiries), which may present little or no opportunity to increase revenue.
- **Access through multiple connection points** – Connectivity may be via public, private, or cellular networks. The users may roam (anytime, anywhere), which likely increases risks but also raises the business opportunities.
- **Prioritize the user and not the data** – Smart device architectures put the user in control. Conflicts with the "expected" user experience tend not to be tolerated. Policy enforcement is challenging, particularly when the device is not owned by your enterprise, as with BYOD-to-work and customers using their own devices.
- **Are easily lost or stolen and sometimes shared** – It is the better policy to assume that the authorized (known) user may not be the only person with access to a smart device. This presents a high risk for lost or stolen data and other ways that those not authorized may have access to confidential data.

These factors would seem to present an alarming and intimidating set of issues and risks that inevitably would lead to many sleepless nights by CIOs and CSOs. It certainly would be easier to stick one's head in the sand and either ignore the risks or very tightly limit what can be accessed (and by whom). However, neither of these alternatives is realistic in an always-on business environment, where such restrictions might drive you out of business very quickly.

Thus, the smart device risks must be managed and access needs to be controlled. What you need for business success is a well-developed and executed strategy for the extension of your current enterprise (systems of record) applications to mobile devices. It shouldn't surprise you that IBM not only has thought about this problem, but also has a range of mobile solutions available, and extensive experience in putting them in place.

The IBM Mobile Security Ecosystem

The IBM Mobile Security ecosystem is structured using four principle pillars. The pillars are defined in a taxonomy that begins at the *device* level, continues through to device *content*, then includes the *mobile application*, and ultimately leads to the final objective, the *transaction*, which, in the situation we are considering, are processed and housed within the enterprise systems of record that reside on the mainframe. (See Exhibit 2, at the top of the next page.)

- **Device Security –** This includes enrolling, provisioning, and configuring devices, settings, and mobile policy; assigning mobile devices with a unique and persistent IDs; remotely locating, locking, or wiping lost or stolen devices; and enforcing device security compliance, including passcodes, encryption, and jailbreak and root detection.[14]
- **Content Security –** This entails restricting copy, paste, and sharing device data; integration *with Connection, SharePoint, Box, Google Drive* and *Windows File Share*; securing access to corporate mail, calendars, and contacts; and securing access to corporate intranet sites and networks.

[14] For instance: **Jailbreaking** – A device hack that provides users with unrestricted access to the entire file system (including operating system), of their mobile devices. See http://mobileoffice.about.com/od/glossary/g/jailbreaking.htm. **Root detection** – Rooting is the process by which the local or a remote operator obtains "privileged control" resulting in the ability to alter or replace system applications and settings. See http://en.wikipedia.org/wiki/Rooting_%28Android_OS%29.

Exhibit 2 — Security Features and Capabilities for the Mobile Enterprise

Device Security	Content Security	Application Security	Transaction Security
• Enroll, provision and configure devices, settings and mobile policy • Fingerprint devices with a unique and persistent mobile device ID • Remotely Locate, Lock and Wipe lost or stolen devices • Enforce device security compliance: passcode, encryption, jailbreak / root detection	• Restrict copy, paste and share • Integration with Connections, SharePoint, Box, Google Drive, Windows File Share • Secure access to corporate mail, calendar and contacts • Secure access to corporate intranet sites and network	**Software Development Lifecycle** • Integrated Development Environment • iOS / Android Static Scanning **Application Protection** • App Wrapping or SDK *Container* • Hardening & Tamper Resistance *IBM Business Partner (Arxan)* • Run-time Risk Detection *Malware, Jailbreak / Root, Device ID, and Location* • Whitelist / Blacklist Applications	**Access** • Mobile Access Management • Identity Federation • API Connectivity **Transactions** • Mobile Fraud Risk Detection • Cross-channel Fraud Detection • Browser Security / URL Filtering • IP Velocity
Security Intelligence			
Advanced threat detection with greater visibility			

Source: IBM

- **Application Security** – Mobile apps should be incorporated into the enterprise life-cycle software management processes and integrated development environment (IDE); applications must be scanned, wrapped, or containerized to ensure hardening and tamper resistance; run-time risk protection that must actively scan for malware; and application whitelists and blacklists must be must be maintained to guide users.
- **Transaction Security** – It begins with managing *access* through the use of a mobile access management system, identity federation (central point of control), and secure API connectivity. At the transaction level, there must be active risk and fraud detection. The use of secure browsers must be ensured and all URLs must be subject to filtering (which user, what URL, etc.). Another means of fraud detection is through the monitoring of IP addresses for unusually high activity or "velocity".

