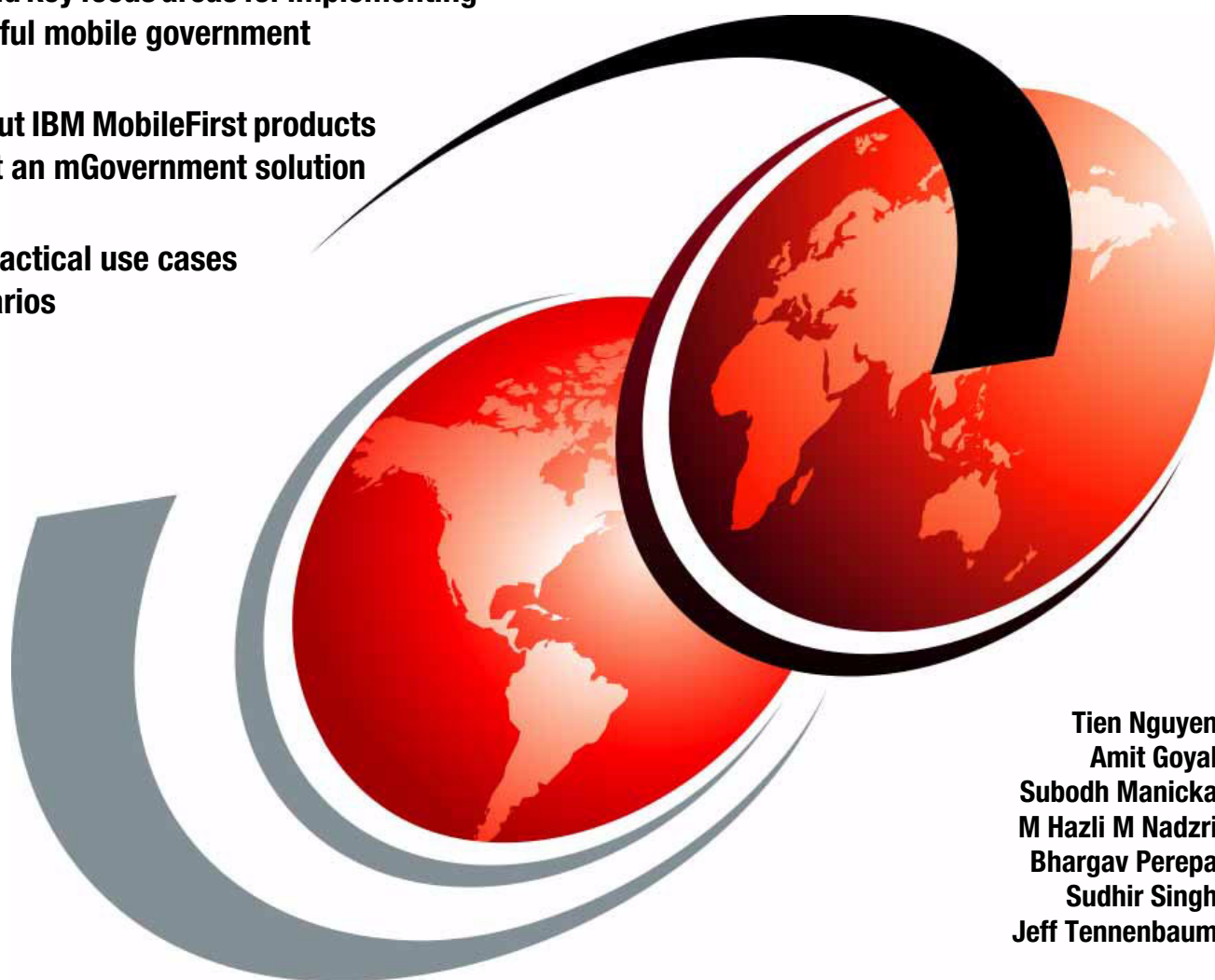


# IBM MobileFirst in Action for mGovernment and Citizen Mobile Services

Understand key focus areas for implementing  
a successful mobile government

Learn about IBM MobileFirst products  
to support an mGovernment solution

Review practical use cases  
and scenarios



Tien Nguyen  
Amit Goyal  
Subodh Manicka  
M Hazli M Nadzri  
Bhargav Perepa  
Sudhir Singh  
Jeff Tennenbaum





International Technical Support Organization

**IBM MobileFirst in Action for  
mGovernment and Citizen Mobile Services**

April 2015

**Note:** Before using this information and the product it supports, read the information in “Notices” on page vii.

**First Edition (April 2015)**

This paper applies to IBM MobileFirst™ enterprise software.

**© Copyright International Business Machines Corporation 2015. All rights reserved.**

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

<b>Notices</b> .....	vii
Trademarks .....	viii
<b>Preface</b> .....	ix
Authors .....	ix
Now you can become a published author, too! .....	xi
Comments welcome .....	xi
Stay connected to IBM Redbooks .....	xii
<b>Chapter 1. Mobile government overview</b> .....	1
1.1 Government, eGovernment, and mGovernment .....	2
1.1.1 eGovernment .....	2
1.1.2 mGovernment .....	3
1.1.3 eGovernment and mGovernment comparisons .....	4
1.2 The mobility landscape in government solutions .....	6
1.2.1 Maturity model in public sector mobile transformation .....	7
1.2.2 Common drivers and focus areas in mGovernment .....	9
1.3 mGovernment interactions .....	10
1.3.1 Government to citizen (G2C) applications .....	11
1.3.2 Government to employee (G2E) applications .....	12
1.3.3 Government to government (G2G) applications .....	12
1.3.4 Government to business (G2B) applications .....	13
<b>Chapter 2. Capabilities for a successful mobile government</b> .....	15
2.1 Provisioning .....	16
2.1.1 The provisioning and deprovisioning process .....	16
2.1.2 Device management provisioning .....	18
2.1.3 User credential provisioning .....	20
2.1.4 Application provisioning .....	21
2.2 Security .....	22
2.2.1 User-level security .....	23
2.2.2 Device-level security .....	23
2.2.3 Data or content-level security .....	25
2.2.4 Application-level security .....	26
2.2.5 Transaction-level security .....	27
2.2.6 Network-level security .....	27
2.3 Governance .....	28
2.3.1 Device governance .....	28
2.3.2 Mobile device management policies .....	29
2.3.3 Application governance .....	29
2.4 Compliance .....	29
2.4.1 Handling personal data and personally identifiable information .....	30
2.4.2 Encrypting data at rest and data in flight .....	30
2.4.3 Enabling accessibility for mobile applications .....	31
2.4.4 Export controls .....	32
2.5 Application disaster management .....	32
2.6 Analytics .....	33
2.6.1 Operational analytics .....	34
2.6.2 Business analytics .....	34

2.7	Application programming interfaces . . . . .	34
2.7.1	APIs and government . . . . .	35
2.7.2	APIs and mobile . . . . .	35
2.8	Mobile application development lifecycle . . . . .	36
2.8.1	Discovery and requirements . . . . .	37
2.8.2	Designing and developing . . . . .	37
2.8.3	Integration . . . . .	38
2.8.4	Instrumenting . . . . .	39
2.8.5	Testing and vetting . . . . .	39
2.8.6	Deployment and management . . . . .	39
2.8.7	Analytics . . . . .	39
2.9	Mobile user experience . . . . .	40
<b>Chapter 3. IBM MobileFirst . . . . .</b>		<b>41</b>
3.1	IBM MobileFirst overview . . . . .	42
3.1.1	Understanding the need for mobile technology for citizens . . . . .	42
3.1.2	IBM MobileFirst introduction . . . . .	42
3.2	IBM MobileFirst portfolio . . . . .	43
3.2.1	IBM MobileFirst Platform . . . . .	44
3.2.2	IBM MobileFirst Protect . . . . .	47
3.2.3	IBM Experience One . . . . .	49
3.3	IBM MobileFirst reference architecture . . . . .	50
3.3.1	Functional model . . . . .	50
3.3.2	Operational model . . . . .	52
3.4	IBM MobileFirst enterprise app lifecycle . . . . .	54
<b>Chapter 4. Reference architecture for the mGovernment solution implementation . . . . .</b>		<b>57</b>
4.1	Key challenges for mGovernment . . . . .	58
4.2	Reference architecture for mGovernment . . . . .	59
4.2.1	Notional view . . . . .	59
4.2.2	Functional view . . . . .	61
4.2.3	Operational view . . . . .	62
4.2.4	IBM technology view . . . . .	63
4.3	Applying the reference architecture to mobile solutions . . . . .	65
4.3.1	Use case 1: Car registration renewal . . . . .	65
4.3.2	Use case 2: Farming application . . . . .	70
4.3.3	Use case 3: First responder . . . . .	74
<b>Chapter 5. Points of view in mGovernment . . . . .</b>		<b>79</b>
5.1	Striving for commonality and uniformity . . . . .	80
5.2	Standards, standards, and standards . . . . .	80
5.3	Balancing cost, function, and security . . . . .	80
5.4	Data protection . . . . .	81
5.5	Lifecycle and governance . . . . .	82
5.6	Third-party application management and control . . . . .	82
5.7	Risk management . . . . .	83
5.8	Assessing the value of the develop-once-deploy-many approach in application development . . . . .	84
<b>Chapter 6. mGovernment trends and directions . . . . .</b>		<b>87</b>
<b>Appendix A. Examples of mGovernment applications . . . . .</b>		<b>89</b>
	mHealth: Blood bank . . . . .	90
	mWrapper: The Mobile portal - Kingdom of Bahrain . . . . .	90

mEducation: M4girls . . . . .	90
mEmergency: SMS broadcasting system . . . . .	91
mEmergency: Emergency service . . . . .	91
mPayment: NFC mobile payment . . . . .	91
mPolicing: Mobile field inspection system . . . . .	92
mTransportation: MOBESE . . . . .	92
mAdministration: Florida Keys mosquito control . . . . .	92
mBusiness: Agroportal . . . . .	93
mBusiness: Uganda Google Trader . . . . .	93
mBusiness: Gateway Sweden . . . . .	93
mBanking: Mobile Money 2.0 . . . . .	94
Crowdsourcing: uRep . . . . .	94
Crowdsourcing: MyGov . . . . .	94
Context aware: Mobile emergency alert service . . . . .	95
<b>Related publications . . . . .</b>	<b>97</b>
IBM Redbooks . . . . .	97
Other publications . . . . .	97
Online resources . . . . .	98
Help from IBM . . . . .	99





# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.


## COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

# Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AppScan®	IBM MobileFirst™	Redpaper™
Bluemix™	IBM UrbanCode™	Redbooks (logo)  ®
Cast Iron®	Informix®	Tealeaf®
CICS®	Insights™	Tivoli®
Cloudant®	Lotus®	Trusteer®
DataPower®	PureApplication®	WebSphere®
Domino®	QRadar®	Worklight®
IBM®	Rational®	
IBM ExperienceOne™	Redbooks®	

The following terms are trademarks of other companies:

Fiberlink, MaaS360, Secure Productivity Suite, and We do IT in the Cloud. device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company.

Evolution, and Inc. device are trademarks or registered trademarks of Kenexa, an IBM Company.

Xtify is a trademark or registered trademark of Xtify, an IBM Company.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.

# Preface

Mobile technology is changing the way government interacts with the public anytime and anywhere. mGovernment is the evolution of eGovernment. Like the evolution of web applications, mobile applications require a process transformation, and not by simply creating wrappers to mobile-enable existing web applications.

This IBM® Redpaper™ publication explains what the key focus areas are for implementing a successful mobile government, how to address these focus areas with capabilities from IBM MobileFirst™ enterprise software, and what guidance and preferred practices to offer the IT practitioner in the public sector.

This paper explains the key focus areas specific to governments and public sector clients worldwide in terms of enterprise mobility and describes the typical reference architecture for the adoption and implementation of mobile government solutions. This paper provides practical examples through typical use cases and usage scenarios for using the capabilities of the IBM MobileFirst products in the overall solution and provides guidance, preferred practices, and lessons learned to IT consultants and architects working in public sector engagements.

The intended audience of this paper includes the following individuals:

- ▶ Client decision makers and solution architects leading mobile enterprise adoption projects in the public sector
- ▶ A wide range of IBM services and sales professionals who are involved in selling IBM software and designing public sector client solutions that include the IBM MobileFirst product suite
- ▶ Solution architects, consultants, and IBM Business Partners responsible for designing and deploying solutions that include the integration of the IBM MobileFirst product suite

## Authors

This paper was produced by a team of specialists from around the world.



**Tien Nguyen** is an IBM Distinguished Engineer working in the IBM Software Services Federal (ISSF) division. He has 25 years of software engineering experience, designing innovative, multi-product client solutions and leading the implementation of these solutions for industry verticals, such as telecom, media/entertainment, and federal government. Tien spent the last 11 years in IT architecture and solution implementation for the Federal sector. Tien also received the Open Group's Distinguished Chief/Lead IT Architect Certification.



**Amit Goyal** is an IT Specialist in the IBM India Software Lab working on the IBM Software Services for WebSphere® team. He has nine years of experience in designing and implementing enterprise mobility, business integration, service-oriented architecture (SOA), business process management (BPM), and Java Platform, Enterprise Edition solutions for industry verticals, such as telecom, media, and entertainment. He holds a Master of Technology degree from IIT, Roorkee, with specialization in communication systems. His areas of expertise include IBM MobileFirst, WebSphere Application Server, WebSphere Process Server, and WebSphere Enterprise Service Bus. He is a subject matter expert on enterprise mobility and middleware integration.



**Subodh Manicka** is an Executive IT Architect in IBM Software Services, Federal Division. During his 25-year professional career, he developed multiple IBM software products, including Enterprise Content Management and security products. For the past 10 years, he focused on creating architecture and leading teams to deliver enterprise solutions using IBM technology to US Federal clients.



**M Hazli M Nadzri** is an Open Group Master Certified IT Architect working for IBM Malaysia. He has over 15 years experience in the industry with solution architecture, pre-sales, and leading implementation designs across various industries, such as government, telecom, and insurance services. Currently, Hazli focuses most of his time helping to design IBM architected solutions to modernize the public services of the Malaysian government.



**Bhargav Perepa** has been with IBM for 21 years. He is an IBM IT Specialist/Architect, working with various US Federal Civilian and Department of Defense government agencies in the IBM Federal Software Group in the Washington, DC, area. He received his M.S. in Computer Science from Illinois Institute of Technology, Chicago IL, and an MBA from University of Texas at Austin, TX. His current interests are in cloud, analytics, mobile, social, security, and Watson technologies. Bhargav received numerous awards and types of recognition during his long IBM career. Most recently, he was awarded an IBM Outstanding Technical Achievement Award for his contributions to mobile computing security.



**Sudhir Singh** is an IBM Software Engineer in IBM India working in IBM Software Lab Services. He has four years of experience in mobile application development for different platforms, such as iOS, Android, and Blackberry. He was responsible for the development and design of enterprise applications in the oil, healthcare, government, and telecom industries. Currently, Sudhir is working on mobile development and integration with IBM MobileFirst products.



**Jeff Tennenbaum** is an IT Architect focused on mobile applications with over 25 years experience at IBM. He started his career as a Support Engineer working on IBM CICS®. He later became an IT Specialist working on products under the WebSphere brand, including WebSphere Application Server and WebSphere Portal Server. He currently spends most of his time supporting Federal mobile opportunities.

Thanks to the following people for their contributions to this project:

Debbie Landon  
Ann Lund  
International Technical Support Organization, Rochester Center

## Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)

## Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

[ibm.com/redbooks](http://ibm.com/redbooks)

- ▶ Send your comments in an email to:

[redbooks@us.ibm.com](mailto:redbooks@us.ibm.com)

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization  
Dept. HYTD Mail Station P099  
2455 South Road  
Poughkeepsie, NY 12601-5400

## Stay connected to IBM Redbooks

- ▶ Find us on Facebook:  
<http://www.facebook.com/IBMRedbooks>
- ▶ Follow us on Twitter:  
<http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:  
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:  
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:  
<http://www.redbooks.ibm.com/rss.html>



# Mobile government overview

The label of e-<everything> was part of the transformation wave that came with the advent of the web. Thin client-based applications were popping up everywhere in the early 2000s. *eGovernment* provides services to citizens through digital channels in addition to or in lieu of its paper-based services that are delivered at its “brick and mortar” locations.

Mobile government or *mGovernment* is the extension of eGovernment with the same evolution path and includes the following transformations:

- ▶ From simple mobile presence to interactive to transactional to user-centric
- ▶ From citizen-facing mobile applications to intranet-based mobile workforce applications to government-to-government collaboration applications
- ▶ From direct access into back-end data to business process participation to API ecosystems

mGovernment is not simply about creating mobile wrappers around existing web applications to mobile-enable them on mobile devices; mGovernment is more of an enterprise transformation.

Although several mGovernment use cases overlap with use cases in the commercial world (for example, invoicing, procurement, claims, healthcare, and education), important differentiations drive a unique transformation path toward a successful mGovernment.

This chapter provides an overview of a mobile government and introduces the concepts of mGovernment and mobile technology in government and public sector solutions.

