

zMB3592

End-to-End Security from your Mobile device to every z/OS transaction

Wilhelm Mild
Executive IT Architect
for Mobile, z Systems and Linux
IBM Lab Boeblingen, Germany



2015

IBM Systems Technical University

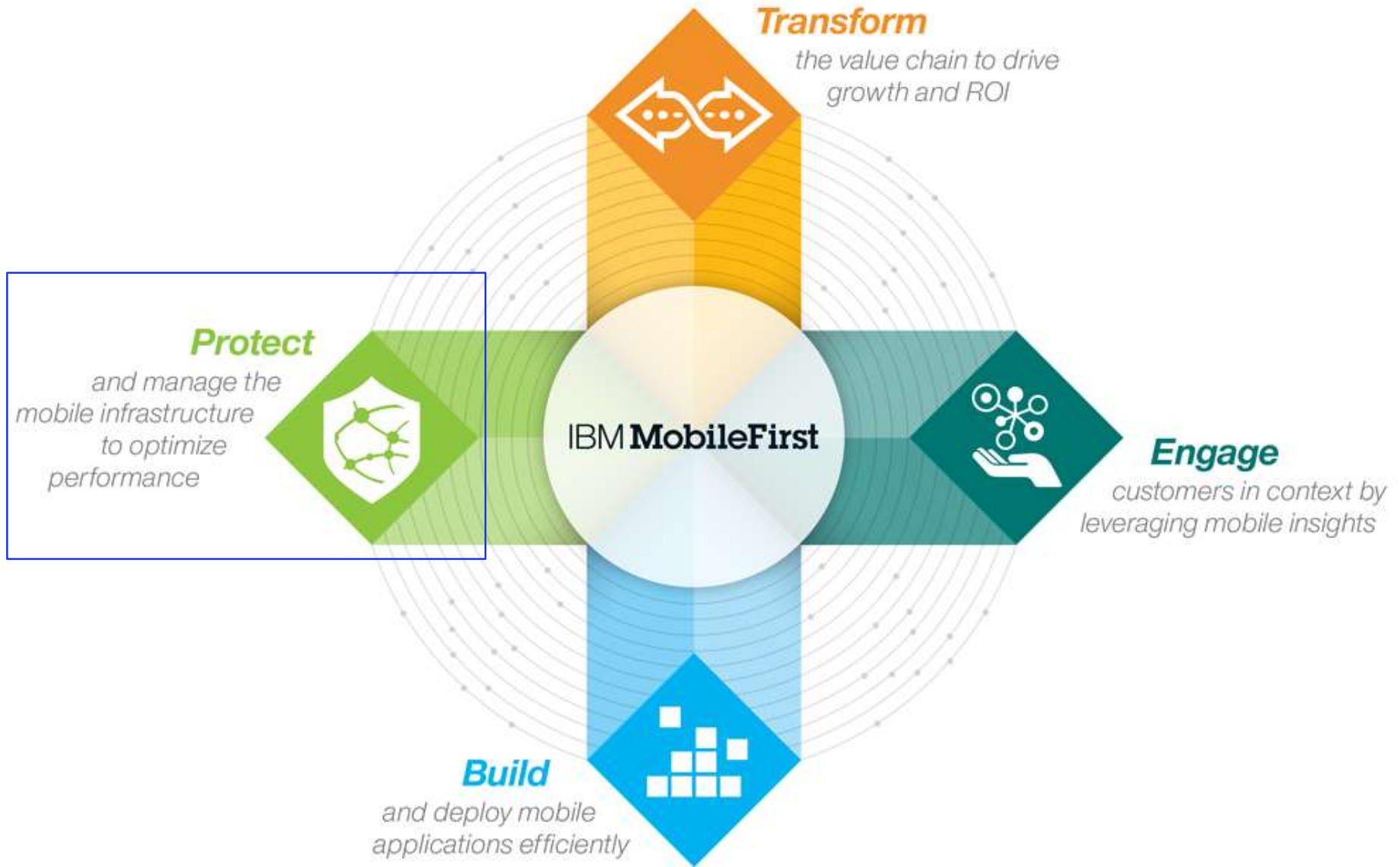
IBM z Systems • IBM Power Systems • IBM Storage

October 5–9 | Hilton Orlando, Florida

Agenda

- Mobile security threats & risks
- IBM mobile security solutions
- Reference Architecture for Mobile Security on System z
- Example scenario
- Discussion

Our strategy: enable enterprises to implement an integrated approach to capitalizing on the mobile opportunity



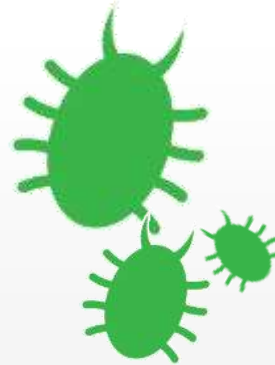
As mobile grows, so do security threats



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

Top Drivers for Mobile App Protection



1. Prevent or detect **bypassing or disabling of security controls** (e.g., jailbreak/root detection, authentication, authorization, encryption, digital rights/licensing)



2. Prevent or detect **bypassing or modification of business logic** (e.g., transactions, restricted functionality, sensitive operations)



3. Prevent **information loss or exposure** (e.g., via compromised user credentials, keys, data storage)



4. Prevent creation of **rogue, cloned, pirated, or modified** versions



5. Prevent or detect **insertion of malicious code** in the app (e.g., prevent remote control, information / identity stealing, financial charging)



6. Prevent **stealing of proprietary code/IP** from the app



7. Prevent **exposure of potential vulnerabilities** and sensitive source code



8. Ensure **compliance with industry guidelines** (e.g., OWASP Mobile Top Ten)

The OWASP Mobile - top 10 Risks

Open Web Application Security Project



www.owasp.org/



M1: Exposed service or API call is implemented using insecure coding techniques

M2: Rooted or jailbroken mobile device circumvents encryption, excessive safety assumptions by developers

M3: Mobile app use SSL/TLS during authentication but not elsewhere, unmonitored networks

M4: Sensitive information or data in a location on the mobile device accessible by other apps

M5: Automated attacks, bypass of mobile app directly to server, done by botnets, malware within the device

M6: Weak or improper encryption, network traffic capture, physical access to a device by a bad guy

M7: Execution of malicious code on the mobile device injected by malware or sent to an unsuspecting app

M8: Parameter tampering, inadequate input field validation, privilege escalation

M9: Capture and misuse of session token, MitM attacks, improper physical access to the device, network traffic capture

M10: Automated tooling to analyze, reverse engineer and modify app code on the device

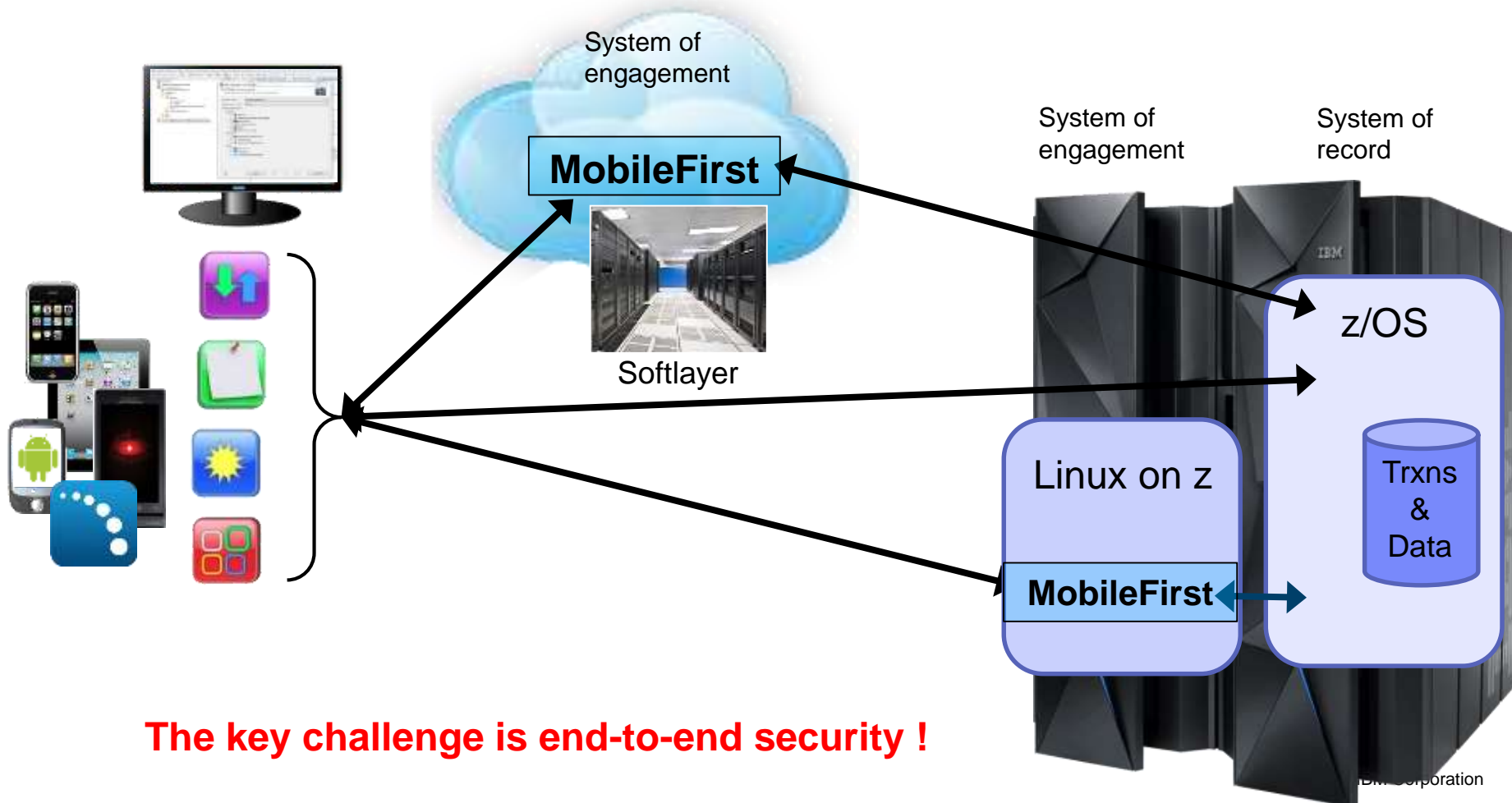
IBM positioning to solve the Mobilizing challenges

MobileFirst Platform – An Enterprise Blueprint



Main Mobile Solution scenarios

- on premise – with the System of Engagement on System z
- off premise – with the System of Engagement offsite – i.e. in IBM Softlayer cloud



The key challenge is end-to-end security !