IBM addresses these security requirements through a wide range of products under the umbrella of the MobileFirst Platform Foundation. As an illustration of how these products address the specific needs outlined above, four products that demonstrate the end-to-end security capabilities of IBM's MobileFirst Foundation portfolio have been selected.[15]

Security at the Smart Device

Fiberlink MaaS360[16] is a rapid time-to-value solution offering comprehensive mobile device management features and functions which can be enabled for on-premises or cloud-based[17] deployments. MaaS360 provides device registration, anti-tampering, OS patch control, application segregation, password policy enforcement, encryption for device and backups, compliance with corporate data access policies, and selective or full-device wiping.

MaaS360 is an exceptionally comprehensive mobile device management solution that supports corporate and personally-owned (BYOD) devices[18]; provides dual persona with full

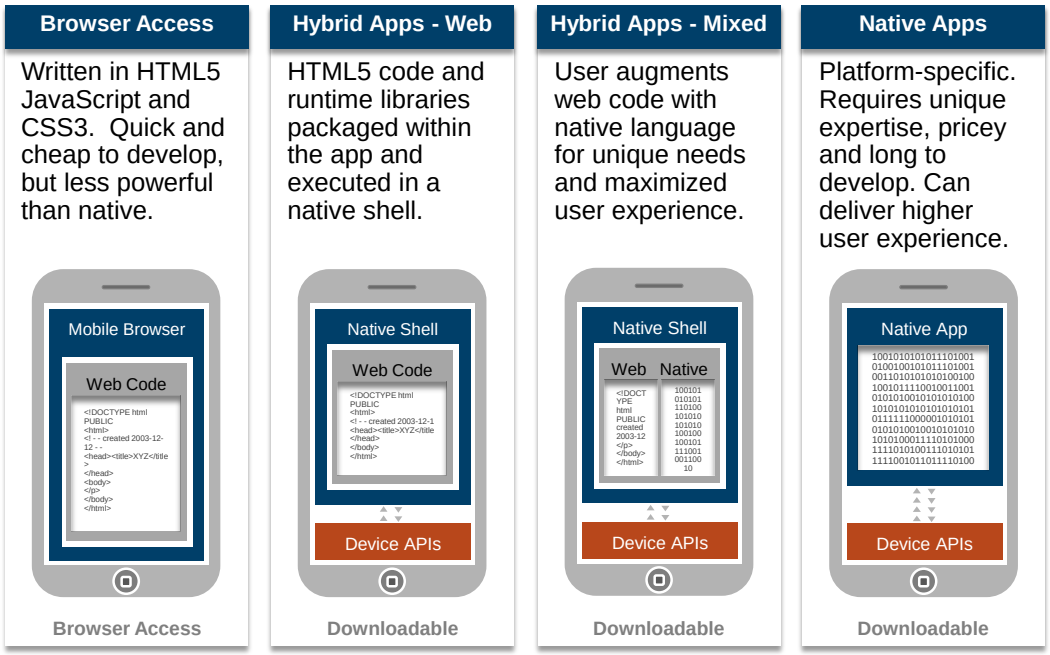
[15] Within the IBM Mobile Security Ecosystem, there are several products that address the specific needs outlined above. All of these products are incorporated and integrated under the umbrella of the IBM MobileFirst Foundation's portfolio. In some cases, there may be some overlapping as well as unique features of each of these products; the choices must be determined by a thorough examination of the goals of the enterprise and its capabilities.

