Redbooks
ibm.com/redbooks

Securing Your Mobile Mainframe

Wilhelm Mild

Martina von dem Bussche

Robert L. Kennedy

Security

z Systems

IBM

Point-of-View

Security challenges evolve, and so does the security environment with IBM z Systems

Highlights

To achieve business goals today, Systems of Record (SoR) that are serving transactional and data services must interface with Systems of Engagement (SoE) that are increasingly represented by mobile devices. System security and integrity is an IBM commitment and a focus for this Point of View. This document is for businesses that are interested in end-to-end security from the mobile device to the transactional end point. The following critical topics are covered:

- Secured mobile transaction challenges
- The mainframe as the backbone for secure mobile workloads
- The four pillars of security
- End-to-end security for a typical mobile application
- Customer examples

When the IBM® mainframe was introduced, system networks were small and few users had access to the mainframe within the organization. To gain access, a user had to be on the premises and usually during regular business hours.

Today, mainframes (such as IBM z Systems™) are connected to a network (the Internet) that spans the globe. Virtually anyone anywhere has 24x7 access by using web interfaces and mobile devices to mainframe-based services. Organizations store their intellectual property, sensitive business data, and core applications on mainframes.

The mainframe is considered the most securable commercial computing platform that is available to customers. System Integrity is a commitment from IBM. Over many decades, IBM featured design and development practices that are intended to prevent unauthorized application programs, subsystems, and users from gaining access, or from circumventing, disabling, altering, or obtaining control of key system processes and resources unless allowed. Now, the question is security (protect and prevent) when mobile devices are used. This paper describes how IBM solves those concerns.

Mobile is changing mainframe security challenges

Mobile devices evolved to the preferred method of accessing business services. Securing data is an evolving process as well. Cyber security is about risk mitigation, not risk prevention. Because IT systems must be running and accessible to provide value, there is always some risk that a system's information or control can be compromised.

IBM z Systems offers a solution for your cyber security needs. The focus of the solution that is described in this document is end-to-end security integration of mobile workloads with z Systems transaction and data services.

The capabilities of running heterogeneous workloads on the same z Systems machine enable mobile and transactional workloads to run side-by-side. With the IBM MobileFirst Platform, enterprises can now minimize the challenges for a secure mobile strategy.

Figure 1 shows the security areas between a mobile device and the integration to back-end data and transactional services.

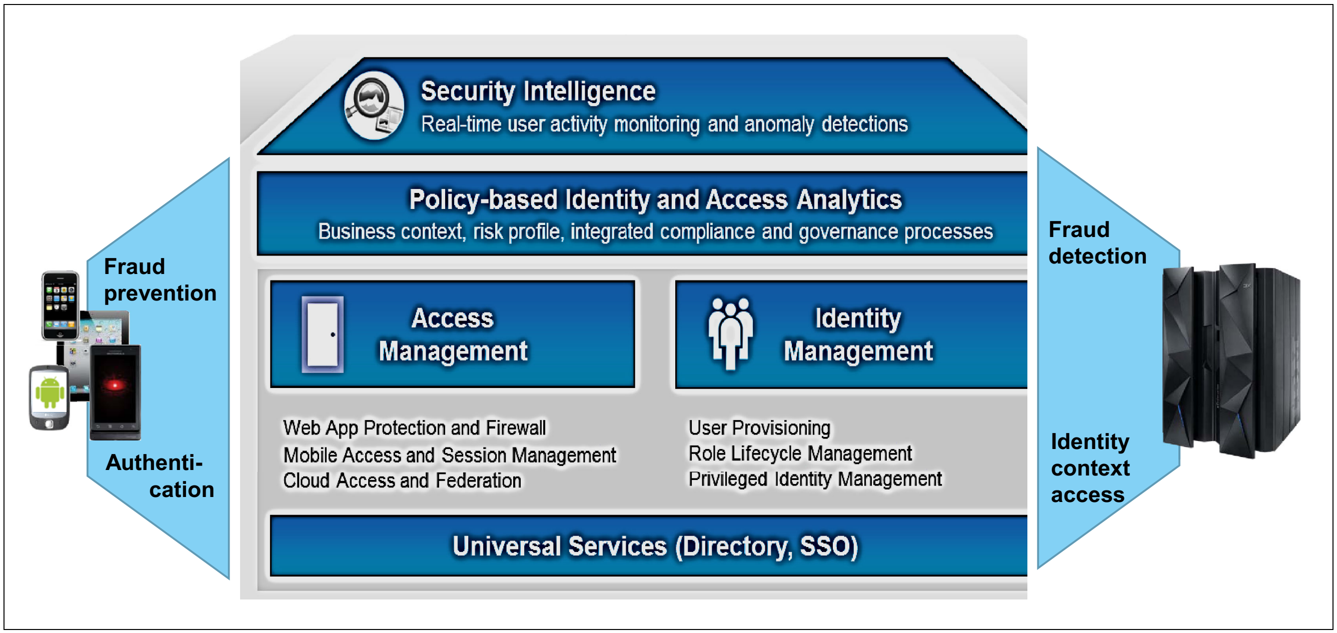
Security Intelligence
Real-time user activity monitoring and anomaly detections
Policy-based Identity and Access Analytics
Business context, risk profile, integrated compliance and governance processes
Access Management
Identity Management
Web App Protection and Firewall
Mobile Access and Session Management
Cloud Access and Federation
User Provisioning
Role Lifecycle Management
Privileged Identity Management
Universal Services (Directory, SSO)
Fraud prevention
Authenti-cation
Fraud detection
Identity context access

