WHITE PAPER | FEBRUARY 2014

Secure Mobile Access for the Public Sector

Simplifying Security & Management for Apps & BYOD

Table of Contents

Executive Summary 3

Section1: 4
Summarizing the Challenge

Section2: 5
Addressing the Challenges of Enterprise/Mobile Integration

Section 3: 8
Layer 7 Solutions for Simplifying Secure Enterprise Mobile Access

Conclusions

Executive Summary

Challenge

"I want us to ask ourselves every day, how are we using technology to make a real difference in people's lives."—President Barack Obama

Mobile technology is beginning to revolutionize the federal government IT landscape. *The Digital Government Strategy*, issued by the Federal Chief Information Officer, Steven Van Roekel in 2012, gave guidance to promote cross-agency sharing and an adoption of mobile workforce solutions. A "Bring Your Own Device" (BYOD) working group was also created to assist agencies with implementing their own BYOD programs. Across the public sector spectrum, the demand is growing for access to high-quality digital government information and services anywhere, anytime, and on any device.

Opportunity

"It is a brave new world. There are a lot of capabilities, there's a lot of innovation that's occurring, and we're all adapting on the fly."—Rear Adm. Ron Hewitt, Director of the Office of Emergency Communications at the Department of Homeland Security.

The *2013 Status of Telework in the Federal Government Report to Congress* acknowledged a growing government-wide commitment to incorporate telework as a standard practice. But, telework is only one part of the mobile revolution: opportunities exist for mobility solutions that will help soldiers better communicate from the battlefield; maintain agency operations during an emergency with Continuity of Operations Programs (COOP); relay time-critical information from the national to local levels; create a future-ready workforce; consolidate and centrally manage IT services, systems, and hardware; deliver critical government services to citizens, and much, much more.

Benefits

"If the addition of smartphones enables Feds to be even 10% more productive, the Federal government could add $2.6B in Federal productivity by 2013."—*Mobile Powered Government, Driving Increasingly Productive, Efficient Agencies*, MeriTalk powerpoint, February 27, 2012

Mobile technology gives government agencies efficiencies that are simply too beneficial to ignore: it widens an agency's reach; increases effectiveness providing citizen services; delivers critical data on the spot; responds faster, and monitors assets and control points.

- In July 2012, the US Equal Employment Opportunity Commission (EEOC) implemented a program where employees could opt-out of the government-furnished Blackberry and run third-party software on their personal mobile devices. The software enabled security on the devices, as well as the capability to remotely wipe data from them. This program created significant long-term savings for the EEOC.
- The State of Delaware initiated an effort to not only embrace the concept of BYOD but to realize significant cost savings by having employees turn in their State-owned device in favor of a personally-owned device, which could save the State approximately half of its current wireless expenditure.
- The Department of the Treasury's Alcohol and Tobacco Tax and Trade Bureau (TTB) implemented a virtual desktop that allowed a BYOD solution with minimal policy or legal implications.
- During the 2010 census special mobile devices were provided by the Census Bureau, and synched with private cloud-based data. For the 2020 census, the bureau is considering BYOD for census takers to increase efficiencies for data collection.

In a 2011 survey of 152 Federal CIOs and IT managers conducted by MeriTalk, the IT professionals reported that a mobile workforce was more productive, helped government achieve its telework initiatives, attracted top talent, and enhanced employee experience.

Section1:

Summarizing the Challenge

Mobile devices are only half the story. Hardware, specifically the emergence of the iPad and similar tablets, has been the catalyst for a revolution in federal enterprise mobility. BYOD shows us that people are already using their devices for work. IDG Connect's *iPad for Business* 2012 study found that 67% of North American iPad owners—including public sector employees—were using their iPads at work. But, to really benefit from mobile, apps need to be designed to meet the specific challenges of the federal workforce.

Making government data and application functionality available to apps residing on employees' mobile devices can be achieved by using application programming interfaces (APIs), to expose on-premise systems and data to developers building mobile apps. Using APIs for enterprise/mobile integration is a recent development requiring a specific solution to ensure the maintenance of security and governance. In this context, a SOA Gateway with API Proxy capabilities can be used as a "Mobile Access Gateway" to address identity, data and application adaptation and sharing control across an API.