[16] Fiberlink MaaS360 was incorporated into the IBM MobileFirst portfolio by the December 2013, acquisition of Fiberlink Communications, Inc. The acronym is derived from the concept of comprehensive Mobility device management as a Service.

[17] Now available as a part of IBM's Software as a Service (SaaS) portfolio and is planned to be available on the IBM *SoftLayer* cloud infrastructure.

[18] Device authentication features, such as near field communication (NFC) capabilities, fingerprint sensing, visual recognition by camera, and voice recognition by microphone should be exploited, where applicable.

Exhibit 3 — IBM Supports Multiple Mobile Application Development Models



Source: IBM

containerization and privacy; and automates actions to ensure compliance with corporate standards and policies. This enables the enterprise to ensure that mobile applications are distributed and managed securely; that e-mail, attachments, and corporate documents are controlled to prevent leakage; and that secure access to the Internet and corporate intranet sites are filtered and controlled.[19]

Security of the Mobile Application

IBM's premier offering for mobile application development is *IBM MobileFirst Platform Foundation*. It is designed to speed the development, integration and management of mobile applications by using standards-based technologies and tools to deliver an enterprise-grade services layer. This directly addresses the one-to-very-many problem[20], as IBM MobileFirst Platform goes beyond mobile app creation to deliver a complete mobile middleware solution. Its key capabilities as mobile-optimized middleware include the following:

- Open approach to third-party integration
- Mix of native[21] and HTML coding
- Strong authentication framework
- Encrypted offline availability/access
- Enterprise back-end connectivity
- Unified push notifications
- Data collection for analytics
- Direct updates and remote disablement
- Packaged runtime skins

This is a good checklist for your "wants" in your application development platform. Equally important are the "wheres" and "hows". All of this happens as described in Exhibit 3, above. Be mindful that there is no "one right way" to approach application development. In fact, in the largeness of an enterprise, it may be right to use several different approaches. **But what you should have is a development vehicle that does not limit you to doing app development in just one way.** IBM MobileFirst Platform provides this range of approaches – all within the same framework.

MobileFirst Foundation's Major Components

There are four major MobileFirst Foundation components.

- ***IBM MobileFirst Platform Studio*** is an Eclipse-based IDE, allowing developers to perform all the coding and integration tasks required to develop a fully operational mobile application.
- ***IBM MobileFirst Platform Server*** is a JAVA-based server that is a scalable gateway between applications, external services, and an

[19] Other IBM products in this category include *IBM Endpoint Manager*, *Trusteer Fraud Protection*, and *MobileFirst Platform Device Runtime.*

[20] One well-controlled and compatible set of applications, middleware, hardware and data (on the mainframe) needing to communicate and work with very many somewhat-unique (slightly different) smart devices.

[21] For example, JavaScript and CSS (Cascading Style Sheets).

enterprise's backend infrastructure. It performs data translation to streamline backend data for smart device consumption, supports physical clustering for high availability, manages push notifications, controls application deployment and versioning, and provides analytics on user adoption and usage. It contains security features to enable connectivity, multi-source data extraction and manipulation, authentication, direct update of web and hybrid apps (on the smart devices),
analytics, and operational management functions. Significantly, the MobileFirst Server is supported by *Linux on System z* (as well as on a number of other platforms), the benefits of which include zEnterprise qualities of service (QoS), flexible and dynamic scaling, world-class virtualization capabilities, and *HiperSockets*[22] connectivity to all other mainframe applications.

- ***IBM MobileFirst Platform Device Runtime Components*** are client-side runtime code that embeds server functionality within the target-environment of deployed apps (on smart devices).
- ***IBM MobileFirst Platform Console*** is a web-based UI dedicated for the ongoing monitoring and administration of the MobileFirst Server and its deployed apps, adapters, and push notifications.

