Securing every transaction

After a review of the main security challenges, this session outlines the options for securing mobile access to System z. We consider different mobile security solutions including secure integration with Worklight, using WebSphere DataPower or IBM Security Access Manager as a mobile security gateway, and the new security features of z/OS Connect.

Mobility is the top target for investment increases in the next two years, ahead of cloud; but security and insufficient skills are barriers to adoption

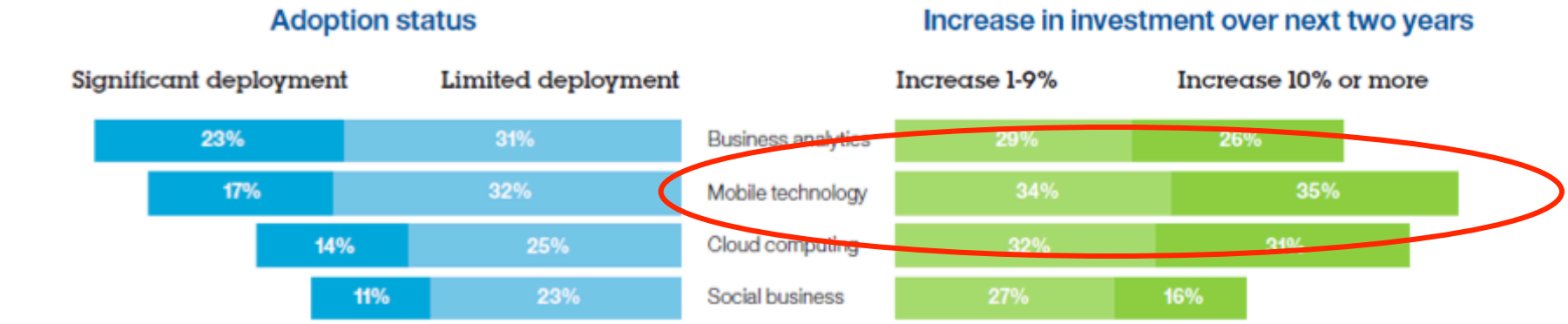
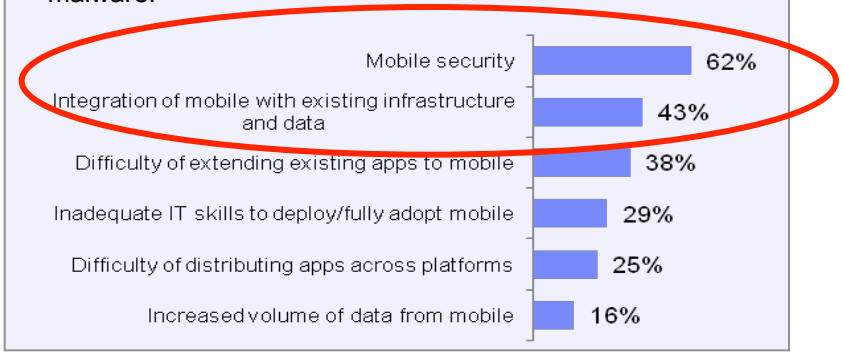


Figure 1: To date, business analytics and mobile are the most extensively deployed. Looking forward, mobile and cloud computing are the top targets for investment increases.

Barriers to Adoption

Security

- Mobile security is the leading inhibitor to adopting mobile
- The leading security concern is the handling of confidential data, followed by identity and access management and virus/ malware.



Skills

- Very few (7%) have no skill gaps at all in mobile.
- Around a quarter have considerable skill gaps in mobile and 40% have moderate skill gaps.

	% will develop/acquire the skill over the next two years
Mobile security and privacy	69%
Mobile integration	68%
Mobile application management	67%
Mobile device management	62%
Mobile application architecture, design, and development	58%

Source: IBM Center for Applied Insights (Bluemine)

Top mobile security concerns

- Risk of theft or loss
- Data leakage
- Man in the middle
- Malware

- Useful sources of information:

IBM X-Force ® Research and Development (Trend & Risk Report)

Open Web Application Security Project (OWASP) Mobile Security Project

Mobile Security Challenges Faced By Enterprises

Achieving Data Separation & Providing Data Protection

- Personal vs corporate
- Data leakage into and out of the enterprise
- Partial wipe vs. device wipe vs legally defensible wipe
- Data policies

Adapting to the BYOD/ Consumerization of IT Trend

- Multiple device platforms and variants
- Multiple providers
- Managed devices (B2E)
- Unmanaged devices (B2B,B2E, B2C)
- Endpoint policies

Providing secure access to enterprise applications & data

- Identity of user and devices
- Authentication, Authorization and Federation
- User policies
- Secure Connectivity

Developing Secure Applications

- Application life-cycle
- Vulnerability & Penetration testing
- Application Management
- Application policies

Designing & Instituting an Adaptive Security Posture

- Policy Management: Location, Geo, Roles, Response, Time policies
- Security Intelligence
- Reporting

What's different about mobile security?

Mobile devices are shared more often

- Personal phones and tablets shared with family
- Enterprise tablet shared with co-workers
- Social norms of mobile apps vs. file systems

Mobile devices have multiple personas

- Work tool
- Entertainment device
- Personal organization
- Security profile per persona?

Mobile devices are diverse

.

- OS immaturity for enterprise mgmt
- BYOD dictates multiple OSs
- Vendor / carrier control dictates multiple OS versions

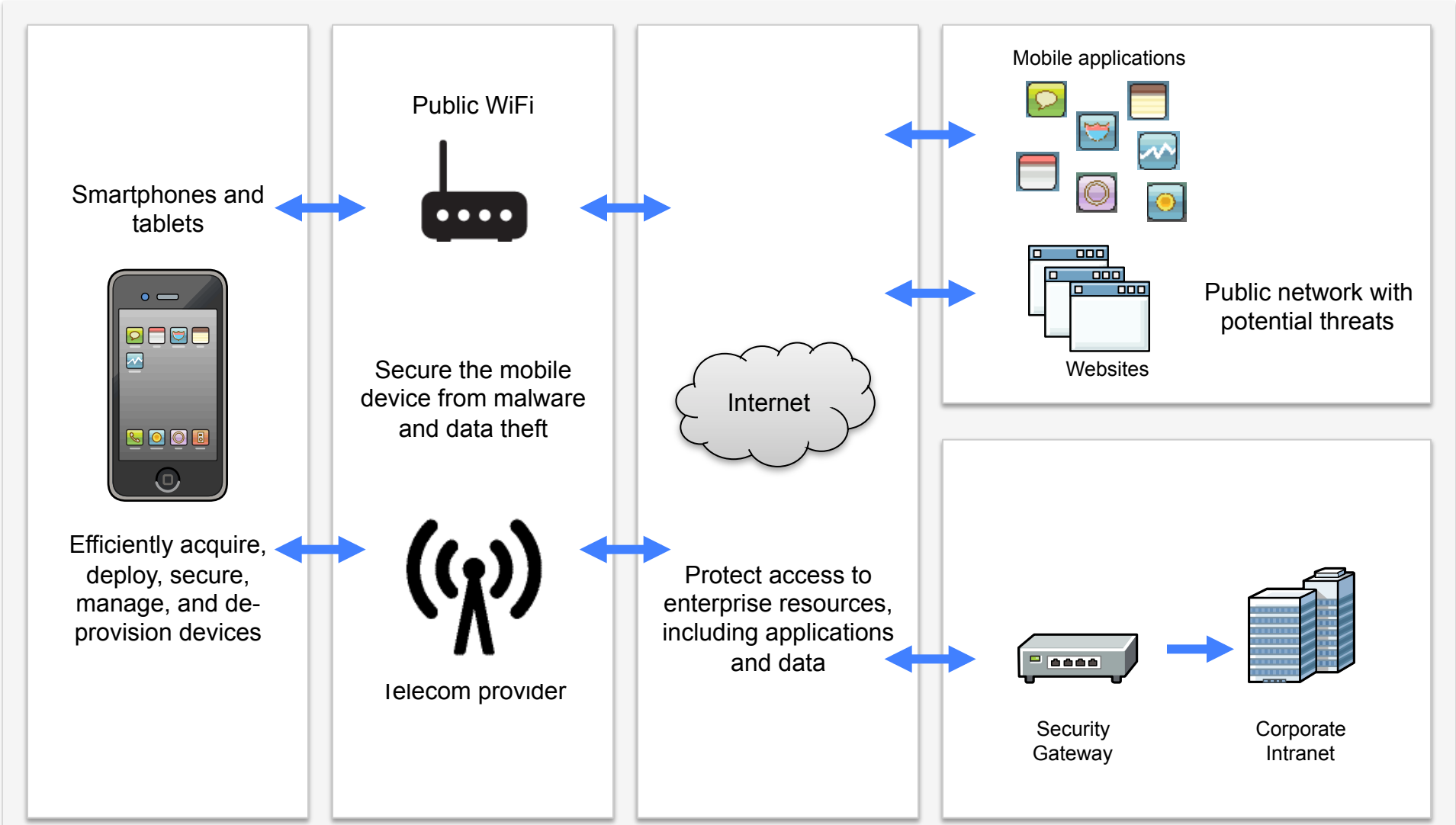
Mobile devices are used in more locations

- A single location could offer public, private, and cell connections
- Anywhere, anytime
- Increasing reliance on enterprise WiFi

Mobile devices prioritize the user

- Conflicts with user experience not tolerated
- OS architecture puts the user in control
- Difficult to enforce policy, app lists