Security features capabilities for the mobile enterprise



Device Security	Content Security	Application Security	Transaction Security
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Restrict copy, paste and share • Integration with Connections, SharePoint, Box, Google Drive, Windows File Share, Dropbox • Secure access to corporate mail, calendar and contacts • Secure access to corporate intranet sites and network 	<p>Software Development Lifecycle</p> <ul style="list-style-type: none"> • Integrated Development Environment • iOS / Android Static Scanning <p>Application Protection</p> <ul style="list-style-type: none"> • App Wrapping or SDK <i>Container</i> • Hardening & Tamper Resistance <i>IBM Business Partner (Arxan)</i> • Run-time Risk Detection <i>Malware, Jailbreak / Root, Device ID, and Location</i> • Whitelist / Blacklist Applications 	<p>Access</p> <ul style="list-style-type: none"> • Mobile Access Management • Identity Federation • API Connectivity <p>Transactions</p> <ul style="list-style-type: none"> • Mobile Fraud Risk Detection • Cross-channel Fraud Detection • Browser Security / URL Filtering • IP Velocity

Security Intelligence

Advanced threat detection with greater visibility

Fast and easy security and management

Fastest Time to Trust



60% deployed IBM MobileFirst Protect in **less than 4 hours**



75% deployed IBM MobileFirst Protect in **less than 8 hours**



0%

100%



Sales & customer support at no additional charge



24x7 customer support by phone, chat or email



Community, forums, blogs, webinars

GARTNER'S
MAGIC
QUADRANT

2014 Leader
Enterprise Mobility
Management
Suites



"Innovator"
Cloud-hosted
mobile device
management



InfoTech Research
Group

"Champion"
Mobile
Device
Management

Secure every transaction: Mobile to Mainframe



Device Security *Content Security* *Application Security* *Transaction Security*

powered by...

	IBM Security AppScan	IBM Security Access Manager	Trusteer <small>an IBM Company</small>	IBM Security zSecure
	Arxan Application Protection for IBM Solutions	IBM RACF IBM Distributed Identity Data	IBM InfoSphere Guardium	
		IBM DataPower		

Security Intelligence

IBM QRadar Security Intelligence Platform

IBM MobileFirst Protect V2.2.0 solutions, formerly known as IBM MaaS360 solutions

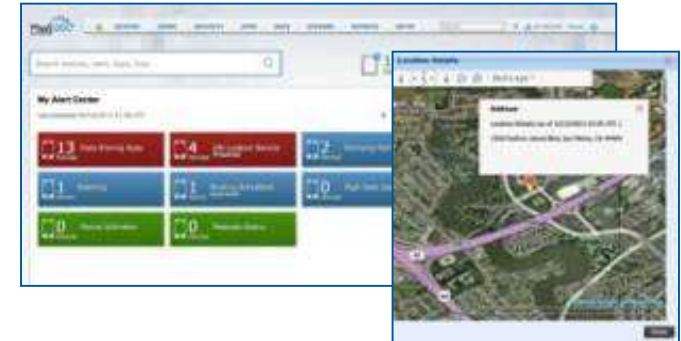
Product number	product name
5725-R20	IBM MobileFirst Protect Management Suite
5725-R21	IBM MobileFirst Protect Productivity Suite
5725-R22	IBM MobileFirst Protect Content Suite
5725-R23	IBM MobileFirst Protect Gateway Suite
5725-R15	IBM MobileFirst Protect Browser
5725-R16	IBM MobileFirst Protect Email Management
5725-R17	IBM MobileFirst Protect for BlackBerry
5725-R18	IBM MobileFirst Protect Expenses
5725-R19	IBM MobileFirst Protect Secure Mail

[Announcement February 2015](#)

IBM MobileFirst Protect Management Suite

MobileFirst Protect Devices

- Manage smartphones, tablets & laptops featuring iOS, Android, Windows Phone, BlackBerry, Windows PC & OS X
- Gain complete visibility of devices, security & network
- Enforce compliance with real-time & automated actions



MobileFirst Protect Applications

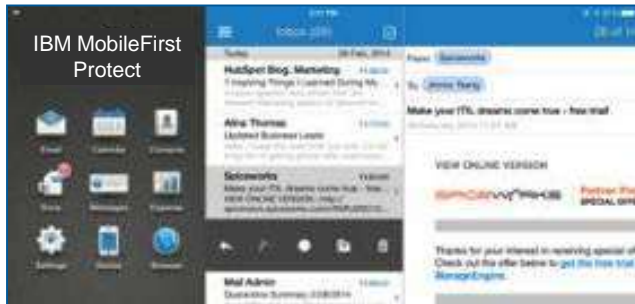
- Deploy custom enterprise app catalogs
- Blacklist, whitelist & require apps
- Administer app volume purchase programs

MobileFirst Protect Expenses

- Monitor mobile data usage with real-time alerts
- Set policies to restrict or limit data & voice roaming
- Review integrated reporting and analytics



IBM MobileFirst Protect Productivity Suite

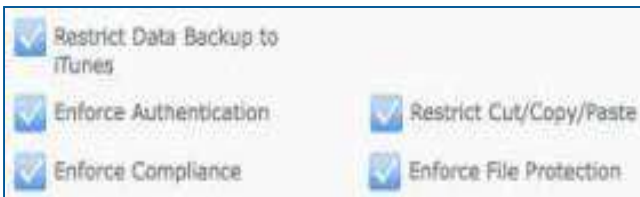


MobileFirst Protect Secure Mail

- Contain email text & attachments to prevent data leakage
- Enforce authentication, copy/paste & forwarding restrictions
- FIPS 140-2 compliant, AES-256 bit encryption for data at rest

MobileFirst Protect Browser

- Enable secure access to intranet sites & web apps w/o VPN
- Define URL filters based on categories & whitelisted sites
- Restrict cookies, downloads, copy/paste & print features



MobileFirst Protect Application Security

- Contain enterprise apps with a simple app wrapper or SDK
- Enforce authentication & copy/paste restrictions
- Prevent access from compromised devices

IBM MobileFirst Protect Content Suite

MobileFirst Protect Content

- Contain documents & files to prevent data leakage
- Enforce authentication, copy/paste & view-only restrictions
- Access IBM MobileFirst Protect distributed content & repositories such as SharePoint, Box & Google Drive



Secure Editor

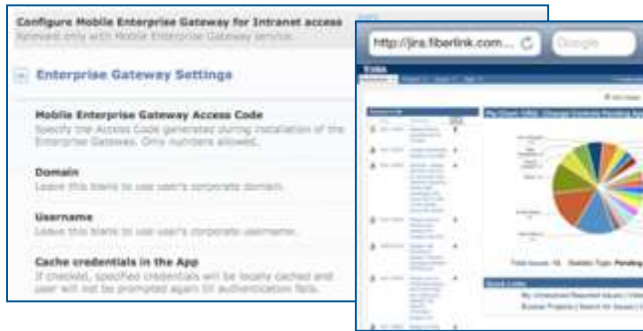
- Create, edit & save content in a secure, encrypted container
- Collaborate on Word, Excel, PowerPoint & text files
- Change fonts & insert images, tables, shapes, links & more

Secure Document Sync

- Synchronize user content across managed devices
- Restrict copy/paste & opening in unmanaged apps
- Store content securely, both in the cloud & on devices



IBM MobileFirst Protect Gateway Suite

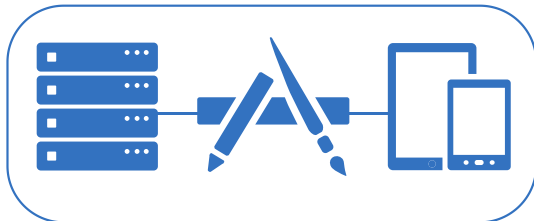


Mobile Enterprise Gateway for Browser

- Enable IBM MobileFirst Protect Secure Browser to access enterprise intranet sites, web apps & network resources
- Access seamlessly & securely without needing a VPN session on mobile device

Mobile Enterprise Gateway for Docs

- Enhance MaaS360 Mobile Content Management with secure access to internal files, e.g. SharePoint & Windows File Share
- Retrieve enterprise documents without a device VPN session



Mobile Enterprise Gateway for Apps

- Add per app VPN to IBM MobileFirst Protect Application Security to integrate behind-the-firewall data in private apps
- Incorporate enterprise data without a device VPN session

IBM MobileFirst Protect Threat Management

Integrated Threat Management
powered by industry leading Trusteer technology



The screenshot shows the MaaS360 interface with a navigation bar (DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, SETUP) and a search bar. The main content area displays 'Advanced Device Security' for device 'srajagopal-GT-I9200'. A table lists various security metrics:

Last Risk Assessment Date/Time	10/22/2014 14:14 IST	Trusteer Configuration Update Status	3 (up-to-date)
OS Version	4.2.2 (up-to-date)	Malware Detected	Yes - DD_Light;
Connected Wi-Fi Security Level	Secure	Allow Installation of Non-Market Apps	No
Suspicious System Configuration Found	Found both an unknown SMS listener and an unknown startup package		

MobileFirst Protect combines the mobile risk assessment capabilities of Trusteer with the real-time control of MaaS360-based EMM in a fully integrated solution