The following topics are covered in this chapter:

- ▶ 1.1, “Government, eGovernment, and mGovernment” on page 2
- ▶ 1.2, “The mobility landscape in government solutions” on page 6
- ▶ 1.3, “mGovernment interactions” on page 10

## 1.1 Government, eGovernment, and mGovernment

A generally understood primary role of a capitalistic, free-market-driven government is to protect its people from internal conflicts or outside interference, provide law and order for people's daily lives, provide for the economic well-being of its society or country, and to administer social programs for the people's benefit. A government typically consists of various agencies with each agency responsible for a certain focus area and with a specific mission.

Government agencies form the public sector in overall economic activity and employ people and other assets to deliver their core missions. Public sector agencies are typically mission driven and not profit seeking. Private sector businesses however are profit-seeking entities, employing people and other assets to generate productive economic activity to maximize profit and generate wealth. Non-government organizations that are not profit seeking or government affiliated are volunteer, not-for-profit entities, employing people and other assets.

A traditional government consists of the following interactions that take place using traditional "brick and mortar" infrastructure elements for delivery of citizen services, active citizen engagements, and for achieving internal effectiveness and efficiencies:

- ▶ Interactions between various inter-government agencies, such as local, city, county, state, or country
- ▶ Interactions between intra-government agencies, for example, between countries and other organizations, such as the International Monetary Fund (IMF), United Nations (UN), and International Criminal Police Organization (INTERPOL)
- ▶ Interaction between government agencies and its citizens
- ▶ Interaction between government agencies and its businesses, and non-government organizations

### 1.1.1 eGovernment

If a government chooses to use digital electronics and communication technologies to achieve its goals and mission, in addition to its "brick and mortar" infrastructure elements, this kind of organization is called an electronic government or *eGovernment*, which complements the traditional government.

eGovernment refers to public sector organizations that adopt new information and communication technologies in an innovative manner to deliver citizen services, engage citizens, and gain internal efficiencies. eGovernment typically uses wired Internet connectivity to deliver services.

eGovernment service offerings are often categorized based on the constituents that are served:

- ▶ Government to citizen (G2C)
- ▶ Government to employee (G2E)
- ▶ Government to business (G2B)
- ▶ Government to government (G2G)

For more information about these categories, see 1.3, "mGovernment interactions" on page 10.



The following types of services are provided by eGovernment agencies:

- ▶ Informational services refer to the dissemination of governmental information through web portals, including online publishing, multi-casting, and broadcasting.
- ▶ Transactional services refer to two-way interactions between government agencies and citizens, businesses, and non-governmental organizations.
- ▶ Operational services refer to services that are geared to achieve internal governmental effectiveness and efficiencies and improved cooperation and collaboration between inter-government agency operations at various operating levels.

Recipients of services invariably use wired connectivity or stationary Wi-Fi connectivity to consume provider services to realize eGovernment transformations. Successful adoption and implementation of eGovernment services require building the provider's side (government) technological infrastructure to provide services and widespread availability of wired connectivity or Wi-Fi connectivity options to consume the eGovernment services by users or consumers of services.

## 1.1.2 mGovernment

If a government chooses to use mobile communication technologies that feature stationary wireless and mobile cellular as part of its digital electronics and communication technologies to achieve its goals and mission, in addition to "brick and mortar" and eGovernment infrastructure elements, this kind of organization is called a mobile government or *mGovernment*, which complements eGovernment and the traditional government.

mGovernment refers to the usage of mobile information and communication technologies with wireless networks by public-sector government agencies to deliver citizen services, engage citizens, and gain internal efficiencies. The mobile devices that are employed by service consumers to engage with the service providers include mobile phones, tablets, notebooks, personal digital assistants (PDAs), and variety of devices that are known as the Internet of Things (IoT).

mGovernment service offerings act as an extension to eGovernment service offerings to connect and reach out to consumers of services by using mobile and wireless information and communication technology means.

The underlying key characteristics of mGovernment services include the following attributes:

- ▶ Services delivery without physical connectivity
- ▶ Portability for consumers to receive services in a location-independent or portable manner
- ▶ Usage of mobile devices for identifying consumer preferences to provide for personalized or customized services because mobile devices are used almost always and almost all of the time by consumers
- ▶ Bidirectional information and interaction between service providers and consumers
- ▶ Service providers that use mobile device capabilities to deliver context-aware services to service consumers, based on the numerous sensors that are present in mobile devices

mGovernment can offer advantages over what eGovernment can offer in the following ways:

- ▶ Provides information and services to citizens on an anywhere and anytime basis
- ▶ Helps overcome the digital divide with the challenges of a lack of wired infrastructure connectivity issues to provide information and services to citizens
- ▶ Provides citizen services in a more cost-effective way

- ▶ Promotes transparency in government
- ▶ Helps to increase the efficiency and effectiveness of government employees
- ▶ Provides another channel for citizens to engage with the government

A significant feature of mobile technologies is that it is always on, always connected, and context aware, with highly portable, connectivity devices to deliver services and capabilities. Typically, eGovernment and mGovernment modes complement “brick and mortar” government infrastructure elements based on the delivery of the same governmental goals and missions.

**Note:** Certain geographies have no eGovernment channel presently and only have an mGovernment channel that complements the government channel as another channel for citizens to engage with the government. This pattern of adoption is due to technology leaping ahead in that geography.

### 1.1.3 eGovernment and mGovernment comparisons

Both mGovernment and eGovernment applications afford certain challenges and risks, some of which are specific to mGovernment applications.

Figure 1-1 depicts the roles of government, eGovernment, and mGovernment and how they interact (note that NGO indicates non-governmental organizations).

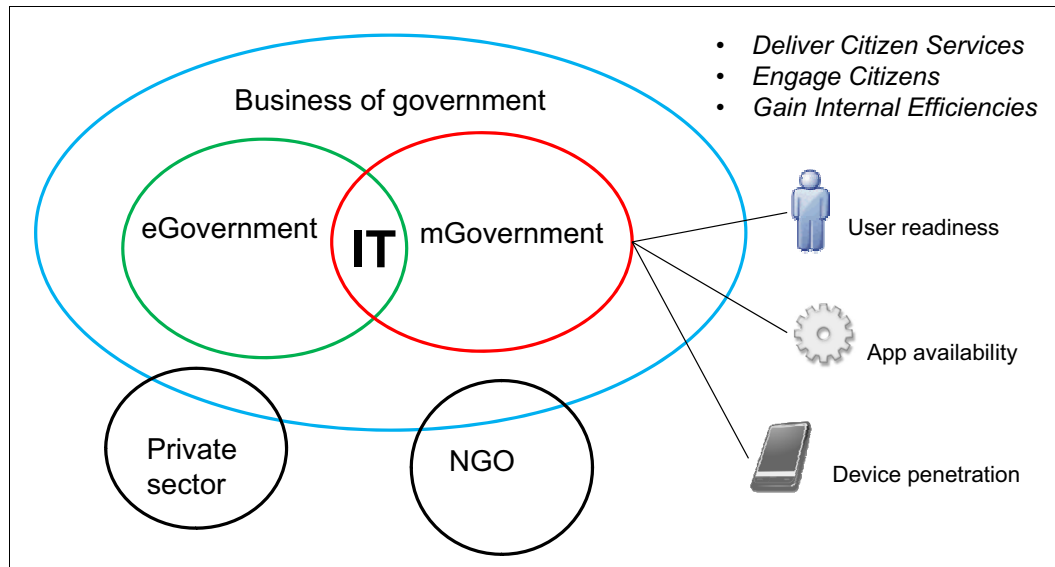


Figure 1-1 Roles of government, eGovernment, and mGovernment

Table 1-1 lists several differences between an eGovernment and mGovernment environment.

Table 1-1 Differences between eGovernment and mGovernment environments

Factor	eGovernment	mGovernment
Networking technology	Wired or wireless stationary.	Wireless or radio (cellular) mobile.
Screen sizes	Typically larger.	Typically smaller.
Input/output	Keyboard and mouse.	Various, including keyboard, mouse, voice, scanner, camera, and so on.
Resources, including processor, RAM, and storage	Rich and high.	Insufficient resources.
Connectivity	High speed and reliable.	Low speed, latency, and unreliable.
Protocols	<ul style="list-style-type: none"> <li>▶ Many and various (Remote Method Invocation (RMI), Common Object Request Broker Architecture (CORBA), SOAP WS, Representational State Transfer (RESTful), and so on).</li> <li>▶ Stateful and stateless.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Lightweight, Internet friendly (HTTP, JavaScript (JS), RESTful, JavaScript Object Notation (JSON)).</li> <li>▶ Stateless.</li> </ul>
Data optimization	Optimized for desktops and notebooks.	Optimized for mobile devices.
Interaction pattern	<ul style="list-style-type: none"> <li>▶ Fewer bigger, monolithic applications that are integrated on the back end with data and processing that are collocated on the server side. Scale up for data and user population needs.</li> <li>▶ Coarse-grained traffic.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Lots of fit-for-purpose, attractive, appealing mobile applications. Data and user population needs to scale out, web, or Internet scale.</li> <li>▶ Fine-grained and bursty traffic.</li> </ul>
Data and processing logic	Primarily server side.	Client and server sides.
Data and query pattern	<ul style="list-style-type: none"> <li>▶ Location independent.</li> <li>▶ Server side.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Location dependent and independent.</li> <li>▶ Client and server sides.</li> </ul>
Data and data structure	<ul style="list-style-type: none"> <li>▶ Atomicity, Consistency, Isolation, Durability (ACID) Semantics.</li> <li>▶ Consistency focused.</li> <li>▶ Schema on Write.</li> <li>▶ Relational database management system (RDBMS).</li> <li>▶ Data integration on the server side.</li> <li>▶ Need to know basis and siloed.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Basically Available, Soft state, Eventual consistency (BASE) Semantics.</li> <li>▶ Availability focused.</li> <li>▶ Schema on Read or Eventual Schema.</li> <li>▶ NoSQL, sparse tabular, graph, and document databases.</li> <li>▶ Data integration on client and server sides.</li> <li>▶ Siloed on client side and integrated on server side.</li> </ul>
Context - Sensory/Geospatial/Temporal	Non-aware.	Aware.
Usage patterns	<ul style="list-style-type: none"> <li>▶ Mostly textual.</li> <li>▶ Online.</li> <li>▶ Always synchronized.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Rich (Textual, voice, video, Short Message Service (SMS), Multimedia Messaging Service (MMS), and so on).</li> <li>▶ Online and offline.</li> <li>▶ Needs synchronization.</li> </ul>

Factor	eGovernment	mGovernment
Battery, data, and voice charges	Non-factor.	Factor.
Transactionality	ACID.	ACID and BASE.
Data usage pattern	Need to know and in silos.	Reuse, repurpose, and govern.

## 1.2 The mobility landscape in government solutions

The mobility landscape in government solutions is non-uniform and varies greatly based on geographies and countries due to digital divide and ecosystem environments. Within a country, access to mobile services by consumers (especially citizens) varies by demographic, economic, and social inequalities.

mGovernment services, applications, and solutions have a range of capabilities that can be categorized in the following manner:

▶ **Emerging**

Online presence that uses static content with information flowing from government to consumers or stakeholders. Consumers or stakeholder participation involves consuming the disseminated information with little or no interaction.

▶ **Enhanced**

Dissemination of more public policy and governance information in the form of archived documents, forms, and reports by using a web API approach.

▶ **Interactive**

With a purpose to provide ease of use and consuming stakeholder convenience, interactive services offer interactive and online services that are multimedia rich and integrated with social networks. These applications provide information and alerts on a mobile channel.

▶ **Transactional**

Transformational in nature, transactional services feature 24x7 and bidirectional flow of information between government and consuming stakeholders. Mobile applications feature payments, registrations, documents, service requests that use the web, SMS, interactive voice response (IVR), IVVR (video), and smartphone devices in an innovative manner.

▶ **Connected**

Connected services are the most integrated, connected, and sophisticated, enabling citizen participation and engagement in the government decision-making process. These services are high quality in nature and are responsive to citizens' needs in emergencies, natural disasters, and other mobilizing events (for example, elections).

The following examples show G2C services of mGovernment in the United States:

- ▶ Tracking election returns
- ▶ Mobile traffic map
- ▶ Emergency notification
- ▶ Parking violation reminder
- ▶ Lobbyist-in-a-Box
- ▶ Wireless notification
- ▶ Wireless state portal

The following examples show the internal efficiency and effectiveness of mGovernment in the United States:

- ▶ Field inspection
- ▶ Internal communication
- ▶ Police applications
- ▶ Enhanced 911
- ▶ Vehicle tracking
- ▶ Tax collection solution
- ▶ Inventory tracking

Rapidly emerging services are categorized as M2M (machine to machine). The following examples show M2M services in mGovernment in the United States:

- ▶ Smart power grids
- ▶ Physical security systems
- ▶ Vending machines or kiosks (for example, the United States Postal Service)
- ▶ Mobile payments for government services (for example, taxes or parking)

### **1.2.1 Maturity model in public sector mobile transformation**

The view of a mobility maturity model describes the stages of mGovernment implementation in a particular administration or country. It depicts an mGovernment evolution from informational to transactional for citizen services and mobile workforce. An mGovernment implementation can be in one the stages that are shown in Figure 1-2 on page 8 or in transition between these stages.

The following considerations are key in developing the maturity model:

- ▶ Establishment of eGovernment
- ▶ Infrastructure availability
- ▶ Device penetration, for example, feature phones or smartphones
- ▶ Mobile application availability
- ▶ Workforce, citizen, or public readiness

Figure 1-2 on page 8 shows the mGovernment maturity model stages.

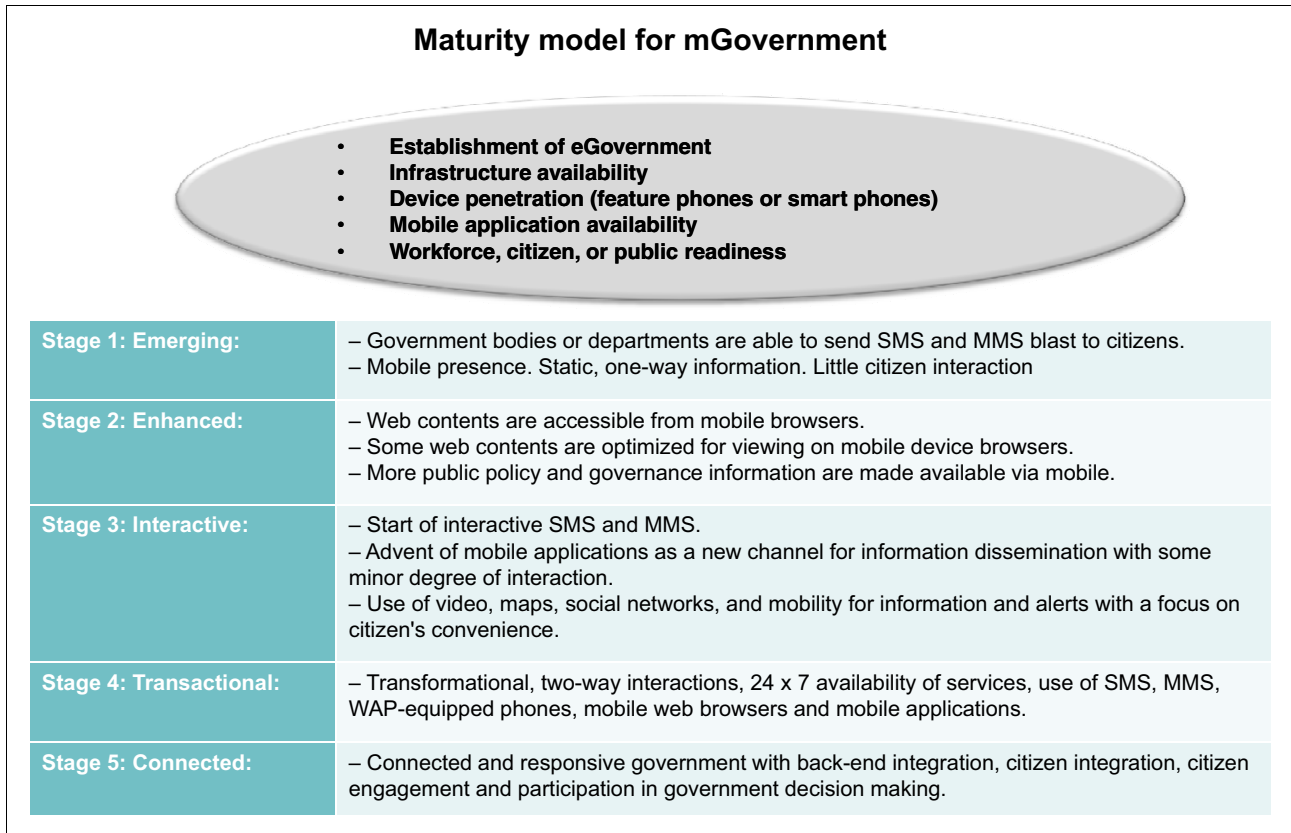


Figure 1-2 mGovernment maturity model

As shown in Figure 1-2 and introduced in 1.2, “The mobility landscape in government solutions” on page 6, you can categorize the mGovernment maturity model into the following stages:

- ▶ **Stage 1: Emerging:**
  - Government bodies or departments are able to send SMS and MMS blasts to citizens.
  - Mobile presence. Static, one-way information. Little citizen interaction.
- ▶ **Stage 2: Enhanced:**
  - Web contents are accessible from mobile browsers.
  - Some web contents are optimized for viewing on mobile device browsers.
  - More public policy and governance information are made available through mobile.
- ▶ **Stage 3: Interactive:**
  - Start of interactive SMS and MMS.
  - Advent of mobile applications as a new channel for information dissemination with some minor degree of interaction.
  - Use of video, maps, social networks, and mobility for information and alerts with a focus on the citizens’ convenience.