Security concerns of mobile devices accessing corporate systems



Attain visibility into enterprise security events to stay ahead of the threats

An example of Risk-Based Access

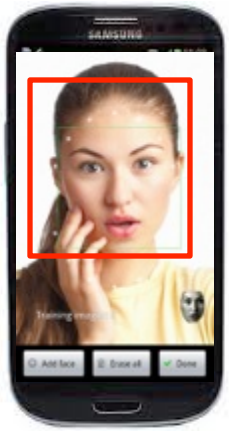
Governed Policy

- Context
  - On-site inside emergency room
  - On the hospital network
  - Authorized doctor on shift
- Function: All app features
- Data: Full data access
- Security: Single-factor authentication

- Context
  - At coffee shop
  - On an unsecured network
  - Authorized doctor on call
- Function: Designated features only
- Data: Specific encrypted data
- Security: Multi-factor authentication

An example of Two-Factor Authorization (2FA)

Payment Request →



← Ask Confirmation to Mobile , Biometrics

→ Confirmation

- Large amount
- Payment is unusual for some reason
- Customer has registered her mobile device

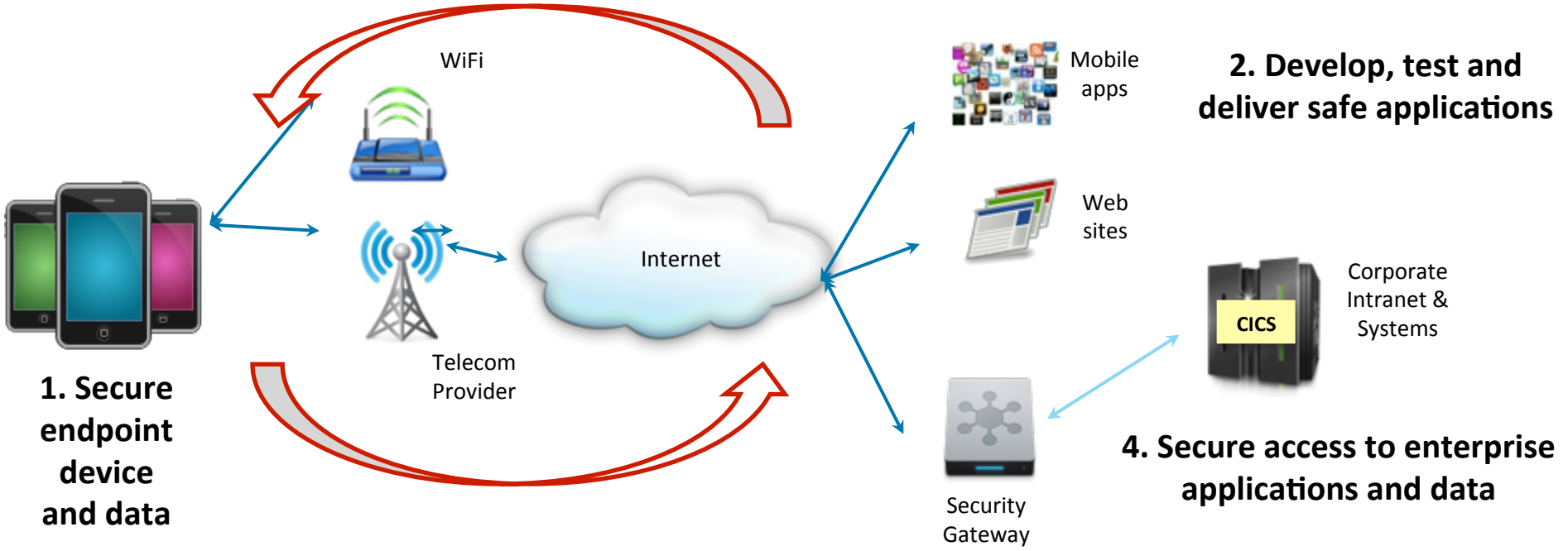
Demand Real Time Confirmation

Confirmed Payment Accepted

Payment Authorization Engine

Addressing mobile security challenges

1. Secure the mobile device
2. Secure the mobile application
3. Secure the transaction over the network
4. Secure the enterprise applications and data



The Mobile Security Ecosystem

At the 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

Manage Applications
Manage applications and enterprise app store

Over the Network

Secure Access
Properly authenticate and identify mobile users and devices • Allow or deny access • Connectivity

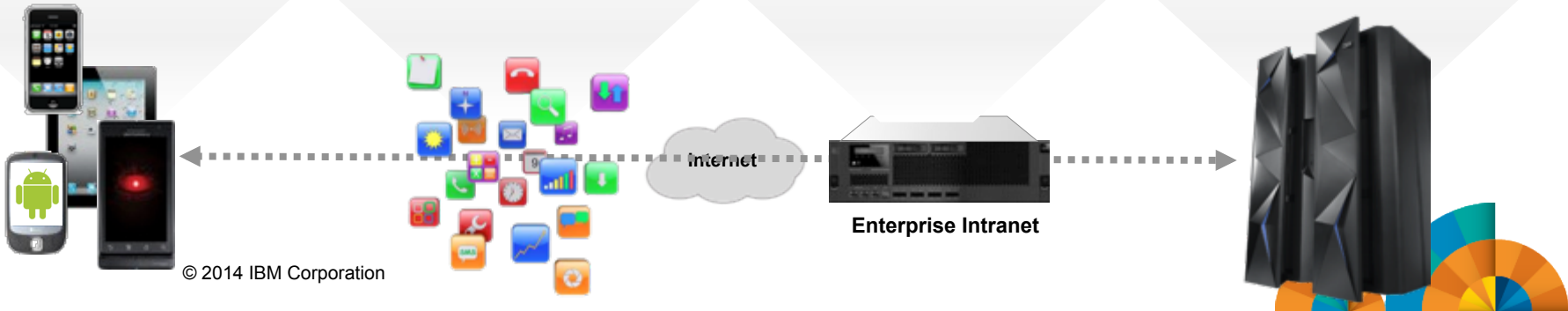
Monitor & Protect
Identify and stop mobile threats • Log network access, events, and anomalies

Secure Connectivity
Secure Connectivity from devices

Within the Enterprise

Transaction Security
Properly identity mobile users and transactions

Access control
Control access to critical applications and data



The Mobile Security Ecosystem – product mapping

Focus for this workshop

At the Device

MaaS360

• Wipe • Lock

Trusteer

Application Security
Offline authentication

WorkLight Runtime

Mobile App

Secure Application
Utilize secure coding

AppScan for Mobile

Integrate Securely

WorkLight Server

Manage applications and enterprise app store

Over the Network

Secure Access

Access Manager for Mobile

Monitor & Protect

QRadar

anomalies

DataPower

from devices

IBM Mobile Connect

Within the Enterprise

Transaction systems security

z/OS Connect

RACF, PKI, Hardware crypto.

Internet

Enterprise Intranet

IBM mobile device requirements

Rooted or jailbroken phones

Mobile Appstore

'Jailbroken' or 'rooted' mobile devices may not be used to conduct IBM business. These devices are blocked from accessing IBM business services and applications such as IBM Traveler.

Encryption

IBM Wi-Fi network

Rooted or jailbroken phones

Mobile Appstore

For access to proprietary IBM and client information, only use mobile applications installed from the IBM CIO Mobile Appstore. Apps installed from external vendors' app stores can only be used to access IBM information approved for public disclosure.

Encryption

IBM Wi-Fi network

IBM mobile device requirements (cont…)

Rooted or jailbroken phones

Mobile Appstore

On most mobile devices, the device's storage cannot be fully encrypted to protect IBM and client information. For this reason, mobile devices are not provided unrestricted access to the IBM network.

Mobile devices are not as secure as workstations for storage of IBM and client information, particularly IBM Confidential and regulated data. Sensitive Personal Information (SPI) must not be stored on mobile devices that do not feature IBM-approved storage encryption.

Encryption

IBM Wi-Fi network

Rooted or jailbroken phones

Mobile Appstore

When working inside of an IBM building, do not connect your mobile device to IBM's internal (production) wireless network. It is permissible to connect to guest wireless networks in IBM office buildings (as available).