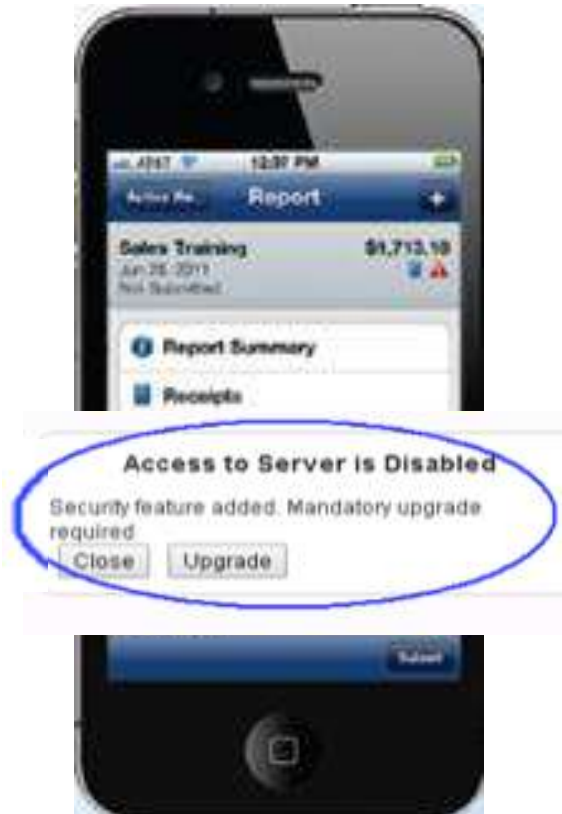


The screenshot shows the 'Trusteer Advanced Security' configuration panel. It includes a checkbox for 'Configure Restricted Applications by Trusteer Ratings' which is checked. Below it, the 'Remediation Action' is set to 'Uninstall App'. The 'App Exceptions' section allows for entering App IDs for apps to allow, with 'com.fiberlink.maas360.android' listed as an example.

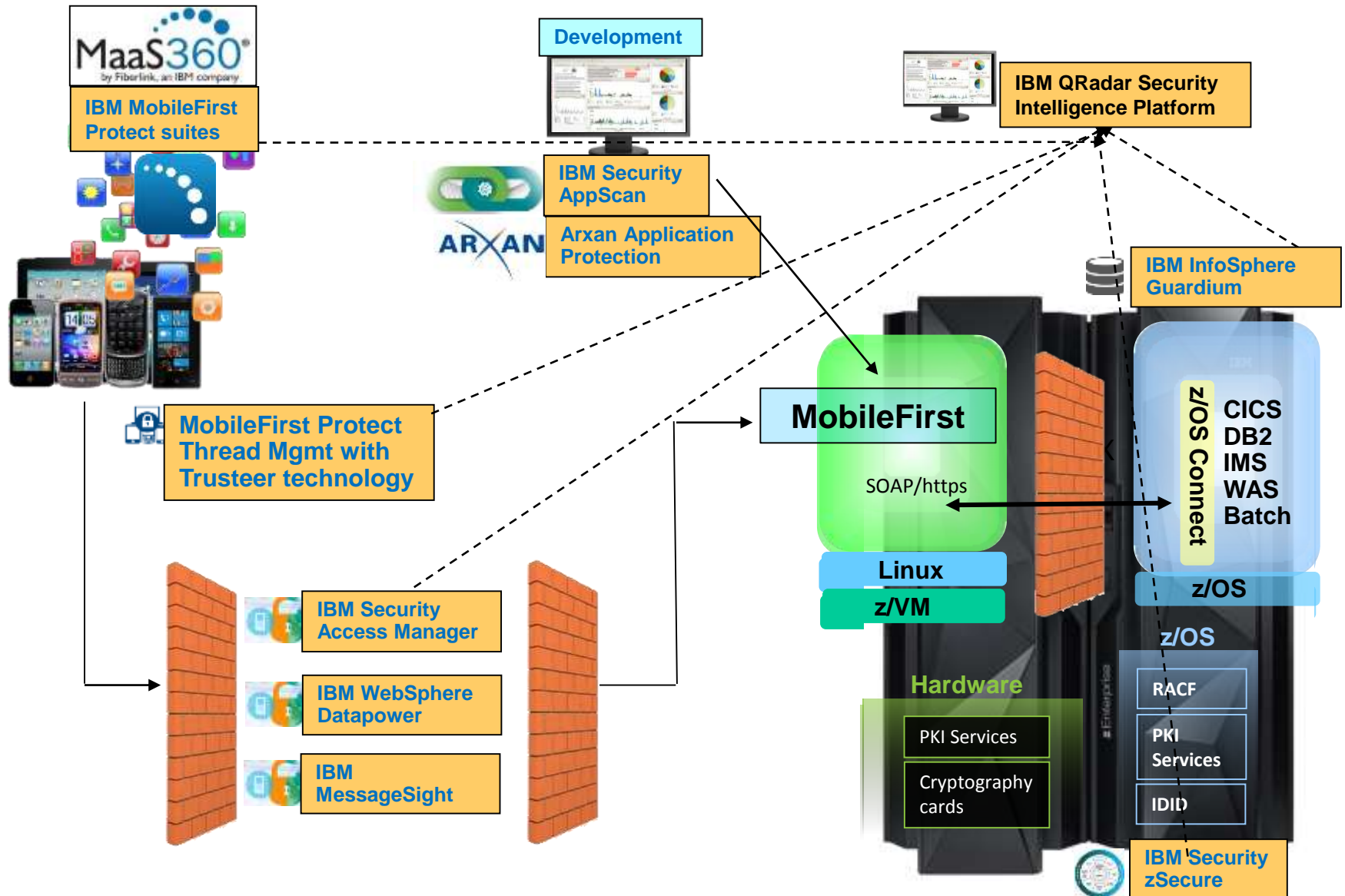
- **Mobile malware detection** detects known malicious files based on their MD5s
- **Rogue app detection** identifies potentially malicious apps based on permission analysis
- **Cloud-based threat intelligence** to augment device context analysis with information such as last known location

MobileFirst Platform V7 with additional Mobile apps security

- **User Authentication (Enhanced)**
 - Plugs into existing enterprise or 3rd party security systems with a variety of authentication methods
 - Certificate-based, Touch ID, LDAP server, Social
 - Multi-factor authentication
 - Disable app version, specific user or devices through the console
- **App Authenticity (Enhanced)**
 - Verify app identity; protect brand reputation, intellectual property and back-end data
 - Take more "fingerprints" from the app to better validate when the app was changed
 - Extend the number of shared secrets
 - New command line to extract the shared secrets
 - MobileFirst console can present app authenticity status
- **Encrypt local data**
 - Leverage user identity to encrypt and retrieve data stored locally on the device



Secure Users & Devices and every Mobile transaction

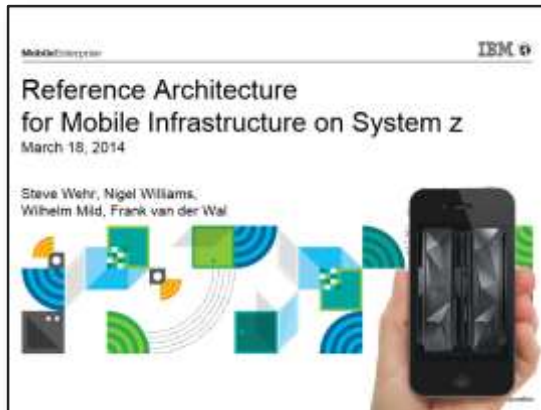


Mobile security areas and IBM solutions

- Development
 - [Appscan](#) – scan existing or new App code for security risks
- Mobile Device and App security:
 - [MaaS360](#) – device protection with secured container and encrypted data
 - [Arxan](#) – mobile device protection
 - [Trusteer](#) security – device and mobile app enforcements
- DMZ zone protection options
 - [ISAM](#) – IBM Security Access Manager
 - [DataPower](#) – massive parallel authentication/validation of requests
 - [MessageSight](#) – massive parallel authentication/validation MQ / MQTT requests
- [IBM MobileFirst security](#)
 - Interfaces / APIs for external security checks
- Back-end security in z Systems
 - [InfoSphere Guardium](#) – Real-time Database security on z Systems
 - [zSecure](#) – RACF automation and proactive compliance
- Security intelligence
 - [Qradar](#) – End-to-End security monitoring and policy enforcement verification

zMobile reference architectures

1



Contents

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

2



Contents

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

3





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.




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.

Use Case	Security Concerns / Issues to be solved
<p>Employee app with non-sensitive data.</p> 	<ul style="list-style-type: none"> ▪ 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
<p>Employee app with sensitive data.</p> 	<ul style="list-style-type: none"> ▪ Company-provided devices. ▪ B2E ▪ Sensitive company and client data will be sent to the device, and <i>stored</i> 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.