Figure 1 Mobile device, areas of security

When a secured mobile device starts a request (as shown on the left side of Figure 1), it must enforce Thread and Fraud prevention, and Authentication, before it accesses the mobile environment. The mobile environment (System of Engagement) must handle Identity and Access Management before it propagates the identity to integrate with the back-end security for transactional services on z Systems (Systems of Record), as shown on the right side of Figure 1.

Secured mobile solutions today are built by a System of Engagement that bridges the gap between mobile devices and Systems of Record on z Systems. The design goals that new Systems of Engagement are challenged to met consist of the following qualities:

- Mobile: Always on, anywhere, anytime and with the most current security always on.
- Real time: The requirement for a mobile request is real-time security, including fraud.
- Secured: End-to-end security for every transaction.

IBM is focusing to ensure that mobile solutions on z Systems enable end-to-end security and transactional integrity, from the mobile device to the back-end transactional system with the following features:

- Protecting sensitive business critical data
- Sharing information internally and externally
- Providing enhanced encryption and key infrastructure capabilities
- Protecting user privacy
- Providing an extensive audit trail with compliance reporting
- Reducing fraudulent activities
- Allowing centralized administration
- Securing virtualization
- Protecting information flowing across the network and maintaining high levels of infrastructure, application, and data availability

“When it comes to identity and access management, organizations often face a trade-off between improving security levels and delivering greater end-user convenience,” said Frost & Sullivan Senior Industry Analyst Mario Fernandez. “IBM breaks the security/end-user convenience trade-off through its IBM Security Access Manager for Mobile appliance.”

Why the mainframe is the backbone for secure mobile workloads

To meet the quality of services for a secured mobile workload, IBM developed a comprehensive portfolio for end-to-end mobile security solutions with IBM MobileFirst Protect. This portfolio of IBM solutions addresses each of the following four key mobile security challenges:

- Device security
- Content security
- Application security
- Transaction security

Figure 2 shows the four pillars of security for Mobile workloads.

