Reference Architecture for Mobile Security on System z

November, 2014
Abstract
This guide is meant to provide education on best practice for creating secure mobile application infrastructures on System z. It covers the MobileFirst security products and how those can be used to secure mobile applications on System z.

Purpose
This guide is meant to be used by
• IT Management and IT Architects – to learn about the MobileFirst security products and how they work with System z.
• IT Architects – to start creating mobile security architecture designs.

This guide is meant to identify the key security components of a mobile solution, where they all run, and how they interact. It also shows examples of some specific mobile environments and how their security requirements can be met.
How to use the z System Mobile guides…
We recommend reading these in this order…

1. Reference Architecture for Mobile Infrastructure on System z
   March 18, 2014
   Steve Wehr, Nigel Williams, Wilhelm Mid, Frank van der Wal

   Contents
   ▪ Components of a mobile architecture.
   ▪ Mobile topology choices.
   ▪ MobileFirst Platform in production.
   ▪ MobileFirst Platform in dev/test
   ▪ Scalability and performance considerations.
   ▪ Conclusion

2. System z Mobile Connectivity Guide
   June 2014
   Steve Wehr

   Contents
   ▪ Summary of z mobile connectivity options, including MobileFirst Platform Foundation
   ▪ Details about
     ▪ Push Notification
     ▪ IBM API Management
     ▪ CICS
     ▪ IMS
     ▪ DB2
     ▪ WMB

3. Reference Architecture for Mobile Security on System z
   November, 2014
   Steve Wehr

   Contents
   ▪ Introduction to the MobileFirst security products – what they do and how they relate to System z.
   ▪ Building a Secure Enterprise Mobile environment using the MobileFirst Security products.
   ▪ Use Cases and Reference Architectures.
Table of Contents

- **Introducing the MobileFirst family of Security products.**
- **Building a Secure Enterprise Mobile environment using the MobileFirst Security products.** More about the MobileFirst security products, where they run, and how they integrate with System z.
- **Use Cases and Reference Architectures.** A set of customer use cases and the reference architectures that secure the mobile application in each use case. Includes guidance on which security products apply best in each use case.

Who Should Read

IT Management, IT architects, and others looking for general information about the MobileFirst Security products.

IT architects designing mobile security solutions.
The Team that wrote this guide.

- Nigel Williams – System z security SME, MOP
- Steve Wehr – System z Mobile Offering Manager
- Romney White – System z Mobile architect
- John Petreshock – System z Security Product Manager
- John Dayka – System z Security Architect
- Jason Keenaghan – SWG Security Systems, ISAM product manager
Introducing the MobileFirst Security family of products.

An introduction to all the products, what they do, and how they help secure mobile applications on System z.
As mobile grows, so do security threats

In 2014 the number of cell phones (7.3 billion) will exceed the number of people on the planet (7 billion).¹

Mobile downloads will increase to 108 billion by 2017.²

Mobile malware is growing. Malicious code is infecting more than 11.6 million mobile devices at any given time.³

Mobile devices and the apps we rely on are under attack. 90% of the top mobile apps have been hacked.⁴
### Imperatives to securing the mobile enterprise

- Mitigate security risk across devices, applications, content and transactions
- Monitor enterprise security across all endpoints
- Manage mobility across the enterprise

<table>
<thead>
<tr>
<th>Device Security</th>
<th>Content Security</th>
<th>Application Security</th>
<th>Transaction Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Manage the mobile enterprise with BYOD, BYOA, secure e-mail and document sharing</td>
<td>• Secure file and document sharing across devices and employees including integration with SharePoint</td>
<td>• Instrument applications with security protection by design</td>
<td>• Secure mobile transactions from customers, partners and suppliers</td>
</tr>
</tbody>
</table>

#### Security Intelligence

Correlate mobile security events with broader infrastructure including log management, anomaly detection and vulnerability management for proactive threat avoidance
IBM Security capabilities for the mobile enterprise

<table>
<thead>
<tr>
<th>Device Security</th>
<th>Content Security</th>
<th>Application Security</th>
<th>Transaction Security</th>
</tr>
</thead>
</table>
| • Solutions to manage a diverse set of mobile devices from corporate owned assets to BYOD, all from the cloud | • Solutions to help secure file and document sharing across devices and SharePoint | • Solutions to develop applications with security by design  
• Protect enterprise data in both the applications you build and the applications you buy | • Solutions to help protect mobile transactions with customers, business partners and temporary workers that are not part of your enterprise mobile management framework |

Security Intelligence

A unified architecture for integrating mobile security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management
### Security features capabilities for the mobile enterprise

#### Device 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

#### Content Security
- 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

#### Application Security
- Software Development Lifecycle
  - Integrated Dev 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

#### Transaction Security
- 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
Security solutions for the mobile enterprise

Device 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

Content Security

- Software Development Lifecycle
  - Integrated Development Environment
  - iOS / Android Static Scanning
  - Application Protection
  - App Wrapping
  - App Hardening & Run-Time Protection
  - Run-Time Risk Detection
  - Whitelist / Blacklist Applications

Application Security

- Access
  - Mobile Access Management
  - Identity Federation
  - API Connectivity
- Transactions
  - Mobile Fraud Risk Detection
  - Cross-channel Fraud Detection
  - Browser Security / URL Filtering
  - IP Velocity

Transaction Security

- IBM Security AppScan
- IBM Security Access Manager
- IBM RACF
- IBM Distributed Identity Data
- IBM InfoSphere Guardium
- IBM DataPower
- z/OS Connect

Powered by:

- IBM MobileFirst Platform
- IBM MobileFirst Protect
- IBM QRadar Security Intelligence Platform
- IBM AppScan
- IBM Access Manager
- IBM RACF
- IBM Distributed Identity Data
- IBM DataPower
- z/OS Connect
- IBM QRadar Security Intelligence Platform
- IBM AppScan
- IBM Access Manager
- IBM RACF
- IBM Distributed Identity Data
- IBM DataPower
- z/OS Connect
What part of the mobile environment does each product Secure?

**Mobile Device**
- Manage device
  - Set appropriate security policies
  - Register
  - Compliance
  - Wipe
  - Lock
- Secure Data
  - Data separation
  - Leakage
  - Encryption

**Application Security**
- Offline authentication
  - Application level controls

**Mobile App**
- Secure Application
  - Utilize secure coding practices
  - Identify application vulnerabilities
  - Update applications
- Integrate Securely
  - Secure connectivity to enterprise applications and services

**Over the Network**
- Secure Access
  - Properly identify mobile users and devices
  - Allow or deny access
- Connectivity
- Monitor & Protect
  - Identify and stop mobile threats
  - Log network access, events, and anomalies

**Within the Enterprise**
- Transaction Security
  - Properly identify mobile users and transactions
- Access control
  - Control access to critical applications and data
What part of the mobile environment does each product Secure?