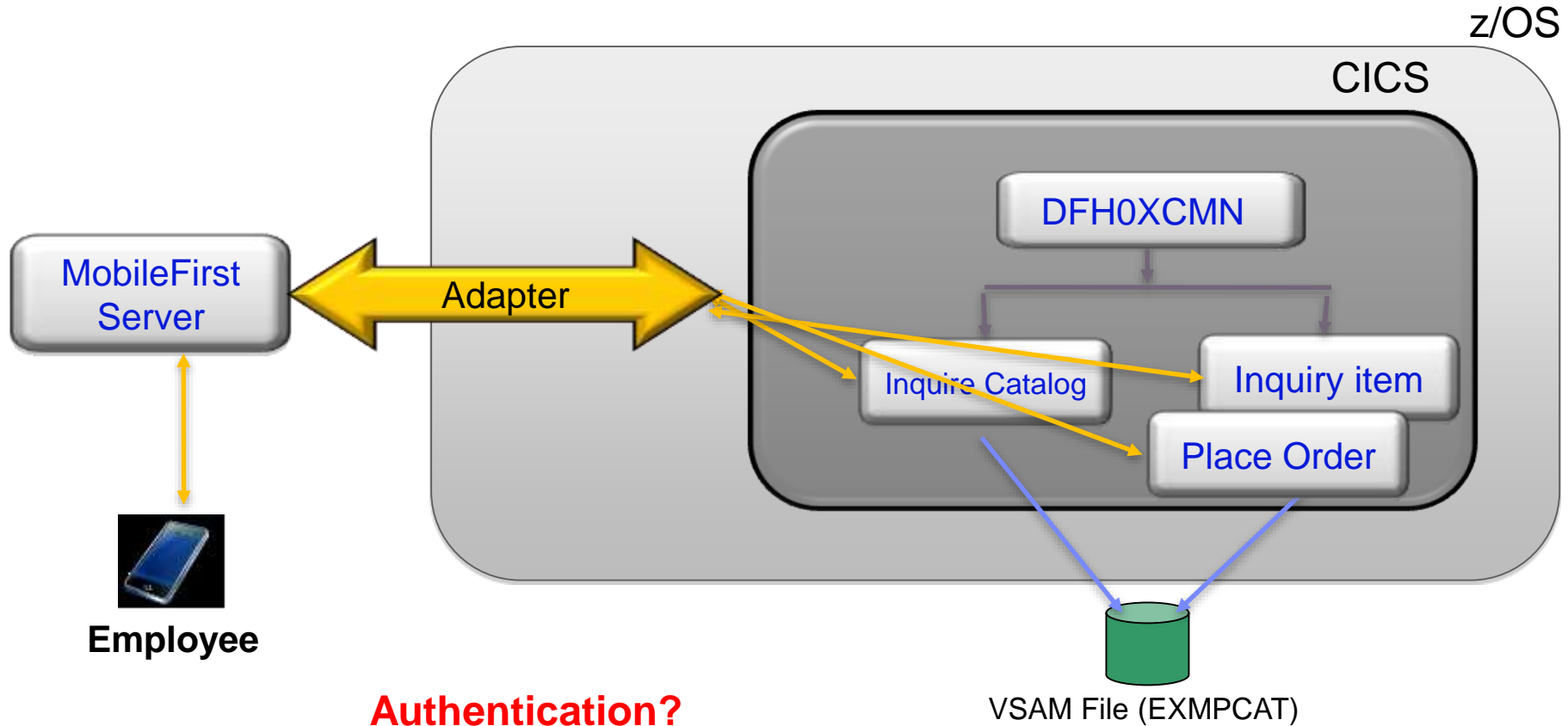
List of Use Cases

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

Use Case	Security Concerns / Issues to be solved
<p>Consumer Retail app</p> 	<ul style="list-style-type: none"> ▪ 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.
<p>Consumer Insurance app</p> 	<ul style="list-style-type: none"> ▪ 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
<p>Consumer Financial Services app</p> 	<ul style="list-style-type: none"> ▪ 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.

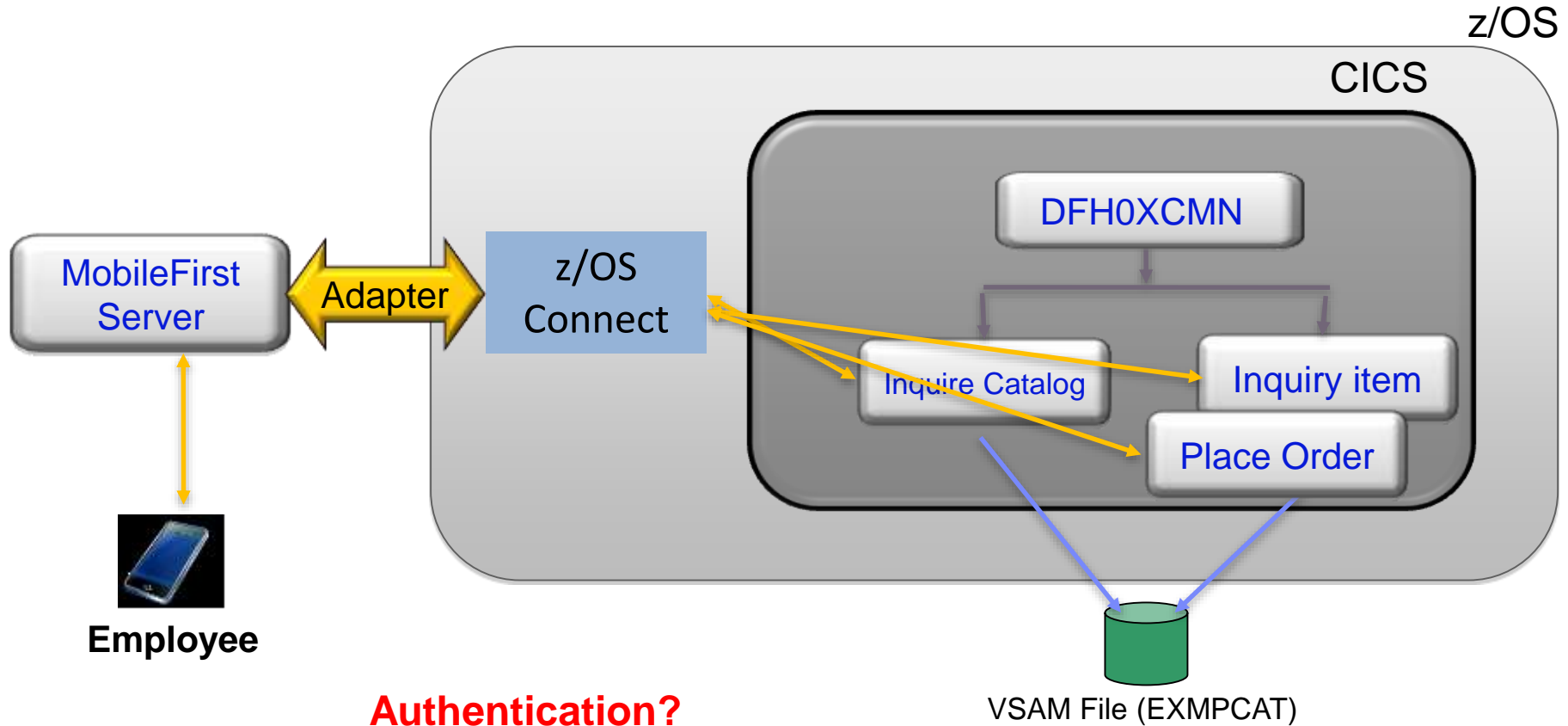
Example scenarios

Catalog Manager– B2E (Business to Employee)



Authentication?
Identification?
Authorization?
Confidentiality/Integrity?

Catalog Manager– B2E (Business to Employee)



Authentication?
Identification?
Authorization?
Confidentiality/Integrity?

Some typical security requirements ...

- Flow identity from mobile device to mainframe
- Block lost or stolen devices
- Prevent corrupted mobile apps from accessing mainframe
- Audit requests
- Identify transactions that have been initiated by mobile devices
- Protect against attack

Considerations that influence a mobile security solution.

Criteria	Considerations
1. Mobile users	<ul style="list-style-type: none"> ▪ Employee (B2E) ▪ Customer (B2C)
2. Mobile devices	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Mainframe or distributed ▪ CICS, IMS, DB2, WebSphere, other ▪ Service-enabled or legacy-access ▪ Enabled for mobile access (Restful, JSON)
5. Type of access	<ul style="list-style-type: none"> ▪ Intranet/extranet or internet ▪ Is a VPN required
6. Number of users	<ul style="list-style-type: none"> ▪ 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

See '[Security Reference Architecture for System z](#)'

Considerations that influence a mobile security solution...

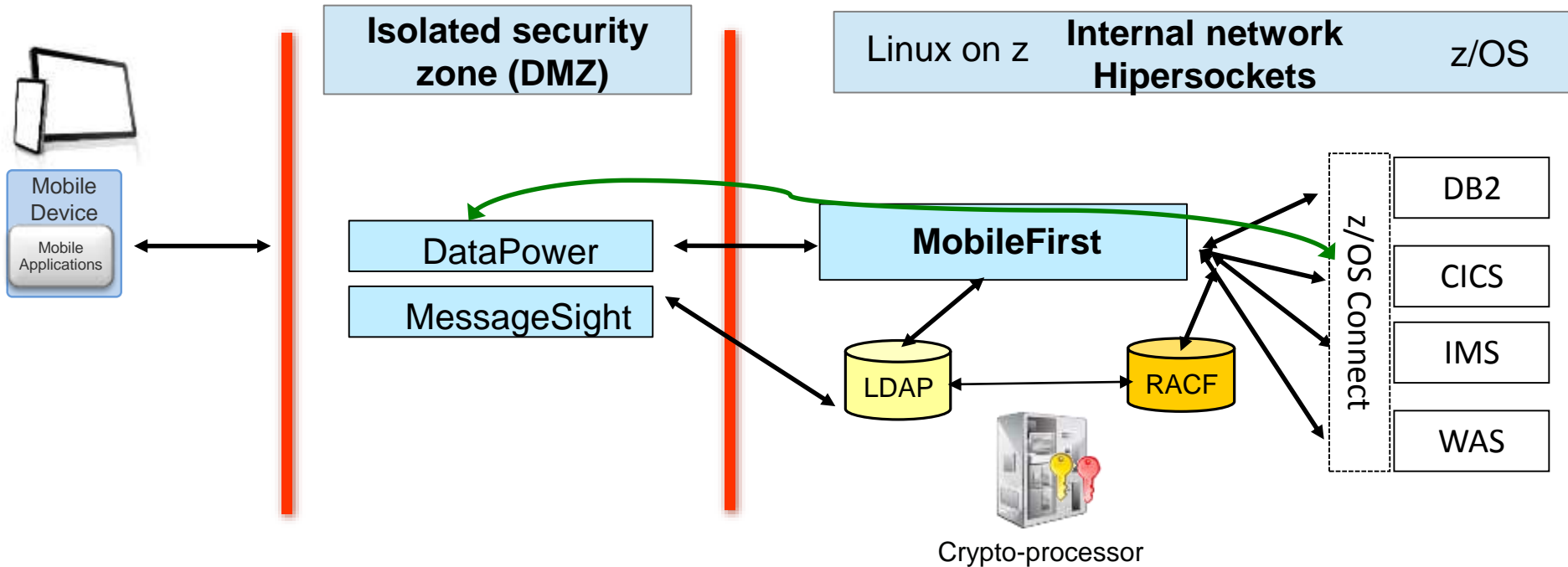
Criteria	Considerations
7. Authentication	<p>User authentication</p> <ul style="list-style-type: none"> ▪ Does each user have a unique identity ▪ How is the mobile user authenticated e.g user name, email address, account number ... ▪ What authentication tokens will be used e.g LTPA ▪ Does the mobile user have a RACF user ID ▪ How is the mobile user's identity mapped to a RACF id? ▪ Is single sign-on (SSO) required ▪ Is risk-based authentication required e.g two-factor authentication <p>Device authentication</p> <ul style="list-style-type: none"> ▪ Are only a certain set of devices allowed to access the application ▪ Does the device need to be authenticated ▪ Are specific device features required e.g <ul style="list-style-type: none"> –Near field communication (NFC) capabilities –Finger print sensor –Camera for visual recognition –Microphone for voice recognition <p>Application authentication</p> <ul style="list-style-type: none"> ▪ Does the authenticity of the application need to be checked
8. Authorization	<ul style="list-style-type: none"> ▪ Does mobile user need to be authorized to access MEAP (Mobile Enterprise Application Platform) application ▪ Is risk-based access required examples: <ul style="list-style-type: none"> –Limit access when mobile user connects from unsecure network –Limit access based on mobile user location. ▪ What authorization tokens will be used e.g OAuth, SAML ▪ Does mobile user need to be authorized to mainframe enterprise applications. What RACF id is used?