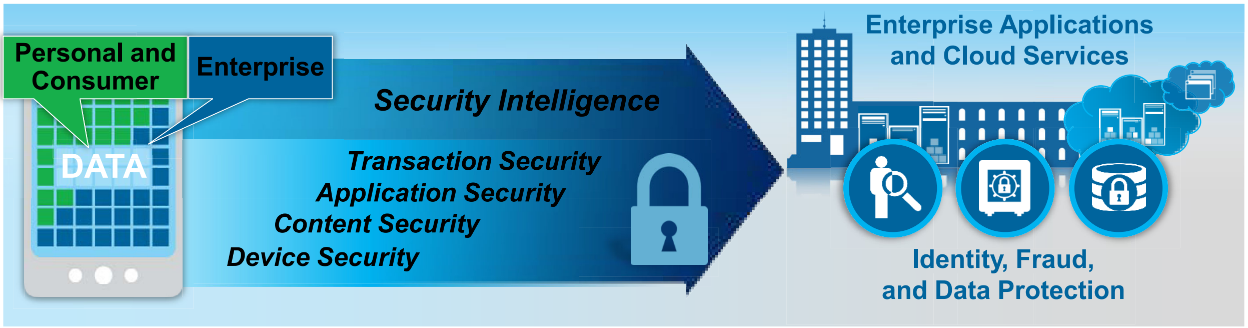

Figure 2 Pillars of security

This portfolio of IBM solutions also integrates with mainframe security and its quality of services and provides the following benefits:

- Integrate mobile with the mainframe
- Secured zones prefixing the mobile environment
- Security intelligence
- End-to-end security

In the following sections, each of these pillars and how IBM secured mobile workloads by using those pillars is described. This section also describes how to integrate with the Mainframe security and its Quality of Services.

Device security

Protecting mobile devices is challenged by the diverse set of available devices that span from corporate-owned assets to employee-owned devices (BYOD). With Fiberlink® MaaS360® Enterprise Mobility Management, IBM delivers a solution to enroll, provision, and configure devices.

The solution has real value for the support of corporate identity policies for mobile workloads. It also enables unique identification of mobile devices and location (locking and wiping remotely if lost or stolen). This first step in the security chain is an important factor in the end-to-end security enforcements.

Content security

Despite the protection of the device, the content that is stored on the device might be corporate owned or confidential data that needs more protection. With Fiberlink MaaS360, IBM provides solutions to control corporate mail, calendar, contacts, intranet sites, and attachments to prevent data leakage. Corporate documents can be stored securely on a mobile device in an encrypted container, which secures the copying and sharing of the data between different apps on the same mobile device.

By using this technology, the data exchange with the mainframe can also be secured on the mobile device.

Application security

Secure mobile apps require application development with security by design. IBM Security AppScan® delivers secure mobile application scanning. This technology mitigates security risks, remediates vulnerabilities, and integrates well with the IBM MobileFirst Platform security interfaces. IBM MobileFirst Platform is a Mobile Enterprise Application Platform (MEAP) that enables the development of mobile applications as an open, comprehensive, and secure platform for mobile apps for various mobile operating environments. It provides functions for safeguarding mobile security at the device, application, and network layer. It also forms a central interface to govern the mobile app portfolio across all Mobile Platforms. Together, AppScan and IBM MobileFirst Platform form the closed loop for mobile applications that integrates with the security enforcements on z Systems.

Transaction security

A mobile transaction requires end-to-end security for every transaction (including user authentication, identity federation, and fine-granular authorization to the logging and auditing functions).

IBM Security Access Manager for Mobile provides mobile access security protection in a modular package. It addresses mobile security challenges by proactively enforcing access policies for web environments and mobile collaboration channels. It also integrates with IBM z/OS® LDAP security server.

The layers of transactional defense can be established by adding runtime protection to secure applications against hacking and malware attacks. This protection is provided by IBM Security Trusteer® Apex Advanced Malware Protection. This feature focuses on fraud detection and Arxan Application Protection for IBM Solutions, which extends AppScan with transactional security. This feature integrates transactional security with fraud detection.

Integrate mobile with the IBM mainframe

Mobile security can be hardened by using the integration points of the IBM z Systems security products and deploying as much of the mobile infrastructure on z Systems as possible.

The z/OS Security Server Resource Access Control Facility (IBM RACF®) is a key component for the most securable and highly certified z Systems platform. The z Systems Processor Resource/System Manager (PR/SM) logical partitioning (LPAR) is rated at Evaluation Assurance Level 5+ (EAL 5+) for secured isolation and is functioning in the following ways:

- A Mobile environment runs in an LPAR and multiple LPARs are Multitenant based on the z Systems security isolation.
- Mobile user identities can be propagated to RACF, which ensures the resource protection of mission critical data and applications.

