Mobile Device Platform and Application Development for Federal Agencies

Accenture Federal Services
# Table of Contents

1. Mobility Trends and Background ............................................3

2. Mobility Challenges ....................................................................4

3. Implementing the Mobility Vision............................................5
   - Approach to Mobile Application Development ..................5
   - Mobile Device and Platform Selection ............................6
   - HTML5 / Mobile Web Approach.........................................6
   - Mobile Application Security ...............................................7
   - Mobile Application Distribution .................................7
   - Mobile Application Testing Across Platforms .................8
   - Creation of Testing Strategy ...............................................8
   - Integration Testing .................................................................8
   - Security Testing .................................................................8
   - Performance and Network Testing .....................................8

4. Getting Started ...........................................................................8

5. Relevant Accenture Mobility Offerings ............................10
1. Mobility Trends and Background

The rapid evolution of commercial mobile devices has made the technology an essential requirement for government and commercial end users. The growing need to produce new and innovative mobile applications that provide mission-critical or enhanced business capabilities to our government workforce, along with common capabilities like secure email, has led to the enormous challenge of providing standardized solutions. Employees and citizens have grown accustomed to the user experience by using more intuitive consumer-based mobile technology and applications—and expect the same from government.

Mobility provides better and faster decision making through improved access to key data and analytics capabilities anytime, anywhere. It also enables access to workflow tools on the job, reducing manual processes, supporting on-the-go secure operations, services and management.

Many of today’s government field force workers still rely on paper-based or offline systems for completing mission-critical tasks. They manually access information at a service center or field depot. The process is time-consuming and burdensome. With rising citizen expectations, it is more critical than ever for the field force to access near real-time information to not only improve productivity, but also improve citizen satisfaction, become more insight-driven and improve relationships with citizens.

During 2013, the number of mobile-connected devices will surpass the population of the world.¹ Combine this fact with research that indicates that a majority of people want to conduct their entire government business online.² The demand for mobile-enabled digital government services is clear.

The federal government is already responding. The White House’s Digital Government: Building a 21st Century Platform to Better Serve the American People provides the expectation that federal agencies transform themselves, delivering public service digitally. This transformation includes digital mobility for federal employees, placing a premium on the need to balance risk management with cost effectiveness.

Historically, much of the federal government has adopted and used the Research in Motion® (RIM) BlackBerry® infrastructure for its secure mobility needs. For many years, only RIM could deliver devices and infrastructure that could meet stringent federal security requirements and, in general, there were not many smartphone competitors that provided a better solution. Today mobility consumerization has led to an explosion in the popularity of other platforms, Apple® iOS® and Google® Android®, and has created a demand for tablets, as well as smartphones, to be used within government. Generations entering the workforce have grown up with mobility, and are demanding to use the latest mobility platforms in the federal work environment. In some cases, employees want to use their personal devices for work tasks, presenting a problem for federal IT departments that want to protect sensitive government data.

In light of all the digital governance changes occurring, it has become imperative to embrace mobility through an experienced and trusted partner in some form of public-private collaborative partnership for achieving the goals that are unique to the digital audience.

In this paper, we will discuss some of the challenges related to developing and deploying mobile applications and devices in a federal government environment, and then present some of the solution approaches.

². Accenture, Build it and They Will Come? The Accenture Digital Citizen Pulse Survey and the Future of Government Operations, 2012. Accenture surveyed more than 1,400 people in Australia, France, Germany, India, Singapore, the United Kingdom and the United States in an online survey conducted from November 29 to November 30, 2011
2. Mobility Challenges

New opportunities mean greater choices, but they also demand a more deliberate decision-making process regarding the hardware, software, security, data and connectivity that’s needed. It has been said that the simpler a device is for users, the more complexity lurks behind it. That has never been truer. Government agencies need to understand a wide variety of business and technical issues. Mobile device proliferation, multiple technology options and citizen-centric agency needs pose multiple challenges to mobile solutions development and deployment. The figure below depicts some of the major technology, market and operational model challenges.

As there are many application scenarios, there are an equal number of elements that must be considered in mobile application development, including data access, security, offline capabilities and backend integration in a secure manner. Mobile devices’ computing power, interoperability, ability to comingle personal data with agency’s business data, and their always-on and synchronized nature make them attractive points of access for cyber attacks. Interoperability between communication channels, a multitude of OSs and the availability of million mobile apps is providing a common ground for security breaches.