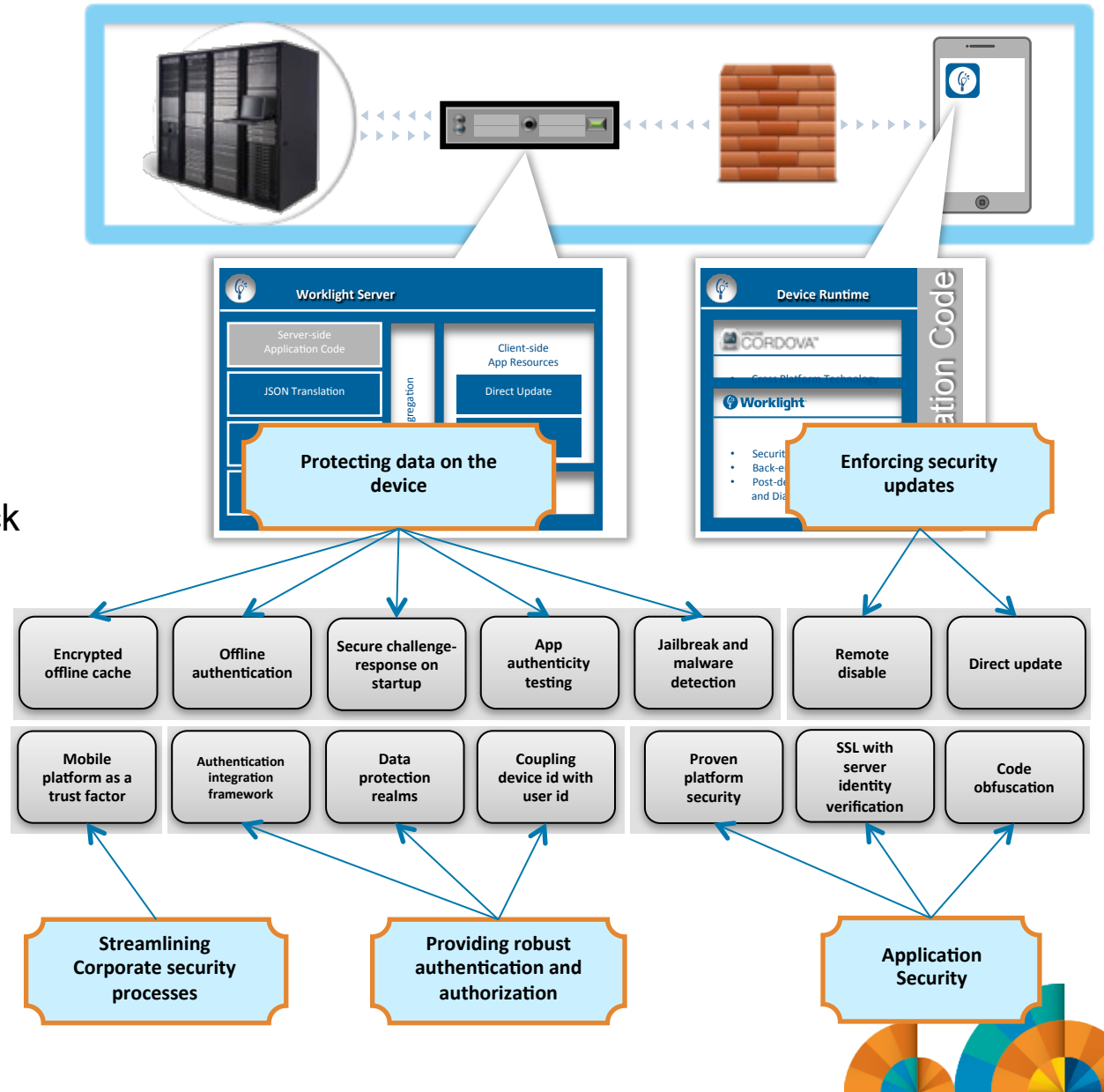
IBM developers working on mobile application projects in IBM labs may connect to IBM's internal wireless networks but must only access only dev or test systems (avoid access to internal IBM production systems, including w3).

Encryption

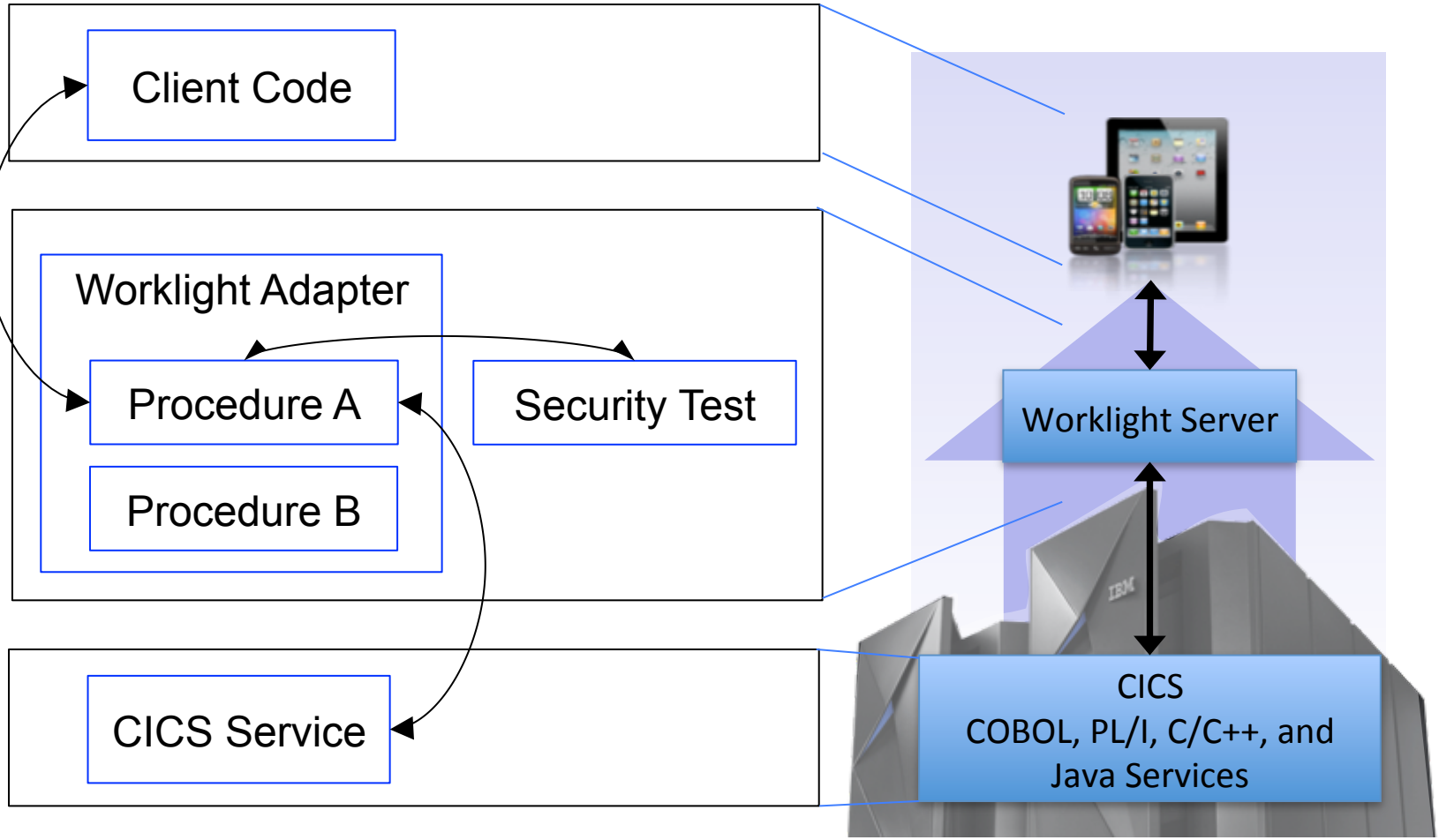
IBM Wi-Fi network

Worklight Security Features

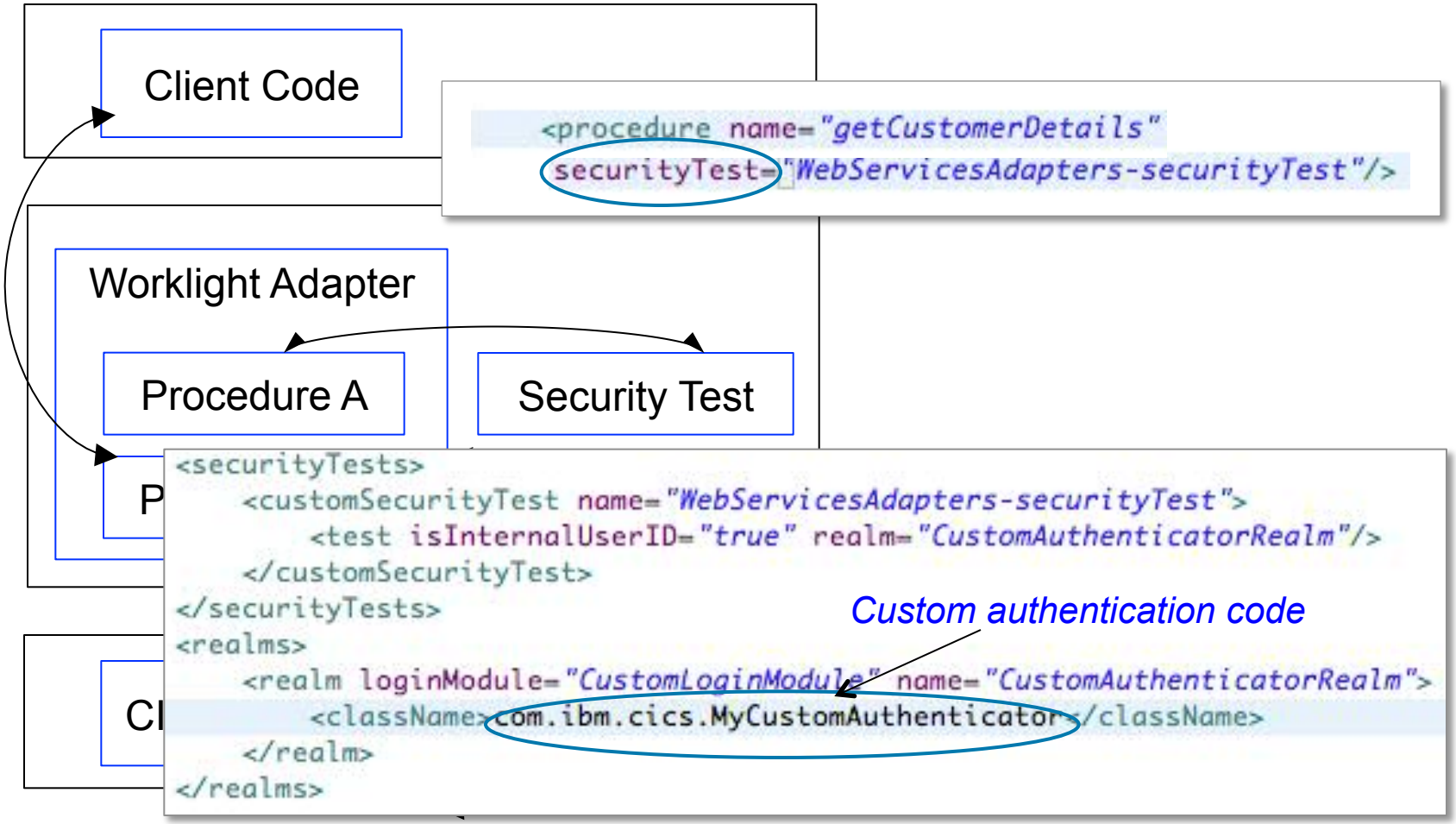
- Extensible framework for authentication of mobile application users
- Ensure that only specific applications on specific devices can connect to enterprise systems
- Application authenticity check
- Encrypt data on the device
- Enforce security updates
- Propagate identity to enterprise systems