**Mobile Device**
- IBM MobileFirst Protect
- Trusteerr an IBM Company
- IBM MobileFirst Platform

**Mobile App**
- IBM Security AppScan
- Trusteerr an IBM Company
- IBM MobileFirst Platform
- Arxan Application Protection

**Over the Network**
- IBM Security Access Manager
- Radar
- DataPower
- IBM Security zSecure
- IBM RACF

**Within the Enterprise**
- Hardware Crypto, PKI
- z/OS Connect
Key Mobile Security Products -- end to end execution flow

- IBM Security AppScan
- Arxan Application Protection
- Trusteer
- IBM Security Access Manager
- DataPower
- MobileFirst Protect
- MobileFirst Platform
- IBM RACF
- IBM Security zSecure
Building a Secure Enterprise Mobile environment using the MobileFirst Security products.

More about the MobileFirst security products, where they run, and how they integrate with System z.
1. Start with the most secure operating system, applications and database

2. Build, deliver, deploy & maintain secure mobile applications

3. Identify and correct security vulnerabilities as the application is developed and maintained
IBM System z Core Capabilities

Resilience and security have long been hallmarks of mainframe computing, making System z the application computing platform of choice.

**Client Challenge**

Customer’s security challenges are compounded by starting with less secure computing platforms.

**Solution**

z/OS has the highest security rating or classification of any commercially available system.

**Key Benefits**

- RACF and IDID provides discrete, end to end authentication, transaction auditing, and identity mapping
- Cryptography options supports advanced encryption processing
- PKI services centrally manage certificates
- High level security connection to backend applications via hipersockets
IBM MobileFirst Platform

Build and manage mobile applications with security

- **Challenge:** Create an open, comprehensive, secure platform that manages HTML5, hybrid and native mobile apps.

- **Solution:** Secure the application, reduce both development and maintenance costs, improve time-to-market and enhance mobile app governance and security.

- **Key benefits**
  - Support multiple mobile operating environments and devices with the simplicity of a single, shared code base
  - Connect and synchronize with enterprise data, applications and cloud services
  - Safeguard mobile security at the device, application and network layer
  - Govern your mobile app portfolio from a central interface

More Information

- Website
- Case Study
- Datasheet
IBM Security AppScan

Static, dynamic and interactive application security testing

- **Challenge:** Build in security during development of mobile applications as well as assess the security of existing applications.

- **Solution:** Mitigate application security risk and establish policies, scale testing and prioritization and remediation of vulnerabilities.

- **Key benefits**
  - Promotes secure mobile application development
  - Provides enhanced mobile application scanning
  - Delivers comprehensive application security assessments to measure and communicate progress to stakeholders
  - Prioritizes application assets based on business impact and highest risk
  - Integrates with IBM MobileFirst Platform projects

**More Information**

- Free Trial
- Client Brochure
- Analyst Report
- Solution Brief
Secure the Users & Devices for the Mobile Enterprise

4. Secure the device

5. Authenticate and authorize the user
MobileFirst Protect Enterprise Mobility Management

*Instantly deploy, manage and secure devices, apps and content in the enterprise*

- **Challenge:** Businesses need flexible and efficient ways to promote their mobile initiatives while protecting data and privacy.

- **Solution:** Deliver comprehensive mobile management and security capabilities for users, devices, apps, documents, email, web and networks.

- **Key benefits**
  - Support corporate and employee-owned devices
  - Promote dual persona with full containerization and BYOD privacy
  - Take automated action to ensure compliance with policies
  - Control emails and attachments to prevent data leakage
  - Distribute, secure and manage mobile applications
  - Allow corporate documents on mobile devices securely
  - Filter and control access to the web and corporate intranet sites

**More Information**

- Data Sheets
- Videos
- Case Studies
- White Papers
- Free 30-day Trial
Trusteer Mobile

Risk-aware mobile application and risk-based mobile transaction assessment

- **Challenge:** Compromised devices and applications create fraud risk and an insecure environment.

- **Solution:** Dynamically detect device risk factors and capture the underlying device.

- **Key benefits**
  - Accurately detects device risk factors
  - Allows or restricts sensitive mobile application functions based on risks
  - Mobile transaction risk can be correlated with cross-channel risk factors to detect complex fraud schemes.
  - Promotes comprehensive risk assessment and secure application development
  - Helps secure transactions from devices to the back office
  - Integrates with IBM MobileFirst Platform projects

More Information

- Website
- Whitepaper
- Trusteer Mobile SDK
- Trusteer Mobile App
IBM Security Access Manager for Mobile

Safeguard mobile, cloud and social interactions

- **Challenge:** Provide secure access to mobile apps and reduce the risks of user access and transactions from the mobile devices.

- **Solution:** Deliver mobile single sign-on and session management, enforce context-aware access and improve identity assurance.

- **Key benefits**
  - Protects the enterprise from high risk mobile devices by integrating with Trusteer Mobile SDK
  - Built-in support to seamlessly authenticate and authorize users of MobileFirst Platform developed mobile applications
  - Enhances security intelligence and compliance through integration with QRadar Security Intelligence
  - Protects web and mobile applications against OWASP Top 10 web vulnerabilities with integrated XForce threat protection
  - Reduces TCO and time to value with an “all-in-one” access appliance that allows flexible deployment of web and mobile capabilities as needed

More Information

- Website
- Whitepaper
- Datasheet
- Demo Video
- Webinar
IBM DataPower

A secure gateway protecting and optimizing mobile interactions

- **Challenge:** Provide secure access to mobile apps and reduce the risks of user access and transactions from the mobile devices.

- **Solution:** Use DataPower to connect Mobile Applications with Enterprise Apps & Services: IMS, CICS, DB2, etc.

- **Key benefits**
  - Highest level of protection for back-end service calls
  - Pre-processing of messages to reduce load on back end
  - Resiliency, scalability, and acceleration at the edge
  - Configuration, not coding
  - Hardened security for mobile access
  - Rapid deployment and change management

More Information

- [Website](#)
- [Redbook](#)
- [Datasheet](#)
- [Demo Video](#)
Secure the Mobile Enterprise Run Time Environment

6. Protect the applications against hacking attacks & malware
7. Monitor databases in real time for vulnerabilities
8. Monitor operating system in real time for vulnerabilities
Arxan Application Protection for IBM Solutions

- **Challenge:** Protect applications to make them self-defending, hardened, and tamper-resistant “out in the wild” against hacking attacks and malware exploits.