Rolling out a mobility solution within a federal agency for back-office or mission-related application may also require having a Mobile Device management (MDM) and Mobile Application Management infrastructure in place, along with Enterprise Mobile Application Store (MAS) to enforce security and policies in order to protect federal data and devices. There are also trends that pose extra challenges, such as the phenomena of Bring Your Own Device (BYOD), which makes it even more imperative to have the right infrastructure and policies in place before deploying agency-wide production solutions. Enterprise data systems need to be secured on citizen-facing mobile applications, and data needs to be protected in-transit, along with on the mobile device.

Challenges do not end with having the right security, policy and infrastructure in place. Within mobile application development, complexities also include selecting the right application approach, such as native vs. mobile web or hybrid.

With the complexities of devices and OS ecosystem, security and data risk, varied development options, user experience and screen size—comes the complexity of testing the mobile applications. It becomes challenging to not only test the functionality but also the variations due to device form factor, wireless network communication channel, security and performance. For example, HTML5 support by various mobile web browser varies on different platforms, thus requires a specialized test planning approach. Mobile network coverage adds complexity to the performance of applications, thus affecting the test design and architecture approach.

Figure 1. Enterprise mobility challenges

1. Multi platform, fragmented device market
2. Increasing user expectation on User Experience (UX)
3. Application design consideration for cross platform development
4. Middleware becomes outdated with rapidly growing application requirements
5. Disparate application certification procedures
6. Device and platform selection
7. Time-to-market, quality and cost implications are more pronounced
8. Application markets driven by top tier application stores (iPhone, operator application stores etc)
9. Traditional delivery models lack economies of scale
10. Need flexible resourcing

Technology Challenges Market Challenges Operational Model Challenges
The first step toward a mobile solution for government agencies is the creation of a mobile strategy. A mobile strategy needs to lay out the roadmap for what initiatives should be undertaken, how they should be managed and governed, and who would be responsible for what.

3. Implementing the Mobility Vision

The first step toward a mobile solution for government agencies is the creation of a mobile strategy. A mobile strategy needs to lay out the roadmap for what initiatives should be undertaken, how they should be managed and governed, and who would be responsible for what. Accenture recommends that federal agencies set up a Mobile Center of Excellence (MCoE). The MCoE is a group of specialists that helps create, implement, drive adoption of and promote standards for digital opportunities across the business. The MCoE provides advice on opportunity creation, technology standards, vendor selection, device management, mobile security and architecture, device selection, development tools and standards, testing methodology and tools, opportunity adoption and quality management.

Establishing governance for mobile is very important. Governance:

- Is the ability to make, sponsor and enforce the right decisions regarding the realization of digital initiatives.
- Drives decisions for digital investments, operations, sourcing, standards and business/IT interactions.
- Focuses on the realization of value, rather than the management of activity.
- Engages leadership to align agency mission and IT, while focusing cross-organization accountability.

A well-designed governance process will ensure that mobile ideas generated by the business are checked for viability, compliance and security before entering the development phase.

Approach to Mobile Application Development

Traditionally, government agencies have been process-oriented, which meant slower time to market, longer release cycles and inability to respond quickly to changes. Mobility, on the other hand, requires agility, quick release cycles and ability to respond to newer platforms, OS features and security considerations. Some recommendations for mobile application development include:

- Determining what SDLC process is being followed:
  - Traditional Waterfall SDLC often times is considered too rigid or expensive.
  - Agile SDLC provides rapid user feedback and iterative builds.
  - Agile development typically has rapid evolution of the functionality as opposed to the “locking in” on the design up-front that happens in Waterfall.
  - Many government agencies have not shifted to Agile and taking an Agile approach can be time- and cost-prohibitive in these cases.

- Custom building software vs. implementing on a package vs. implementing commercial off-the-shelf (COTS):
  - All three choices are valid, depending on requirements and solution options.
  - Conduct a trade study when appropriate to feed into Governance review process.

- Distributed development and/or testing can also yield significant benefits:
  - Consider an Application Factory model for rapid creation of applications.
  - Consider a Remote Testing Factory model for rapid testing of applications.

Irrespective of the methodology adopted for mobile development, it is important to respond quickly to frequent device platform OS releases, middleware and application updates/releases. Key to the success of the project is rapid iteration during UX Design and Prototyping, as well as iterating on Design, Build and Test.
Mobile Device and Platform Selection

Once the process and methodologies are selected, the next step is how to build the apps. Agencies need to look at the audience and analyze usage cases to determine which architectural approach makes most sense. For example, a native approach can support offline usage and can deliver a more compelling user experience including taking advantage of the rich features of the device. However, native application development can be more expensive and time-consuming if the target is to deploy across multiple platforms and OSs. Figure 2 above depicts an approach for selecting the mobile app delivery channel.