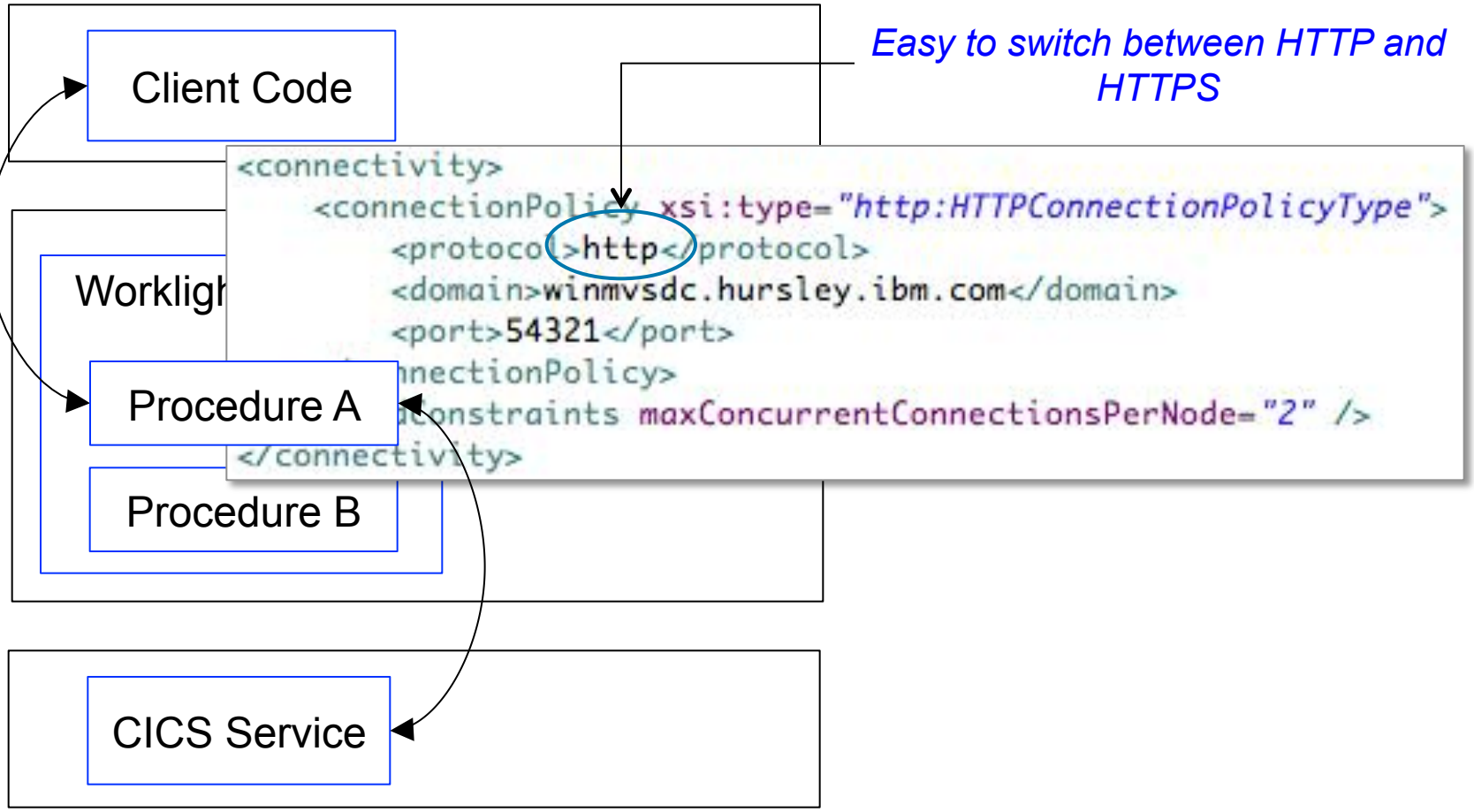
Worklight Components – basic flow



Worklight Components – security check

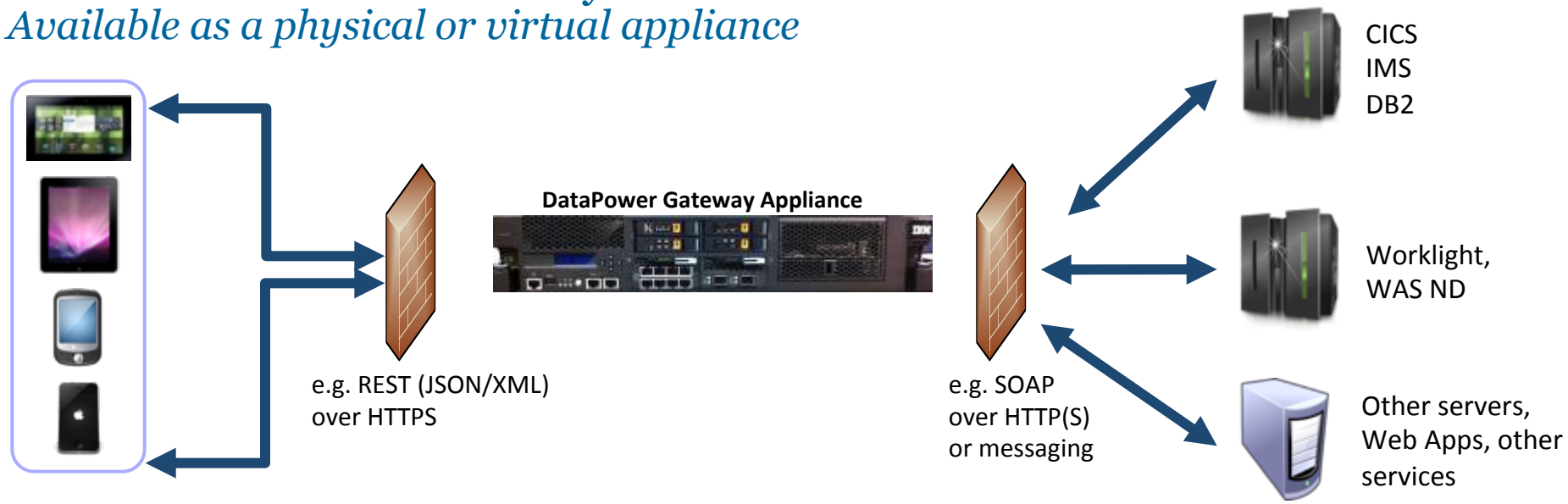


Worklight Components – connectivity



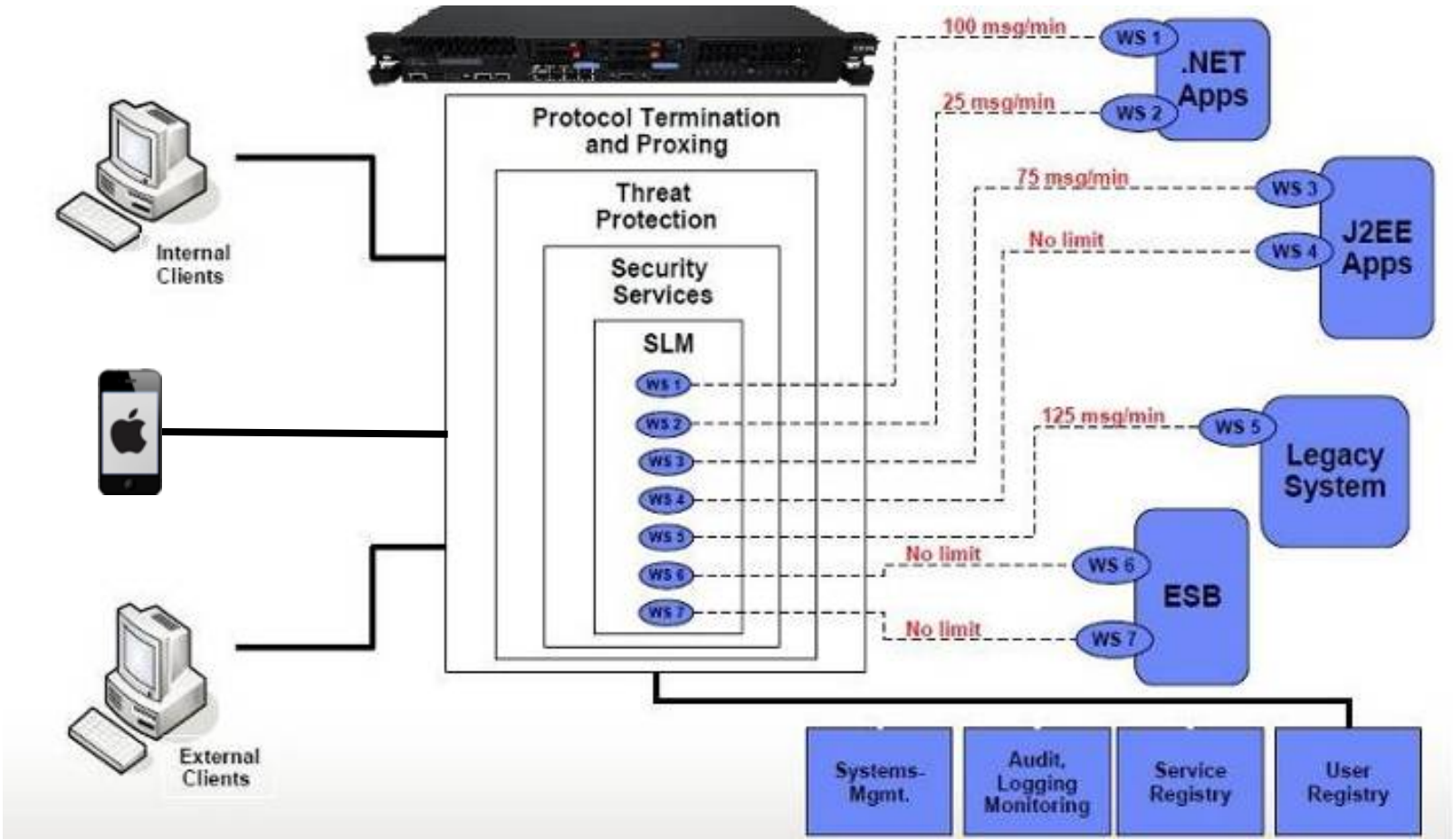
DataPower Mobile Security Features

Available as a physical or virtual appliance

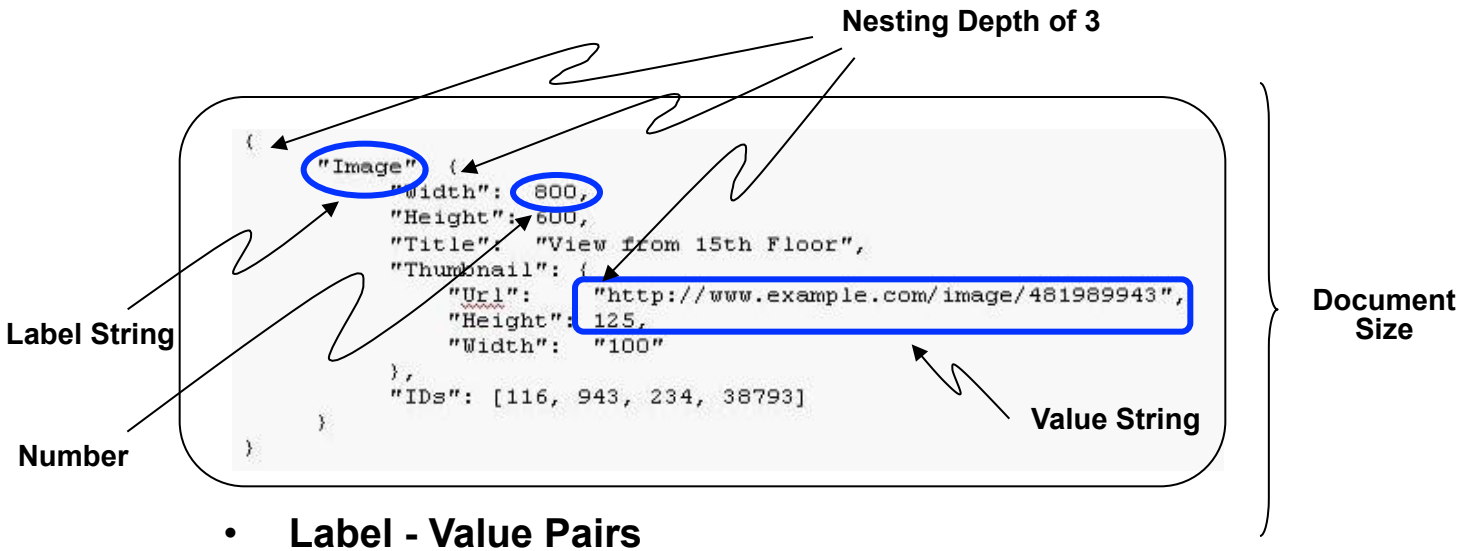


- Security, Control, Integration & Optimization of mobile workload
- Enforcement point for centralized security policies
- Authentication, Authorization, SAML, OAuth 2.0, Audit