- **Solution:** Instrument a risk-based custom Guard Network in the application binary that enables it to defend against compromise, detect attacks at run-time, and react to ward off attacks.

- **Key benefits**
  - “Multi-layer interconnected Guard Network for defense-in-depth and no single point of failure
  - Breadth of static & run-time Guard types vs. threats
  - Automated variability and randomization for each build
  - No source code changes with binary-based guard injection engine
  - Broadest multi-platform support to enable standardization
  - No impact to user experience, negligible performance impact
  - Validated with MobileFirst Platform and AppScan, tested with Trusteer

More Information

- Website
- Whitepaper
- Datasheet
- Webinar
IBM Security zSecure

*Automates routine RACF administration tasks and provides proactive compliance reporting for the mainframe operating system and sub-systems*

**Client Challenge**

The mainframe is a complex platform; inattention to configuration management details can create vulnerabilities

**Solution**

Automate proactive security scans and provide real-time alerts of suspicious activities

**Key Benefits**

- Enables more efficient and effective RACF administration, using significantly less resources
- Automatically analyzes and reports on security events and detects security exposures
- Provide real-time mainframe threat monitoring allowing you to monitor intruders
IBM InfoSphere Guardium

IBM Guardium Provides Real-Time Database Security & Compliance for Data at Rest, Data in Motion, and Configuration Data

Client Challenge

Companies must proactively prepare for data breaches and be made immediately aware when their data is at risk.

Solution

Protect data assets with activity monitoring, vulnerability analysis, data classification, data masking, entitlement reporting, actions blocking and data quarantine

Key Benefits

- Continuous, policy-based, real-time monitoring of all database activities, including actions by privileged users
- Database infrastructure scanning for missing patches, misconfigured privileges and other vulnerabilities
- Data protection compliance automation
Real-time security intelligence for the Mobile Enterprise

9. Aggregates and analyzes security event to identify high priority concerns
IBM QRadar Security Intelligence

*Deliver mobile security intelligence by monitoring data collected from other mobile security solutions – visibility, reporting and threat detection*

**Client Challenge**
Visibility of security events across the enterprise, to stay ahead of the threat, show compliance and reduce risk.

**Solution**
Use event correlation to identify high probability incidents and eliminate false positive results.

**Key Capabilities**
- Document user, application and data activity to satisfy compliance reporting requirements
- Protect private data and intellectual property by detecting advanced persistent threats
- Inspect network device configurations, visualize connections and perform attack path simulations to understand assets at risk
- Perform scheduled and real time asset vulnerability scanning and prioritization to stay ahead of possible attacks
Use Cases

Use cases for mobile security, and the reference architectures to implement each of them.
List of Use Cases
These use cases represent some common mobile implementations.

<table>
<thead>
<tr>
<th>Business to Employee</th>
<th>Business to Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee app</td>
<td>Employee app</td>
</tr>
<tr>
<td>with non-sensitive data</td>
<td>with sensitive data</td>
</tr>
<tr>
<td>Jump to this use case</td>
<td>Jump to this use case</td>
</tr>
<tr>
<td>Consumer Financial Services app</td>
<td>Consumer Insurance app</td>
</tr>
<tr>
<td>Jump to this use case</td>
<td>Jump to this use case</td>
</tr>
<tr>
<td>Consumer Retail app</td>
<td>Jump to this use case</td>
</tr>
</tbody>
</table>
List of Use Cases
These use cases represent the most common mobile implementations, and address most of the security considerations that are described on the following pages.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Security Concerns / Issues to be solved</th>
</tr>
</thead>
</table>
| **Employee app with non-sensitive data.** | - BYOD, or company-provided device.  
- B2E  
- No sensitive data will be sent to the device.  
- Intranet and internet access.  
- Limited (but large) number of users.  
- Single sign-on |
| **Employee app with sensitive data.** | - Company-provided devices.  
- B2E  
- Sensitive company and client data will be sent to the device, and stored on the device. (MobileFirst Platform Studio provides encryption for stored JSON data on the device)  
- Risk-based access to data. (Only certain data available when off the company intranet, for example)  
- Start with intranet access (on the company network) to data only, then add on the components required for internet (public network) access.  
- Limited (known) number of users.  
- Users must be authenticated with RACF. Ease of authentication is not an issue.  
- User authentication must use at least 2 factors. How to secure or narrow the window for SMS authentication phishing.  
- Ensure other apps or social media settings can not share sensitive data. |
## List of Use Cases

These use cases represent the most common mobile implementations, and address most of the security considerations that are described on the following pages.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Security Concerns / Issues to be solved</th>
</tr>
</thead>
</table>
| **Consumer Retail app**   | ▪ B2C app  
▪ No sensitive data (company or consumer) will be sent to the device.  
▪ Must work on any mobile device.  
▪ Browse only, no purchasing from within the app. If so then we revert to the banking app reqs.  
▪ Unlimited number of users. |
| **Consumer Insurance app** | ▪ B2C app  
▪ Hybrid app developed using IBM MobileFirst platform  
▪ Customer owned and varied device types  
▪ Reuse CICS services  
▪ No financial data  
▪ No data stored on device |
| **Consumer Financial Services app** | ▪ B2C app  
▪ Sensitive personal information will be sent to the device, but no data stored on the device.  
▪ Authentication must be easy to use.  
▪ Existing core banking application is re-used to serve the mobile app.  
▪ Detect most common cases of fraud. Risk-based access required  
▪ Must work on any mobile device.  
▪ Unlimited number of users. |
Considerations that influence a mobile security solution.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| 1. Mobile users               | ▪ Employee (B2E)  
▪ Customer (B2C)                                                            |
| 2. Mobile devices             | ▪ Customer owned and varied device types or BYOD or company-defined device  
▪ Is there a requirement for device register, locate, lock or wipe capabilities |
| 3. Mobile apps                | ▪ Android, iOS, Windows, other  
▪ Web, native or hybrid  
▪ Industry e.g banking, insurance, retail  
▪ Developed with MobileFirst Platform studio or with another mobile development platform  
▪ How are apps downloaded e.g public app store or enterprise app store  
▪ How are apps refreshed |
| 4. Services used by mobile app| ▪ Mainframe or distributed  
▪ CICS, IMS, DB2, WebSphere, other  
▪ Service-enabled or legacy-access  
▪ Enabled for mobile access (Restful, JSON)                                      |
| 5. Type of access             | ▪ Intranet/extranet or internet  
▪ Is a VPN required                                                             |
| 6. Number of users            | ▪ Small (10s to 100s), medium (1000s) or large (many thousands)  
▪ Known or unknown number  
▪ Is it necessary to protect against surges of requests  
▪ Is it necessary to protect against denial of service attacks                   |
Considerations that influence a mobile security solution…