- ▶ Stage 4: Transactional:
  - Transformational, two-way interactions.
  - 24x7 availability of services.
  - Use of SMS, MMS, and Wireless Application Protocol (WAP)-equipped phones, mobile web browsers, and mobile applications.
- ▶ Stage 5: Connected:
  - Connected and responsive government with back-end integration.
  - Citizen integration, engagement, and participation in government decision making.

## 1.2.2 Common drivers and focus areas in mGovernment

The widespread adoption of mobile devices and mobile technologies in all sectors of developed economies, including the government sector, by stakeholders (public sector employees, citizens, and partners) and the emergence of an ecosystem are significant factors for mGovernment inception. The other contributing reasons for emergence of mGovernment are convenience, interoperability, potentially enhanced citizen to government engagement, and the cost-effectiveness of services delivery when compared with eGovernment.

The following drivers are common for ushering in mGovernment services:

- ▶ Enhanced service availability and access
 

mGovernment services act as another channel to engage stakeholders while also delivering services across an always on and anywhere accessible 24x7 quality of service (QoS) delivery channel characteristic. Additionally, mobile channels act as a complement to eGovernment channels in reaching out to those stakeholders who are geographically dispersed or who are disadvantaged otherwise. For consuming stakeholders, mGovernment services turn out to be more convenient.
- ▶ Enhanced service responsiveness
 

For certain services that feature automation, the mGovernment channel offers an enhanced capability to deliver improved responsiveness to consuming stakeholders compared to services delivered by telephone or in-person office visits.
- ▶ Enhanced service quality and efficiencies
 

Services that are delivered to stakeholders that are disadvantaged by demographic, economic, and social inequalities by using the mGovernment channel contribute to improved quality outcomes for government missions and an increased realization of efficiencies.
- ▶ Enhanced services scalability
 

Cost-effectiveness in the delivery of services through an mGovernment channel help realize effectiveness, efficiencies, and services scalability. Similar to eGovernment services, mGovernment services afford even more flexibility and reduced costs to the government in terms of capital and operational expenditures that are incurred in delivering services.
- ▶ Enhanced stakeholder engagement and experience
 

mGovernment channel services, by being able to better bridge demographic, economic, and social inequalities, contribute to improved stakeholder engagement and experience.

## 1.3 mGovernment interactions

Figure 1-3 illustrates the four common types of mobile government interactions.

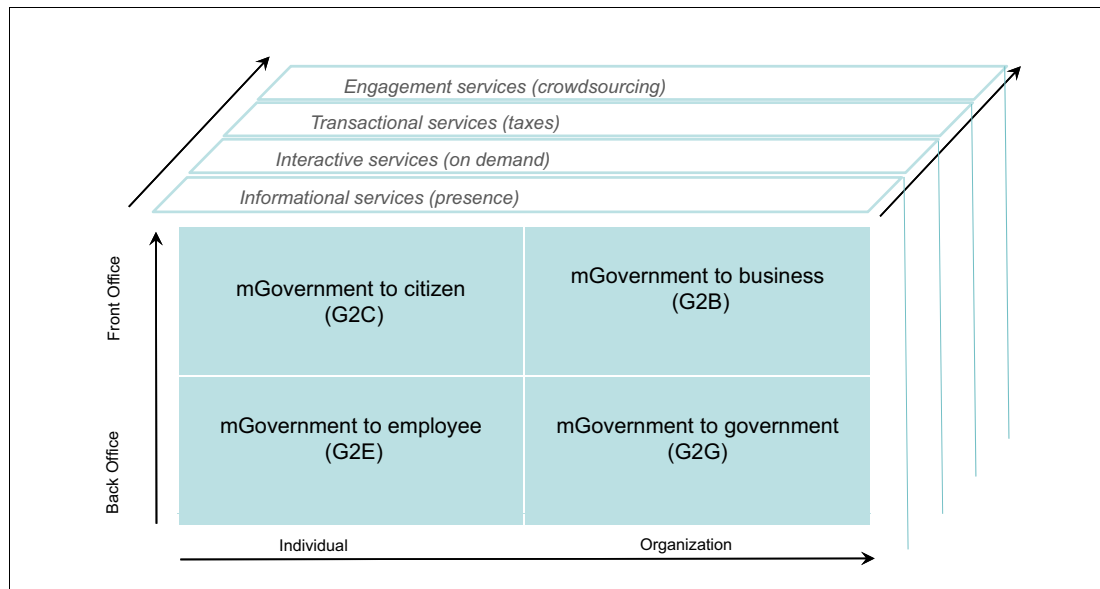


Figure 1-3 Common types of mobile government interactions

Another categorization of mGovernment interactions is by service types that correspond with the technology used, who initiates communication, and the direction of information flow:

- ▶ Informational services (Push services)

Informational services involves information dissemination. This government service mainly consists of pushing information. Much of the information is static and limited interaction exists among the entities.

- ▶ Interactive services (on demand)

Through interactive mobile services, entities can engage in interaction with the government and send inquiries, comments, or service requests to specific agencies. Entities can access forms, applications, and databases. In this type of service, the interaction becomes more personalized, detailed, and targeted to specific entity interests and service needs, and specific agency divisions and service areas. The communication is one-to-one.

- ▶ Transactional services

With transactional mobile services, government and entities get into two-way communication. Entities can complete their transactions with the government electronically and at their convenience. This service type includes self-service options for paying taxes, making payments, filing tax returns, and applying for services and grants. Transactional services demand robust back-end systems that can be called by using a business process. For example, integrating mobile with back-end enterprise systems with a Business Process Management (BPM) Suite enables fast and easy execution process modifications and workflow reorientation.

- ▶ Engagement services (crowdsourcing)

Mobile channels and social media provide increased opportunities to collaborate with stakeholders in real time and provide them with up-to-date government information regardless of their location.



The rest of this section provides application examples for each of the following types of mobile government interactions:

- ▶ 1.3.1, “Government to citizen (G2C) applications” on page 11
- ▶ 1.3.2, “Government to employee (G2E) applications” on page 12
- ▶ 1.3.3, “Government to government (G2G) applications” on page 12
- ▶ 1.3.4, “Government to business (G2B) applications” on page 13

See Appendix A, “Examples of mGovernment applications” on page 89 for examples of actual mobile government applications that are being implemented today and the types of mobile government interactions that are involved in these various examples.

### 1.3.1 Government to citizen (G2C) applications

As shown in Figure 1-3 on page 10, government to citizen (G2C) applications are front-office applications that refer to the interaction between the government and the citizens.

G2C applications can include the following types of services:

- ▶ Unidirectional communication from the government to the citizens (Information services):
  - General information for citizens (for example, weather, tourism, recreation, health, public safety, contact information, services, and regulations)
  - Emergency alerts (for example, severe weather, terrorism, fires, accidents, and health risks)
  - Notifications (for example, library book deadlines, security notifications, social media posts, and Really Simple Syndication (RSS) feeds for news and updates)
  - Health and safety education (for example, prevention and preparedness)
- ▶ Unidirectional communication from citizens to government (Interactive services):
  - Health services (for example, screening and tests, monitoring, and health forms)
  - Education services (for example, grades, admissions, and exam results)
  - Information inquiry services (for example, account information, traffic and transportation availability, service request status, and schedules (airline flights and field crew locations))
  - Filing claims and reporting problems (for example, service interruptions, suspicious activity, and complaints about government officials)
- ▶ Bidirectional communication between the government and citizens (Transactional and Engagement services):
  - Seeking employment (for example, job postings, applications, matching services, and interviews)
  - Government transfer programs (for example, food coupons, unemployment compensation, basic income grants, and social benefits, such as Medicaid)
  - Transportation services (for example, buying train tickets, parking, bus tickets, and airline flights)
  - Signing a transaction with a mobile signature
  - Citizen engagement to strengthen a citizen-centered approach to government and to involve citizens in policy development and decision making

### 1.3.2 Government to employee (G2E) applications

As shown in Figure 1-3 on page 10, government to employee (G2E) applications are back-office applications that refer to the interaction between the government and its employees.

G2E applications can include the following types of services:

- ▶ Unidirectional communication from the government to the employee (Information services):
  - General information for employees (for example, policies, training, regulations, contact details, and meeting schedules)
  - Notifications (for example, timesheet submission deadlines, security notifications, and updates)
- ▶ Unidirectional communication from employees to the government (Interactive services):
  - Information inquiry services (for example, employee search and transport availability)
  - Filing claims (for example, expense reimbursement and timesheets)
- ▶ Bidirectional communication between the government and employees (Transactional and Engagement services):
  - Remote workforce management
  - Capture and transfer of data

### 1.3.3 Government to government (G2G) applications

As shown in Figure 1-3 on page 10, government to government (G2G) applications are back-office applications that refer to the interaction between government agencies.

G2G applications can be among government agencies or between central and local government agencies.

G2G applications can include the following types of services:

- ▶ Unidirectional communication from government to government (Interactive services):
  - Access to knowledge bases and records (for example, public safety, health, and education)
- ▶ Bidirectional communication between governments (Transactional and Engagement services):
  - Coordination of government activities for inspections, controls, and supervisions
  - Security services (for example, law enforcement and citizen security)
  - Emergency management
  - Transmission of discussion agendas to legislators

### 1.3.4 Government to business (G2B) applications

As shown in Figure 1-3 on page 10, government to business (G2B) applications are front-office applications that refer to the interaction between the government and businesses.

G2B applications can include the following types of services:

- ▶ Unidirectional communication from governments to businesses (Information services):
  - General information for business (for example, policies and regulations)
  - Notifications (for example, sales tax payment deadlines, and adherence to new policy deadlines)
- ▶ Unidirectional communication from businesses to government (Interactive services):
  - Information inquiry services (for example, procurement and taxation)
  - Filing forms for licensing
- ▶ Bidirectional communication between the government and businesses (Transactional services):
  - Mobile payments (for example, sales tax and mobile wallet)





## Capabilities for a successful mobile government

This chapter describes the various capabilities that are required for a success mobile government.

The following topics are covered in this chapter:

- ▶ 2.1, “Provisioning” on page 16
- ▶ 2.2, “Security” on page 22
- ▶ 2.3, “Governance” on page 28
- ▶ 2.4, “Compliance” on page 29
- ▶ 2.5, “Application disaster management” on page 32
- ▶ 2.6, “Analytics” on page 33
- ▶ 2.7, “Application programming interfaces” on page 34
- ▶ 2.8, “Mobile application development lifecycle” on page 36
- ▶ 2.9, “Mobile user experience” on page 40

## 2.1 Provisioning

*Provisioning* in a government enterprise is the process of getting a device ready for the user to use in a prescribed way.

The nature of the mobile use case and the sensitivity of the data that is accessed by using it can dictate how provisioning is done. At one end of the spectrum is the device that is provided by the government with specific applications and used to access sensitive national security systems. At the other end of the spectrum, citizens use their own devices to access public information, which can host both government-specific applications and other applications that are installed for personal use. Depending on the nature of the user, authentication to provision the device can range from using public key infrastructure (PKI) credentials, to a device with basic credentials, to no credentials at all.

### 2.1.1 The provisioning and deprovisioning process

For many mGovernment use cases, government organizations need to define a strategy and processes for provisioning. Along with provisioning the devices, organizations need to track and manage those devices. Processes need to be put in place to perform device accreditation and acquisition. Organizations might maintain a list of approved devices and the approved operating systems that these devices are running. Depending on the security requirements, policies can also be used to define the features of the mobile device that are restricted, such as the camera or removable storage. Processes need to be put in place to provision users, apps, and so on.

A governance board can help define and review these processes and ensure that they are consistent with stakeholder goals, policies, and requirements. Different use cases need to be identified and examined to define to what degree a device is managed.

The US Federal Mobile Security Reference Architecture defines four use cases for device management that you might consider:

<https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf>

These four device-managed use cases are described:

- ▶ Fully managed government-furnished mobile device

A government organization-furnished mobile device provides organizations with the most control. The organization controls the key characteristics of the device, including the service provider, the type of hardware, the device capabilities that are enabled, the supported OS, and the deployed applications. Although controls still might not be available to stop a user from updating the OS or installing a specific app, controls can be put in place to restrict the device from accessing the enterprise if the device is not in compliance or the device can be wiped clean.

Personal use of the device can be extremely restrictive or not permitted at all. Ideally, the device behaves as an extension to the enterprise's internal network. A request from the device can be granted access to sensitive enterprise data after authentication, which can be at multiple levels.

- ▶ **Partially managed government-furnished mobile device (dual persona)**  
In this use case, the device is also government furnished, but managed enterprise applications can coexist with unmanaged user applications. For this use case, a dual persona is configured on the device.

A dual persona can be implemented as a virtual operating system or it can be accomplished by using a container, which is typically implemented as an application running on the device. The container can serve as a wrapper around the enterprise applications. Sensitive content can also be accessed by using the container and enterprise applications can be granted access to sensitive enterprise data.

- ▶ **Partially managed user-furnished mobile device**  
This use case is one of two use cases where the user provides, selects, and owns the device. Government apps can still be provided by using a dual persona capability. With the user’s consent, the government is still able to enforce policy requirements. These policies can be used to determine what apps and content the device has access to. However, in this use case, user privacy concerns typically need to be addressed.

- ▶ **Unmanaged user-furnished mobile device**  
These devices are unmanaged but still can be given access to systems that are part of the organization’s infrastructure, such as web mail. Little or no enterprise data is typically stored on the mobile device. The device is owned and controlled by the user.

As shown in Figure 2-1, the amount of provisioning and the level of security and management for these devices directly correspond to the type of use case.

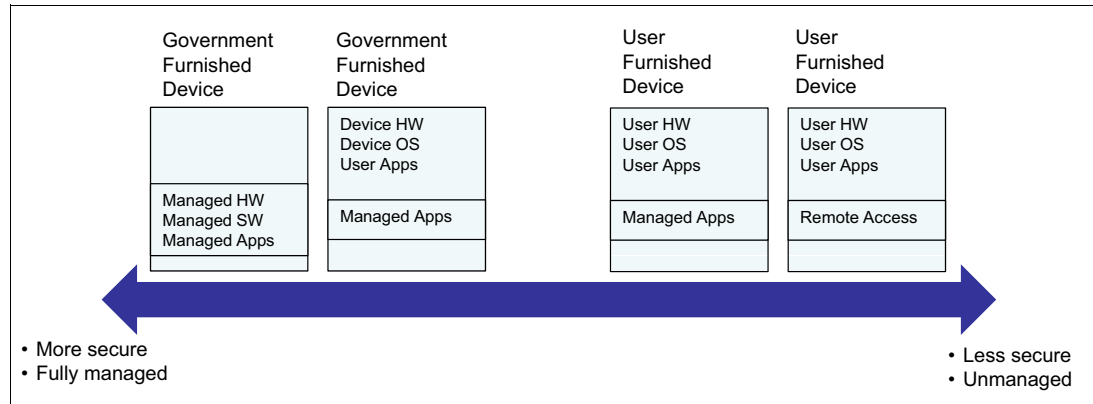


Figure 2-1 Use cases for managing mobile devices

Just as organizations need to define a strategy for device provisioning, they also must consider a strategy for deprovisioning devices. Devices need to be decommissioned and disposed of securely. Device sanitization must also be required for devices to be reissued to new users.

For more information about the topic of device sanitization, see the US Department of Commerce, National Institute of Standards and Technology, *Guidelines for Media Sanitization*, NIST SP800-88, publication, which is available at the following link:

<http://dx.doi.org/10.6028/NIST.SP.800-88r1>

## 2.1.2 Device management provisioning

When devices are provisioned, they need to be enrolled, fingerprinted, and managed. Security policies must be defined for these devices. All of these steps are typically performed by using a *mobile device management (MDM)* or *enterprise mobility management (EMM)* solution.

Some device vendors provide programs that incorporate MDM enrollment into the provisioning process. These programs can be used for government-furnished equipment. This method helps to streamline the provisioning process. If an organization supports “bring your own device” (BYOD), user-configured devices also commonly need to be managed.

MDM solutions can provide capabilities for bulk provisioning of devices, which is a common requirement to help expedite the distribution of mobile devices. Help desk services for device provisioning are also often required to help facilitate the distribution and management process.

MDM solutions are typically used when provisioning a mobile device. For government-furnished equipment, when the user receives the device, it might already be configured with an MDM client, or the MDM client might need to be installed on the device after the user receives the device.