- Threat protection for XML and JSON
- Message validation and filtering
- Centralized management and monitoring point
- Traffic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

DataPower traffic control and rate limiting



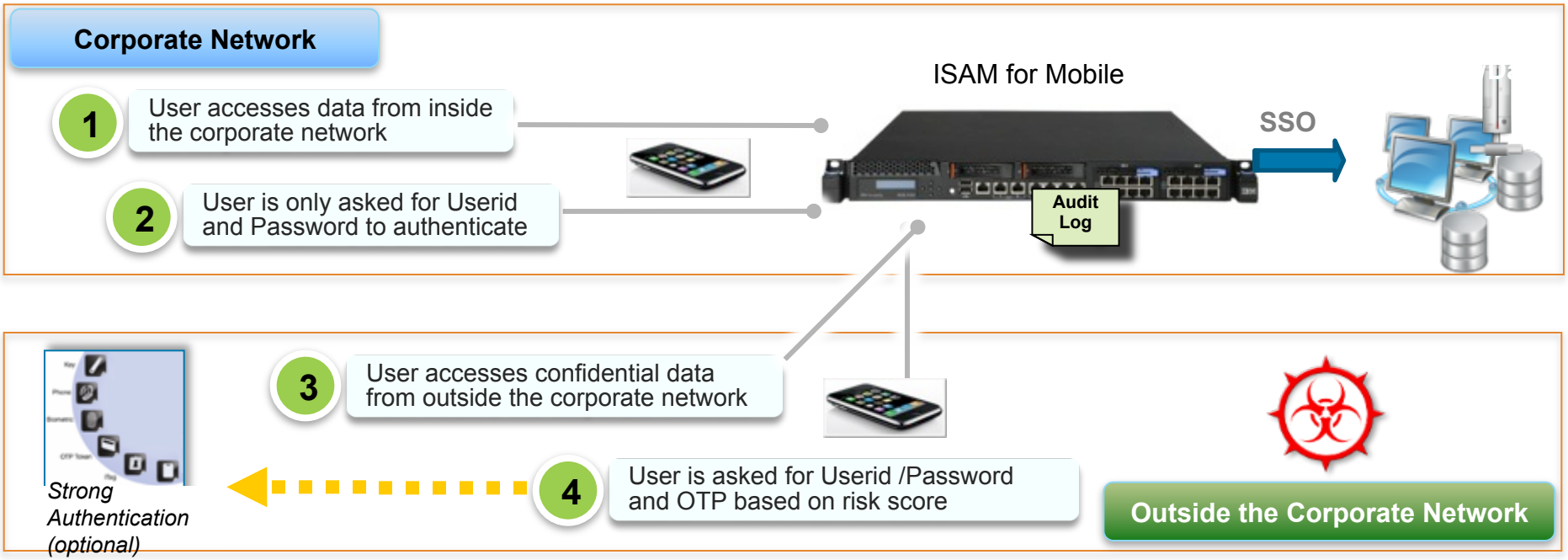
DataPower JSON protection



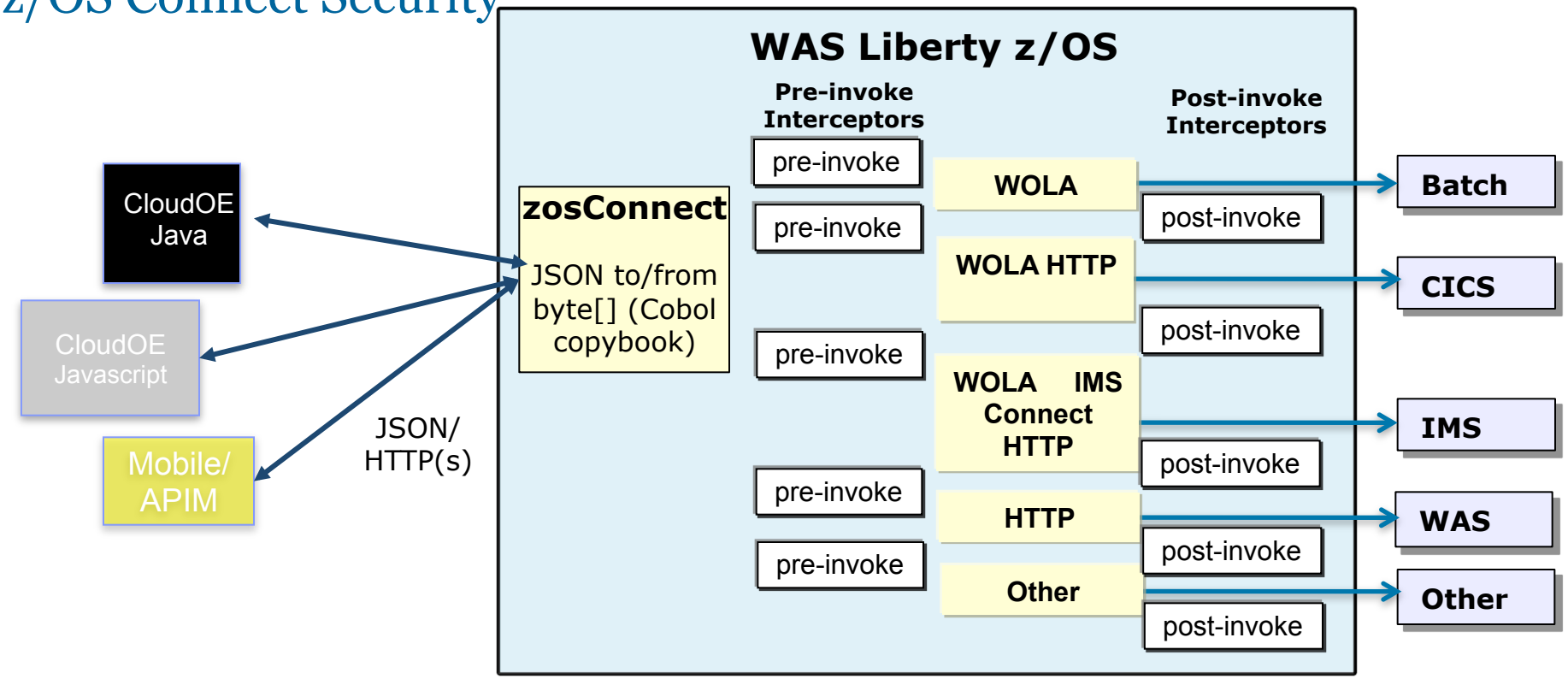
- **Label - Value Pairs**
  - Label String Length (characters)
  - Value String Length (characters)
  - Number Length (characters)
- **Threat Protection**
  - Maximum nesting depth (levels)
  - Maximum document size (bytes)