Mobile Integration: using apps to leverage internal information

Over the last decade, more and more enterprise architects have adopted an approach driven by APIs in order to make data and application functionality available to other applications. These architects create "services" that allow them to easily consume and re-use existing IT investments while creating new business processes by composing multiple operations together into higher-level applications.

This approach, known as “Service Oriented Architecture” (SOA), can be leveraged in the government enterprise mobile context. Key data and applications can be extended and delivered as services, through APIs, to mobile apps. More specifically, Service Oriented interfaces can be quickly adapted into mobile-friendly APIs that expose internal enterprise information assets to mobile developers and the apps they build, using formats and security models mobile devices can easily consume.

Section2:

Addressing the Challenges of Enterprise/Mobile Integration

APIs provide the technical components internal developers need to integrate on-premise information assets with the apps they build for employees’ mobile devices. However, for this approach to work, four challenges must be met:

1. Adapting Information Assets for Mobile Consumption
2. Optimizing App Performance When Accessing Enterprise Information
3. Securing Mobile Access to Enterprise APIs
4. Making APIs Discoverable & Consumable for Developers

Adapting information assets for mobile consumption

There are a number of challenges associated with making internal information assets usable by a mobile app. First, information assets in legacy formats need to be reworked as RESTful APIs that can be accessed as XML or JSON data messaging formats. This requires an efficient system for translating any backend information asset into a RESTful API that communicates over HTTP/S using JSON messaging. It may also require a reconstitution or “re-composition” of internal information assets into new APIs customized to specific users or apps.

This kind of data translation and API re-composition is ideally suited to the SOA Gateways that are commonly used to integrate applications in SOA by translating data formats, orchestrating service interactions, virtualizing APIs and bridging different protocols and transports. Connecting a mobile app to an enterprise application is therefore rendered as just another integration problem. Some API Proxies can similarly handle this kind of integration challenge for a simpler subset of enterprise applications.

Optimizing app performances when accessing enterprise information

When integrating enterprise applications with mobile apps, performance is always a key consideration. An enterprise that is publishing mobile APIs will need ways to accelerate the delivery of data while reducing traffic volumes because:

a. The data will be traveling on relatively low-bandwidth mobile networks

b. Mobile usage can scale geometrically as the enterprise opens applications first to employees and then to consumers. Again, a SOA Gateway or API Proxy may be able to help the enterprise address these challenges. This is because some SOA Gateways deliver a wide range of functionality for managing and optimizing data traffic loads including:

    - Throttling requests that exceed a certain threshold or shaping traffic based on considerations like location, time of day or subscriber level, which selectively limit performance-sapping load on back-end applications.
    - Using sophisticated caching capabilities in order to minimize the number of requests that get passed to back-end applications, and improve latency response times.
    - Compressing data on the fly to minimize traffic sent to and from a mobile app. Some Gateways can load balance across multiple back-end instances, ensuring more evenly distributed load across APIs and simplifying a scale-punch of back-end applications.
    - Prioritizing API calls to ensure that paid subscribers or key users receive a consistent quality of service, with guaranteed access to enterprise resources. This function can also be used to reserve API access capacity based on a specific traffic type.

When deployed in the Cloud, some SOA Gateways can also help auto-scale back-end services and even dynamically add Gateway nodes to a cluster in order to process more traffic.

Securing mobile access to enterprise APIs

Security is a major concern whenever a mobile app needs to access information inside the enterprise. APIs have to be protected against attack or misuse. The data transmitted to and from the API needs to be secured (through encryption, tokenization or redaction), and its integrity verified. And access to the information resources exposed via the APIs needs to be controlled at a granular level, based on the identity or role of the requestor.

Control of access to information exposed through an API is an even thornier issue. A user may use different apps on different devices to access a piece of data or functionality exposed through the same enterprise API. Those apps can be built by different groups or designed as mash-ups of different information assets. Each app may use a different user ID, complicating the identification of the user.