For example, as shown in Figure 2-2, as part of the enrollment process, the MDM client app or agent can be downloaded from a public app store or an enterprise app store. After the MDM client is successfully downloaded and installed on the mobile device, the user configures the client to work with the MDM server. This step can include entering information, such as the server name and a supplied user ID. The user then uses the client to authenticate against a configured enterprise server. After authentication, an encrypted configuration policy is pushed down to the device. The policy definition is based on criteria, such as the user’s role or the device type and operating system. The MDM solution can then help enforce that policy and ensure that the device complies with the organization’s security requirements.

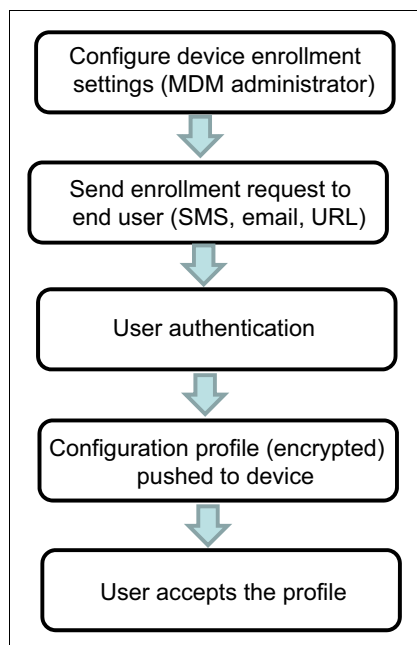


Figure 2-2 Example of MDM provisioning workflow



## Device provisioning and enrollment requirements

Government requirements for device provisioning and enrollment for the MDM solution might include the following requirements:

- ▶ Define and target device profiles and policies that are based on the operating system, including versions and platforms, for example, BlackBerry OS, Android, iOS, and Microsoft Windows 8.
- ▶ Define and target profiles and policies that are based on the device type or model.
- ▶ Integrate with an organization's existing user registry (for example, Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory).
- ▶ Allow users to self-enroll.
- ▶ Perform bulk user or device enrollment.
- ▶ Send a confirmation to a user after their device is enrolled.
- ▶ Allow users to enroll more than a single device.
- ▶ Support different profiles and policies for each device that is assigned to a specific user.
- ▶ Assign more than one profile or policy to a device based on specific criteria, such as device location, type, or user group membership. A more restrictive profile or policy needs to override less restrictive policies or profiles.
- ▶ Provide in-the-cloud or on-premises implementations to support device provisioning.
- ▶ Provide scale-out capability (for example, over 500,000 users).
- ▶ Log information and provide reports about provisioned devices.

## Bulk enrollment and provisioning

MDM providers might also provide bulk auto-enrollment capabilities. Examples include the Apple Configurator tool or the Apple Device Enrollment Program (US only), which can be used to help streamline the enrollment process.

A key feature of a device enrollment program is the ability to make the MDM enrollment "lockable", so if a user wipes the device, the device is not usable unless the device is re-enrolled against the MDM server.

Apple devices can also be configured in supervised mode as a way to restrict specific iOS capabilities and to better protect sensitive data. An example of configuring in a supervised mode is described in the Australian Government Department of Defence, *iOS Hardening Configuration Guide*, which is available at the following link:

<https://itunes.apple.com/us/book/asd-ios-hardening-configuration/id881697251?mt=11>

**Tip:** Check the Apple website to see whether these capabilities are available for a specific country.

## Hardware management

As devices are provisioned, requirements often dictate that the MDM solution needs to manage and track these devices. Requirements also might exist for privacy, such as the ability to turn tracking off (GPS coordinates). Requirements to manage these devices might include the ability to report and track devices based on the following criteria:

- ▶ Device owner or assignee (user ID or other criteria, such as an email address)
- ▶ Device model
- ▶ Device OS

- ▶ Device ownership - organization owned or BYOD
- ▶ Device Media Access Control (MAC) address

### 2.1.3 User credential provisioning

*Authentication* is the process of verifying that an entity is who it claims to be. The entity can be a user, application, or device. *Authorization* is the process of determining whether the entity has the permission to access or use a resource. An entity is authenticated before checking for authorization and the credentials that are used for authentication can vary from basic authentication by using a user ID and password to public key infrastructure (PKI) credential-based mutual authentication.

To increase security, many governments, including the US Federal Government, adopted a multifactor authentication model. A multifactor authentication model typically relies on the following factors:

- ▶ What you know, for example, a password or a PIN
- ▶ What or who you are, for example, a person’s finger print, iris scan, or voice print
- ▶ What you have, for example, various forms of physical tokens, transaction authentication number, matrix card, or a Short Message Service (SMS) one-time password

Multifactor authentication models offer higher security. Multifactor authentication models also increase the effort that is required to provision, maintain, and manage credentials.

Table 2-1 can be used as a guide for choosing the appropriate user authentication and authorization model. Depending on the criticality of the resource that is protected, the enterprise can choose an appropriate authentication model.

Table 2-1 Comparison of authentication models

Authentication model	Use cases	Pros (P) and cons (C)
No authentication	Information dissemination	<ul style="list-style-type: none"> <li>▶ No overhead (P)</li> <li>▶ Limited value (C)</li> </ul>
Basic authentication	Citizen services	<ul style="list-style-type: none"> <li>▶ Easy to manage (P)</li> <li>▶ Storage by users (C)</li> <li>▶ Use in public (C)</li> <li>▶ Prone to brute force attack (C)</li> <li>▶ Prone to social engineering (C)</li> </ul>
<b>Multifactor authentication</b>		
SMS-based one-time password	G2C, G2E	<ul style="list-style-type: none"> <li>▶ More secure than basic authentication (P)</li> <li>▶ Need for additional infrastructure (C)</li> </ul>
Software-based one-time password	G2E	<ul style="list-style-type: none"> <li>▶ More secure (P)</li> <li>▶ Need for an additional native application (C)</li> </ul>
Hardware-based one-time password	G2E	<ul style="list-style-type: none"> <li>▶ More secure (P)</li> <li>▶ Higher provisioning cost (C)</li> </ul>
Soft PKI certificate	G2E, specifically, national security applications	<ul style="list-style-type: none"> <li>▶ More secure (P)</li> <li>▶ Higher provisioning cost (C)</li> </ul>
Hardware-based PKI certificate	G2E, specifically, national security applications	<ul style="list-style-type: none"> <li>▶ More secure (P)</li> <li>▶ Higher provisioning cost (C)</li> </ul>

Authentication credentials can be pre-provisioned by the government to their users. In certain cases, authentication credentials can be self-provisioned, particularly if the authentication credentials are basic credentials where the government can validate the user, based on a combination of data, such as a government issued ID, date of birth, place of birth, or tax records. To provision a PKI-based credential, a public key infrastructure and registration/certification authority need to be configured. In either case, the user credential is typically published to an enterprise LDAP directory.

These authentication models can also participate in open standards-based authentication and authorization, such as Security Assertion Markup Language (SAML) or OAuth, in which case, the enterprise has the necessary infrastructure to provision these tokens.

Additional credentials for virtual private network (VPN) access can also be provisioned.

## 2.1.4 Application provisioning

Government organizations need a mechanism to distribute applications to mobile devices safely and securely. Administrators need the ability to deploy and host enterprise applications by using an enterprise app store. They also might need to push applications to specific devices, groups, or users over the air. These applications are generally available commercial apps, or apps that are developed specifically for the organization.

Distributing the app to the device is one part of a larger application lifecycle. As part of the application lifecycle, apps must be properly vetted to ensure that they comply with the organization's requirements before they are provisioned. A process needs to be in place to identify which commercial apps are required by users. A valid government account might be used to provision approved commercial apps from a commercial app store. In certain cases, the device can be preconfigured and loaded with the required apps that are needed by a government employee before the employee receives the actual device.

For more information about commercial mobile application adoption in the United States, see the CIO Council document at the following link:

<https://cio.gov/wp-content/uploads/downloads/2013/05/Commercial-Mobile-Application-Adoption-DGS-Milestone-5.4.pdf>

*Mobile application management (MAM)* capabilities can be included or bundled with MDM as part of an enterprise mobility management solution. A MAM solution can be used to provision apps on to mobile devices. Many MAM solutions include an enterprise app catalog or store.

Depending on the mGovernment use case, these apps are installed inside a MDM/MAM-managed container. Policies for the app are defined and enforced as part of the MAM solution. The amount of control that organizations have about app provisioning is influenced by the mGovernment use case, such as limiting how and determining where users get their apps.

Government requirements for app distribution can include the following needs:

- ▶ The ability to host an enterprise app store that supports multiple platforms, including iOS, Android, Windows 8, and BlackBerry.
- ▶ The ability to deploy apps that are available on public app stores (linking to public app stores from an enterprise catalog or store).
- ▶ The ability to deploy apps based on a configured policy. The policy can be assigned to a specific device based on a specific context, such as group membership, device type, or location.
- ▶ The ability to push apps to devices over the air (OTA).

- ▶ The ability to push apps to devices over a private network.
- ▶ The ability to control access to specific apps that are hosted in the store based on context, such as group membership.
- ▶ The ability to support bulk purchase of apps (when app vendors provide this option).

**Note:** Apple provides a Volume Purchase Program (VPP), which gives agencies the ability to purchase app store apps in bulk. The Apple VPP program is only available in certain countries or regions.

- ▶ Support for multiple or federated app stores.
- ▶ Support for application signing for trusted distribution.
- ▶ The app catalog or store needs to integrate with the organization's existing security infrastructure.
- ▶ The ability to preconfigure the apps for a specific environment before the apps are distributed.

## 2.2 Security

As government organizations architect and build their mobile ecosystem, the need exists to secure the mobile ecosystem to meet security objectives for confidentiality, integrity, and availability.

Securing the mobile ecosystem presents several unique challenges:

- ▶ Mobile devices are much more easily lost or stolen.
- ▶ Mobile apps can be run on an untrusted device or data can flow over an untrusted network.
- ▶ Mobile apps, unlike traditional enterprise web apps, run outside the enterprise firewall, which makes it easier for hackers to access these apps that they can then reverse engineer. Malicious variants can be found for many of the top selling commercial apps.
- ▶ Enterprise applications might be running on a device that is also running untrusted commercial apps or malware.
- ▶ The mobile device and operating landscape is fragmented. Due to that fragmentation, operating system patches that address security exposures might take longer to disseminate to mobile devices versus other types of devices, such as PCs.

To meet government security objectives, a layered security approach that includes security at the following levels must be examined:

- ▶ 2.2.1, "User-level security" on page 23
- ▶ 2.2.2, "Device-level security" on page 23
- ▶ 2.2.3, "Data or content-level security" on page 25
- ▶ 2.2.4, "Application-level security" on page 26
- ▶ 2.2.5, "Transaction-level security" on page 27
- ▶ 2.2.6, "Network-level security" on page 27

The levels of security that can be implemented are determined by the mGovernment delivery model.

For more information about the security threat for mobile apps, see the following links:

- ▶ *Adoption of Commercial Mobile Applications within the US Federal Government*:  
<https://cio.gov/wp-content/uploads/downloads/2013/05/Commercial-Mobile-Application-Adoption-DGS-Milestone-5.4.pdf>
- ▶ US Department of Commerce, National Institute of Standards and Technology, *Guide to Storage Encryption Technologies for End User Devices*:  
<https://www.arxan.com/resources/white-papers/>

## 2.2.1 User-level security

The need to control access to the resources, such as applications and data, exists in government specifically when dealing with non-G2C environments. Likely, in a G2C information dissemination or collaboration environment, the information is public.

However, some level of authorization needs to exist to prevent the unauthorized deletion or update of the information. Also, even in a G2E environment, different users are likely to have different levels of access and even the same user might have different levels of access, depending on the role of the user. As a result, authorization becomes critical and unauthorized access to the system or data is a threat that must be addressed.

The good news is that most of the mechanisms that are used to control the access of the resources in an eGovernment environment still apply to an mGovernment environment. Yet many secure environments now use *risk-based authentication*, where the risk profile of the user is considered during authentication. These risk profiles typically rely on the user's geographic location, usage pattern, and keystroke dynamics. When any of these risks or a combination of these risks become atypical, a higher risk profile is used, which presents a more complex authentication with an additional challenge, such as a dynamically generated one-time password (sent via SMS) with the usual credential. Features, such as the GPS that is available in mobile devices, allow an enterprise to use risk-based authentication easily. However, the core piece of information to manage authentication and authorization is still the user credential, which can be as simple as a user ID and password or more complex, such as multifactor credentials.

A typical security architecture for authentication and authorization includes a boundary component at the DMZ tier that intercepts the user to ensure that the user has the appropriate credential to access the environment. This check is typically performed with an enterprise directory server. Upon authentication of the user, additional access control and management components typically authorize the user's access to the resources. Depending on the granular nature of the resource accessed, this validation can be performed either in the DMZ tier or at the application tier. For example, the check for a coarse-grained authorization to access a specific hosted application can be performed at the DMZ tier, and a check for a fine-grained authorization to access specific data can be performed at the application tier.

## 2.2.2 Device-level security

When you consider device-level security, see the US Department of Commerce, National Institute of Standards and Technology, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 800-124. This document provides guidelines that need to be considered by government entities:

<http://dx.doi.org/10.6028/NIST.SP.800-124r1>

As described in this document, many of the same requirements are common across federal, state, and local governments. Common themes are also in other government-issued documents, such as the UK Centre for the Protection of National Infrastructure documentation about best practice security for mobile devices:

<https://www.cpni.gov.uk/advice/cyber/mobile-devices/>

Device-level security begins by understanding the device security capabilities and potential vulnerabilities. The device security capabilities and potential vulnerabilities need to be examined at the hardware level and the operating system level. For example, the device's security features need to be understood.

Create a strategy for mobile device security that includes a process for approving devices and operating systems and whether BYOD is supported. For government entities, a device approval process needs to be streamlined to support devices that are not considered outdated by the time that the approval process is completed. Organizations might also consider whether a device received a certification against common criteria security specifications.

Developing a system threat model to help understand the existing threat vectors and what their impact can be on the organization helps to better shape security requirements. This threat model needs to be reexamined regularly.

## **Mobile device management**

Mobile device management (MDM), as part of an enterprise mobility management solution, provides government organizations with a way to manage and better secure mobile devices that access the enterprise. By using an MDM strategy, organizations can define device policies for the device, including device configuration settings. An MDM strategy can help enforce the compliance of these policies by triggering actions when the device is non-compliant.

Government MDM requirements for device security can include the following actions:

- ▶ MDM implementation:
  - Support for in-the-cloud implementations
  - Support for on- premises implementations
  - Integration with the existing security infrastructure
  - Security Content Automation Protocol (SCAP) support
  - Mutual authentication support
- ▶ Define and enforce policies about the device capabilities:
  - Ability to detect rooted devices
  - Ability to detect jailbroken devices
  - Ability to enable and disable specific device capabilities:
    - Camera
    - Audio recording
    - USB interface
    - GPS (location services)
    - Restrict writing data to removable storage (sdcard)

- Ability to enable and disable communications:
  - Wi-Fi
  - Bluetooth
  - Near field communication (NFC)
  - VPN
- Disable backup to the cloud
- ▶ Authentication capabilities:
  - Define enforcement policies about configured authentication capabilities:
    - Biometrics (fingerprint)
    - Password requirements (length and required characters)
  - The ability to reset passwords remotely
  - Policies about autolocking the device after a configured period

For more information about the governance of mobile device management policies, see 2.3.2, “Mobile device management policies” on page 29.

For more information about requirements for mobile device and application management, see the US General Services Administration Mobile Device and Application Management website:

<http://www.gsa.gov/portal/content/177475>

### 2.2.3 Data or content-level security

Confidentiality of the information that is stored on a user’s mobile device is critical. In today’s environment, many threats can compromise the confidentiality of the information that is stored on the mobile device. Although compromising personally identifiable information can result in inconvenience to the individual, compromising information that deals with national security can pose grave danger to the nation. Typically, federal governments worldwide dictate how to handle data-level security, specifically when dealing with a user’s personal information, sensitive data, or national security data.

The US Federal Office of Management and Budget Memorandum M-06-16 is directly related to the security of the data that is stored on devices. It specifically requires that agencies secure all data stored on mobile devices by encrypting them, unless they are determined to be non-sensitive. And, when agencies use encryption, they must use approved encryption algorithms.

For more information about compliance that relates to encryption, see 2.4.2, “Encrypting data at rest and data in flight” on page 30.

The following legislation also relates to this topic:

- ▶ The Privacy Act of 1974 regulates the collection, use, maintenance, and dissemination of personal information.
- ▶ The Health Insurance Portability and Accountability Act of 1996 (HIPAA) dictates the storage security of health information.
- ▶ The Gramm-Leach-Bliley Act dictates protecting customers’ financial data by their financial institutions. Although at the surface, this act does not seem applicable to an mGovernment solution, it applies to taxing agencies.

For more information, see the following National Institute of Standards and Technology (NIST) documents:

- ▶ *Guide to Storage Encryption Technologies for End User Devices*:  
<http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf>
- ▶ The HIPAA Security Rule is documented in section 4.14 of the NIST SP 800-66 publication:  
<http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

**Note:** Securing sensitive data on the mobile device, and off the device, is of paramount importance in an mGovernment environment. Although the general guidance is likely to be similar to the US Federal Government dictates, we advise that you check with your respective government's requirements.