Considerations that influence a mobile security solution...

Criteria	Considerations
9. Audit	<ul style="list-style-type: none"> ▪ Should access to MEAP application be audited? ▪ Should access to enterprise applications be audited? ▪ What information needs to be audited -- mobile user id, device location, RACF user id, resource accessed, device id
10. Confidentiality	<ul style="list-style-type: none"> ▪ What is the nature of the data e.g financial or personal ▪ Does data in transit need to be encrypted <ul style="list-style-type: none"> –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	<ul style="list-style-type: none"> ▪ Does the integrity of the data in transit need to be protected <ul style="list-style-type: none"> –Between the mobile device and MEAP –Between the MEAP and enterprise systems
12. Existing security infrastructure	<ul style="list-style-type: none"> ▪ Will the existing security infrastructure be reused for securing mobile access ▪ What components and products are used in the existing security infrastructure <ul style="list-style-type: none"> –Security gateway –User registry –Identity management and mapping –Network security –Digital certificates –Security intelligence solution
13. Security standards	<ul style="list-style-type: none"> ▪ 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

Topology – DataPower as a reverse proxy for MobileFirst Platform

Capabilities	Deployment scenarios	System z benefits
<ul style="list-style-type: none"> • Combined capabilities of MobileFirst and DataPower • Datapower in an isolated secured network zone DMZ – DeMilitarized Zone 	<ul style="list-style-type: none"> • When hybrid mobile apps use a combination of web and Restful interactions • High volume or internet mobile access 	<ul style="list-style-type: none"> • Additional benefits of DataPower as a mobile security gateway for MobileFirst on zLinux • LDAP user registry shared between DataPower and MobileFirst



Example Security requirements – B2E (Business to Employee)

- **Authentication**

- ✓ Employee must login to use certain functions of the app
- ✓ Employees login with RACF user ID and password
- ✓ The authenticity of the mobile app must be assured

- **Identification**

- ✓ Against existing RACF user registry
- ✓ App single sign-on

- **Authorization**

- ✓ RACF user id is used for authorization checking. All authenticated users are authorized to listCatalog and listSingle services. Subset of employees are authorized to placeOrder service.
- ✓ Mobile-initiated CICS transactions must run with RACF user id and specific trans id

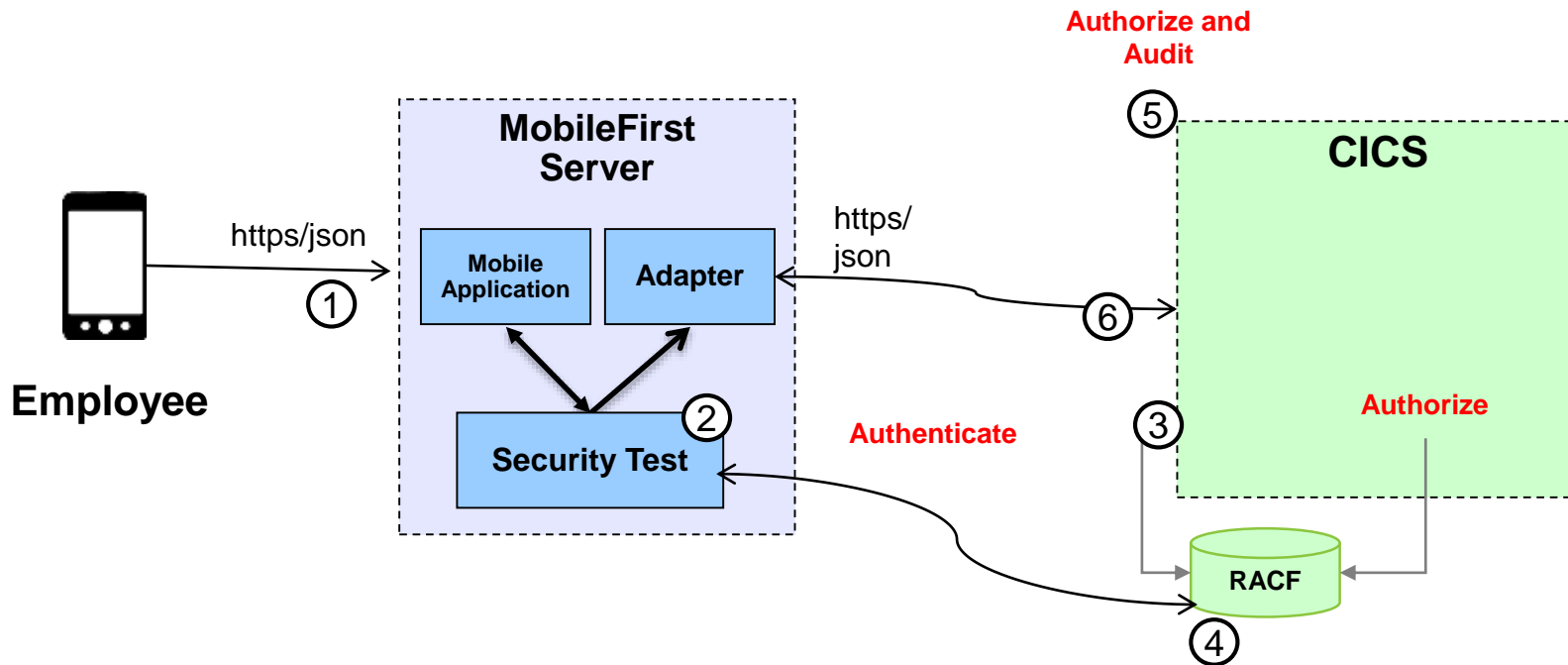
- **Confidentiality and integrity**

- ✓ Confidentiality and integrity of data in transmit must be protected

- **Audit**

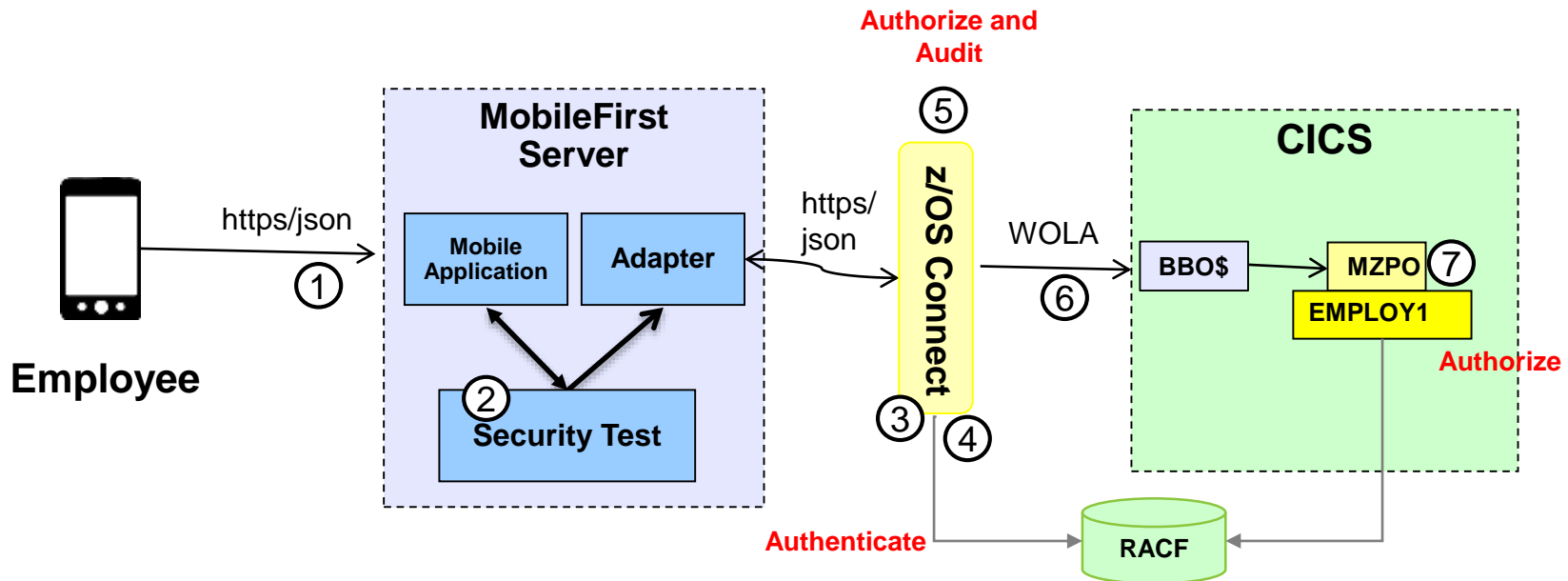
- ✓ Order requests must be audited

Example Security solution – B2E (Business to Employee)