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>7. Authentication</strong></td>
<td><strong>User authentication</strong></td>
</tr>
<tr>
<td></td>
<td>▪ Does each user have a unique identity</td>
</tr>
<tr>
<td></td>
<td>▪ How is the mobile user authenticated e.g user name, email address, account number …</td>
</tr>
<tr>
<td></td>
<td>▪ What authentication tokens will be used e.g LTPA</td>
</tr>
<tr>
<td></td>
<td>▪ Does the mobile user have a RACF user ID</td>
</tr>
<tr>
<td></td>
<td>▪ How is the mobile user’s identity mapped to a RACF id?</td>
</tr>
<tr>
<td></td>
<td>▪ Is single sign-on (SSO) required</td>
</tr>
<tr>
<td></td>
<td>▪ Is risk-based authentication required e.g two-factor authentication</td>
</tr>
<tr>
<td></td>
<td><strong>Device authentication</strong></td>
</tr>
<tr>
<td></td>
<td>▪ Are only a certain set of devices allowed to access the application</td>
</tr>
<tr>
<td></td>
<td>▪ Does the device need to be authenticated</td>
</tr>
<tr>
<td></td>
<td>▪ Are specific device features required e.g</td>
</tr>
<tr>
<td></td>
<td>– Near field communication (NFC) capabilities</td>
</tr>
<tr>
<td></td>
<td>– Finger print sensor</td>
</tr>
<tr>
<td></td>
<td>– Camera for visual recognition</td>
</tr>
<tr>
<td></td>
<td>– Microphone for voice recognition</td>
</tr>
<tr>
<td></td>
<td><strong>Application authentication</strong></td>
</tr>
<tr>
<td></td>
<td>▪ Does the authenticity of the application need to be checked</td>
</tr>
<tr>
<td><strong>8. Authorization</strong></td>
<td>▪ Does mobile user need to be authorized to access MEAP (Mobile Enterprise Application Platform) application</td>
</tr>
<tr>
<td></td>
<td>▪ Is risk-based access required examples:</td>
</tr>
<tr>
<td></td>
<td>– Limit access when mobile user connects from unsecure network</td>
</tr>
<tr>
<td></td>
<td>– Limit access based on mobile user location.</td>
</tr>
<tr>
<td></td>
<td>▪ What authorization tokens will be used e.g OAuth, SAML</td>
</tr>
<tr>
<td></td>
<td>▪ Does mobile user need to be authorized to mainframe enterprise applications. What RACF id is used?</td>
</tr>
</tbody>
</table>
## Considerations that influence a mobile security solution

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| 9. Audit                        | - Should access to MEAP application be audited?  
- Should access to entreprise enterprise applications be audited?  
- What information needs to be audited -- mobile user id, device location, RACF user id, resource accessed, device id |
| 10. Confidentiality             | - What is the nature of the data e.g. financial or personal  
- Does data in transit need to be encrypted  
  - Between the mobile device and MEAP  
  - Between the MEAP and enterprise systems  
- What hardware offload capabilities are currently used for SSL/TLS  
- Is data stored on the device  
- Does data on the device need to be encrypted |
| 11. Integrity                   | - Does the integrity of the data in transit need to be protected  
  - Between the mobile device and MEAP  
  - Between the MEAP and enterprise systems |
| 12. Existing security infrastructure | - Will the existing security infrastructure be reused for securing mobile access  
- What components and products are used in the existing security infrastructure  
  - Security gateway  
  - User registry  
  - Identity management and mapping  
  - Network security  
  - Digital certificates  
  - Security intelligence solution |
| 13. Security standards          | - What company standards need to be respected e.g. limits on encryption algorithms or authentication protocols, FIPS-140  
- What industry standards need to be respected e.g. PCI-DSS, HIPAA |
Use Case

Employee app with non-sensitive data
Mobile Employee Lookup app - Overview

- Employee app with non-sensitive data
  - Single Sign on access

- Using the Employee Lookup app an employee can perform the following:
  - View peer contact information
  - Find skills to match needs
  - View management hierarchy

- Employee Lookup is an application supporting Web and mobile clients. It can make calls to backend services using a variety of different interfaces (Restful services, web services, JDBC, for example...)

## Employee Lookup mobile app security requirements

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Mobile users</td>
<td>▪ Employee (B2E)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Mobile devices</td>
<td>▪ BYOD or company-defined device</td>
<td>Ability to enforce security requirements on device such as PW length, company ability to wipe phone, etc.</td>
<td>MobileFirst Protect</td>
</tr>
<tr>
<td></td>
<td>▪ Customer owned and varied device types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Mobile apps</td>
<td>▪ Android, iOS, Windows, other</td>
<td>Build in security during development</td>
<td>MobileFirst Platform</td>
</tr>
<tr>
<td></td>
<td>▪ Web, native or hybrid</td>
<td>Use MEAP capabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Type of enterprise services reused by mobile app</td>
<td>▪ Mainframe or distributed</td>
<td>Secure adapter which provides interface between mobile app and DB2 services</td>
<td>• MobileFirst Platform adapter security</td>
</tr>
<tr>
<td></td>
<td>▪ DB2, WebSphere, other</td>
<td></td>
<td>• RACF</td>
</tr>
<tr>
<td></td>
<td>▪ Service-enabled or legacy-access</td>
<td></td>
<td>• DB2</td>
</tr>
<tr>
<td></td>
<td>▪ Enabled for mobile access (Restful, JSON)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Type of access</td>
<td>▪ Intranet and Internet</td>
<td>Access via DMZ</td>
<td>Reuse existing DataPower security gateway</td>
</tr>
<tr>
<td>6. Number of users</td>
<td>▪ Varies dependent on company size</td>
<td>Protect against denial-of-service attacks</td>
<td>DataPower threat protection and traffic control</td>
</tr>
</tbody>
</table>