## 2.2.4 Application-level security

As part of the security layer approach, government organizations need to implement security for mobile apps that they host, provision, and develop. Different types of security vulnerabilities can exist for apps based on the platform that the apps run on.

For more information about platform-specific vulnerabilities, see US Department of Commerce, National Institute of Standards and Technology, *Technical Considerations for Vetting 3rd Party Mobile Applications*, 800-163:

[http://csrc.nist.gov/publications/drafts/800-163/sp800\\_163\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf)

Organizations need to consider the following requirements:

- ▶ The ability to host apps in an enterprise app store or catalog. App store requirements are covered under app distribution (provisioning); see 2.1.4, “Application provisioning” on page 21.
- ▶ The ability to wrap applications to enforce policies and restrict or modify application capabilities. A good explanation of this wrapping is in the UK government's *End User Devices Security Guidance: Apple iOS Application Security Guidance* publication:  
<http://bit.ly/10TEE0P>
- ▶ Data requirements:
  - Application data needs to be Federal Information Processing Standard (FIPS) 140-2 encrypted.
  - Application data is not allowed to be stored on the device.
  - Data and file sharing need to be restricted.
- ▶ Cache:
  - Cache data must be encrypted.
  - Cached data must be deleted.
- ▶ Time-based.
- ▶ Event-based.
- ▶ Apps must communicate to the enterprise by using a MicroVPN.



## 2.2.5 Transaction-level security

Due to the unique characteristics of the mobile architecture, security needs to be looked at from many layers. Security cannot merely be enforced at the network perimeter. Device security, application security, and network security all help protect sensitive data and assets, but security at the transaction level can provide an additional safeguard for government mobile users.

In many cases, users who are accessing the enterprise, such as constituents, might be using devices that are not managed by the enterprise. The devices might be infected with malware, jail broken, or not configured securely (for example, no password that is required to access the device). Mobile transaction security takes a holistic approach that examines different factors and contexts associated with a transaction to determine the level of risk associated with the request and ultimately to help determine whether that request needs to be approved, denied, or restricted.

In the future, mobile payment for services in government becomes more common. For example, consider the app where citizens are using Apple pay to gain admittance to a national park:

<http://www.imore.com/us-national-parks-and-other-federal-services-will-support-apple-pay-come-september>

As constituents conduct more transactions with the government by using their mobile devices, this change can be the impetus for agencies to employ a holistic risk-based approach when they approve or deny transactions.

## 2.2.6 Network-level security

When it comes to the network layer, a mobile device inherently does not differ much from a non-mobile device after the signal from the mobile device reaches the telecom office. Beyond that point, the network security applies to the mGovernment environment in the same way that it applies to the eGovernment environment.

However, until the signal reaches the telecom office, differences exist in mobile devices. These differences are a result of the mobile devices' use of Wi-Fi and cellular network communications. Therefore, mobile devices are more exposed than typical wired devices. Mobile devices also use a variety of wireless protocols for data and voice over the air that can be intercepted and compromised, for example:

- ▶ Wi-Fi, where mobile devices use IEEE 802.11x standards. Typically, the devices support a range of encryptions although Wired Equivalent Privacy (WEP) was proven to be too insecure. Wi-Fi Protected Access II (WPA2) is recommended as of this writing. Data can also be intercepted and compromised by rogue access points.

For more information, see the US Department of Commerce, National Institute of Standards and Technology, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, Chapter 5, "Threats and Vulnerabilities":

<http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>

- ▶ Cellular, where mobile devices use various cellular protocols, such as Global System for Mobile Communications (GSM), Enhanced Data rates for GSM Evolution® (EDGE), Code division multiple access (CDMA), and Long-Term Evolution (LTE), to secure data. Although the data is encrypted, the data can be compromised by a rogue cellular tower, which can mimic a legitimate cellular tower and intercept the data.

- ▶ Bluetooth, where a mobile device can use short-range wireless connectivity. Although Bluetooth provides a native encryption and authentication mechanism, known vulnerabilities exist.

For more information, see the US Department of Commerce, National Institute of Standards and Technology, *Guide to Bluetooth Security*:

[http://csrc.nist.gov/publications/drafts/800-121r1/Draft-SP800-121\\_Rev1.pdf](http://csrc.nist.gov/publications/drafts/800-121r1/Draft-SP800-121_Rev1.pdf)

- ▶ Infrared communication, where the infrared spectrum is used for short-range communication. Vulnerabilities exist and care must be taken.

In all of these cases, using a VPN with strong government-approved encryption provides the best security for network communication.

## 2.3 Governance

Government organizations need to develop a strategy for mobility to help meet the objectives of the organization's stakeholders. Defining processes, policies, and putting performance measurements in place ultimately helps organizations to deliver on and realize the value of mobile. Many of the governance models are predicated on the mGovernment delivery model. For example, defining a device governance model might be more relevant for a G2E delivery model than a G2C delivery model.

### 2.3.1 Device governance

When government organizations consider device delivery and support models, including a G2E delivery model, they need to put a strategy and governance in place for mobile devices. Organizations might consider the following key topics:

- ▶ BYOD versus government-furnished equipment (GFE) considerations. How much control of the device, content, and applications on the device is required by the organization or an individual group within the organization? What about privacy?
- ▶ BYOD Wipe policies (partial or full). What are the legal ramifications if a government agency wipes an employee's personal data from a BYOD device?
- ▶ What platforms and specific devices need to be supported? Is multiple platform support a requirement? What is an acceptable amount of risk (associated with these platforms and devices) for an organization?
- ▶ Define the process for the provisioning and disposal of devices. Fragmentation in the mobile space poses challenges, where different processes might need to be defined for different OS platforms.
- ▶ What type of data and apps are allowed on the device? This topic relates to the amount of risk and control that an organization is willing to assume.
- ▶ What tools need to be used to manage these devices and what are the requirements for these tools? Typically, enterprise mobility management solutions play a major role here.

## 2.3.2 Mobile device management policies

Just as governance must exist about the mobile devices to use and how to use them, governance must exist about the mobile device management policies that are established, for example:

- ▶ Policies for specific groups. How are groups and roles defined? Does a policy for one group supersede the policy for another group or role?
- ▶ Policies for specific devices or types of devices. Different device and OS vendors provide different capabilities for the level of control that can be applied by an MDM or EMM vendor.
- ▶ What processes exist to approve MDM policies? Who are the approvers for these MDM policies?

For more information about mobile device management, see “Mobile device management” on page 24.

## 2.3.3 Application governance

Governance must exist for application management, for example:

- ▶ What type of apps are allowed on the device (whitelist/blacklist). What sort of action must be taken when unauthorized apps are found on a device?
- ▶ Will enterprise apps be separated (containerization/personas)? What are the processes in place for wiping that container?
- ▶ What is the approval vetting process for apps that are deployed to an enterprise app store?
- ▶ What is the established process to discontinue (withdraw from support) apps? What is the entire application lifecycle?
- ▶ How are policies defined about the data that apps are allowed to access?
- ▶ How are commercial applications analyzed and approved?
- ▶ What data will apps be allowed to store, if any? What are the security and encryption requirements for the data? Consider these questions for both data that is stored on the device and data that is in transit.
- ▶ Who owns the data on the device?

## 2.4 Compliance

Many countries have strict laws that deal with compliance, including the development of applications for mobile devices. Compliance in mGovernment comes mainly in the following forms:

- ▶ Handling personal data and personally identifiable information
- ▶ Encrypting data at rest and data in flight
- ▶ Enabling accessibility for mobile applications
- ▶ Export controls

## 2.4.1 Handling personal data and personally identifiable information

In these days of ever increasing security breaches and identity theft, protecting personal data and personally identifiable information (PII) is paramount. Many countries created laws about how personal information must be handled. The definitions of personal data and PII, however, vary between various countries and in certain instances among states within the country. However, PII is broadly defined as information that permits the identity of an individual to be directly or indirectly inferred. Private information can include the name, national identity number, biometric data, IP address, medical x-rays, and even vehicle registration number.

When you develop mGovernment applications, you must seriously consider how to handle personal data. Compliance and governance differ from one country to another, but in general they cover the following areas:

- ▶ Registration. The requirement to register with the data protection authority, which consists of the data controllers who process personal data by automatic means. This registration is common in most European countries, although registration is not as prevalent in the US.
- ▶ Data protection office or officer. The need for a data protection office or officer. This need varies between countries.
- ▶ Collection and processing. What personal data can be collected and processed? Typically, European Union countries have stricter rules about the collection and processing of personal data.
- ▶ Transfer. The ability to transfer personal data that was collected. Typically, European Union countries have stricter rules about transferring collected personal data.
- ▶ Security. The requirement that dictates how personal data is secured. In the US, the health sector has special requirements about securing health-related data.
- ▶ Breach notification. The requirement to notify the authorities about a security breach of personal data.
- ▶ Electronic marketing. The regulation of how personal data can be used for marketing.
- ▶ Online privacy. How data, such as cookies and location information, must be handled.

For more information, see the following documents:

- ▶ US Department of Commerce, National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*:  
<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
- ▶ US Department of Homeland Security's *Handbook for Safeguarding Sensitive Personally Identifiable Information*:  
[http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_guide\\_sp\\_i\\_handbook.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_sp_i_handbook.pdf)
- ▶ *Data Protection Laws of the World*:  
<http://www.dlapiperdataprotection.com>

## 2.4.2 Encrypting data at rest and data in flight

Storing sensitive data on a mobile device or transmitting data from the mobile device to back-end servers is often necessary. When these actions are performed in applications that are developed for the government, such as the US, strict guidelines need to be followed to get approval to deploy the application in a production environment.

In the US, the National Institute of Standards and Technology (NIST) dictates the policies that must be enforced. For example, the NIST 140 series of Federal Information Processing Standards (FIPS 140-2) specifies approved cryptographic algorithms.

The UN agency, International Telecommunication Union, works with countries to develop broad legislation to improve cyber security. Checking with the country-specific compliance requirements when you implement cryptographic standards on data at rest and data in flight is considered a best practice.

The following web resources provide guidance:

- ▶ Cryptographic policies of various countries:  
<http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/cryptographic-policies-countries.htm>
- ▶ “International Cryptography Regulations and the Global Information Economy” by Nathan Saper in *Northwestern Journal of Technology and Intellectual Property*, September 2013:  
<http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1205&context=njtip>
- ▶ Professor Bert-Jaap Koops’ Crypto Law website:  
<http://www.cryptolaw.org/>

### 2.4.3 Enabling accessibility for mobile applications

As information technology, Internet, and web applications become more prevalent worldwide, many governments enact national laws and policies to address accessibility in these areas. Countries, such as the US, started on this path as early as 1986, with revisions in 1998. Similar laws were enacted in various other countries. Typically, the laws are approached either from a human or civil rights perspective or from a government technology acquisition perspective.

The World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) website aggregates various country policies that relate to accessibility:

<http://www.w3.org/WAI/Policy/>

Enabling websites for accessibility is common. Many resources, such as guidelines, checklists, and tools for authoring and testing, are available on the W3C’s WAI website.

Although most accessibility enablement for mobile devices is similar to desktop interfaces; however, differences exist due to the sheer form factor of the mobile devices. For more information about mobile accessibility, see the following websites:

- ▶ W3C WAI mobile accessibility:  
<http://www.w3.org/WAI/mobile/>
- ▶ BBC’s Mobile Accessibility Guidelines:  
<http://www.bbc.co.uk/guidelines/futuremedia/accessibility/mobile/about>

## 2.4.4 Export controls

*Dual-use technologies* can be used for both peaceful and non-peaceful purposes. Although many examples exist, such as the nuclear technology that is used for civilian nuclear power plants versus technology that is used for nuclear weapons, other innocuous technologies also fall into the dual-use technology category. Examples that fit this category include the highly accurate Global Positioning System (GPS) and the implementation of strong encryption algorithms.

The Wassenaar Arrangement was established to promote regional and international security and stability by way of the participating 41 nations providing transparencies in their trade of conventional arms and dual use goods and technologies. Category 5, Part 2 of the Wassenaar Arrangement document deals with information security, including data encryption technology.

Although the data, specifically personal data that is stored on the mobile device, needs to be secured by encryption, mobile application developers also must ensure that they abide by export controls where the strong encryption technology does not inadvertently break the export control regulations. The current export controls for Category 5, Part 2 are published on the Wassenaar Arrangement website:

<http://www.wassenaar.org/controllists/index.html>

## 2.5 Application disaster management

For mGovernment, disaster management is important. Disaster management keeps the IT infrastructure available via redundancy and disaster recovery strategies. However, it mainly provides emergency ad hoc citizen services while keeping existing services operational. The objective of disaster management is to decrease human casualties in natural events, such as earthquakes, floods, and thunderstorms, as well as in air crashes or large-scale accidents. Mobile satellite services (MSS) and remote sensing satellites are used for this purpose.

The application disaster management team needs to be ready with alternative services and applications to address any situation. The government is an important entity on which every person depends. Therefore, the government needs to take the appropriate steps to re-establish the connection between its applications and the users. A government organization needs to define a model for handling disaster management. At the time of a disaster, such as a cyclone, earthquake, or major terrorist attack, not only mobile applications but certain services might also be unavailable.

The maintenance of essential services, such as telecommunication services and mobile services, is required for overall disaster management, including search and rescue. Therefore, telecom and mobile services might be considered the lifelines of these operations.

Because a disaster can occur suddenly with or without warning, disaster prevention is better than disaster response. It is difficult even for the best measures to replace disaster preparedness, and even the highest level of preparedness can never cover all aspects of disaster response.

The occurrence of disastrous events cannot be prevented fully but their impact can be reduced by preparing the appropriate advance operational plans, establishing warning systems, training emergency response personnel, educating citizens, and testing emergency procedures.

Information collection and communication to the disaster area are extremely important to extend help in that area. Mobile plays an important role by communicating and disseminating disaster information to residents as promptly as possible, as well as ensuring the restoration of a speedy communication system after a disaster occurs. This restoration requires the establishment of links between disaster coordinators, telecommunication authorities, service providers, and mobile applications on each level. Because mobile and telecommunication are the lifelines for the rescue and relief operation, you must plan for mobile and telecommunication to withstand the effect of the disaster so that they can provide uninterrupted services.

The following ways re-establish the application and communication at the time of a disaster:

- ▶ Use of wireless (stationary or mobile) systems at the time of a disaster
- ▶ Use of SMS gateway or Unstructured Supplementary Service Data (USSD) to establish connection between people and devices
- ▶ Use of satellite systems, such as the Internet, through dish satellite or use of satellite phones
- ▶ Peer to peer communications by using Bluetooth

## 2.6 Analytics

Data is becoming the important asset for any organization and is key to the organization's success. Most organizations, whether public or private, have large data repositories that contain valuable information about their customers and services. The private sector recognizes the value of this data and takes its use seriously, offering better services and products as a result. Although this data is valuable for understanding past performance, it can also be used as the basis for proactive decision making and planning to provide better public services at a lower cost. Because cost reduction and non-for-profit operations are the main drivers for government, the justification for budget allocations and funding relies heavily with statistics and data analytics.

Mobile platforms, especially with better location precision, are facilitating this transformation. Open data empowers citizens to hold governments accountable for the use of taxpayer money, provides access to important business development information, and enables governments to provide and obtain specific and current information in emergencies. Also, open data helps to target relevant data for diverse citizen needs, interests, and geographic locations.

When vetting commercial-off-the-shelf software in the area of mobile analytics, governments are increasingly looking for deeper and richer capabilities to address these key citizens' needs in the following ways:

- ▶ How are my citizens experiencing my mobile apps?
- ▶ Are my mobile systems performing optimally? Where are things going wrong and can I fix them?
- ▶ Am I measuring mobile app usage metrics across various dimensions, such as responsiveness, device platform, device type, time, and location?
- ▶ What are my citizens saying about my mobile apps?

## 2.6.1 Operational analytics

With mobile and mobile apps becoming the primary channels for government, the availability and performance of the government mobile infrastructure are critical to an IT operations team. A scalable, operational analytics platform for government is needed to search across logs and events that are collected from various devices, apps, and the servers. This analytics platform must look for patterns, determine problems, and summarize the various statistical measurements of platform usage.

This operational-type of analytics platform includes these capabilities:

- ▶ Device usage summary and reports
- ▶ Geographic view of mobile activity
- ▶ Near real-time reporting of app crash events
- ▶ Ability to search on free text occurrences across logs for keywords and the ability to contextually narrow or expand the search result
- ▶ A scrolling view of the server-side log information in a table form with the ability to filter the view by keywords

## 2.6.2 Business analytics

Using analysis to make decisions based on facts is a key factor in meeting an organization's goals for profitability, revenue, and cost reduction. The decision makers in an organization need a wide variety of analysis capabilities so they can compile the facts and trends necessary for better and smarter decisions.

Business analytics offers flexible solutions that are designed to provide a broad range of analysis capabilities:

- ▶ Analytical reporting. Find the answers to business questions fast with guided report analysis, dashboards, navigable reports, and mobile business intelligence.
- ▶ Trend analysis. Fully explore data and track business developments with capabilities for tracking patterns and adding them to charts and graphs.
- ▶ What-if analysis. Model scenarios with capabilities for reorganizing, reshaping, and recalculating data so that you can identify the optimal solutions to business problems.
- ▶ Advanced analysis. Uncover patterns in your business and apply algorithms to business intelligence data to predict outcomes.