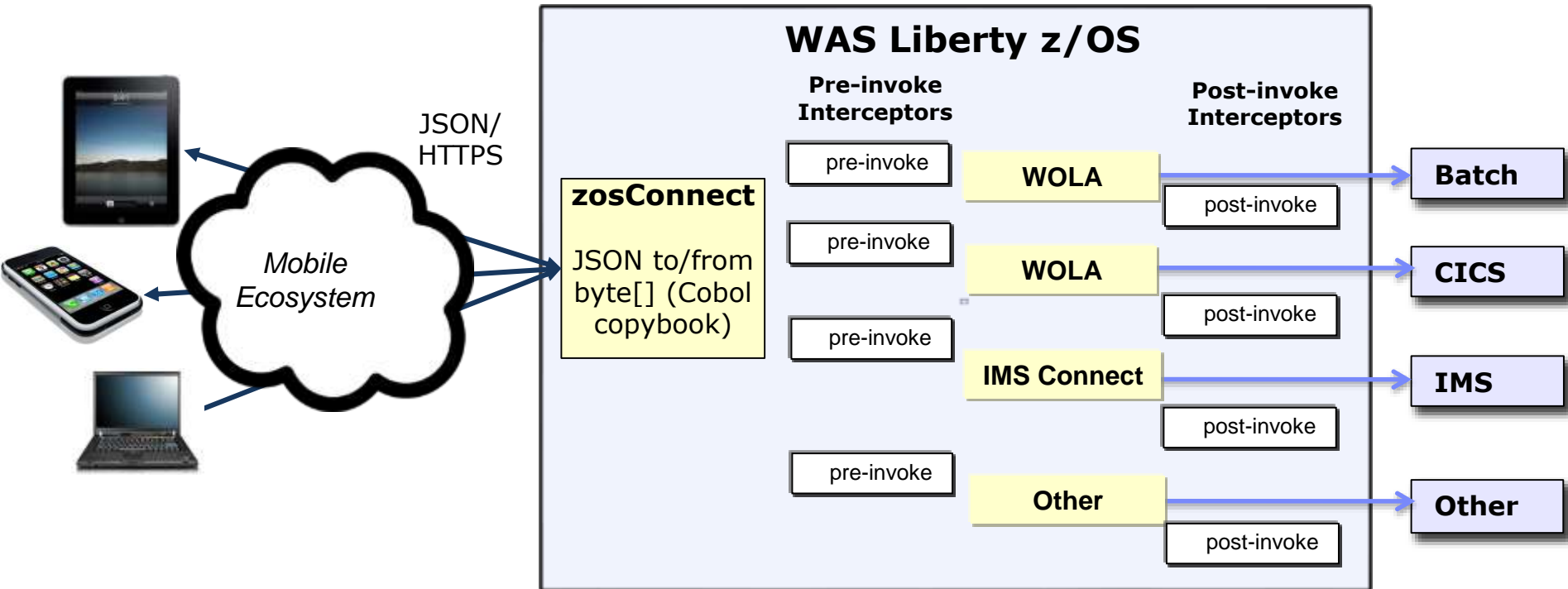
1. Employee logs in to mobile app using RACF user id (EMPLOY1) and password
2. MobileFirst server performs app authentication, propagates credentials to z/OS (NonValidatingLoginModule) and allows device blocking
3. z/OS authenticates employee credentials
4. RACF user id is used for authorization checking. All authenticated users are authorized to listCatalog and listSingle services. Subset of employees are authorized to placeOrder service.
5. Order requests are audited by z/OS itself
6. Employee user id is propagated to CICS server for CICS authorization
7. CICS task runs with specific trans id so that it can be identified as a mobile transaction

Example Security solution – B2E (Business to Employee)



1. Employee logs in to mobile app using RACF user id (EMPLOY1) and password
2. MobileFirst server performs app authentication, propagates credentials to z/OS Connect (NonValidatingLoginModule) and allows device blocking
3. z/OS Connect authenticates employee credentials
4. RACF user id is used for authorization checking. All authenticated users are authorized to listCatalog and listSingle services. Subset of employees are authorized to placeOrder service.
5. Order requests are audited by z/OS Connect
6. Employee user id is propagated to CICS server for CICS authorization
7. CICS task runs with specific trans id so that it can be identified as a mobile transaction

z/OS Connect Security



- Framework that allows interceptors to be executed around the invocation of the service
- Authentication with RACF or LDAP
- Authorization interceptor e.g is user in 'Invoke' group for requested service)
 - **com.ibm.wsspi.zos.connect.Authorization()**
- Audit interceptor for SMF-based auditing
 - **com.ibm.wsspi.zos.connect.Audit()**

Example security requirements – B2C (Business to Consumer)

• Authentication

- ✓ Employees login with '**distributed id**' and password
- ✓ The authenticity of the mobile app must be assured

• Identification

- ✓ Against existing **LDAP** user registry
- ✓ Distributed user id must be **mapped** to RACF user id (1:1 mapping for employees, Many:1 mapping for customers)
- ✓ App single sign-on

• Authorization

- ✓ RACF user id is used for authorization checking.
- ✓ Mobile-initiated CICS transactions must run with RACF user id and specific trans id

• Confidentiality and integrity

- ✓ Confidentiality and integrity of data in transmit must be protected

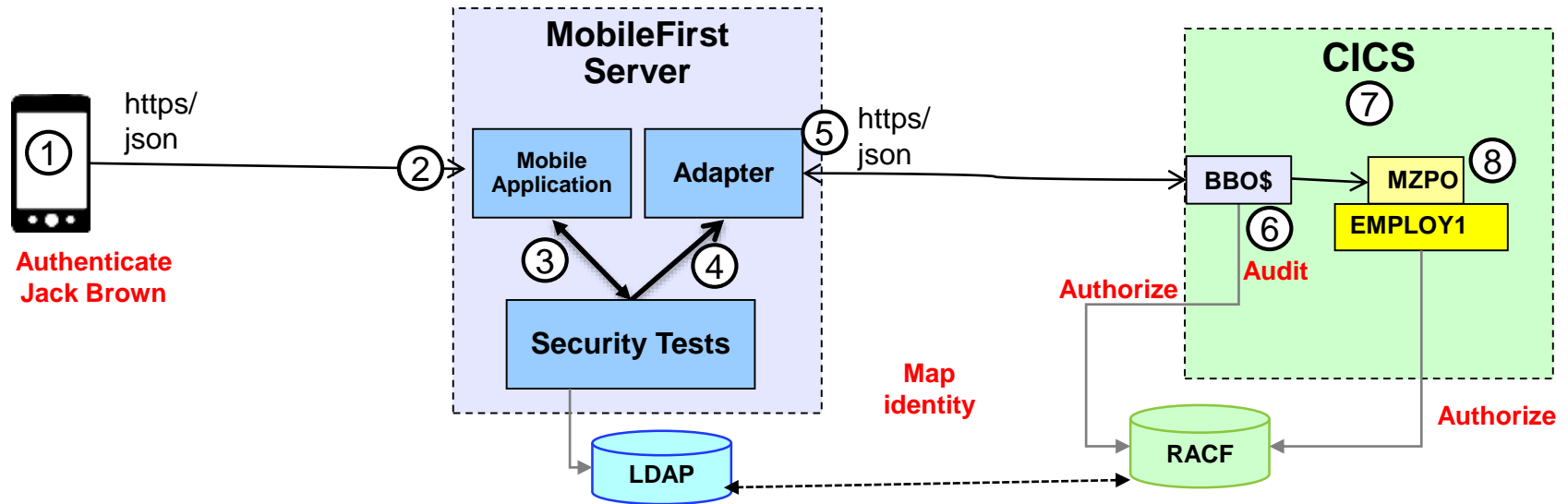
• Audit

- ✓ Order requests must be audited

• Threat protection

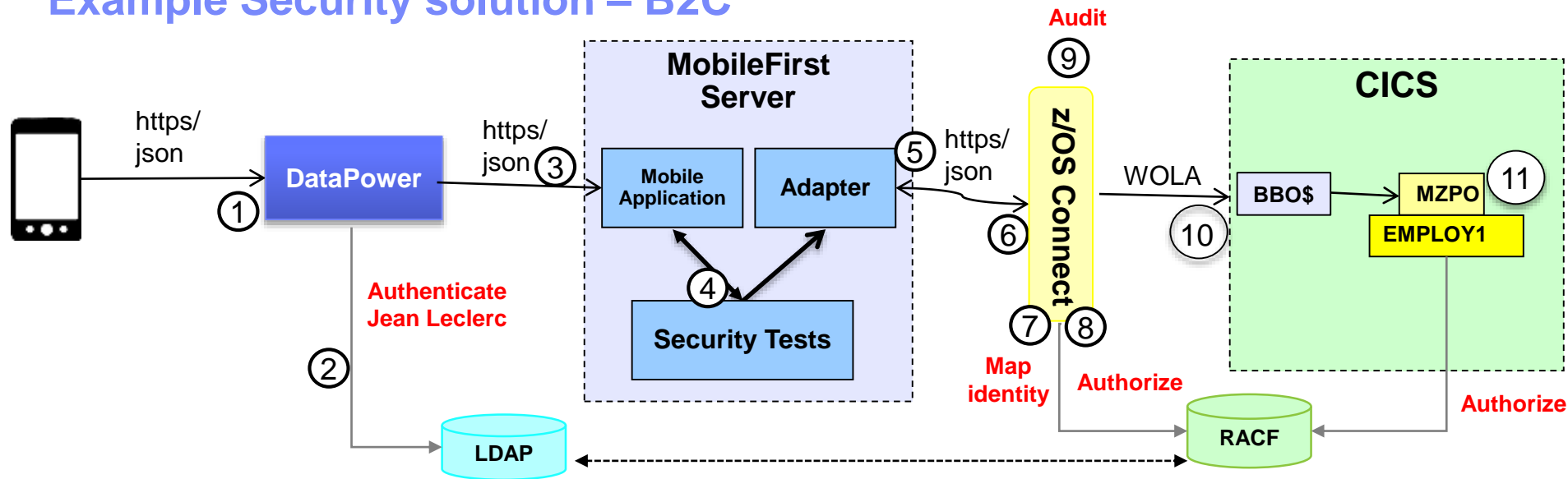
- ✓ Need to protect against **unexpected surges** in mobile requests