Jumbo JSON Payload

IBM Security Access Manager for Mobile



z/OS Connect Security



- Framework that allows interceptors to be executed around the invocation of the service
- z/OS Connect provides interceptor implementations of service security authorization and SMF-based auditing
  - **com.ibm.wsspi.zos.connect.Authorization()**
  - **com.ibm.wsspi.zos.connect.Audit()**
- z/OS Connect performs authorization checking e.g is authenticated user in '**Invoke**' group for requested service

Audit (SMF) Interceptor

The audit interceptor writes SMF 120.11 records with the following information captured:

Liberty Profile z/OS

z/OS Connect

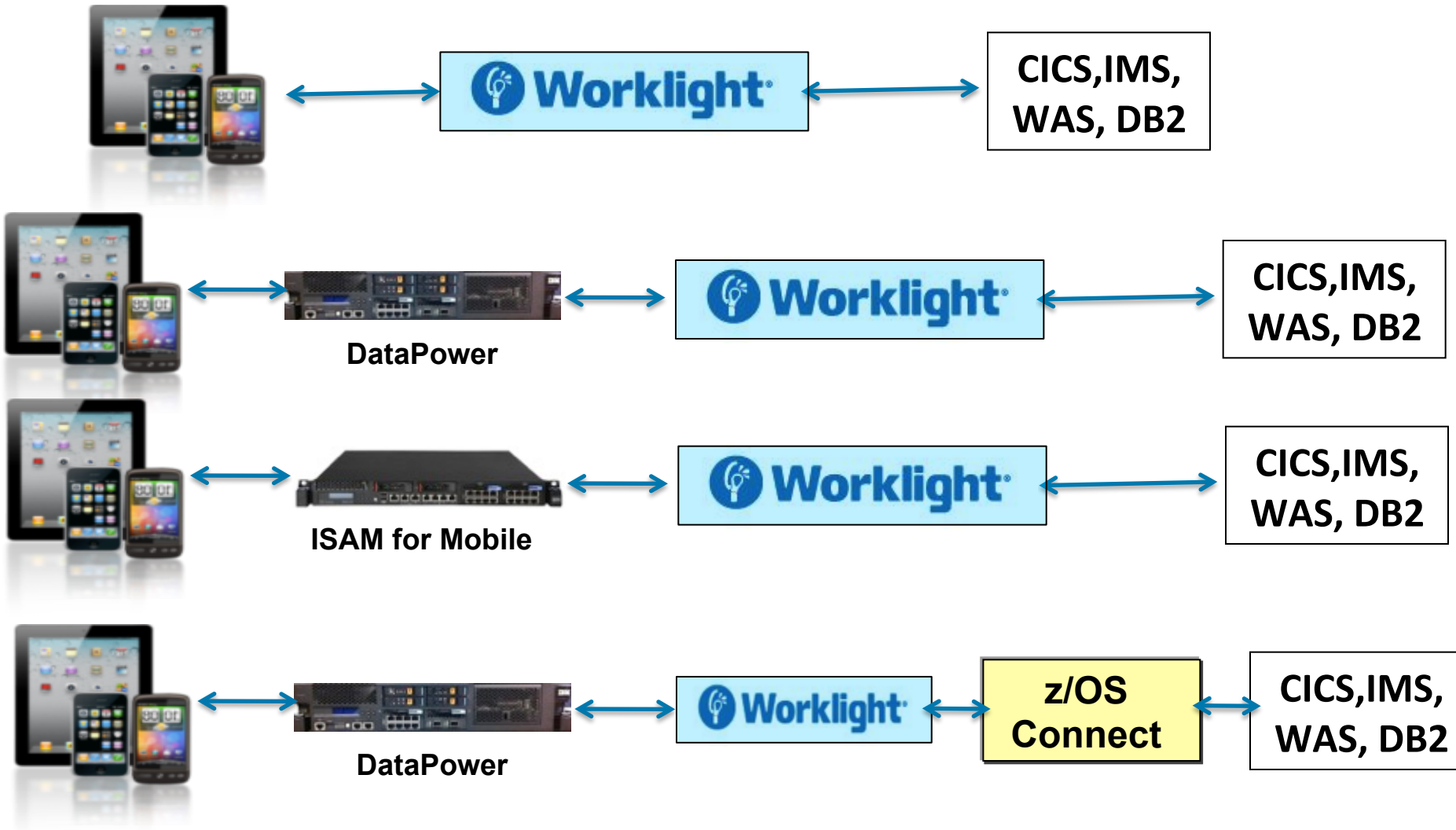
- System Name
- Sysplex Name
- Job Name
- Job Prefix
- Address Space Stoken

Server Identification Section

- Arrival Time
- Completion Time
- Target URI
- Input JSON Length
- Response JSON Length
- Method Name
- Service Name
- Userid
- Grouping Name