© 2014 IBM Corporation
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
</table>
| 7. Authentication | **User authentication**  
• Mobile users must authenticate with a employees email address/userid and password | Mobile user authenticated by security gateway. Use Lightweight Third-Party Authentication (LTPA) as a single sign-on (SSO) token. | • Implement SSO between mobile device, **DataPower** and **MobileFirst Platform** server.  
• MobileFirst Protect for Device authentication |
| 8. Authorization |                                                                                | MobileFirst Platform ID to be used for authorization to DB2                               | **MobileFirst Platform Server**                                      |
### Employee Lookup mobile app security requirements (cont…)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Audit</td>
<td>Not required.</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>10. Confidentiality</td>
<td>Employee info is confidential, SSL connection</td>
<td>Secure Connections</td>
<td>openSSL</td>
</tr>
<tr>
<td>11. Integrity</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>12. Existing security infrastructure</td>
<td>Reuse RACF and DB2 access controls</td>
<td>RACF</td>
<td>DB2</td>
</tr>
<tr>
<td>13. Security standards</td>
<td>None</td>
<td>None</td>
<td>none</td>
</tr>
</tbody>
</table>
1. AppScan is used to scan the Employee Lookup mobile application for security vulnerabilities
2. MobileFirst Protect for company security policy enforcement and app deployment
3. DataPower is used for threat protection and traffic control
4. User authentication is done against the existing IBM Security Directory Server LDAP user registry
5. MobileFirst Platform pushes application updates and tests the authenticity of the mobile application
6. Crypto HW exploitation on openssl though Linux on System z Stack
7. Mobile initiated DB2 stored procedure invocations are presented by the MobileFirst Platform Server
8. Existing RACF access control mechanisms are used to authorize DB2 Queries
Mobile Employee Lookup app—security solution steps
(Map to numbers on previous chart)

1. **Built-in Security** – Develop mobile application using IBM MobileFirst Platform Studio and employ IBM AppScan to identify potential security exposures.

2. **Automation** – Use MobileFirst Protect to provide the ability to take automated action to ensure compliance with security policies on device such as remote wipe, PW format requirements. Also, APP store allows the securely distribute and manage mobile applications.

3. **Threat protection and traffic control** – Deploy WebSphere DataPower for threat protection and traffic control.

4. **Integration with existing user directory** - User authentication is done against the existing IBM Security Directory Server LDAP user registry.

5. **Application updates and application authenticity testing** – Use IBM MobileFirst Platform server to push application updates and verify the authenticity of the mobile application.

6. **Hardware Acceleration** – Exploit openssl to leverage IBM Cryptographic HW acceleration for faster SSL transaction.

7. **Mobile initiated transactions to run under user id associated with MobileFirst Platform server** - Mobile initiated DB2 stored procedures are run under the MobileFirst Platform Server’s ID

8. **Data base access controls:** Exploit RACF/DB2 Exit support for additional security flexibility.
## Architectural decisions - summary

<table>
<thead>
<tr>
<th>Architectural Decision</th>
<th>Rationale and decision points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build security into the development process</td>
<td>Use MobileFirst Platform to simplify the development process for multiple mobile platforms and provide application authentication. Use AppScan to scan mobile application during development and QA.</td>
</tr>
<tr>
<td>MobileFirst Protect</td>
<td>Ability to take automated action to ensure compliance with policies, security on device, remote wipe, PW format requirements, APP store to distribute, secure and manage mobile applications.</td>
</tr>
<tr>
<td>Use MEAP security capabilities</td>
<td>Use MobileFirst Platform features to deliver automatic updates.</td>
</tr>
<tr>
<td>Run MobileFirst Platform Server on LPAR for Linux for system z</td>
<td>Platform security (EAL 5+) for LPAR and EAL4 certification with Linux on System z.</td>
</tr>
<tr>
<td>LDAP on Z</td>
<td>The LDAP server can be configured to provide read/write access to RACF user, group, connection, and general resource profiles using the LDAP protocol.</td>
</tr>
<tr>
<td>Use a reverse proxy in the DMZ and place the MobileFirst Platform Server in the Intranet</td>
<td>Use DataPower as a mobile security gateway to protect against malicious attacks and control the rate at which mobile requests are accepted.</td>
</tr>
<tr>
<td>Use RACF/DB2 Exit for additional Control</td>
<td>Exploitation of RACF/DB2 Exit will allow centralized policy controls for your enterprise.</td>
</tr>
</tbody>
</table>
Use Case

Employee app with sensitive data
Use case writeup coming soon.
Use Case

Consumer Retail Application
Retail application (Mega Store) - Overview

- Using the Mega Store mobile application a customer can perform the following:
  - Find stores
  - Browse products
  - Compare products
  - Determine product quantity available in store
  - Receive special offers
  - Exploit location awareness

- Mega Store is a retail application supporting mobile clients
- It exploits backend capabilities using DB2 stored procedures
Mega Store – Architecture

1. Mobile user starts application and formulates search for product information or store
2. MobileFirst Platform server receives request
3. MobileFirst Platform server ensures mobile application is valid and current – automatically updates application if necessary
4. MobileFirst Platform SQL adapter transforms mobile request and calls DB2 to retrieve product information and potential special offers
5. DB2 stored procedure retrieves data
6. Product data is returned through the SQL adapter to the mobile application
Mega Store mobile application characteristics

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Mobile users</td>
<td>▪ Customer (B2C)</td>
<td>▪ Support popular mobile devices</td>
<td>▪ IBM MobileFirst Platform</td>
</tr>
<tr>
<td>2. Mobile devices</td>
<td>▪ Customer owned and varied device types</td>
<td>▪ Available via public application stores</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Mobile apps</td>
<td>▪ Android, iOS, Windows, other</td>
<td>▪ Minimize development costs</td>
<td>▪ IBM MobileFirst Platform</td>
</tr>
<tr>
<td></td>
<td>▪ Hybrid apps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Enterprise services reused</td>
<td>▪ Mainframe and distributed</td>
<td>▪ Ensure applications do not breach enterprise integrity</td>
<td>▪ IBM AppScan</td>
</tr>
<tr>
<td></td>
<td>▪ DB2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Type of access</td>
<td>▪ Internet</td>
<td>▪ Audit database access</td>
<td>▪ Guardium</td>
</tr>
<tr>
<td></td>
<td>▪ JDBC or DB2 Stored Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Number of users</td>
<td>▪ Unlimited</td>
<td>▪ Protect against denial-of-service attacks</td>
<td>▪ DataPower</td>
</tr>
</tbody>
</table>
### Mega Store mobile application characteristics (cont…)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Authentication</td>
<td><strong>User authentication</strong></td>
<td>▪ Validate application when initialized</td>
<td>▪ IBM MobileFirst Platform</td>
</tr>
<tr>
<td></td>
<td>▪ None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Application authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Must ensure app has not been compromised</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Authorization</td>
<td>▪ None</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>9. Audit</td>
<td>▪ Primarily for problem diagnosis</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>10. Confidentiality</td>
<td>▪ N/A</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>11. Integrity</td>
<td>▪ No need to protect data in transit</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>12. Existing security architecture</td>
<td>▪ RACF</td>
<td>▪ Audit database accesses</td>
<td>▪ IBM Guardium</td>
</tr>
<tr>
<td>13. Security standards</td>
<td>▪ None</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
Mega Store security solution requirements