Security Over the Network

The most effective mechanism for enforcing proper access policies is through a *centralized mobile security gateway*. IBM offers several alternatives including the *IBM WebSphere DataPower* gateway appliance. Available as a physical or virtual appliance, WebSphere DataPower, as a mobile security gateway, provides a rich set of capabilities that enable secure access to corporate data, applications, and services to external clients and business partners. It provides the following:

- Dynamic routing and intelligent load distribution
- Traffic control and policy enforcement
- Message and transport protocol transformation
- Message validation and filtering
- XML off-loading
- Integration with MobileFirst Platform

Additionally, WebSphere DataPower can provide high levels of certified security assurance, for example, Transport Protocol Security (SSL/TLS), message level security, as well as authentication, authorization, and audit. Its System z integration capability allows CICS and IMS transactions to consume external web services and delivers a secure path for mobile access to System z services. The WebSphere DataPower gateway appliance is an exceptional vehicle for centralized management and monitoring point that will provide secure control, integration, and optimization of mobile workloads.[23]

Security Within the Enterprise

In many enterprises, the choice of the System z mainframe as the host for the most valuable applications and data was based on that platform's QoS, but any reservations about that decision were overcome when data and transaction security was an essential requirement. System z is the most trusted platform due, in large part, to its inherent architecture and the continued development of the most stringent standards and facilities throughout the platform.

The IBM Security Server

The *IBM Security Server* is broad range of systems services that provide the means to control the access of users to the system (user ID and password) and restrict the function that an authorized user can perform on the system's data files and programs. For example, the security components include *Lightweight Directory Access Protocol (LDAP) Server*, *z/OS Firewall Technology* (*IPv4 and IPv6*), *Network Authentication Service for z/OS* (*Kerberos* security services), and its primary component, *Resource Access Control Facility (RACF)*.

RACF Protects Your System Resources

Computer-based access controls are called *logical access controls*. These are protection mechanisms that limit users' access to information to only what is appropriate for them. RACF is

[22] HiperSockets provide high-speed TCP/IP connectivity within a central processor complex. Thus, it eliminates the need for any physical cabling or external networking connection between servers running in different LPARs, thus speeding and securing access and updates to data.

[23] For those IBM zEnterprise clients who are considering or have installed a *zEnterprise BladeCenter Extension (zBX)*, the *IBM WebSphere DataPower Integration Appliance XI50, (DataPower XI50z)* is a multifunctional appliance that provides XML hardware acceleration, secure web services including routing, protocol and data transformation, and auditing. It may be used to provide an additional layer of security for protecting access to CICS, DB2, IMS, or WAS applications. Because the DataPower XI50z appliance is installed in a zBX, it benefits from tighter integration, a faster and secure link, and centralized management under z/OS. For more detail, see *IBM zEnterprise Really Stretches It Boundaries – New Windows are Opened* in **The Clipper Group Navigator** dated October 12, 2011, and available at http://www.clipper.com/research/TCG2011034.pdf.

IBM's offering, a no-charge program product available for z/OS and z/VM (which, among other features, manages Linux images). RACF protects resources by granting access only to authorized users of the protected resources. RACF retains information about users, resources, and access authorities in special structures called profiles in its database, and it refers to these profiles when deciding which users should be permitted access to protected system resources. To accomplish its goals, RACF provides the ability to do the following.

- Identify and authenticate users.
- Authorize users to access protected resources.
- Log and report various attempts of unauthorized access to protected resources.
- Control the means of access to resources.
- Allow applications to use the RACF macros.

RACF uses a user ID and a system-encrypted password to perform its user identification and verification. A facility is provided to enforce password policies, such as length, use of characters, numeric, or special characters, and change frequency. An important function of RACF is to complement the System Authorization Facility (SAF), an integral component of z/OS, which provides the interfaces to the callable services provided to perform authentication, authorization, and logging. Also, it is important to note that IBM's major mainframe middleware subsystems such as CICS, DB2, IMS, and WAS can use the same RACF facilities to protect their transactions and files.

IBM Security zSecure Suite

The *IBM Security zSecure Suite* is a family of products that enhance mainframe administration by providing audit and compliance reporting and management within a z/OS infrastructure. Its components are in two categories.