- Products, such as IBM Security zSecure™, help security administrators to understand access permissions to Mainframe resources, such as data, applications, and transactions. It also detects vulnerabilities and performs compliance checks against internationally recognized security standards.
- RACF can form the back-end for an LDAP server, such as IBM Tivoli® Directory Server for z/OS, which provides an easy integration between mobile workloads and z Systems security.
- RACF provides logging of security events. It can also integrate the mainframe security events into an enterprise-wide Security Information and Event Management (SIEM) solution, such as IBM QRadar® Security Intelligence Platform, by using IBM Security zSecure. This integration provides holistic security monitoring for the mobile transactions.

Secured zones prefixing mobile

A secured mobile solution can be prefixed by creating a Security Gateway in an isolated Security zone, which is sometimes called a demilitarized zone (DMZ), as shown in Figure 4 on page 7. The implementation can be done by using technologies, such as IBM DataPower Gateway, IBM MessageSight, or IBM Security Access Manager for Mobile. This zone can be responsible for identity verification, validation, and caching to relieve the mobile environment.

Security intelligence

The security intelligence layer represents the unification of the security information and enforcements for mobile workloads end-to-end. Every second, hundreds of security events occur in your IT environment. The challenge is deciding which of these events form a real incident that requires further investigation. A SIEM solution delivers visibility and clarity to defeat advance threats and spot malicious insiders. IBM QRadar Security Intelligence provides a unified architecture for integrating mobile SIEM, log management, anomaly detection, and vulnerability management. To achieve this goal, QRadar integrates with a large set of security devices and applications (such as IBM Security Access Manager for Mobile and Security zSecure). This configuration enables a single point of control for end-to-end security.

Figure 3 shows many of these products and where they are in the topology of an overall solution.