- DataPower for traffic management, Denial-of-Service (DoS) prevention,
  - Firewall provides some protection
- AppScan recommended but not required to ensure application does not introduce security exposures
- MobileFirst Platform recommended but not required to provide application authentication and simplify the development process
- Guardium recommended but not required to ensure that mobile database access is read-only
1. AppScan is used to scan the MegaStore mobile application for security vulnerabilities
2. DataPower is used for threat protection and traffic control
3. MobileFirst Platform pushes application updates and tests the authenticity of the mobile application
4. Mobile initiated DB2 stored procedure invocations are presented by the MobileFirst Platform Server
5. Guardium ensures that only appropriate stored procedures are employed and that database access from mobile-initiated transactions is read-only
Mega Store – security solution steps

1. **Built-in Security** – Develop mobile application using IBM MobileFirst Platform Studio and employ IBM AppScan to identify potential security exposures.

2. **Threat protection and traffic control** – Deploy WebSphere DataPower for threat protection and traffic control.

3. **Application updates and application authenticity testing** – Use IBM MobileFirst Platform server to push application updates and verify the authenticity of the mobile application.

4. **Data base access authentication** – Use a technical identifier with no user identifying information to indicate that the stored procedure invocation is for a mobile device.

5. **Data base access integrity** – Use IBM Guardium to ensure that mobile data base transactions are authorized and that those transactions are read-only.
### Mega Store Architectural decisions - summary

<table>
<thead>
<tr>
<th>Architectural Decision</th>
<th>Rationale and decision points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build security into the development process</td>
<td>Use MobileFirst Platform to simplify the development process for multiple mobile platforms and provide application authentication. Use AppScan to scan mobile application during development and testing.</td>
</tr>
<tr>
<td>Use MEAP security capabilities</td>
<td>Use MobileFirst Platform security features to authenticate mobile application and deliver automatic updates.</td>
</tr>
<tr>
<td>Run MobileFirst Platform Server on Linux for System z</td>
<td>Platform security (EAL 4+) and proximity.</td>
</tr>
<tr>
<td>Use a reverse proxy in the DMZ and place the MobileFirst Platform Server in the Intranet</td>
<td>Use DataPower as a mobile security gateway to protect against malicious attacks and control the rate at which mobile requests are accepted.</td>
</tr>
<tr>
<td>Use Guardium to ensure appropriate database access</td>
<td>Use Guardium to ensure that only appropriate stored procedures are invoked by mobile requests and that those procedures are limited to read-only data base access.</td>
</tr>
</tbody>
</table>
Use Case

Consumer Insurance Application
General insurance application (GENAPP) - Overview

- Using the GENAPP mobile app a customer can perform the following:
  - View insurance policies
  - Apply for new Home, Car, or Endowment policy
  - Start an insurance claim

- Mobile app makes calls to insurance application (GENAPP) which is a CICS COBOL application that insurance company uses to create and manage customer and insurance policy data.
General insurance application (GENAPP) – architecture and transaction flow

1. Mobile user logs in to app
2. MobileFirst Platform application receives request
3. MobileFirst Platform application calls security test
4. MobileFirst Platform adapter transforms mobile request and calls CICS to retrieve customer policies
5. CICS web service framework converts the request to the channel interface of the GENAPP application
6. GENAPP Cobol application processes the insurance policy request and queries the GENAPP database
7. Policy data is returned to the mobile app
# GENAPP mobile security requirements

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Mobile users</td>
<td>• Customer (B2C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Mobile devices</td>
<td>• Customer owned and varied device types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Mobile apps</td>
<td>• Support Android, iOS and Windows devices</td>
<td>Hybrid app</td>
<td><strong>MobileFirst Platform</strong></td>
</tr>
<tr>
<td></td>
<td>• Protect against app security vulnerabilities</td>
<td>Build in security during development</td>
<td>Static code analysis with <strong>Appscan</strong>. Direct Update feature using the MobileFirst Platform</td>
</tr>
<tr>
<td></td>
<td>• App distributed using public app store</td>
<td>Use MEAP capabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• May need frequent app updates (e.g to distribute security fixes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Enterprise services reused</td>
<td>• CICS web services</td>
<td>Secure adapter which provides interface between mobile app and CICS services</td>
<td><strong>MobileFirst Platform</strong> adapter security</td>
</tr>
<tr>
<td>5. Type of access</td>
<td>• Internet</td>
<td>Access via DMZ</td>
<td><strong>DataPower</strong> security gateway</td>
</tr>
<tr>
<td>6. Number of users</td>
<td>• Unknown but estimate medium to large (1000s)</td>
<td>Limit number of requests that can be sent to MEAP</td>
<td><strong>DataPower</strong> threat protection and traffic control</td>
</tr>
<tr>
<td></td>
<td>• Need to protect against unexpected surges in mobile requests, for example when a large storm occurs that triggers lots of requests..</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criteria</td>
<td>Considerations</td>
<td>Architectural decisions</td>
<td>Product solution</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 7. Authentication| **User authentication**  
- Mobile users must authenticate with a customer number and password before they are allowed to access their insurance policy data  
- Single sign-on (SSO) required for app  
**Application authentication**  
Must ensure the app is secure by making sure that it has not been modified and redistributed containing malware or exploits that can potentially compromise systems or capture confidential customer data. | Mobile user authenticated by security gateway.  
Use Lightweight Third-Party Authentication (LTPA) as a single sign-on (SSO) token.  
Sign the mobile app. | Implement SSO between mobile device,  
**DataPower** and  
**MobileFirst Platform** server.  
**MobileFirst Platform** application authenticity check. |
| 8. Authorization | **Authenticated mobile users are authorized to access MEAP application**  
**Mobile initiated CICS transactions are only authorized if the request comes from the MobileFirst Platform Server**  
**Need to identify mobile-initiated CICS transactions for access control, tracking the workload impact of the mobile app and for Mobile Workload Pricing.** | Mobile initiated transactions to run under unique CICS transaction id and user id associated with MobileFirst Platform server | Each MobileFirst Platform server is assigned a **RACF** user id, which is then authorized to run CICS transactions. |
## GENAPP mobile security requirements (cont…)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
</table>
| **9. Audit** | • Access to MEAP application should be audited (time, customer number, type of request…)  
• Mobile app usage should be captured (device types, OS types, procedures called …)  
• Mobile-initiated CICS transaction should be audited (time, customer number, trans id, MobileFirst Platform server id …) | Audit in security gateway  
Collect analytics data in MEAP  
Audit in CICS | Use **DataPower AAA policy**  
Use **MobileFirst Platform analytics**  
Use **CICS message handler** and collect SMF 110 records |
| **10. Confidentiality** | • Data is not highly sensitive or confidential  
• Data in transit needs to be encrypted  
  – Between the mobile device and MEAP  
  – Between the MEAP and CICS  
• No data stored on the device | Use TLS/SSL for all connections | Use **RACF** to create X.509 certificates  
Use **System SSL** and **System z hardware crypto** (CEX4 and CPACF) to optimise SSL/TLS |
## GENAPP mobile security requirements (cont…)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>11. Integrity</strong></td>
<td>Integrity of the data in transit needs to be protected</td>
<td>Use TLS/SSL for all connections</td>
<td>Use <strong>System SSL</strong>, <strong>RACF</strong> and <strong>System z hardware crypto</strong></td>
</tr>
<tr>
<td></td>
<td>- Between the mobile device and MEAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Between the MEAP and enterprise systems</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **12. Existing security architecture** | ▪ DataPower already used as an SOA Security Gateway  
▪ Solution needs to use the same user directory that the insurance company maintains for customer user accounts and passwords which is a Lightweight Directory Access Protocol (LDAP) directory  
▪ Requires integration with RACF | Reuse existing security infrastructure as much as possible | **IBM Security Directory Server** hosted on the IBM System z.                     |
| **13. Security standards** | Insurance company standard is encryption for all data in transit, with specific encryption algorithms    | Limit cypher suites      | **DataPower**, **MobileFirst Platform** and **CICS** can all be configured to limit cypher key lengths and algorithms |
1. AppScan is used to scan the GENAPP mobile app for security vulnerabilities
2. HTTPS is used to protect data in transit
3. DataPower is used to authenticate the mobile user
4. User authentication is done against the existing IBM Security Directory Server LDAP user registry
5. DataPower is used for threat protection and traffic control
6. MobileFirst Platform enforces application updates and tests the authenticity of the mobile application
7. Mobile initiated CICS transactions are run with specific trans ids (e.g. MGCD) and RACF user id that represents the MobileFirst Platform Server (WKLTMOBP)
8. Existing RACF access control mechanisms are used to authorize the MobileFirst Platform Server to the set of GENAPP CICS transactions
GENAPP Mobile – security solution steps