Example Security solution – B2C



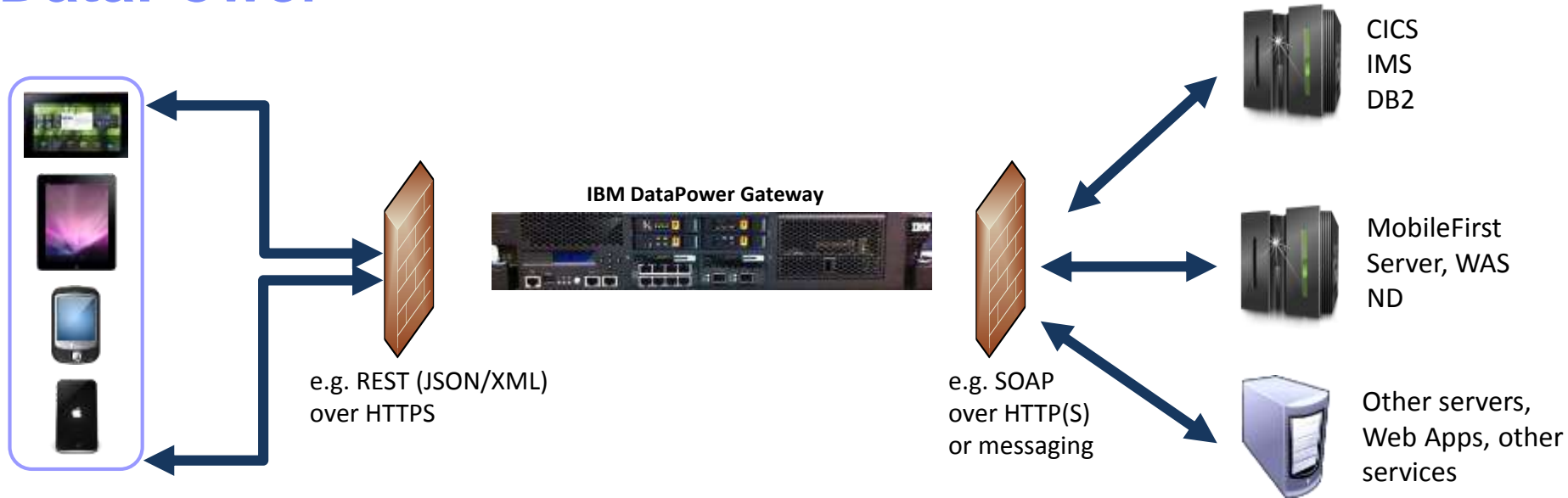
1. User logs in to mobile app using 'distributed id' (e.g Jack Brown) and password
2. MobileFirst server validates security token (WebSphereLoginModule) and optionally performs device and application authentication (part of MobileFirst)
3. Mobile Application maps security token in LDAP - distributed user id to RACF user id (1:1 mapping for employees, Many:1 mapping for customers)
4. When Mobile application calls Adapters – Adapter usage validation is performed
5. z/OS Identity propagation uses RACF user id for transaction authorization checking. All authenticated users are authorized to list single services. Subset of employees are authorized to placeOrder service.
6. Order requests are audited by z/OS with the RACF id used
7. RACF user id is propagated to CICS server for CICS authorization ([APAR PI38851](#))
8. CICS task runs with specific trans id so that it can be identified as a mobile transaction

Example Security solution – B2C



1. User logs in to mobile app using 'distributed id' (e.g Jean Leclerc) and password
2. DataPower security gateway authenticates user credentials in LDAP
3. DataPower forwards distributed user id in LTPA token to MobileFirst server
4. MobileFirst server validates LTPA token (WebSphereLoginModule) and optionally performs device and application authentication
5. MobileFirst server forwards LTPA token to z/OS Connect
6. z/OS Connect validates LTPA token
7. z/OS Connect maps distributed user id to RACF user id (1:1 mapping for employees, Many:1 mapping for customers)
8. RACF user id is used for authorization checking. All authenticated users are authorized to listCatalog and listSingle services. Subset of employees are authorized to placeOrder service. ([APAR PI38852](#))
9. Order requests are audited by z/OS Connect (are distributed id and RACF id audited?)
10. RACF user id is propagated to CICS server for CICS authorization ([APAR PI38851](#))
11. CICS task runs with specific trans id so that it can be identified as a mobile transaction

DataPower

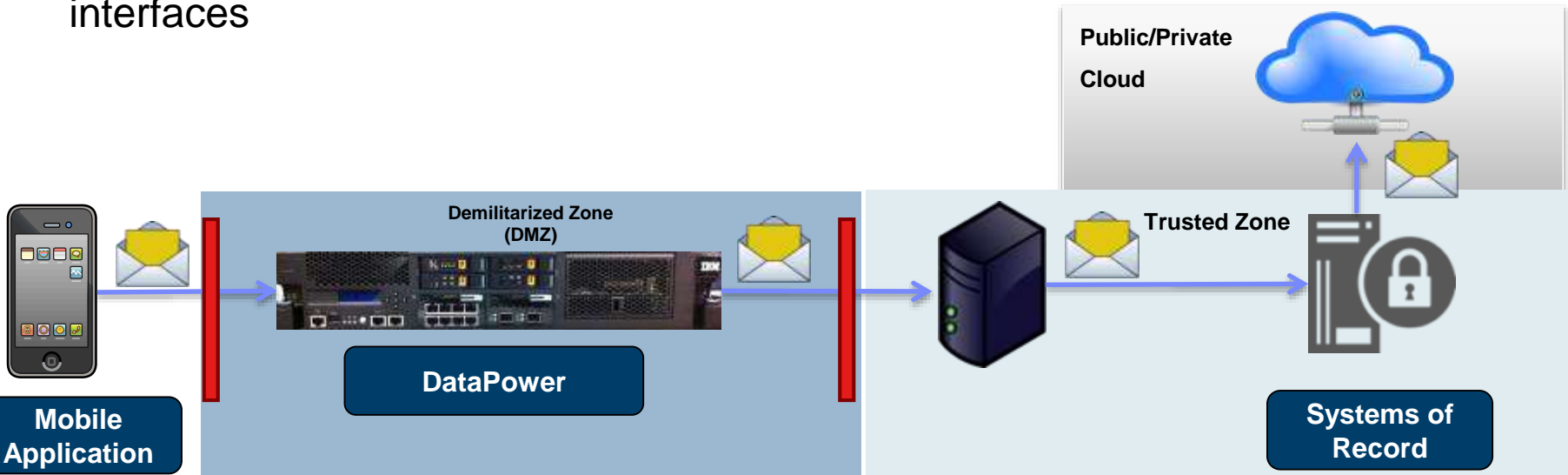


- Security, Control, Integration & Optimization of mobile workload
- Enforcement point for centralized security policies
- Authentication, Authorization, SAML, OAuth 2.0, Audit
- Threat protection for XML and JSON
- Message validation and filtering
- Centralized management and monitoring point
- Traffic control / Rate limiting
- Integration with MobileFirst Server