Cross-platform development tools provide a way to implement applications for deployment across multiple device platforms by building once. These are referred to as Mobile Enterprise Application Platforms (MEAP) or Mobile Consumer Application Platform (MCAP). With cross-platform development tools, agencies can support both mobile web and native applications across all or required device platforms, but selecting the right tool requires structured decision framework based on time to market, discoverability and manageability of mobile application and maintenance of code as well as initial device deployment, authentication, remote wipe and more.

The table on the following page lists the drivers for selecting the right development approach and target platform:

<table>
<thead>
<tr>
<th>High-Level Decision Criteria</th>
<th>Mobile Delivery Channel</th>
<th>End User</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Form factor / platform diversity</td>
<td>Mobile Web App</td>
<td></td>
</tr>
<tr>
<td>• Frequency of content changes</td>
<td>Native Mobile Apps</td>
<td></td>
</tr>
<tr>
<td>• Integration with native device features</td>
<td>Thin Client</td>
<td></td>
</tr>
<tr>
<td>• Online versus offline usage and network connectivity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Richness of user experience</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Instantaneous user communication and engagement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• One / multiple sources of data to maintain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security: data in transit / data at rest issues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Software development capabilities / cost</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Below are some of the pros and cons of pursuing a multi-platform package approach.

Pros:
• Facilitates multi-platform development
• Facilitates mobile to back-end integration
• Helps enable re-use across mobile applications

Cons:
• Additional cost compared to native development
• Risk of vendor lock-in
• Changing vendor landscape

There are some features of the physical form factor of devices that also needs to be considered and can be an important driver for platform selection. Criteria can include: battery life, processing power, network connectivity (whether 3G, 4G or Wi-Fi), security features—FIPS certified encrypted storage on device, secure and firewalled containers using hypervisor or Trusted Execution Environment (TEE) for BYOD, etc. If ruggedness is a criterion—how rugged? Does it meet required ruggedness standards for temperatures, shock and liquid? Business factors could include device warranty, replace-ability, vendor agreements and depot services.

HTML5 / Mobile Web Approach:
HTML5 is a path to cross-platform mobile development and represents a new standard for creating applications for multiple channels including desktops, laptops and mobile devices such as smartphones and tablets. There are obvious advantages to HTML5/browser-based applications in terms of total cost of ownership (TCO) and time-to-market (TTM), and an increasing number of compelling arguments, but there are also challenges and limitations to understand.
It is important to note that HTML5 is not an answer to cross-platform portability. Designers must keep in mind and analyze appropriately that HTML5 feature availability varies across various mobile browsers and OS versions. Hence, it requires testing across a wide range of devices across multiple device manufacturers.

Regardless of the specific tools being used, agencies often get a great economic benefit by industrializing their development capability. Consider an Application Factory model for rapid creation of applications.

**Mobile Application Security**

Agencies seeking higher security for mobile applications need to develop a defined process and guidelines for a secure mobile application development lifecycle, as well as enterprise data touch points. Four layers of security need to be considered: network protection, end point protection, application protection and back-end data systems protection. All applications, whether built internally or bought from 3rd party vendors, need to be vetted. Some of the recommendations for verifying app security at different points in the development lifecycle include:

- Enforceable methodology to meet federal requirements and industry best practices. Agencies must evaluate and provide tools to development teams in order to identify vulnerabilities during development. They should also invest in a security training program to keep developers current on the latest security methodologies.
- Whether apps are being built in-house or purchased, they should perform thorough security testing to include static as well as dynamic analysis. For example, it is particularly critical to test when the application performs read/writes to the file system, accesses the network and provides output—or gathers input—from the graphical user interface.

Once applications are developed and tested, agencies should deploy them using a private enterprise app store.

**Mobile Application Distribution**

There are many commercially available Application Management tools which are applicable for provisioning apps and pushing updates in an environment that targets thick and thin desktops as well as mobile devices. App provisioning and updates for mobile devices are made Over-The-Air (OTA). These tools provide personalized self-service portals or container apps that give the user flexibility to browse and install enterprise approved apps. These also provide the IT administrators the tools to configure and deploy applications to end-user devices as well as make policy changes, track performance/usage and respond to security incidents.