1. **Build in security during development** – using Appscan capability integrated with MobileFirst Platform studio.

2. **Data integrity and encryption for all mobile communications** – HTTPS is used for all communications between the mobile app and MobileFirst Platform server. Hardware crypto is used to reduce the cost of SSL handshakes and data encryption.

3. **User authentication and single sign-on (SSO)** - WebSphere DataPower is used to authenticate the mobile user. DataPower creates an LTPA token which is exchanged between the mobile app and the MobileFirst Platform server, providing an application single sign-on capability.

4. **Integration with existing user directory** - User authentication is done against the existing IBM Security Directory Server LDAP user registry.

5. **Threat protection and traffic control** - WebSphere DataPower is used for threat protection and traffic control.

6. **Application updates and application authenticity testing** - MobileFirst Platform enforces application updates and tests the authenticity of the mobile application.

7. **Mobile initiated transactions to run under unique transaction id and user id associated with MobileFirst Platform server** - Mobile initiated CICS transactions are run under a RACF user id that represents the MobileFirst Platform Server. This is achieved using SSL client authentication between the MobileFirst Platform server and CICS. RACF certificates are used by MobileFirst Platform and CICS.

8. **Integration with existing RACF access control** – Existing RACF access control mechanisms are used to authorize the MobileFirst Platform Server to the set of GENAPP CICS transactions.
## Architectural decisions - summary

<table>
<thead>
<tr>
<th>Architectural Decision</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build security into the app development process</td>
<td>Use <strong>AppScan</strong> scan mobile application</td>
</tr>
<tr>
<td>Use MEAP security capabilities</td>
<td>Use wide range of <strong>MobileFirst Platform</strong> security features including flexible authentication and authorization framework and automatic updates</td>
</tr>
<tr>
<td>Run MobileFirst Platform Server in Linux for system z</td>
<td>Platform security (EAL 4+) and hardware crypto integration Co-location of MEAP and CICS services improves security and network latency</td>
</tr>
<tr>
<td>Use a reverse proxy in the DMZ and place the MobileFirst Platform Server in the intranet</td>
<td><strong>DataPower</strong> is already used as an SOA and security gateway. Extend as mobile security gateway, for user authentication, protecting against malicious attacks and controlling the rate of mobile requests that are accepted.</td>
</tr>
<tr>
<td>Mobile initiated CICS transactions run under a RACF user id that represents the MobileFirst Platform Server</td>
<td>Mobile security solution should integrate with existing <strong>RACF</strong> access control MobileFirst Platform server is authorized to run CICS transactions Track mobile-initiated transactions in order to qualify for <strong>Mobile Workload Pricing</strong> (MWP)</td>
</tr>
</tbody>
</table>

For more information see Redbook ‘**IBM System z in a Mobile World**’
Use Case

Consumer Financial services app
PolyBank app - Overview

- Using the PolyBank mobile app a customer can perform the following:
  - View accounts
  - Make account transfers
  - Pay Bills
  - Deposit Checks
  - Find Nearby Branch
  - Spend Analysis
  - Mobile Cash (Cardless ATM Withdrawal)
  - Prepaid Card Top-up
PolyBank app - Architecture

- PolyBank has a multi-channel banking application supporting 3270, Web and mobile clients
- Native mobile apps reuse the same core banking services as the PolyBank web applications
- Backend banking services are called using a Restful service interface
## PolyBank mobile security requirements

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Mobile users</td>
<td>▪ Customer (B2C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Mobile devices</td>
<td>▪ Customer owned and varied device types</td>
<td>Limit app functionality if device is compromised</td>
<td>Trusteer Mobile SDK</td>
</tr>
<tr>
<td></td>
<td>▪ Uniquely identify user device</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Detect mobile device risk factors such OS level, jailbroken or rooted, location, device orientation ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Mobile apps</td>
<td>▪ Mobile app access to bank accounts</td>
<td>Limit app functionality if malware is detected</td>
<td>Trusteer Mobile SDK</td>
</tr>
<tr>
<td></td>
<td>▪ Native Android and iOS apps are developed by separate development teams</td>
<td>Build in security during development</td>
<td>Static code analysis with Appscan</td>
</tr>
<tr>
<td></td>
<td>▪ Protect against app security vulnerabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ App distributed using public app store</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Enterprise services reused</td>
<td>▪ Mainframe and distributed</td>
<td>Evolve towards architecture of unified access to enterprise banking services</td>
<td>z/OS Connect</td>
</tr>
<tr>
<td></td>
<td>▪ CICS, DB2, WebSphere and other</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Core-banking application has Restful service interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Type of access</td>
<td>▪ Internet</td>
<td>Access via DMZ</td>
<td>IBM DataPower Gateway</td>
</tr>
<tr>
<td>6. Number of users</td>
<td>▪ Unknown but estimate very large (100s of 1000s)</td>
<td>Protection against DoS attacks</td>
<td>IBM DataPower Gateway for threat protection and traffic control</td>
</tr>
</tbody>
</table>
### PolyBank mobile security requirements (cont…)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
</table>
| **7. Authentication** | **User authentication**  
- Mobile users must authenticate with a user identity and password before they are allowed to access their account data.  
- Two factor authentication required for high risk requests  