Furthermore, users dislike retyping app-specific identities on mobile devices and would prefer to delegate that authentication to a pre-existing trusted app. To address the dilemmas created by the need to provide flexible-yet-secure access control for APIs in these more complicated mobile (and similar Web-based) scenarios, a new standard—OAuth—has emerged. OAuth is an evolving protocol that makes it possible to identify a user and the resources that user is interested in accessing via an intermediate app, without necessarily requiring the user to enter a username–password combination specific to the app.

The OAuth specification allows enterprises to grant authorization rights to an app based on: (a) the user's pre-existing credentials within the organization; (b) a trust relationship between the enterprise and the intermediate app. This kind of transitive trust and rights passing happens in the background—the user only needs to establish trust once for the intermediate app.

While OAuth solves prickly access problems particular to mobile app dynamics, it remains complicated for enterprises to set up. In particular, there are challenges around integrating OAuth with an enterprise's existing identity infrastructure. To address these challenges, an API Proxy may come with an OAuth Toolkit or token server, which will simplify the process of deploying and maintaining an OAuth access infrastructure on top of an API.

But access control is normally just the beginning of the security challenges facing an enterprise—and these challenges are exacerbated in a BYOD scenario, where the enterprise cannot lock-down mobile devices the way it could with desktop computers. Key challenges include:

a. Protecting against denial of service, cross-site scripting, SQL injection, and URL tampering attacks
b. Preventing accidental damage caused by poorly-written apps
c. Deploying a scalable system for preserving data security in communication to and from APIs, in order to meet data privacy stands like FIPS, PCI-DSS, and HIPAA.

Some SOA gateways and APR proxies can help enterprises address these challenges by providing a range of API, data, and URL security features.

Making APIs discoverable & consumable for developers

A critical element in enabling integration between mobile apps and enterprise services occurs before the first byte of data is exchanged. In order to build mobile apps based on enterprise APIs, developers and developer teams need certain information on the APIs they can call. This may include information on the functionality an API exposes, the data it returns, best practices for its use and so forth. Enterprises therefore need systems for developer on-boarding (i.e., registering developers to use an API) and management. This can be achieved by deploying an API Portal—a central location where developers go to get documentation on an API, test its behavior, sign up for usage, track API health and collaborate with other developers. Some SOA Gateway and API Proxy vendors provide integrated API Portals to ease the governance of APIs and the developers that use them.

Section 3:

Layer 7 Solutions for Simplifying Secure Enterprise Mobile Access

Layer 7 Technologies' API Management Suite of products delivers all the extended Mobile Access Gateway functionality necessary for secure enterprise/mobile integration. The API Management Suite represents the most comprehensive API management solution available and has been used in multiple successful integrations, including the use cases described in this white paper. The API Management Suite includes:

- SecureSpan API Proxy

  The API Proxy delivers all the core functionality required for an effective Mobile Access Gateway, including API security, data filtering, content transformation and out-of-the-box integration with leading access control systems and standards.

- Layer7 API Portal

  The API Portal provides everything enterprises need in order to on-board and manage mobile app developers, making it simple to create a portal through which developers can discover, learn about and register for available APIs.

- Layer 7 Enterprise Service Manager

  The Enterprise Service Manager provides a central dashboard that makes it simple to monitor Proxy operations and manage API versioning, lifecycle and deployment across internal datacenters and the Cloud.

- Layer 7 OAuth Toolkit

  The OAuth Toolkit makes it simple to implement OAuth in enterprise/mobile integrations, facilitating efficient identity federation and secure access management when using the SecureSpan API Proxy as a Mobile Access Gateway.

Conclusions

The US Federal Government stands to gain considerable benefits from enabling their staff to use mobile devices for mission-critical daily work tasks. With the BYOD movement gaining momentum, many employees are already using their own mobile devices for work. The real pay-off will come as the public sector agencies—including state and local—find ways to build apps that securely and efficiently interface with on-premise systems and data.

Connect with CA Technologies at ca.com

Agility Made Possible: The CA Technologies Advantage

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit **ca.com/customer-success**. For more information about CA Technologies go to **ca.com**.

WHITE PAPER | MONTH 2013

DRAFT

Service Assurance Specific Title Goes Here

Cover subhead. Incia volupta veratur audam qui cum volupti auda nit estium fugit est, quis illaceratiis reptus audipsumenim explica boriame commolo ribusam usciate.

[Author Name]
[Title/Department]