- **Administration and Management** – Administration of RACF databases is the cornerstone of a secure mainframe environment. Included are zSecure Admin, zSecure Visual (Windows-based), zSecure for RACF on z/VM, and zSecure CICS Toolkit.
- **Security Audit and Compliance** – These tools assist in assuring compliance with industry and governmental standards and enterprise security policy. Included are zSecure Audit, zSecure Alert, and zSecure Command Verifier.

z/OS Connect – a RESTful Interface

One of the emerging and most widely proliferating technologies for integrating mobile applications with existing services is the use of *Representational State Transfer (REST*). These so-called *RESTful* interfaces provide an application programming interface (API) that conforms to a set of architectural principles, which are defined by the following:

- The explicit use of HTTP.
- Stateless functionality.
- Exposure of directory structure-like URIs.[24]
- Support for the transfer of XML and/or JavaScript Object Notation (JSON)[25].

*IBM WebSphere Liberty z/OS Connect (*a.k.a. *z/OS Connect)* provides a native RESTful interface that enables API connectivity between mobile environments and z/OS back-end systems. It is shipped, without additional charge, with the most current releases of WAS, IMS, and CICS. This interface is best used inside the enterprise where users are trusted and there is no need for additional layers to access control security beyond the built-in security of z/OS.[26] z/OS Connect is designed to provide a fast, reliable, unified, and secure connector to access and invoke z/OS-based business assets in CICS, IMS, Unix System Services, and batch environments. As its name suggests, z/OS Connect is based on the *WebSphere Liberty Profile*, and functions as a bridging technology to convert HTTP REST requests with JSON payloads into the target system's expected format. Among its services, z/OS Connect provides interceptor implementations for service security authorization and SMF-based[27] auditing. An example is the audit interceptor, which writes SMF (type) 120.11 records that capture user request data, such as arrival and completion time, target URI, user ID, and the length of JSON inputs and responses, as well as a number of other data elements essential to the management of mobile

[24] URI = Universal Resource Identifier, a superset of an URL.

[25] *JSON (JavaScript Object Notation)* is a lightweight data interchange text format and is the common language of many mobile app programmers. It is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and others.

[26] If additional access control beyond z/OS Connect is required, whether inside or outside, *IBM API Management*, a for-charge software product, provides a comprehensive control point for client access to System z or any system in the enterprise. It is a highly secure, scalable, and robust solution that is provided by the IBM DataPower Gateway appliance.

[27] SMF = System Management Facilities, an optional (but essential) feature of z/OS that provides you with the means for gathering and recording information that can be used to evaluate system usage for accounting, chargeback, and performance tuning.

and other smart device workloads.

Alternative Secure End-to-End Topologies

As discussed earlier, IBM has a wide range of products that are available and map to the four pillars of the IBM Mobile Security Ecosystem. The illustrations above highlight Fiberlink MaaS360 at the device, IBM MobileFirst Platform managing the mobile application, WebSphere DataPower over the network, and RACF and z/OS Connect within the enterprise system. There are a number of alternative solution topologies that may include other IBM or ISV products that also can satisfy enterprise security strategies and requirements. The illustration presented here is just a representative of the choices that should be considered in the development and implementation of that strategy that best fulfils the security needs of your enterprise and perhaps, as an added benefit, allows your CIO a "RESTful" night's sleep.

System z Cryptographic Technology

Encrypted files and communications are essential elements of any secure application strategy. There can be no discussion of how the mainframe substantially contributes to the security of its hosted mobile solutions without mentioning the zEnterprise's exceptional cryptographic functionality and which is evolving continually. Crypto synchronous functions are provided by the *CP Assist for Cryptographic Function (CPACF)*. (A CP is a core built on the System z architecture.) CPACF is a no-charge feature that must be enabled explicitly; its callable services may be invoked by all of IBM's supported operating systems, including Linux on System z. Crypto asynchronous functions are provided by the optional *Peripheral Component Interconnect Express (PCIe)* cryptographic coprocessor – the *Crypto Express4S* – which complements the capabilities of the CPACF. It is a state-of-the-art, tamper-proof programmable cryptographic feature that provides a secure cryptographic environment.