**Device authentication**  
- Mobile device must be registered. Access to accounts from new device is flagged as a risk. | User authenticated by security gateway  
Support required for one time password (OTP) | IBM DataPower Gateway (combines DataPower and ISAM for mobile capabilities) |
| **8. Authorization**    | **Bank account access based on state of device and account access patterns**  
- Mobile gateway is authorized to access z/OS Connect Liberty server and authorized to invoke specific services  
- Mobile initiated CICS transactions are only authorized if the request comes from z/OS Connect  
- Need to identify mobile-initiated CICS transactions for access control, tracking the workload impact of the mobile app and for Mobile Workload Pricing. | Risk assessment based on mobile and non-mobile channel factors  
Control access to Restful banking services  
Control access to CICS core banking regions  
Mobile trans run under unique CICS trans id and user id of Liberty Profile server | Trusteer Mobile Risk Engine and ISAM for Mobile  
z/OS Connect authorization interceptor  
RACF CBIND profile  
Set trans id on WOLA request and propagate region id of Liberty Profile server |
PolyBank mobile security requirements (cont…)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Audit</td>
<td>▪ Access to mobile gateway should be audited (time, request id, user identity, account number, type of request…)</td>
<td>Audit records across different tiers of architecture</td>
<td>IBM DataPower Gateway (AAA policy)</td>
</tr>
<tr>
<td></td>
<td>▪ Access to Restful services should be audited (time, request id, server identity, target URI, service name …)</td>
<td></td>
<td>z/OS Connect audit interceptor</td>
</tr>
<tr>
<td>10. Confidentiality</td>
<td>▪ Data is financial therefore high confidentiality is required</td>
<td>Use TLS/SSL for all connections</td>
<td>Use System z hardware crypto (CEX4 and CPACF) to optimise SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>▪ Data in transit needs to be encrypted</td>
<td>No data to be stored on device</td>
<td></td>
</tr>
</tbody>
</table>
## PolyBank mobile security requirements (cont…)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Considerations</th>
<th>Architectural decisions</th>
<th>Product solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>11. Integrity</td>
<td>Integrity of the data in transit needs to be protected</td>
<td>Use TLS/SSL for all connections</td>
<td></td>
</tr>
</tbody>
</table>
| 12. Existing security architecture | Existing infrastructure components  
  - LDAP registry of customer credentials  
  - IBM Security Access Manager (ISAM) used for securing internet banking access  
  - CICS  
  - IMS  
  - DB2 for z/OS  
  - RACF | Reuse existing security infrastructure                                       |                                         |
| 13. Security standards          | FFIEC (Federal Financial Institutions Examination Council)                   | Implement continuous risk assessment and multiple security layers to detect fraudulent transactions. | Trusteer Mobile SDK and ISAM for Mobile |
PolyBank mobile security solution

1. AppScan is used to scan the PolyBank mobile app for security vulnerabilities
2. When app is launched a risk-score is calculated based on device factors (is the device jailbroken or rooted, geolocation, orientation of device, missing OS patches ...) as well as other factors like account transaction history, user access patterns and device-to-account correlation. Risk-score is sent in http header with mobile banking request.
3. IBM DataPower Gateway authenticates user and enables threat protection
4. ISAM proxy calls ISAM for Mobile for risk-based access check
5. Decision can be to deny access, allow access or request additional authentication (e.g. OTP)
6. Restful service requests are sent to z/OS Connect where they are authorized and audited
7. RACF CBIND profile is used to control access to CICS core banking regions
8. RACF access control mechanisms are used to authorize the Liberty Profile server to the set of CICS banking transactions
PolyBank mobile – security solution steps

1. **Build in security during development** – use Appscan capability

2. **Risk-based access for mobile banking transactions** – the Trusteer Mobile SDK installed on the mobile device collects device and account data which is used to create a risk score. The risk score is sent in an HTTP header with the mobile banking request.

3. **User authentication, threat protection and traffic control** – IBM DataPower Gateway is used to authenticate the mobile user and to protect the mobile platform from workload surges or attack

4. **Risk-based access** – implemented by Trusteer Mobile Risk Engine and ISAM for Mobile

5. **Real-time fraud detection** – ISAM for Mobile makes decision to allow request, deny request or ask for additional authentication

6. **Unified service enablement** – z/OS Connect provides a secure Restful interface to z/OS programs and applications

7. **Controlled access to core banking systems** – using RACF CBIND profiles

8. **Integration with existing transaction access control** – existing RACF access control mechanisms are used to authorize the z/OS Connect server to the set of core banking transactions.
## Architectural decisions - summary

<table>
<thead>
<tr>
<th>Architectural Decision</th>
<th>Rationale and decision points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build security into the app development process</td>
<td>Use <strong>AppScan</strong> to scan the mobile application</td>
</tr>
<tr>
<td>Limit app functionality based on device factors and account usage patterns</td>
<td>Use <strong>Trusteer Mobile Risk Engine</strong> to perform mobile risk assessment</td>
</tr>
<tr>
<td>Use a reverse proxy in the DMZ and place the mobile platform in the intranet</td>
<td>Deploy <strong>IBM DataPower Gateway</strong> which combines DataPower and ISAM for mobile capabilities</td>
</tr>
<tr>
<td>Unified access to banking services</td>
<td>Enable corebanking application as a set of Restful services using <strong>z/OS Connect</strong></td>
</tr>
<tr>
<td>Control mobile access to corebanking applications</td>
<td>Control access to CICS regions using <strong>RACF</strong> access control</td>
</tr>
<tr>
<td>Identify mobile-initiated CICS transactions</td>
<td>Tag and track mobile-initiated transactions in order to qualify for <strong>Mobile Workload Pricing</strong> (MWP)</td>
</tr>
</tbody>
</table>