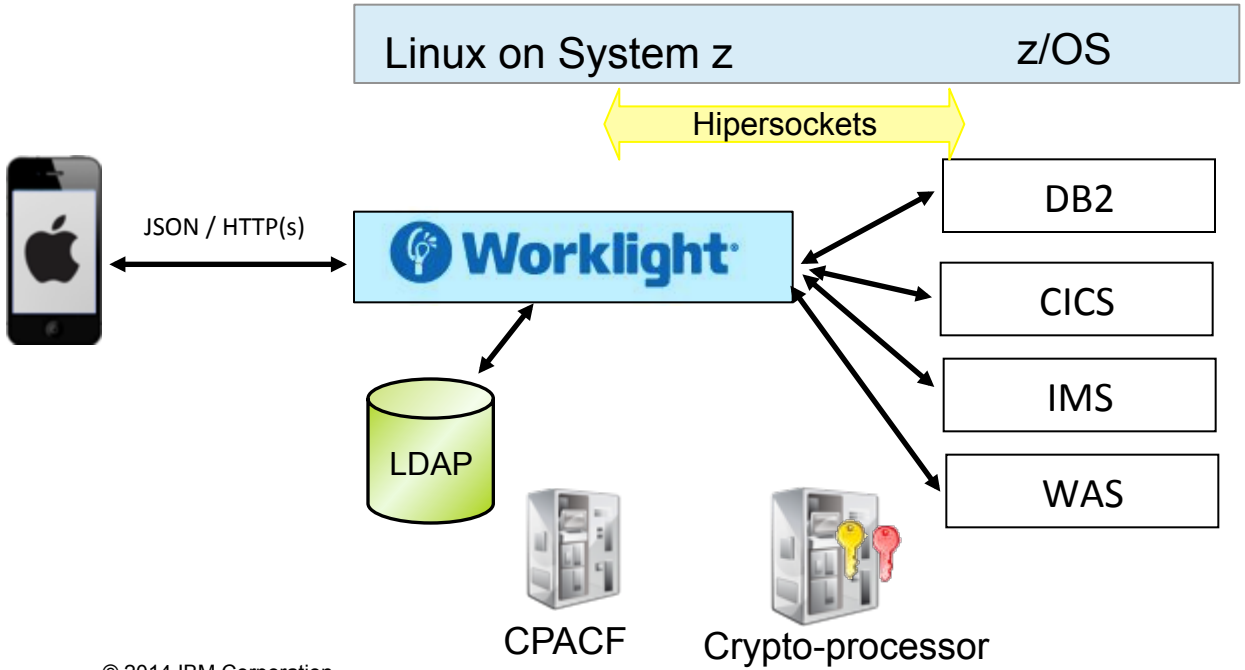
z/OS Connect User Data Section

Some security topologies



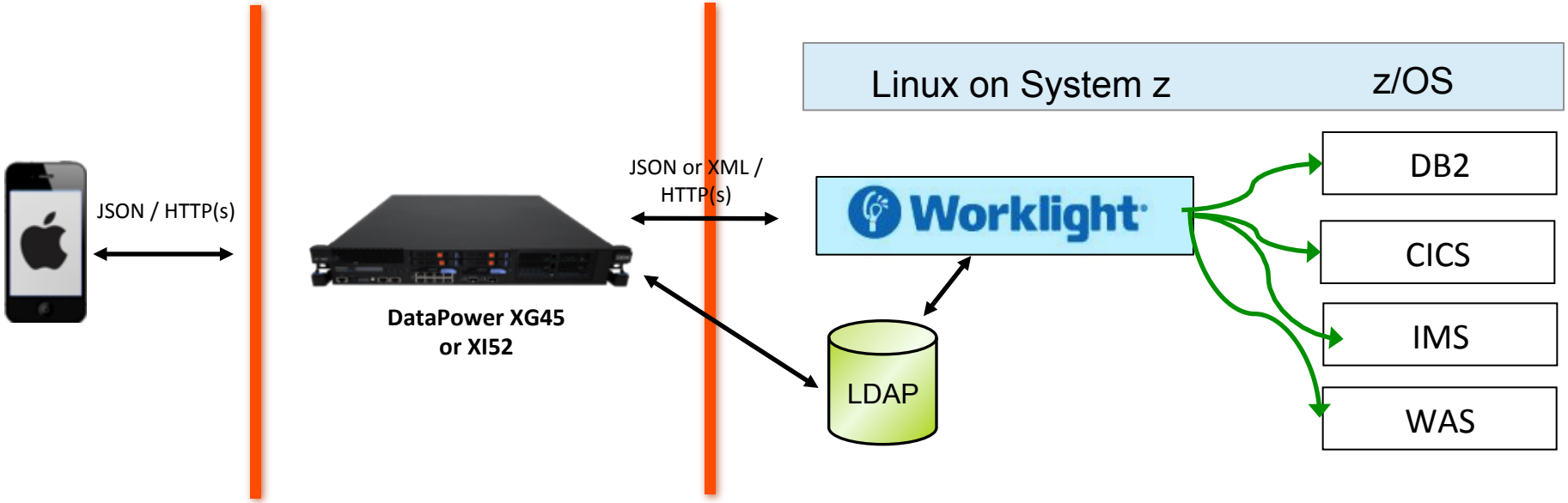
Worklight security

Worklight capabilities	Deployment scenarios	Benefits
• **Authentication:** HTTP Basic, form-based, Custom • Device authentication • Offline authentication • Application updates and authenticity • **Authorization:** Policy • **Interoperate:** LDAP, WebSphere	• **Small enterprise, B2E app** • Traditional web user authentication mechanisms are sufficient • Minimal interoperability required with enterprise-wide security solutions	• Take advantage of Worklight security capabilities Additional security benefits when Worklight server is deployed to Linux for System z: • Opportunity to eliminate encryption between Worklight server and CICS • Hardware crypto, Hipersockets, EAL4+ certification



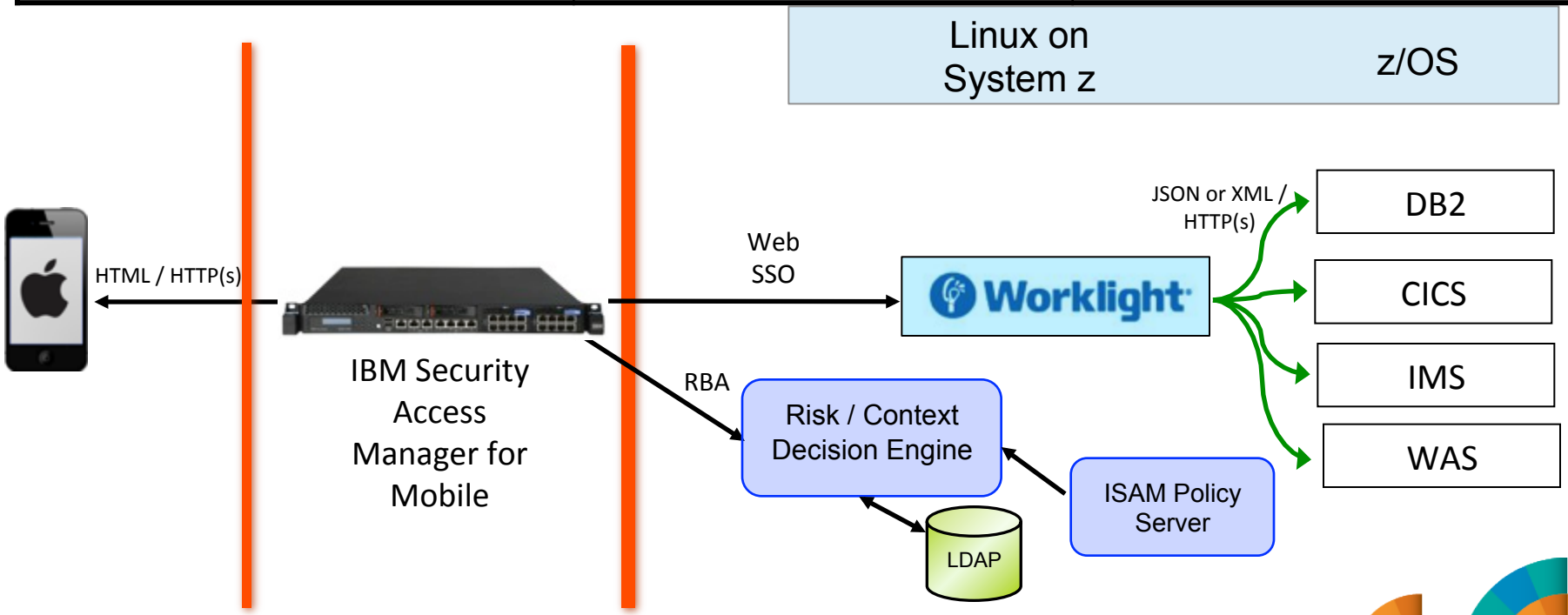
DataPower as a Policy Enforcement Point (PEP)

DataPower capabilities	Deployment scenarios	Benefits
• **Authentication:** HTTP Basic, form-based, WS-*, SSL, Kerberos, SAML, LTPA, OAuth • **Authorization:** LDAP, ISAM, SiteMinder, SAML, XACML, OAuth, System z (RACF) • **Interoperate**: LDAP, SiteMinder, ISAM, TFIM, WebSphere	• When mobile apps are heavily focused on REST/API/web service based interactions • **High volume or internet (B2C) mobile access** • Support for Web APIs	Additional benefits of DataPower as mobile security gateway • Threat protection and intelligent routing • Supports a wide range of authentication and authorization models • DataPower can provide single sign-on capability



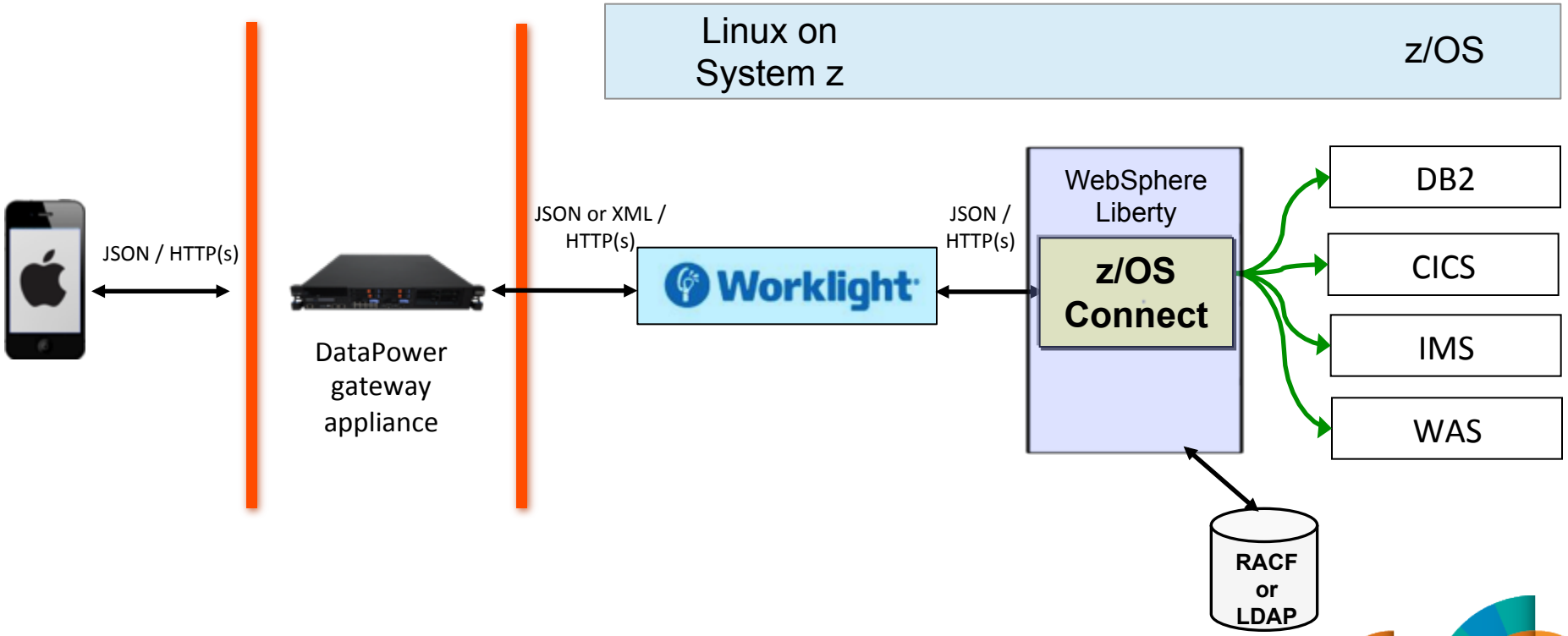
ISAM for Mobile as a Policy Enforcement Point (PEP)

ISAM for Mobile capabilities	Deployment scenarios	Benefits
• Authentication: HTTP Basic, form based, SSL, Kerberos, SAML, LTPA, NTLM, OAuth, multi-factor, step-up, Risk based • Device authentication • Authorization: LDAP, ISAM, SiteMinder, SAML, XACML, OAuth, System z (RACF) • Interoperate: LDAP, SiteMinder, TFIM, .NET, WebSphere, QRadar, Trusteer	• Mobile apps are heavily focused on mobile web/browser interactions • Strong authentication (2FA,MFA) or risk based authentication (RBA) is required • Comprehensive SSO and session management is required	• ISAM is very effective as a web application firewall (WAF) • Integrates well with security intelligence solutions like QRadar • Integrates with fraud detection solutions like Trusteer **Note**: DataPower and ISAM can also be used together



z/OS Connect

Capabilities (z/OS Connect)	Deployment scenarios	Benefits
• **Authentication:** HTTP Basic, SSL client authentication • **Authorization:** RACF, LDAP • **Confidentiality/integrity**: SSL/TLS	• When want unified interface to z/OS back-end applications that run in CICS, IMS, WebSphere or batch jobs	• Provides unified security for different back-end systems • **Provides a way to discover with a simple REST call all the services that z/OS supports**



How to chose the right mobile security solution?