zEnterprise Pricing for Mobile Workloads

Earlier in this paper, one aspect of mobile-based transactions is large volumes of low revenue producing transactions[28] Think of an active client of a bank checking on his/her account balances, the type of transaction that will occur very frequently, and since the client is an existing customer, the value of that transaction to the bank is nil and not likely to lead to an up-selling or cross-selling opportunity. Admittedly, each of these transactions may not consume a large amount of resource individually, but when summed up at the end of the day, and especially at peak load hours, these transactions can affect server and storage resources significantly. IBM has recognized this issue and, to encourage the use of the mainframe as a mobile workload host, it announced *Mobile Workload Pricing for z/OS (MWP)* in May of this year. Putting aside the technical details of exactly how this is accomplished, essentially **IBM will discount up to 60% of the software license fees** of z/OS and certain middleware products, e.g., CICS, IMS, and DB2, (called *Mobile Workload Pricing Defining Programs*) due to mobile workloads, if that workload is impacting the peak usage. This offer is limited to data centers that run the latest zEnterprise systems, the *zEC12* or the *zBC12*. In addition, the client must install the *Mobile Workload Pricing Tool*, collect the appropriate SMF records, and submit the results of the reporting tool on a monthly basis. IBM will then adjust the software license fees for that period, but only when the mobile workload results in higher transaction volumes that cause a spike in machine utilization. This process is quite similar and therefore familiar to data center managers in any enterprise currently running System z, z/OS, and its information management middleware.

Conclusion

Supporting mobile applications within your enterprise is necessary, desirable, and inevitable. It may be the most important next technology that inevitably and dramatically will change your enterprise's relationship with its employees, business partners, and the loyalty of its clients. At the same time it may present the most complex set of issues that CIO's and IT staffs to understand, master, and implement because of the inherent risks of allowing access to the most valued data resources of the enterprise. These risks can be managed but only by engaging the most mature and comprehensive security tools, both hardware and software. In this paper, I have described and shown how IBM's Mobile Security Ecosystem and the System z mainframe constitute the ideal systems platform to fulfill a comprehensive and secure mobile application strategy. Mobile is here and now. It is time for you to build your enterprise's mobile strategy on the best platform that will lead to enterprise (and personal) success – IBM's zEnterprise.

[28] Though not necessarily exclusive to mobile workloads.

About The Clipper Group, Inc.

The Clipper Group, Inc., now in its twenty-second year, is an independent publishing and consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 40 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

***Stephen D. (Steve) Bartlett* is a Senior Contributing Analyst for The Clipper Group.** Mr. Bartlett's interests include enterprise solutions including servers, system software, middleware, their underlying technologies, and their optimal deployment for responsiveness to emerging business requirements. In 2010, he joined the Clipper team after over 42 years with the IBM Corporation as an account and program manager in large system sales, product development, strategy, marketing, market research, and finance. During that time, he received several awards for his contributions in innovative market research and contributions to the business. He has a B.S. from Rensselaer Polytechnic Institute, and an M.S. from Union College.

- ***Reach Steve Bartlett via e-mail at steve.bartlett@clipper.com or at 845-452-4111.***

Regarding Trademarks and Service Marks

Disclosures

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

After publication of a bulletin on *clipper.com*, The Clipper Group offers all vendors and users the opportunity to license its publications for a fee, since linking to Clipper's web pages, posting of Clipper documents on other's websites, and printing of hard-copy reprints is not allowed without payment of related fee(s). Less than half of our publications are licensed in this way. In addition, analysts regularly receive briefings from many vendors. Occasionally, Clipper analysts' travel and/or lodging expenses and/or conference fees have been subsidized by a vendor, in order to participate in briefings. The Clipper Group does not charge any professional fees to participate in these information-gathering events. In addition, some vendors sometime provide binders, USB drives containing presentations, and other conference-related paraphernalia to Clipper's analysts.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.