Analytics can be much better if you are performing the analytics in terms of context, location, and text. Because mobile applications can send data with the location, the outcome of the analytics is more accurate for a particular location and can be analyzed better with more accurate results.

## 2.7 Application programming interfaces

The convergence of web application programming interfaces (APIs) and mobile technologies with government content can lead to significant productivity implications for the next-generation innovative platform for digital business.



## 2.7.1 APIs and government

Web APIs enable businesses and governments to offer their internal assets, such as information, data, and services, to external customers and markets in new and innovative ways by overcoming traditional enterprise boundaries. APIs can be used internally in an agency (private) or externally (public) to interested stakeholders. API users can be user citizens or other partnering entities that develop applications for users (developers).

Mobile devices and mobile applications are fueling an explosion of the consumption of web API services by moving away from the browser-based consumption style to a mobile applications running on mobile devices-based consumption model.

Governments tend to typically hold large amounts of raw data. This data contains a rich, high-quality source of digital government information. Applications and services can be built to use the insights that are gained from this wealth of data. Governments must ensure that the data is open, machine-readable, and accessible anywhere and anytime. The data must be available on any device in a device-agnostic fashion with safety, security, and privacy engineered in, at a lower cost to improve the quality of services for citizens.

Creating APIs to access government data involves starting with the data or content, understanding and documenting the data clearly, and creating a comprehensive taxonomy to make data searchable. Governments must create APIs to annotate the data adequately to make it authoritative with metadata, and finally expose the data to other computers in a machine-readable format for exploitation and value realization.

The purpose of governments to use APIs is to increase transparency and openness in governance, increase return on IT investments, reduce waste and duplication, and improve the effectiveness of IT solutions implemented in government programs. Additionally, government use of APIs helps to streamline and improve internal and external stakeholder service delivery at lower cost by innovating with less to deliver more.

Embedding security and privacy controls into structured data, unstructured data, and metadata enables governments to focus more effort on ensuring the safe and secure delivery of data to the customer with fewer resources, while improving the quality of information that is accessible, current, and accurate at any time with enhanced security and privacy.

## 2.7.2 APIs and mobile

Web API and mobile technologies offer a compelling and unique synergetic value when governments intend to deliver the following function:

- ▶ High-quality digital government information and services anywhere, anytime, and on any device to mobile-savvy stakeholders in a device-agnostic and cost-effective manner.
- ▶ The capability to unleash and extend the value of government/enterprise data to usher in innovation across governing/enterprise boundaries (community, local, city, county, state, country, or global). This data must be in an open and machine-readable manner, therefore improving the quality of services that are provided to consuming stakeholders.

The mobile landscape is dramatically changing people's lives. Mobile web surpassed the personal computer in 40 nations, including countries, such as India, Nigeria, and Bangladesh, according to the mobithinking news article dated 19 September 2014, at the following website:

<http://mobiforge.com/news-comment/mobile-web-has-now-overtaken-pc-40-nations-including-india-nigeria-and-bangladesh>

For the first time in history, global smartphone shipments of nearly one billion units exceeded personal computer shipments in 2011. Mobile broadband subscriptions are expected to reach 5 billion by 2016. More citizens are accessing the Internet by using mobile devices than personal computers. For more information about these facts, see the mobiForge website:

<http://mobiforge.com/>

Certain considerations apply when you design APIs to consume from mobile devices. In particular, you need to consider the following mobile device features:

- ▶ Smaller screen sizes
- ▶ Availability of fewer simultaneous remote connections
- ▶ Lower quality and reliability of network connectivity
- ▶ Resource-challenged device environment
- ▶ Device-specific fragmented browser ecosystem

## 2.8 Mobile application development lifecycle

The mobile application development lifecycle for mGovernment is similar to the mobile application development lifecycle for commercial environments.

As shown in Figure 2-3 on page 37, a common set of steps is typically required when you develop mobile apps:

1. Discovering and gathering requirements
2. Designing and developing the mobile app
3. Identifying and exposing key integration points
4. Instrumenting the app
5. Testing and vetting the app
6. Deploying and managing the app
7. Gathering and interpreting the analytics that are generated by the app

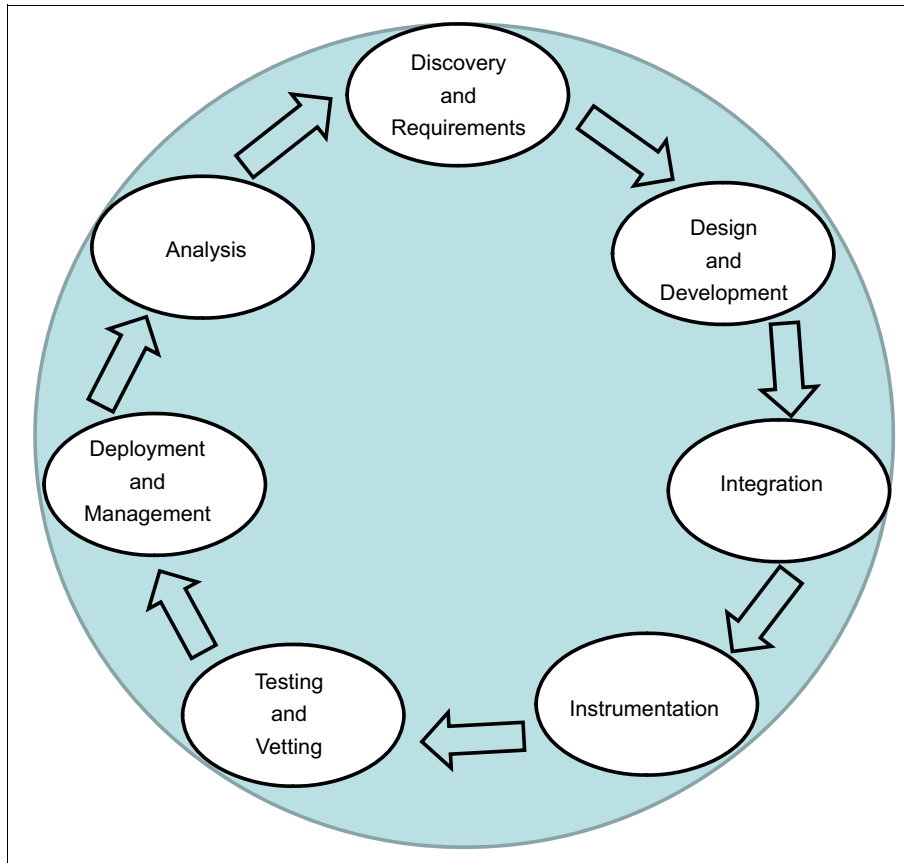


Figure 2-3 Mobile application development lifecycle

The following sections describe each of these mobile application development lifecycle steps in more detail.

## 2.8.1 Discovery and requirements

Before developing a new mobile app, determining the assets that are already available or being developed is important. How can existing assets be used? Is a similar app already available that meets the requirements?

As an example, the US Department of Veterans Affairs (VA) provides an overview of considerations about app discovery on the following website:

<http://mobilehealth.va.gov/content/discovery-overview>

The VA website covers app discovery and identifying objectives for the proposed app. Searching for existing approved apps might seem obvious, but is an important consideration. Decisions need to be made based on stakeholder requirements, the platforms that will be supported, security, compliance to the regulations, and much more.

## 2.8.2 Designing and developing

Multiple approaches exist to designing and developing mobile apps for government. Different approaches are needed based on the identified requirements and skill sets of the developers. For design, existing in-house tools might be sufficient for building wireframes.

For example, the US Department of Health and Human Services provides several basic guidelines about wireframing on this website:

<http://www.usability.gov/how-to-and-tools/methods/wireframing.html>

And, the DigitalGov website provides further information at this website:

<http://www.digitalgov.gov/2014/01/20/mobile-gov-user-experience-resources-and-design-tools/>

Strategies and processes also need to be defined for the actual app development. Depending on the gathered requirements, decisions are needed whether to take a native approach, a mobile web app approach, or a hybrid approach to mobile development.

Whether government organizations develop apps in-house or use third parties to develop them, standardizing on mobile application middleware can help streamline the development process. Standards can be defined and governance can be enforced.

### **Accessibility compliance**

One of the key requirements for US government organizations in relation to mobile apps is accessibility or Section 508 compliance. The United States Access Board states the following requirement:

*“The Section 508 Standards are part of the Federal Acquisition Regulation (FAR) and address access for people with physical, sensory, or cognitive disabilities.”*

For more information, see the following website:

<http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards>

The US General Services Administration (GSA) created accessibility requirements for mobile applications. This document maps requirements to Section 508 at the following website:

[http://www.gsa.gov/portal/content/103565#\\_mobile](http://www.gsa.gov/portal/content/103565#_mobile)

Topics that are covered include requirements about controls and display, descriptive and alternative text, timeouts, and tables (for example, providing sorting information of columns for the visually impaired).

The Veterans Health Administration also released high-level testing guidelines about Section 508:

<http://mobilehealth.va.gov/content/section-508>

Other countries can also have their own accessibility requirements. For example, countries might have requirements that relate to the Web Content Accessibility Guidelines (WCAG) 2.0.

## **2.8.3 Integration**

The emergence of service-oriented architecture (SOA) and Representational State Transfer (RESTful) APIs provided developers with more standard ways to integrate with back-end systems. Government websites, such as <http://www.data.gov>, also provide endpoints, but these endpoints might not be optimized for mobile development.

Government organizations face unique challenges. Endpoints might be exposed on security networks at different levels. Context-based security and multifactor authentication might be considered for apps that access specific endpoints.

For example, access to a specific endpoint might be restricted based on the location of the device. Data flowing to and from these endpoints often needs to be encrypted by using FIPS 140-2 cryptographic modules. Without the correct tools and strategy in place, integration with back-end systems can delay and adversely affect the development lifecycle.

## 2.8.4 Instrumenting

Instrumenting apps is typically done for multiple reasons. Instrumenting apps can be done to collect operational or business analytics, to enable testing, and to better secure the app. These analytics help organizations determine whether the mobile apps meet their defined objectives. Instrumenting apps can also help operations debug user issues more efficiently, therefore saving money, time, and resources.

## 2.8.5 Testing and vetting

Testing and vetting of mobile apps are essential to help confirm that the apps meet the stakeholders' requirements. Testing and vetting are essential to help identify potential security exposures, reduce risk, and help find and diagnose problems. Testing and vetting must be performed for both apps that are developed in-house and third-party apps.

Government organizations need to create processes to automate testing and vet mobile apps as part of their software assurance strategy. By using a common framework to test and vet apps, governments can help streamline these processes.

For more information, see the US Department of Commerce, National Institute of Standards and Technology, *Technical Considerations for Vetting 3rd Party Mobile Applications*, publication 800-163:

[http://csrc.nist.gov/publications/drafts/800-163/sp800\\_163\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf)

Third-party apps that are targeted for consumers might not address government requirements. For example, apps might store unencrypted data in the cloud.

## 2.8.6 Deployment and management

Mobile application deployment refers to distributing apps to mobile devices safely and securely. Application binary files can be deployed to an enterprise app store and then pulled down by the device, or apps can run behind the enterprise firewall as mobile web applications that are invoked by a browser on the device. Enterprise mobility management solutions might also deliver apps to mobile devices. Access to third-party apps on commercial app stores and government licensing need to be considered.

Government organizations need to manage apps throughout the application lifecycle. Multiple versions of the app might be required to support different platforms or to provide additional functionality based on requirements.

## 2.8.7 Analytics

Government organizations need to understand how their mobile apps are being used, which apps are being used, what types of devices are running the apps, and so on. Use of analytics can help organizations develop better future apps by helping teams learn the features that are providing the most value to users today. Instrumented mobile apps can provide both business and operational analytics.

This information can also be used to determine whether service level agreements (SLAs) are being met or to help identify bottlenecks when mobile users access enterprise services or systems.

## 2.9 Mobile user experience

The user experience in any mobile application initiative is of the utmost importance, especially for government mobile application initiatives. These government mobile applications need to create a user experience that is focused on each of the stakeholders, particularly the citizens. The following key factors might affect a conducive user experience for governments:

- ▶ Mobile device type distribution needs to be analyzed and identified. Certain countries have more smartphones compared to smart devices and vice versa. For example, for countries with more citizens that use smartphones, the mobile applications that are developed need to focus on using the features that are available on these devices to provide the mobile application functionalities and capabilities to the masses.
- ▶ Infrastructures and data network availability for the targeted areas need to be identified. Countries with nationwide data network availability benefit from an application that fully uses it. For countries where the data networks are only available in the urban areas and no coverage exists in the rural areas, and the targeted users are people in the rural areas, the mobile application needs to be tailored to the infrastructure availability in that particular area.
- ▶ Rules and governing policies for mobile applications need to be observed in each country where the mobile app will be deployed. The mobile applications need to implement the required capabilities to be compliant, for example, the US Section 508 Standards for Electronic and Information Technology.
- ▶ The mobile applications that are developed need to use at least the national language of the country. Also, support for additional languages that are used by the target users is an added advantage. Ideally, create mobile apps that support the major languages that are spoken in the country.



# IBM MobileFirst

This chapter provides an introduction and brief overview of the IBM MobileFirst capabilities.

The following topics are covered in this chapter:

- ▶ 3.1, “IBM MobileFirst overview” on page 42
- ▶ 3.2, “IBM MobileFirst portfolio” on page 43
- ▶ 3.3, “IBM MobileFirst reference architecture” on page 50
- ▶ 3.4, “IBM MobileFirst enterprise app lifecycle” on page 54

For more information about MobileFirst, see the MobileFirst website:

<http://www.ibm.com/mobilefirst/us/en/>

## 3.1 IBM MobileFirst overview

For consumers, mobile is the preferred medium for constant interaction. Today, mobile citizens are no different from consumers. Citizens expect to engage with government services by using every available channel, including mobile. MobileFirst can play a key role in this paradigm shift of citizens toward a mobile environment.

### 3.1.1 Understanding the need for mobile technology for citizens

Each day, mobile technologies grow one step closer to becoming the primary means of interaction and communication among employers, family and friends, customers, governments, and their citizens. The average mobile phone user checks their phone 150 times per day. In 2014, it was estimated that more people used their mobile device to access the Internet than desktop computers.

This “mobile explosion” of information and technology created a shift in perception from the citizen point of view. Starting with eGovernment initiatives, and now moving into mobile government (mGovernment), people started to change their expectations. They expect to engage with their government by using every available channel, including desktop computing, call centers, in-person, social media, and now mobile technologies.

The unique capabilities of mobile devices are changing the way that leaders at government agencies interact with citizens, employees, and businesses. Mobile technologies provide you with the ability to reach people and give people the ability to reach you, virtually anytime and anywhere. Mobile technologies use millions of devices as sensors. These technologies provide access to an expanse of data and insights, which make it possible for the government to become a learning organization that is able to adapt quickly to changing conditions.

### 3.1.2 IBM MobileFirst introduction

IBM created the concept of MobileFirst because mobile cannot be an afterthought. Mobile success requires a fundamental shift to the business of government, altering how services are provided and leading to the development of new services that are only possible through mobile technologies.

The use of mobile technologies represents an opportunity for government leaders to reinvent how their organizations interact with citizens, businesses, and employees. You must embrace mobile technologies and you must embrace all of the opportunities and challenges that are part of the mobile approach.

The government leaders who embrace this shift will move beyond mere provisioning of information and services. They will have the opportunity reinvent the interaction between their government and all of their constituents, including citizens, businesses, and their own employees. Leaders use Internet sites that are structured to be accessible from mobile devices. They explore mobile technologies as a way to pay for parking by using smartphones, track wait times in airport security lines, and so on. But to realize true value, mobile execution must go beyond these scenarios. Your mobile approach must be context-aware and location-aware, and your processes must integrate the unique functionalities that mobile provides.

IBM thoroughly invested in the core mobile capabilities while rounding out the MobileFirst portfolio with strategic acquisitions, such as Fiberlink®, IBM Trusteer®, and UrbanCode.



## 3.2 IBM MobileFirst portfolio

As shown in Figure 3-1, MobileFirst employs a four-part strategic approach to help government leaders set their mobile agenda. With the MobileFirst portfolio of product offerings, government leaders can efficiently perform the following tasks:

- ▶ Build and run mobile applications that extend to a wide variety of devices.
- ▶ Protect the mobile infrastructure with leading management and security capabilities to address every layer of the mobile enterprise.
- ▶ Engage with constituents in context through advanced analytical capabilities that help governments deliver targeted and relevant experiences.
- ▶ Transform and create growth by tapping into deep industry expertise and cutting-edge technologies that help to address complex business challenges.