- **Type of user**
  - B2E
  - B2C
- **Type of mobile app**
  - Web
  - Native
  - Hybrid
  - Worklight
- **Type of access**
  - Intranet/extranet
  - Internet
- **Number of users**
  - Small (10s to 100s)
  - Medium (1000s)
  - Large (many thousands)
  - Known or unknown number
- **Security requirements**
  - Authentication
  - Authorization
  - Confidentiality
  - Integrity
- **Sensitivity of data and transactions**
  - Financial?
  - Personal?
  - Will data be stored on the device?
- **Security standards**
  - Company
  - Government or external body
- **Existing security architecture**
  - User registry
  - Security products

GENAPP Mobile - Architecture

1. Mobile user sends an insurance policy request

4. CICS service handler converts the request to the Channel interface of the GENAPP application

Worklight

GENAPP Mobile

Inquire Adapter

Security Test

CICS

Service Pipeline

GENAPP

DB2

2. Custom security test

3. On successful authentication the CICS application is invoked by a Worklight adapter

5. The GENAPP Cobol application processes the insurance policy request and updates the GENAPP database

GENAPP - Security requirements

- **Type of user**
  - B2E
  - B2C
- **Type of mobile app**
  - Web
  - Native
  - Hybrid
  - Worklight
- **Type of access**
  - Intranet/extranet
  - Internet
- **Number of users**
  - Small (10s to 100s)
  - Medium (1000s)
  - Large (many thousands)
  - Known or unknown number
- **Security requirements**
  - Authentication (userid/password)
  - Authorization (see next chart)
  - Confidentiality (https)
  - Integrity (https)
- **Sensitivity of data and transactions**
  - Financial? (no)
  - Personal? (yes but not very sensitive information)
  - Will data be stored on the device? (no)
- **Security standards**
  - Company (all transactions must be audited)
  - Government or external body (data encryption regulations)
- **Existing security architecture**
  - User registry (LDAP)
  - Security products

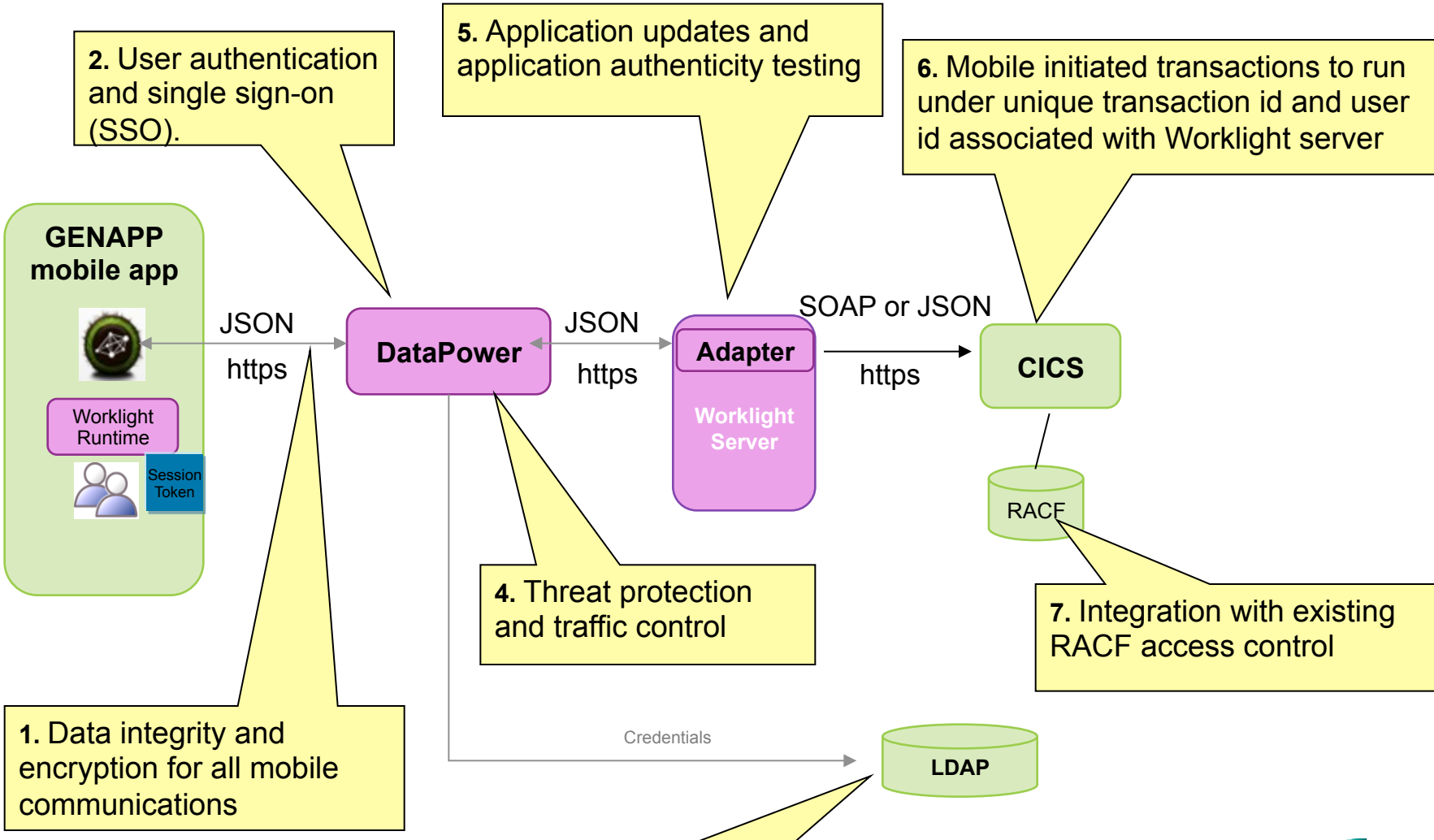
GENAPP Mobile – security requirements

1. **Data integrity and encryption for all mobile communications** - All of the data transferred by the mobile app requires encryption to comply with industry regulatory standards.
2. **User authentication and single sign-on (SSO)** - Mobile users must authenticate with a customer number and password before they are allowed to access their insurance policy data.
3. **Integration with existing user directory** - Mobile security 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 using the IBM Tivoli Directory Server hosted on the IBM System z.
4. **Threat protection and traffic control** - In order to protect against unexpected surges in mobile requests, for example when a large storm occurs that triggers lots of inquiries or claim activity, or a denial of service attack, the insurance company wants to limit the number of requests that can be sent to the Worklight Server.

GENAPP Mobile – security requirements (cont…)

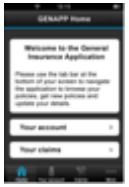
5. **Application updates and application authenticity testing** - When providing a mobile app on an employee's device, the insurance company must ensure the app is secure by addressing the following requirements:
   - It is not tampered with or modified in any way
   - It is not used to access restricted areas of their systems
   - It has not been modified and redistributed containing malware or exploits that can potentially compromise systems or capture confidential customer data
6. **Mobile initiated transactions to run under unique transaction id and user id associated with Worklight server** - The insurance company wants to be able to identify mobile-initiated transactions across their CICS systems so that they can enable access control, track the workload impact of the mobile app and apply for special mobile pricing.
7. **Integration with existing RACF access control** – Mobile initiated CICS transactions are only authorized if the request comes from the IBM Worklight Server. Each Worklight server has an assigned RACF user id.

GENAPP security solution



GENAPP Mobile – security solution steps

1. **Data integrity and encryption for all mobile communications** – HTTPS is used for all communications between the mobile app and Worklight server. Hardware crypto is used to reduce the cost of SSL handshakes and data encryption.
2. **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 Worklight server, providing an application single sign-on capability.
3. **Integration with existing user directory** - User authentication is done against the existing IBM Tivoli Directory Server LDAP user registry.
4. **Threat protection and traffic control** - WebSphere DataPower is used for threat protection and traffic control.
5. **Application updates and application authenticity testing** - Worklight enforces application updates and tests the authenticity of the mobile application.
6. **Mobile initiated transactions to run under unique transaction id and user id associated with Worklight server** - Mobile initiated CICS transactions are run under a RACF user id that represents the Worklight Server. This is achieved using SSL client authentication between the Worklight server and CICS. RACF certificates are used by Worklight and CICS.
7. **Integration with existing RACF access control** – Existing RACF access control mechanisms are used to authorize the Worklight Server to the set of GENAPP CICS transactions.



Wrap-up

- **Security is one of the top client concerns**
- **End-to-end comprehensive security requires a focus on**:
  - Device security
  - Mobile App security
  - Connectivity over the network
  - Access to Enterprise applications
- **IBM offers a full set of mobile security products and services**
- **System z has unique characteristics to support and secure mobile applications**