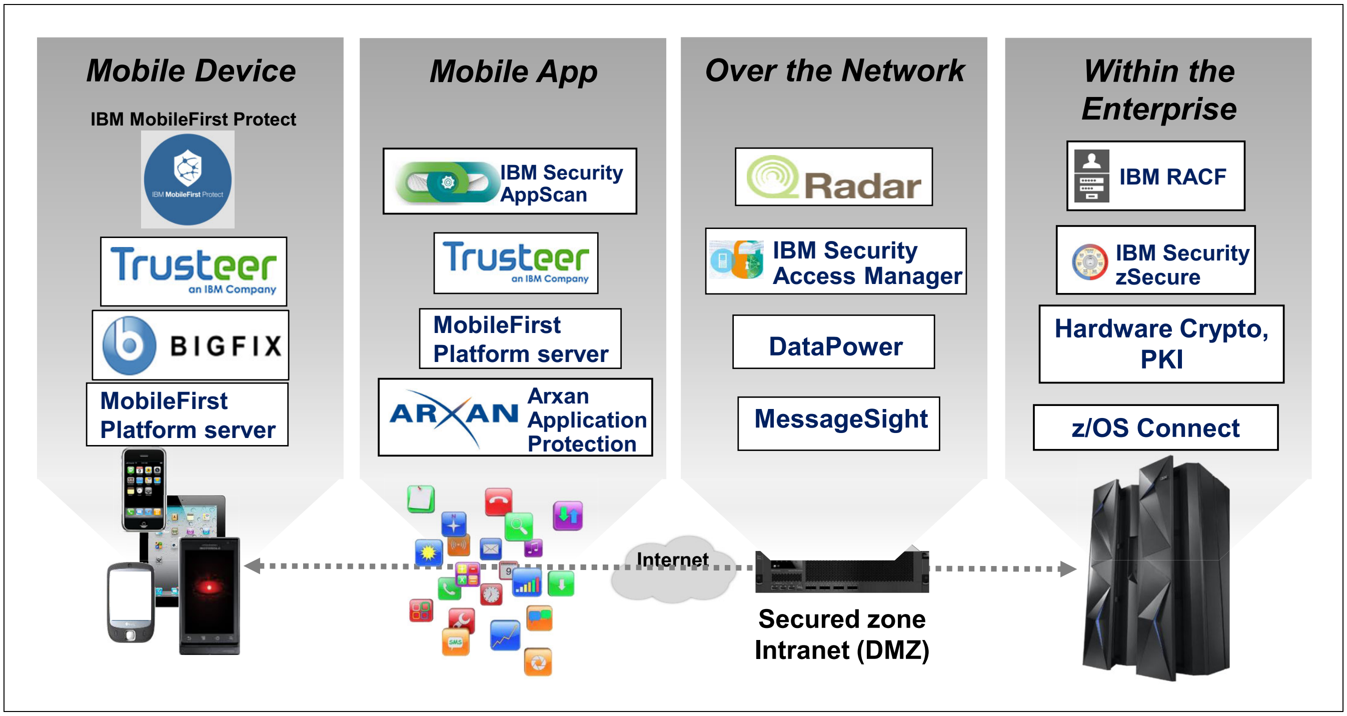

Figure 3 Available solution products and what they secure

What's next: How IBM can help

With the rich portfolio for mobile solutions and the world class experience, IBM can help build your end-to-end secured mobile solutions.

Recommended end-to-end security

End-to-end security solutions can require that the mobile user's identity flows with the request message; passing through different layers of the application architecture until it arrives in the back-end mainframe. This process is important to ensure end-to end integrity.

Figure 4 shows the transactional end-to-end security check points from a mobile device, which uses a Security Gateway with DataPower that then integrates with z Systems security. This implementation is recommended for optimal end-to-end security.

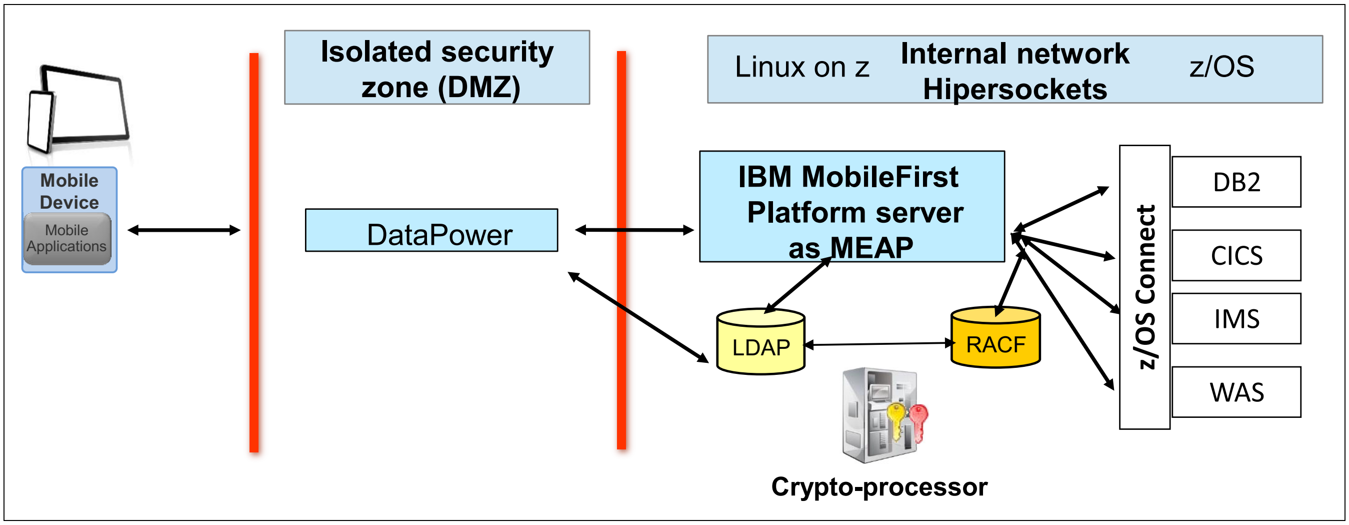

Figure 4 End-to-end security checkpoints

The following components are involved in end-to-end security and shown in Figure 4:

- MEAP server is protected by a security gateway. The mobile client must authenticate and validate credentials upon encountering the gateway.
- With successful validation, the request is sent to the IBM MobileFirst Platform Server. The following requirements must be met for an end-to-end secured application:
  - The Mobile App is developed to store all its local data in an encrypted container and uses secured connections, which also use the z Systems hardware crypto facilities. This configuration ensures secured communication from the mobile application to the MEAP.
  - With IBM DataPower Gateway, user authentication and single sign-on (SSO) is used to authenticate the mobile user that is exchanging a security token (LTPA). This requirement ensures authentication between the mobile application and the MEAP.
  - The user authentication is propagated to the IBM Security Directory Server (formerly IBM Tivoli Directory Server) LDAP user registry, which can be linked to the RACF z Systems security repository. This configuration ensures secure authentication from the MEAP to the System of Record.
  - In addition to the authentication process, threat protection and traffic control can be enabled by using DataPower Gateway, which provides data flow control.
  - Mobile App updates and application authenticity can be implemented with IBM MobileFirst Platform enforcements. This implementation prevents fraud and enforces central control of the mobile application accessing the MEAP.
  - Mobile-initiated transactions run under unique mainframe transaction IDs and associated user IDs, which ensures transactional integrity.
  - Integration with RACF access control mechanisms is used to authorize the IBM MobileFirst Platform Server and Adapters to the back-end IBM CICS® transactions with the IBM z/OS Connect offering. This feature increases flexibility to access back-end data and transactional services. It also adds security interfaces to isolate and prioritize mobile workloads by using enterprise security policies.
- To secure the network, the communication inside z Systems can be HiperSocket (IBM technology for high-speed communications between partitions and Virtual servers). It provides hardware TCP/IP connections between different operating systems, including IBM z/VM®, Linux on IBM z Systems, and z/OS.

The mainframe also can be the corporate directory or form the certificate and key management platform.

IBM is focused on mobile solutions that are hosted on z Systems that enable end-to-end security and transactional integrity from the mobile device to the SoR. This focus includes the following areas:

- Protecting the privacy of sensitive business data and the controlled sharing of information, whether internal or external to an enterprise.
- Services that are designed to provide enhanced encryption technologies for mobile applications to help protect privacy, provide an audit trail, and help reduce fraudulent activities.

The IBM z13™ provides a platform that can host SoE and SoR with visualization that isolates workloads. This platform helps ensure the privacy and security of workloads and critical data while maintaining high levels of infrastructure, application, and data availability. Mobile workloads benefit from the enhanced virtualization capabilities of the Crypto Express5S that supports up to 85 LPARs (a 5X improvement over the zEC12). This feature enables SoE and SoR to maximize the security of hardware-based cryptography, which helps to ensure the privacy of communications and sensitive data. Over 300 functions are accelerated with the new Crypto Express5S, which brings a new level of capability to applications on IBM z Systems.

> *“Running our mobile banking service on Linux on IBM zEnterprise® is another step forward in our continual evolution on the mainframe. The key value for our business is that the most important services can be managed together on a consistent, stable, and highly secure platform that offers enormous scalability and performance.”*
>
> *Daniele Cericola, ICT Governance Manager, Banca Carige.*

Customer examples

Secured Mobile solutions on IBM z Systems include a broad range of industries and organizations. Use cases apply to financial institutions, healthcare, education, computer services, retail, and many more.

The following three examples give more information about how IBM helped customers with their security solutions.

Secured mobile app (public sector)

A government institution proposed a line of business (LoB) service delivery model in which human resource (HR) services must meet customer demands. The demands were for mobile access to highly secure, mainframe-based HR and payroll Systems of Record at all the service centers across the country.

Starting with one HR service center, IBM proved the end-to-end security for mobile access of mainframe-centric, older HR, and payroll systems and the integration of the mobile security with the z Systems policies. The service center used the IBM MobileFirst Platform development suite and IBM DataPower Gateway as the security gateway. Authentication (and by using internal networks for the secured Identification propagation to the Systems of Record collocated on z Systems) enabled them to meet their business objectives for an end-to-end mobile security system that complies with strong mainframe security rules.

Secured mobile solution (financial)

A bank required a secure mobile solution that ensures secure and easy access for customers and accelerating development and deployment of new mobile functions while using banking functions on z Systems.