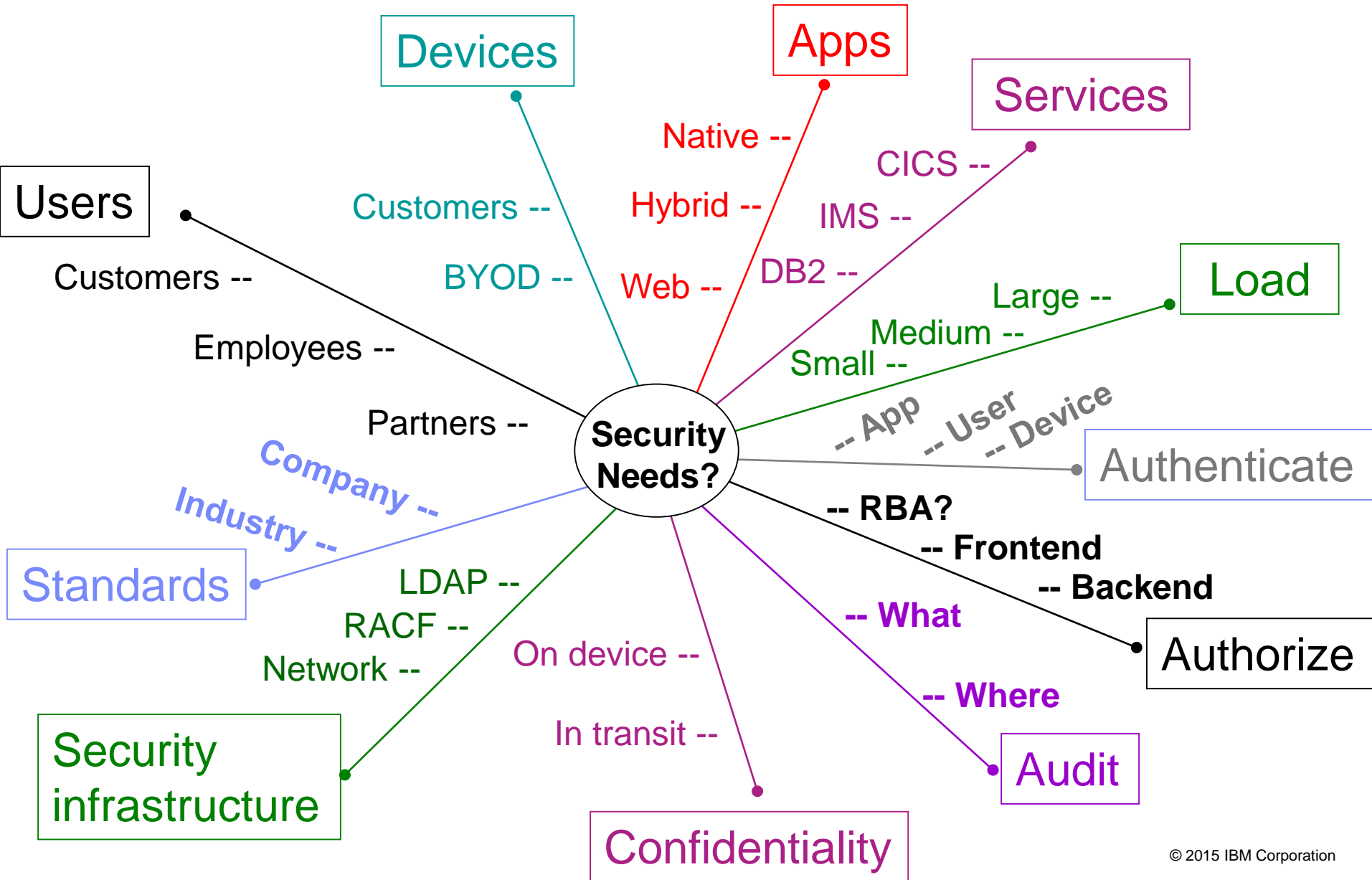
DataPower 7.2 – mobile enhancements

Available
June 19th, 2015

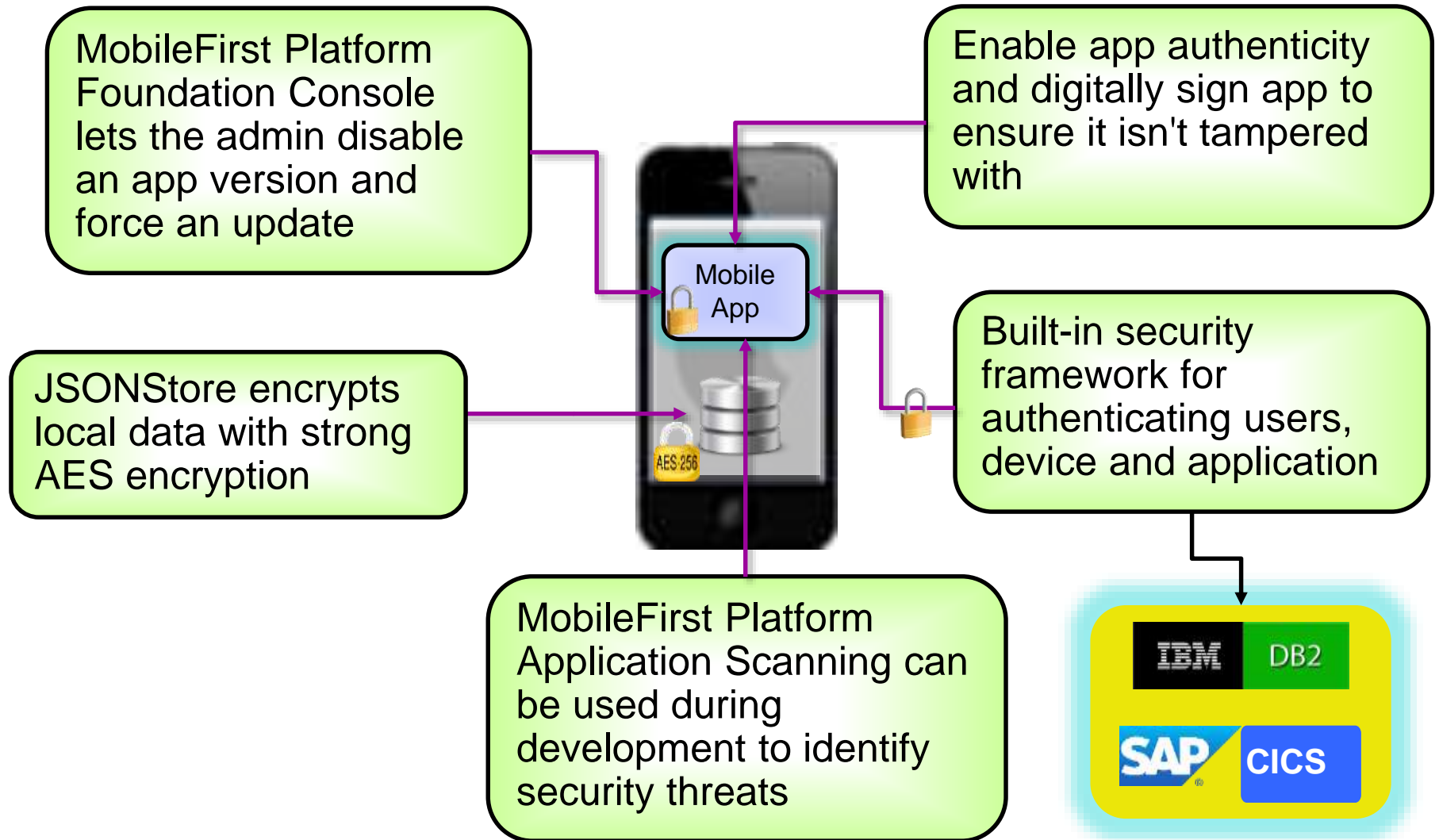
- Provide enhanced message-level security for mobile, API, and web workloads
 - JSON Web Encryption for message confidentiality
 - JSON Signature for message integrity
 - JSON Web Token to assert security assertions for Single Sign On (SSO).
 - JSON Web Key (JWK) to represent cryptographic key
- Provides **end-to-end security** between Mobile application and System of Record applications
- Secure sensitive data (credit card data) between multiple untrusted or unmanaged systems without compromising the data to help support PCI compliance
- GatewayScript enhancements to transform between XML and JSON messages
 - Easily integrate System of Records data sources with Systems of Engagement interfaces



How to chose the right mobile security solution?



MobileFirst Platform Foundation security for device and app



WW z Systems Mobile Centres of Competency



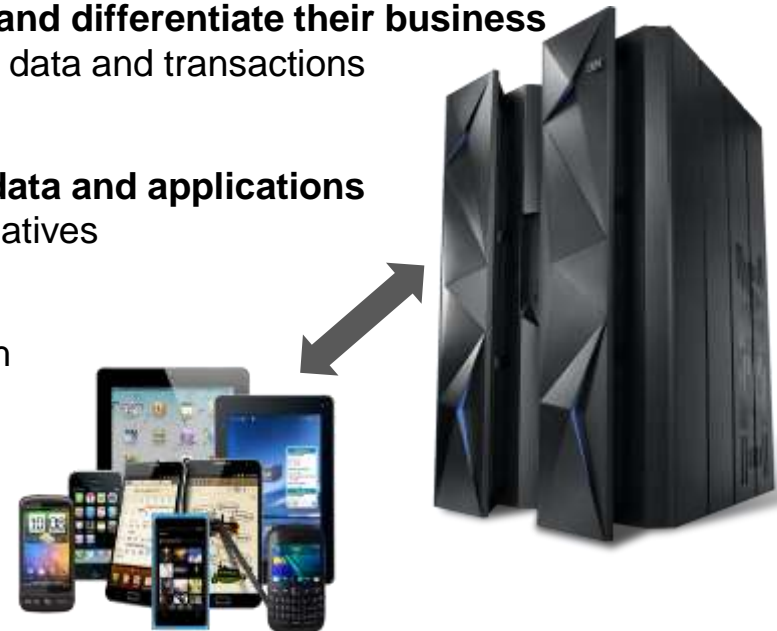
End-to-end reference architecture
from MobileFirst Platform to CICS and IMS

z Systems end-to-end **Mobile Security architecture**

Sample MobileFirst apps for
CICS, IMS and z/OS Connect

IBM Mobile Test Drive

- **Partner with IBM resources to work on a Mobile Test Drive of your choice:**
 - Select an entry point such as building a **mobile front end for an existing 3270 application**, composing a **Bluemix mobile app** connected to a system of record, assessing the benefits of **Mobile Workload Pricing**, leveraging API enablement using **API Management or z/OS Connect**, and others
- **Benefits:**
 - Work with IBM mobile specialists to **review existing mobile projects, priorities and requirements**
 - Leverage **best practices and subject matter expertise** for input into your enterprise mobile infrastructure strategy and enterprise mobile roadmap
 - Learn what others are doing to **accelerate time to value and differentiate their business with mobile projects** by integrating high value enterprise data and transactions
- **Who should be interested?**
 - Clients that are looking to **leverage existing z Systems data and applications via mobile channels** to drive more value from mobile initiatives
- **What is the commitment?**
 - **1-2 days Discovery** that IBM mobile experts facilitate with your business and technical team, followed by a **deeper Mobile Test Drive**, for **up to a two weeks engagement**
- **How much will it cost?**
 - We will provide **no-cost** technical expertise and access to resources during the Proof-of-Concept



Contact: Nathan Brice (nbrice@uk.ibm.com)

Questions?

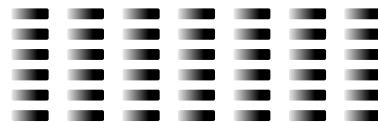


Wilhelm Mild
IBM Executive IT Architect



*IBM Deutschland Research
& Development GmbH
Schönaicher Strasse 220
71032 Böblingen, Germany*

*Office: +49 (0)7031-16-3796
wilhelm.mild@de.ibm.com*



YOUR OPINION MATTERS!



Submit **four or more** session evaluations by **5:30pm Wednesday** to be eligible for drawings!

*Winners will be notified Thursday morning. Prizes must be picked up at registration desk, during operating hours, by the conclusion of the event.



Continue growing your IBM skills



ibm.com/training

provides a comprehensive portfolio of skills and career accelerators that are designed to meet all your training needs.

If you can't find the **training that is right for you** with our Global Training Providers, we can help.

Contact IBM Training at dpmc@us.ibm.com



Global Skills Initiative