<table>
<thead>
<tr>
<th>Criteria / Driver</th>
<th>Mobile Web App (HTML)</th>
<th>Native/Hybrid Mobile App</th>
<th>Thin Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off-line usage</td>
<td>Limited capability with new technologies</td>
<td>Offline capability available</td>
<td>Very limited offline capability, if any</td>
</tr>
<tr>
<td>User experience</td>
<td>Increasing with new technologies</td>
<td>Richest UI</td>
<td>Panning and zooming required; not optimized</td>
</tr>
<tr>
<td>User reach</td>
<td>Accessible via mobile browser</td>
<td>Limited to device specific OS</td>
<td>Can be used on almost all platforms</td>
</tr>
<tr>
<td>Integration with native device features</td>
<td>Increasing with new technologies</td>
<td>Access to native feature and data (accelerometer, camera, GPS, etc.)</td>
<td>Some with APIs, but custom development required. Citrix farther along</td>
</tr>
<tr>
<td>Content/version changes</td>
<td>Users receive most current content and layout</td>
<td>1. Static apps provide static content that is imbedded in current version. 2. Content updated on the fly with web service integration</td>
<td>Users receive most current content</td>
</tr>
<tr>
<td>Sources to maintain</td>
<td>One central source</td>
<td>1. Multiple code repositories (per device OS) 2. One central source if using MCAP (Mobile Consumer Application Platform)</td>
<td>One central source</td>
</tr>
<tr>
<td>Zero footprint on device</td>
<td>Limited info on device</td>
<td>App and data on device</td>
<td>Minimal to none</td>
</tr>
<tr>
<td>Processing speed</td>
<td>Dependent on network connection</td>
<td>Dependent on device processor</td>
<td>Dependent on network connection</td>
</tr>
<tr>
<td>Speed to market/cost</td>
<td></td>
<td>Custom development required; single OS or Cross platform tool</td>
<td>No change to app. Can deploy “as is”</td>
</tr>
</tbody>
</table>

**Applicability**

- Very high
- High
- Medium
- Low
- Very low
Enterprise Application Management tools provide greater governance and control over applications used by employees, license fees and lifecycle management. Many available solutions for Mobile App Management are typically part of Mobile Device Management (MDM), Mobile App Management (MAM) and Mobile Enterprise Application Platform (MEAP), and can be deployed as standalone solutions.

A significant challenge for government agencies is implementing a solution that brings government-grade security to secure devices, applications and data.

Finally, to address large volumes of users and transactions (e.g. when an app goes viral), it is important to ensure that enterprise architecture and infrastructure can effectively scale. In addition, it is important to understand any licensing costs that are driven by numbers of users or transactions ahead of time so as to plan for that cost. Also it is important to consider bandwidth requirements of applications so as to limit costs and ensure good performance. Building user-friendly, self-service features into applications, as well as FAQs and other tools, can also help to keep support costs down and avoid high volumes into agencies’ call centers.

Mobile Application Testing Across Platforms

Before enterprises can reap benefits of implementing their mobility apps to achieve their business and productivity goals, they need to overcome mobility testing challenges within fragmented devices and platforms. The top four challenges are:

Creation of Testing Strategy:
The mobile landscape today embraces a much more diverse range of devices and platforms, reflecting the preferences of both employees and customers. This means that deploying an enterprise application has to cater to a much larger number of smartphone and tablet devices operating on multiple platforms, with different display configurations, network options, power and memory requirements, touchscreens and platform roadmaps. What this demands in practice is to create an agile testing strategy with the ability to rapidly test applications, taking into account different programming languages, debuggers, emulators, integrated development environments, cross-platform development tools, installer packaging options, development and testing and automation tool costs.

Integration Testing:
For enterprise applications to be available on mobile devices, they need to be integrated with the larger systems such as ERP, billing systems, CRM and several other sub systems of the database for access, security, utility services, device management, integrity and authentication. Deployments can fail to deliver if their integration points are not sufficiently tested, or can drive up costs if they are not deployed with a rollout plan that encompasses the complexity and variety of mobile users’ needs.

Security Testing:
Mobility means that large volumes of information and sensitive data now flow across the enterprise and into the outside world. Security on the mobile device therefore has to be aligned with the overall security policies of the enterprise, and enhanced to address additional threats arising from the inherent vulnerability of mobile devices. These threats can be even more pronounced as users interact with mobile applications that co-exist with their personal applications on the device. While using those personal applications can appear innocuous to the user, they can lead to devastating consequences if security is not sufficiently rigorous. Developing and testing enterprise applications therefore must adopt a far more robust and responsible approach to security in comparison to general purpose applications that are available on app stores across the world.