By using IBM MobileFirst Platform on z Systems, the bank used its security system. IBM MobileFirst Platform integrates with the company's directories, data stores, and authentication mechanism on z Systems, which provided the end-to-end security solution that they needed. To ensure secure and easy access for customers, the single sign-on feature of the IBM MobileFirst Platform enables customers to start the stock trading application if they are authenticated already with the mobile banking application. This configuration also depended on the global security policy in place and the bank's core back-end transactional environment that is secured with RACF and the IBM Security zSecure suite.

The bank can notify their customers by using push notifications if important changes are required or if banking transactions occurred with a specified amount. Customers are easily, securely, and accurately informed of important matters that are relevant to their banking accounts.

Secured mobile app (healthcare)

A hospital wanted to build a secure platform and increase responsiveness and their perceived value by reducing multi-platform development costs. They built a secure platform that was based on IBM MobileFirst Platform, which they developed once for multiple mobile platforms. It incorporates an extensible authentication model as part of its functions. To comply with the Federal Information Processing Standard (FIPS), the hospital protects the application and associated access adapters for the back-end servers and data. This configuration ensures that doctors have access to their patient's information, and medical suppliers have access to check inventory and update stock that is based on z Systems security policies in place.

The hospital increased responsiveness and perceived value perception with an application that provides instant and secure communication for doctors and nurses to find colleagues without stopping their activities. Patients can now pre-register for appointments and enter their allergies and health history by using mobile devices and secured connections to the back-end z Systems processes.

Resources for more information

For more information about the concepts that are described in the paper, see the following resources:

- IBM MobileFirst Platform:

  `http://www.ibm.com/software/products/en/mobilefirstplatform`
- IBM Mobile Security:

  `http://www.ibm.com/software/solutions/mobile-enterprise/security/solutions.html`
- Mainframe software for IBM System z (includes mobile):

  `http://www.ibm.com/software/os/systemz/mobility/`
- *IBM System z in a Mobile World Providing Secure and Timely Mobile Access to the Mainframe*, SG24-8215:

  `http://www.redbooks.ibm.com/abstracts/sg248215.html`
- IBM - 2014 Global Frost & Sullivan Award for Customer Value Leadership (mobile security, mobile identity, and access management solutions):

  `http://www.frost.com/prod/servlet/press-release.pag?docid=290770232`
- MaaS360 main page:

  `http://www.maas360.com/products/`
- IBM Security AppScan:

  `http://www.ibm.com/software/products/en/appscan`
- IBM Security Access Manager for Mobile:

  `http://www.ibm.com/software/products/en/access-mgr-mobile/`

- IBM Security Trusteer Apex™ Advanced Malware Protection:

  http://www.trusteer.com/products/trusteer-apex
- Arxan Application Protection for IBM Solutions:

  http://www.ibm.com/software/products/en/arxan-application-protection
- IBM Security zSecure suite:

  http://www.ibm.com/software/security/products/zsecure/products.html
- IBM DataPower Gateways:

  http://www.ibm.com/software/products/en/ibm-datapower-gateways
- IBM MessageSight:

  https://developer.ibm.com/messaging/messagesight/
- IBM QRadar Security Intelligence:

  http://www.ibm.com/software/products/en/qradar
- IBM MobileFirst Protect:

  https://www.ibm.com/partnerworld/wps/servlet/ContentHandler/pw_sol_smp_mobilefirst-protect

A special Thank You to the authors of the previous edition of this point-of-view:

- Wilhelm Mild
- Martina von dem Bussche
- Robert L. Kennedy

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AppScan®
CICS®
DataPower®
IBM®
IBM MobileFirst™
IBM z13™
PR/SM™
QRadar®
RACF®
Redbooks (logo) ®
System z®
Tivoli®
Trusteer®
WebSphere®
z Systems™
z/OS®
z/VM®
z13™
zEnterprise®
zSecure™

The following terms are trademarks of other companies:

Fiberlink, MaaS360, and We do IT in the Cloud. device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company.

Trusteer Apex, and Trusteer logo are trademarks or registered trademarks of Trusteer, an IBM Company.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

REDP-5176-01

ISBN 0738454885

Printed in U.S.A.