MobileFirst products and solutions help turn virtually every mobile interaction into an opportunity to create value. For more information about MobileFirst, see the MobileFirst website:

<http://www.ibm.com/mobilefirst/us/en/>

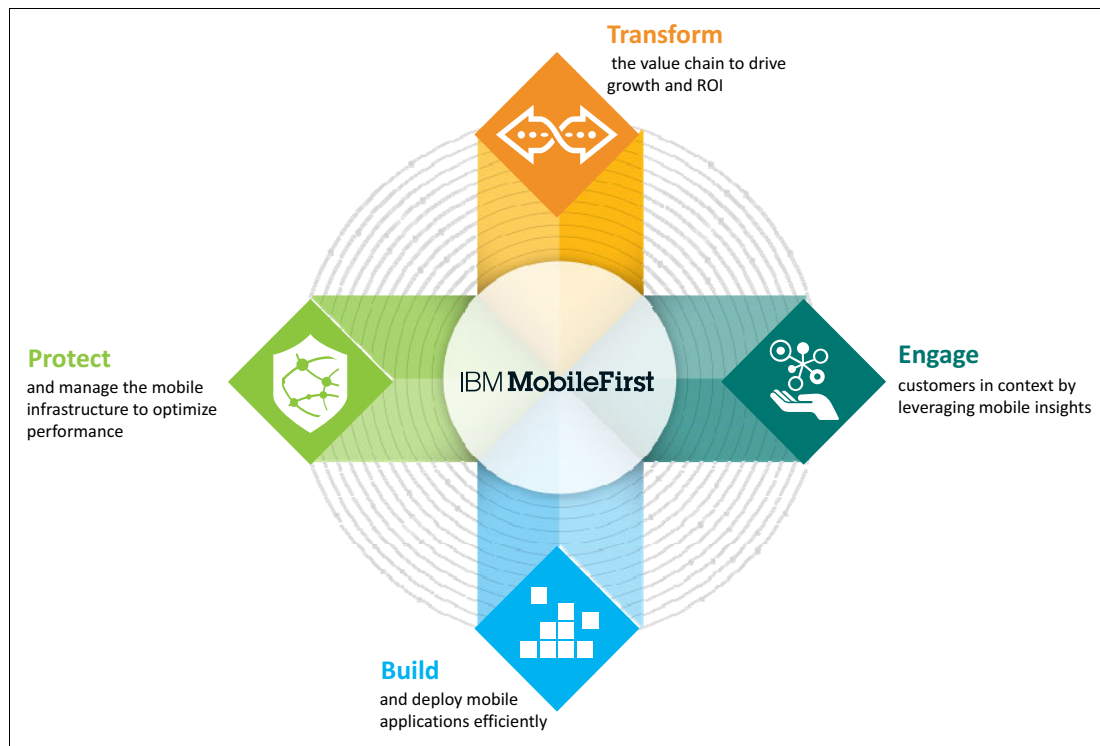


Figure 3-1 MobileFirst four-part strategic approach

As shown in Figure 3-2, the MobileFirst portfolio transforms businesses in a new way by introducing the following three core components:

- ▶ IBM MobileFirst Platform
- ▶ IBM MobileFirst Protect
- ▶ IBM Experience One

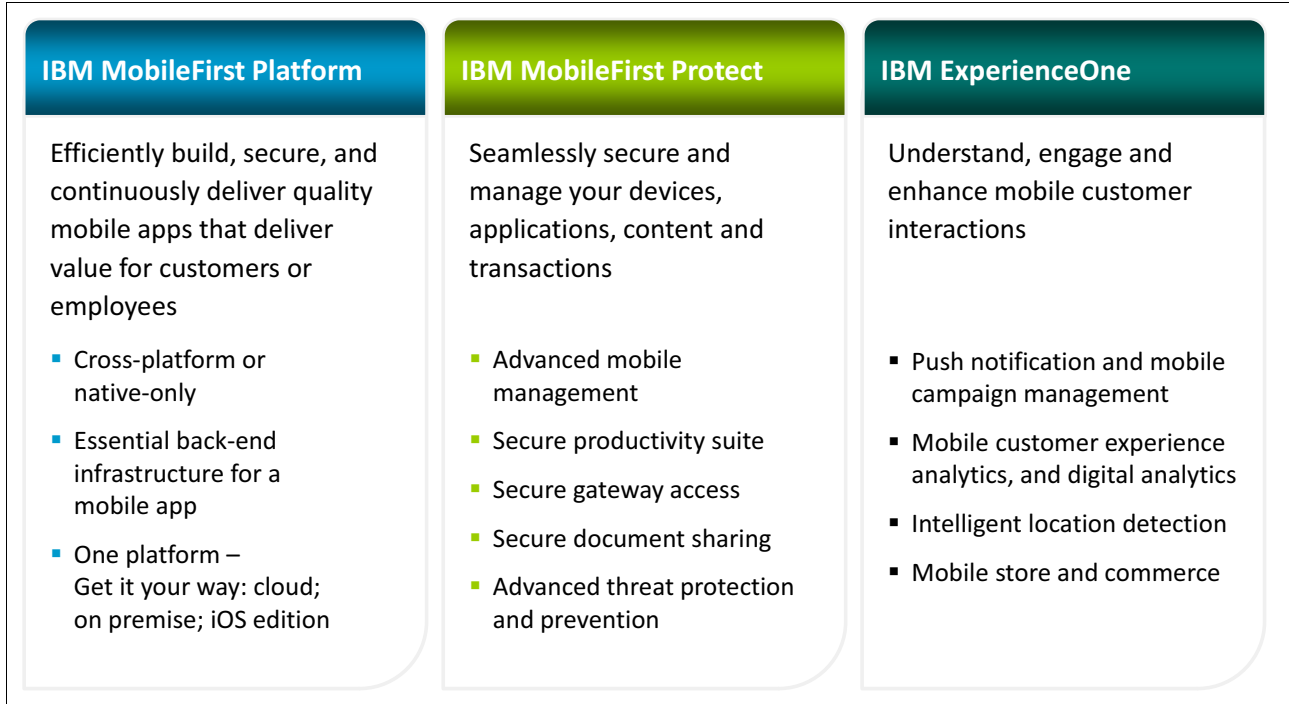


Figure 3-2 IBM MobileFirst portfolio

### 3.2.1 IBM MobileFirst Platform

IBM MobileFirst Platform is a mobile enterprise application platform that helps you deliver a superior user experience, whether coding native, web, or hybrid apps. Because it is based on open standards, the MobileFirst Platform enables rapid changes for new devices, platforms, operating systems, and capabilities.

MobileFirst can help governments to deliver a compelling mobile experience to its employees, partners, and citizens across many device types and operating systems. MobileFirst can enable governments to efficiently develop, connect, run, and manage mobile and omni-channel applications.

Governments are continuously looking for new ways to fully engage their citizens by extending network applications and web experiences, and connecting to back-end enterprise data. MobileFirst can help governments to build an agile and scalable approach to app development to rapidly deliver a superior user experience across multiple devices and platforms, by using the strongest native, hybrid, or web code. By building a single, cross-platform app, you can lower risk and reduce total cost while still delivering a rich mobile experience.

MobileFirst Platform offers different sets of products for different roles of application development, including the following products:

- ▶ IBM MobileFirst Platform Foundation, which is formerly known as IBM Worklight®, helps enterprises deliver on their mobile strategy. It provides an open and comprehensive platform to not only build, but test, run, and manage native, hybrid, and mobile web apps. Available as an on-premises or private cloud solution, MobileFirst Platform Foundation can help reduce both application development and maintenance costs, improve time-to-market, and enhance mobile application governance and security.

MobileFirst Platform Foundation consists of the following components:

- IBM MobileFirst Studio offers leading tools for mobile app development that help maximize code reuse and accelerate development.
- IBM MobileFirst Server is mobile-optimized middleware that serves as a gateway among applications, back-end systems, and cloud-based services.
- IBM MobileFirst Device Runtime Components offer runtime client application programming interfaces (APIs) that are designed to enhance security, governance, and usability.
- IBM MobileFirst Platform Cloudant® Data Layer Local is a database management system that is designed to support scaling demands and form an optimized data back end for mobile applications.
- IBM MobileFirst Application Center enables you to set up an enterprise app store that manages the distribution of production-ready mobile apps.
- IBM MobileFirst Console is an administrative GUI that is designed to provide real-time operational analytics for the server, adapters, and applications and push services to help manage, monitor, and instrument mobile apps.

With MobileFirst Foundation, you can perform these functions:

- Build apps for any mobile operating environment and device with your preferred development approach, including native, hybrid, or mobile web
  - Connect and synchronize mobile apps with enterprise data, applications, and cloud services, including IBM Bluemix™
  - Safeguard mobile security at the device, application, data, and network layer
  - Manage your mobile app portfolio from a single central interface with detailed operational analytics
  - Use scalable data services and your own development tools
- ▶ IBM Rational® Test Workbench provides a comprehensive test automation solution for mobile applications, regression testing, integration technologies and performance, and scalability testing. It helps you build intelligent and interconnected enterprise applications that can be deployed on traditional and cloud infrastructures. With Rational Test Workbench, you can significantly reduce test cycle times, moving integration testing earlier in the development lifecycle.

Rational Test Workbench delivers test automation for all types of applications, including mobile using a physical device or mobile emulator. It also offers these functions:

- Simplifies test creation with storyboard testing and code-free test authoring
- Allows you to quickly develop complex performance test scenarios with scriptless, visual, performance test, and workload models
- Provides earlier, end-to-end continuous integration testing throughout hardware, software, and cloud-based dependencies

- Emulates workloads accurately so that you can create a server workload that represents realistic user scenarios
- Is extensible and supports standards and protocols to help you meet the challenges of your testing environment

The following products, which are listed according to their categories, are available under the IBM MobileFirst Platform:

► App lifecycle:

- IBM MobileFirst Foundation (formerly known as IBM Worklight):  
<http://www-03.ibm.com/software/products/en/mobilefirstplatform>
- IBM MobileFirst Platform Application Scanning:  
<http://www-03.ibm.com/software/products/en/mobilefirst-platform-application-scanning>
- IBM MobileFirst Quality Assurance:  
<http://www-03.ibm.com/software/products/en/ibm-mobilefirst-quality-assurance>
- IBM Rational Test Workbench:  
<http://www-03.ibm.com/software/products/en/rtw>
- IBM Domino® Designer (formerly known as IBM Lotus® Domino Designer):  
<http://www-03.ibm.com/software/products/en/ibmdominodesigner>
- IBM UrbanCode™ Deploy:  
<https://developer.ibm.com/urbancode/>

► User experience:

- IBM Mobile Portal Accelerator:  
<http://www-03.ibm.com/software/products/en/ibmmobiportacce/>
- IBM Tealeaf® CX Mobile:  
<http://www-03.ibm.com/software/products/en/cx-mobile/>
- IBM MessageSight:  
<http://www-03.ibm.com/software/products/en/messagesight/>
- Xtify®:  
<http://www-01.ibm.com/software/info/xtify/>
- IBM WebSphere Cast Iron® Hypervisor Edition:  
<http://www-03.ibm.com/software/products/en/cast-iron-hypervisor>

► Cloud:

- IBM Bluemix:  
<https://console.ng.bluemix.net/>
- SoftLayer:  
<http://www.softlayer.com/>
- Cloudant:  
<https://cloudant.com/>
- IBM Cloud Orchestrator:  
<http://www-03.ibm.com/software/products/en/ibm-cloud-orchestrator>

- IBM Cloud Manager with OpenStack:  
<http://www.ibm.com/developerworks/servicemanagement/cvm/sce/index.html>
- IBM PureApplication® Service on SoftLayer:  
<http://www.ibm.com/developerworks/cloud/services.html>

### 3.2.2 IBM MobileFirst Protect

Remember when IT owned all of the equipment and software? Today, that environment is no longer realistic. Employees now bring their own mobile devices to work and use them for both personal and business activities. How do you optimize all of this equipment and software and safely provide access?

IBM MobileFirst Protect is a security and management platform for all of your assets. MobileFirst Protect protects and manages the mobile infrastructure to optimize performance and enable people to work anytime and anywhere. MobileFirst Protect provides trusted mobile interactions by adding greater security to your infrastructure and optimizing performance.

MobileFirst Protect seamlessly secures and manages devices, applications, content, and transactions with advanced mobile management, secure productivity suite, secure gateway access, secure document sharing, and advanced threat protection and prevention.

As shown in Figure 3-3, MobileFirst Protect integrates comprehensive security to enhance productivity on mobile devices and give organizations the confidence that their sensitive data is protected.

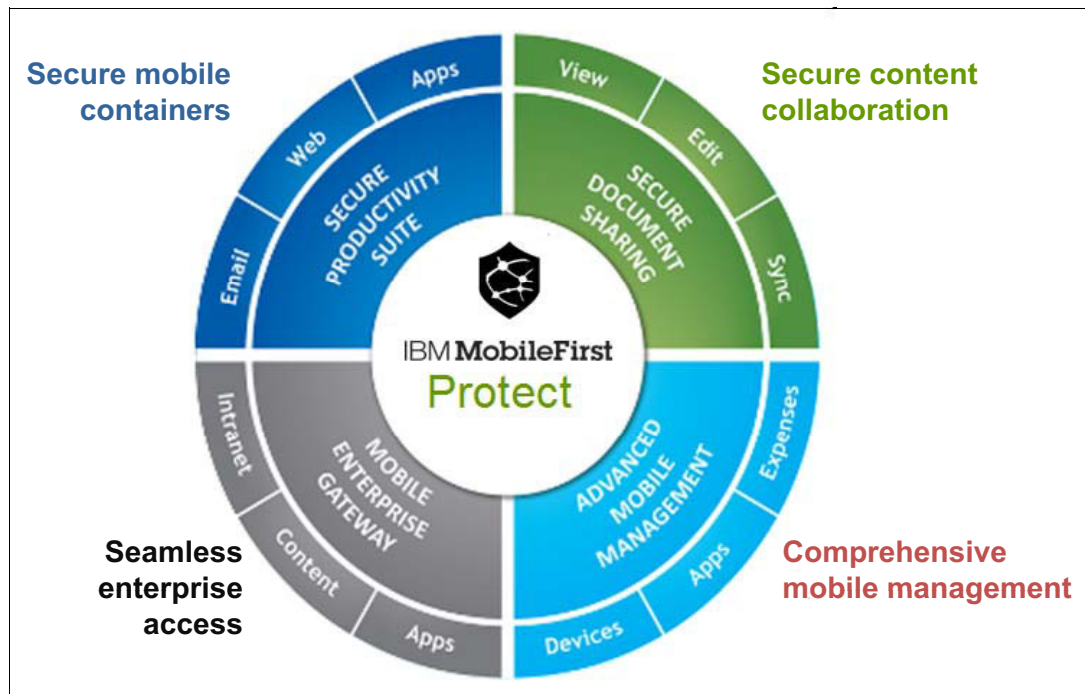


Figure 3-3 IBM MobileFirst Protect

There are four key solution bundles with MobileFirst Protect that provide for total enterprise mobility:

- ▶ The foundational IBM MobileFirst Protect Advanced Mobile Management enables organizations to manage and secure enterprise-owned and personal “bring your own” (BYO) smartphones, tablets, and notebooks. It simplifies deploying private and public apps by delivering an easy-to-use enterprise app catalog with full security and operational lifecycle management.
- ▶ IBM MobileFirst Protect Secure Productivity Suite™ delivers a comprehensive set of cross-platform solutions to isolate and contain work emails, web access, and app data to prevent data leaks. It is a complete solution that enables secure access to data while preserving the mobile experience on the mobile devices.
- ▶ IBM MobileFirst Protect Mobile Enterprise Gateway offers simple and secure access to behind-the-firewall business resources, such as SharePoint, Windows File Share, intranet sites, and databases.
- ▶ IBM MobileFirst Protect Secure Document Sharing provides a secure, encrypted container and productivity suite to distribute, view, create, edit, and share documents on mobile devices, giving organizations the control they need and employees the access they demand.

All of these services work together seamlessly and provide multiple layers of management and security, and granular-level policy options for you to configure.

MobileFirst Protect has various products to make your application secure and managed over the wireless networks. The following list describes several of these products:

- ▶ Fiberlink MaaS360®

Fiberlink is the trusted leader in enterprise mobility management from the cloud. Fiberlink, an IBM company, has over 20 years of experience in delivering enterprise mobility management and security solutions for organizations of all sizes. Thousands of clients rely on MaaS360 to accelerate deployment, reduce risk, increase employee productivity, and simplify mobile device management. MaaS360 by Fiberlink provides secure cloud-based mobile device management, mobile application management, mobile content management, and enterprise application container capabilities.

- ▶ IBM Trusteer

Trusteer is a leading provider of endpoint cyber crime prevention solutions that help protect organizations against financial fraud and data breaches. Trusteer solutions assist organizations that are trying to protect their clients and prospects from online fraud, and organizations that want to protect their employees from allowing corporate data to end up in the hands of those individuals with criminal intent.

Trusteer Fraud Protection Solutions deliver an intelligence-based, cyber crime prevention platform that helps prevent the root cause of fraud, reduces operational impact, improves your client’s experience, and uses a real-time intelligence service. Trusteer Fraud Protection Solutions helps organizations in the following ways:

- Stop malware and phishing-driven fraud
- Prevent account takeover attacks
- Control mobile channel risk

Trusteer helps protect against account takeover by providing compromised mobile device detection, complex device fingerprinting of mobile devices, and a global fraudster database.