Performance and Network Testing:
Application performance is dependent on various parameters and all of them should be tested for high usability experience. Interaction with enterprise back-end, CPU the performance and power management on the device are some of the critical parameters. Unlike PC apps connected over Ethernet, performance of native mobile and mobile web apps is highly dependent on the wireless network coverage. Mobile applications needs to be tested in exceptional network conditions such as low signal strength, Cellular to Wi-Fi handover, soft/softer handover or 4G to 2G handover etc. Agencies must invest in a network simulation lab infrastructure and setup or utilize managed test services for mobile application testing before deploying enterprise mobile apps which are either mission-critical, back office productivity apps for agency employees or provide citizen self-services.

4. Getting Started

Mobility clearly is transformational and has benefits for government agencies at all levels. Agencies should look for a partner that brings in-depth knowledge in a variety of specialized areas. Such a partner can apply lessons and insights it gathers from working across industries and agencies. These lessons may include developing a governance model, defining and developing methodologies, selecting development and test tools, procedures and policies for application lifecycle management, setting up test labs and other infrastructure, evaluation of third-party components, device and platform selection, skills development for staff and, most importantly, multi-level security.

Since the mobility landscape is continuously changing, conducting a thorough and updated assessment of the mobility environment, along with its user and mission requirements, would help define strategy, identify gaps to determine the right set of solutions, define the governance and operating model, identify solutions which have greater ROI, business benefits of transformation and define an implementation roadmap. Agencies can also consider a more centralized model and establish a Mobile Center of Excellence (MCoE) that implements mobility strategy and can act as a proactive knowledge center, advisor counselor for all mobility activities within an agency or various agencies.
5. Relevant Accenture Mobility Offerings

Since the mobility landscape is continuously changing with evolving technologies, conducting a thorough assessment of an agency’s mobility environment, along with its end user requirements, would help to identify needs for enterprise mobility services. Accenture has supported a number of government agencies and commercial companies with strategy and technology consulting services that included conducting mobility assessment as the first step to identifying the requirements to determine the right set of solutions to meet those requirements. In addition, our services included assessing mobile security, developing policies, establishing a Mobile Center of Excellence (MCoE), defining mobile architectures and roadmaps, establishing a mobility governance structure, end-to-end mobile solutions, including Mobile Device Management (MDM) and Mobile Application Management (MAM) projects. Accenture is also a long-time resource for the federal community, with more than 4,000 dedicated US employees providing unequaled understanding of government needs and systems.

Accenture can meet the needs of federal agencies’ demand to define and deploy an enterprise-wide mobility technical environment for Government to employee (G2E), Government to citizen (G2C), Government to business (G2B) and machine to machine (M2M). Accenture offers a full complement of services and experienced staff to meet agencies’ needs:

Mobile Security: Our mobile security professionals support our clients by providing mobile security assessment, strategy development, integration and analysis of security solutions, vulnerability and penetration testing, security policy development, security testing and pilots, secure mobile application and architecture development, and operational support.

Application Development and Testing: Our Mobile Application Factory combines best-of-breed commercial and custom applications, middleware and platforms for organizations to deploy secure and manageable solutions. We support all mobile operating systems and HTML5. Accenture’s mobility testing automation framework—ROSA (Remote, Offsite, Simulation, Automation) enables testers to develop and execute tests on real devices along with network simulation labs.

Device and Platforms: A range of embedded software services for clients to enable a product or device containing embedded software, such as mobile phones, vehicles, industrial solutions, and household appliances or consumer electronics. This includes helping clients with device profiling to overcome the challenge of selecting the right device to launch applications.

Mobility Managed Services: Accenture offers a number of managed services including Mobile Device Management (MDM) and Mobile Application Management (MAM) as well as vertical solutions, such as mobile wallet, mobile coupons and loyalty, and machine to machine solutions such as vehicle tracking.

Business Integration Services: BI provides large-scale, integrated solutions utilizing the full complement of Accenture Mobility’s offerings such as mobile workforce management and mobile sales force enablement.

Contact
For more information, please contact:
Inderpreet Singh
Inderpreet.singh@accenture.com
+ 1-973-301-1088

Accenture Federal Services, based in Arlington, VA, a wholly owned subsidiary of Accenture LLP, helps US federal agencies build the government of the future. Visit http://www.accenture.com/federal for information regarding Accenture Federal Services, including our perspectives on agency and cabinet challenges and experience delivering results.
About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 275,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$28.6 billion for the fiscal year ended Aug. 31, 2013. Its home page is www.accenture.com.