- ▶ IBM Security Access Manager for Mobile

Security Access Manager for Mobile provides mobile access security protection in a modular package. It addresses mobile security challenges by proactively enforcing access policies for web environments and mobile collaboration channels.

Security Access Manager for Mobile is highly scalable and configurable. It is available as a virtual or hardware appliance and provides faster time to value and lower total cost of ownership.

- ▶ IBM Security Access Manager for Mobile

Security Access Manager for Mobile enables secure access to mobile and web applications with single sign-on (SSO) and session management. It improves identity assurance with built-in and flexible authentication schemes, such as one-time password (OTP) and Rivest-Shamir-Adleman algorithm (RSA) SecurID token support. Security Access Manager for Mobile enforces context-aware authorization by integrating with Trusteer Mobile software development kit (SDK) and supporting device fingerprinting, geographic location awareness, and Internet Protocol (IP) reputation techniques.

Security Access Manager for Mobile enhances security intelligence and compliance through integration with IBM Security QRadar® products and other software products. It provides flexible deployment and simplified configuration options through the modular access management platform called IBM Security Access Manager.

The following products are available under MobileFirst Protect:

- ▶ MaaS360:

<http://www.maas360.com/>

- ▶ IBM Security Access Manager:

<http://www-03.ibm.com/software/products/en/access-mgr-web>

- ▶ Security Trusteer family:

<http://www-01.ibm.com/software/security/trusteer/>

- ▶ IBM Security AppScan®:

<http://www-03.ibm.com/software/products/en/appscan>

- ▶ IBM Security QRadar Security Information and Event Management (SIEM):

<http://www-03.ibm.com/software/products/en/qradar-siem>

- ▶ IBM DataPower® Gateway:

<http://www-03.ibm.com/software/products/en/datapower-gateway>

- ▶ IBM Security Network Intrusion Prevention System:

<http://www-03.ibm.com/software/products/en/network-ips/>

- ▶ IBM Tivoli® Netcool/OMNIBus:

<http://www-03.ibm.com/software/products/en/ibmtivolinetcoolomnibus/>

### 3.2.3 IBM Experience One

IBM Experience One helps commerce managers and analytics managers drive mobile client engagement by understanding their clients, delivering relevant content and offers to them on mobile devices, and supporting seamless m-commerce.

ExperienceOne is a set of software capabilities supported by technology and services expertise to deploy and use in client engagement solutions. Their offerings include Tealeaf, Mobile Customer Engagement, Presence Zones, and WebSphere Commerce. These capabilities allow you to perform the following functions:

- ▶ Increase the opt-ins and “stickiness” of mobile apps via intelligent personalization and context-awareness
- ▶ Deliver fine-grained segmentation for optimal targeting with the ability to design and manage mobile campaigns
- ▶ Provide in-depth analysis of mobile app usage to facilitate the optimization of the mobile client experience
- ▶ Integrate with enterprise client data, as well as external information, such as the weather and location

With IBM ExperienceOne™, you can use the correct set of products to analyze raw data and obtain the right results. To achieve these capabilities, IBM offers a set of products to get the result that you want at run time:

- ▶ IBM Tealeaf CX Mobile:  
<http://www-03.ibm.com/software/products/en/cx-mobile>
- ▶ IBM Digital Analytics:  
<http://www-03.ibm.com/software/products/en/digital-analytics/>
- ▶ IBM eMessage:  
<http://www-03.ibm.com/software/products/en/email-marketing/>
- ▶ IBM MobileFirst Platform Presence Insights™:  
<http://www-03.ibm.com/software/products/en/ibm-mobilefirst-platform-presence-insights>
- ▶ IBM Customer Experience Suite:  
<http://www-03.ibm.com/software/products/en/ibmcustxpersuit>

For more information about IBM ExperienceOne, see the following website:

<http://www-01.ibm.com/software/marketing-solutions/experienceone/>

## 3.3 IBM MobileFirst reference architecture

IBM MobileFirst offers true end-to-end mobile solutions. Application development is more than writing an app. Application development involves users, device management, monitoring, security, integration, design, development, testing, and so on. The MobileFirst reference architecture provides details to help governments to accelerate their mobile journey by using an iterative approach to define an enterprise mobility strategy, architecture, and transformation.

### 3.3.1 Functional model

Figure 3-4 on page 52 displays the overall functional model of a mobile application development environment. The architecture shows how to manage the security, analytics, mobile management, and data management. The model works for any kind of mobile application, whether it is native or hybrid.



The functional model contains the following components:

- ▶ Mobile App Authoring covers all the behavior about the application lifecycle development.
- ▶ Mobile Management covers all the behavior about the mobile management of the application when the application is distributed over different geographical locations and networks.
- ▶ Mobile App Protection provides the entire feature that relates to mobile application protection over the device and the network.
- ▶ Mobile Analytics provides tools to analyze the raw data of the mobile application and user behavior.
- ▶ Mobile Secure Access helps to ensure the correct security so that no one can breach the mobile application.
- ▶ Mobile Secure Container is responsible for sharing the application over different channels.
- ▶ The Cloud, Internet, and Social data source component supplies the ability to deploy the application over a cloud network and connect the application user to other social networks for greater reach.
- ▶ Mobile application and data platform gives you the flexibility to store data in both SQL and non-SQL format. APIs are available to give you the ability to use the data in any context to connect the application to the enterprise data.

**Examples:** For examples of the mGovernment reference architecture in the context of three different sample mobile solution scenarios, see Chapter 4, “Reference architecture for the mGovernment solution implementation” on page 57.

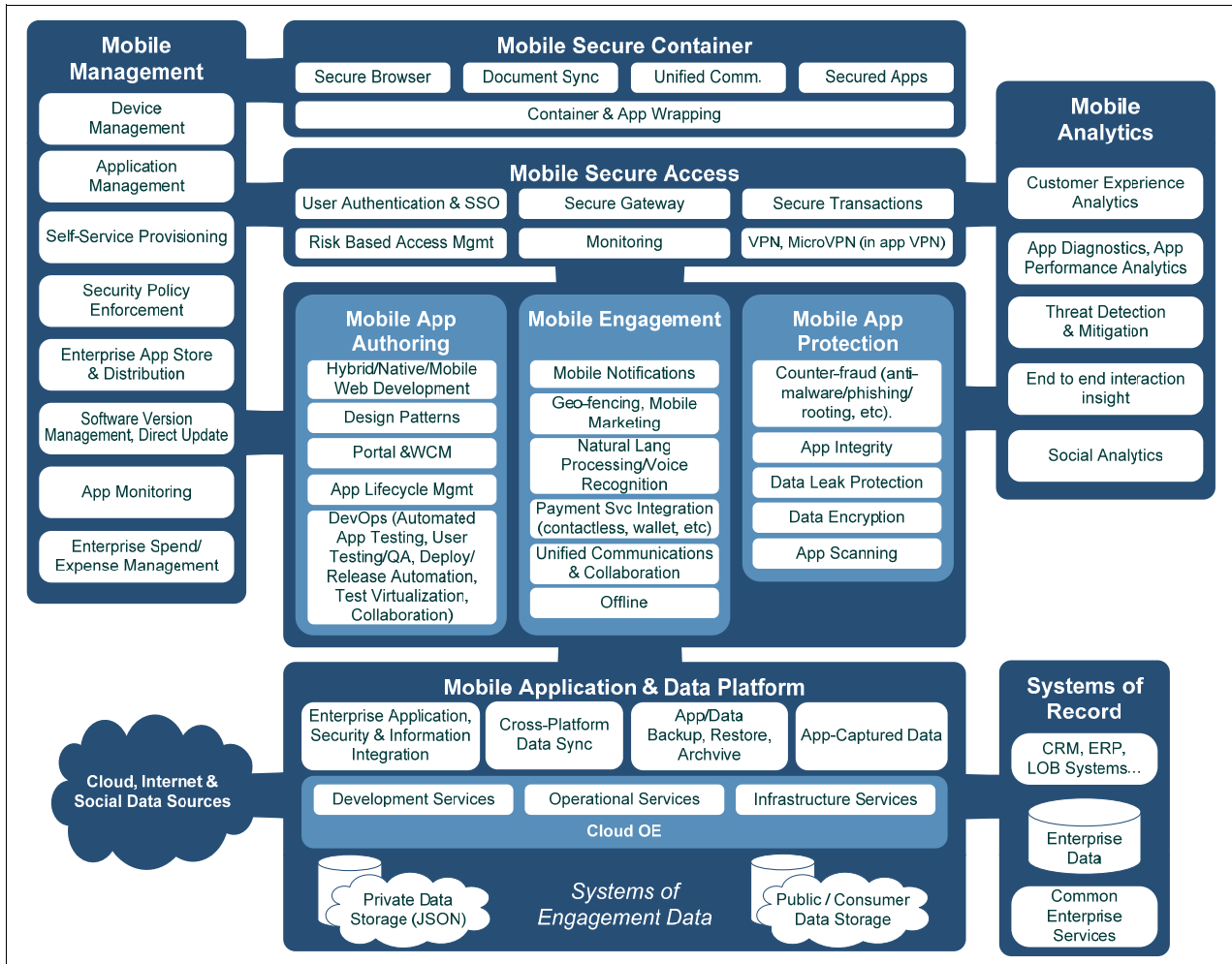


Figure 3-4 Functional model of the IBM MobileFirst reference architecture

### 3.3.2 Operational model

The operational model of the MobileFirst Architecture shows how the MobileFirst products can work with the different sets of products to provide the best-in-class application without compromising the best-of-breed security.

Figure 3-6 on page 55 provides a view of the operational model of the MobileFirst architecture.

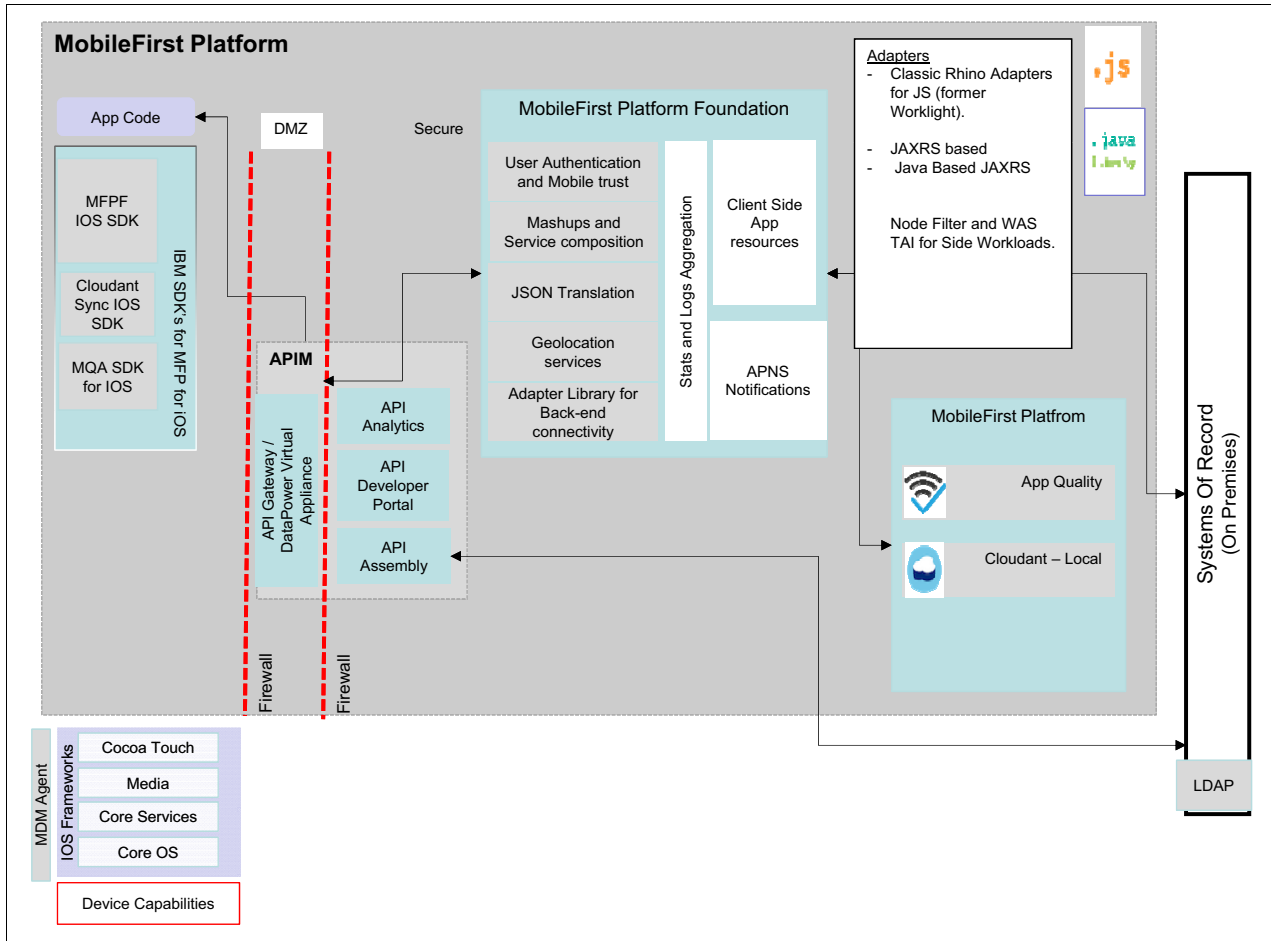


Figure 3-5 Operational model of the MobileFirst architecture

The IBM SDKs for MobileFirst Platform gives you flexibility to create applications for mobile operating systems, such as Android, iOS, and Microsoft Windows.

IBM MobileFirst Platform SDK for iOS allows you to develop native applications for iOS devices. With MobileFirst Platform SDK for iOS, you can integrate the application with different SDKs, such as Cloudant, to build and deploy in the cloud. Optimized for iOS, IBM MobileFirst Software Services includes several essential functions, such as security, data and analytics integration, workflow control, and end-to-end device management. MobileFirst Platform Foundation can be used for user authentication and mobile trust through Lightweight Directory Access Protocol (LDAP).

The application can be integrated with any type of services by using various adapters. The adapters deploy on the server, out of reach of the application user, therefore providing enterprise-level security. The server also gives you flexibility to change the services without any knowledge of the app users and without compromising the security. It is easy to deploy the adapters on the cloud with the new Cloudant API.

Security is provided over the adapter transaction through integration with LDAP. To secure the transaction over the DMZ network, use the IBM WebSphere DataPower Virtual Appliance or API gateway.

Push notification and Short Message Service (SMS) features are integrated into the MobileFirst Foundation. The API gives you flexibility to connect to Apple Push Notification service (APNS), Google Cloud Messaging (GCM), or other SMS gateway servers with minimum coding.

**Examples:** For examples of the mGovernment reference architecture in the context of three sample mobile solution scenarios, see Chapter 4, “Reference architecture for the mGovernment solution implementation” on page 57.

## 3.4 IBM MobileFirst enterprise app lifecycle

Figure 3-6 on page 55 displays the complete lifecycle of a mobile application. The IBM Mobile Enterprise Development Lifecycle codifies a set of preferred practices for mobile project teams. This framework is theoretical; therefore, not all organizations undertake all of these activities for each project. However, this framework is a way of thinking about the continuous development of mobile apps and applying the same discipline to this lifecycle that you apply to any critical business process.

The following steps are in this lifecycle:

1. **Design.** Start with designing the user experience, optimally by using an outside-in approach.
2. **Develop.** Design the architecture and develop the application by using a cross-platform development approach that maximizes code reuse.
3. **Instrument.** Instrument the application for analytics, security, and management control.
4. **Integrate.** Integrate with back-end data, systems, and cloud services.
5. **Test.** Test the application.
6. **Certify.** Use a vulnerability analysis tool to scan, evaluate, and certify your application.
7. **Deploy.** Distribute the applications by using a combination of internal and external app stores.
8. **Manage.** Manage authentication, enforced updates, and versions.
9. **Obtain insight.** Analyze and improve the effectiveness of your application design by viewing detailed client usage patterns.



Figure 3-6 Lifecycle of a mobile application





# Reference architecture for the mGovernment solution implementation

This chapter describes several key challenges that are faced by an mGovernment and then explains the reference architecture for mGovernment solutions. The chapter explains the mGovernment reference architecture in the context of three mobile solution scenarios.

The following topics are covered in this chapter:

- ▶ 4.1, “Key challenges for mGovernment” on page 58
- ▶ 4.2, “Reference architecture for mGovernment” on page 59
- ▶ 4.3, “Applying the reference architecture to mobile solutions” on page 65

## 4.1 Key challenges for mGovernment

The most common challenges to be addressed by any mGovernment in addition to existing mobile solutions are described:

- ▶ Privacy and security

Privacy and security are significant concerns that citizens have about mGovernment. The general fear is that their mobile phone numbers are traced when they send transactions or their opinions and inquiries to the government. The government and related parties must overcome this mistrust and assure mobile users that people's privacy is protected and that the information will not be sold to third parties. Strong security is even more important to for transactional applications that handle sensitive data or enable mobile voting. The following areas need special focus:

- User authentication: A lack of a robust user identity authentication mechanism that complies with federal mandates and maintains mobile device ease of use
- Data encryption: A growing need for validated, secure, and efficient cryptography that is suitable for mobile devices
- Application security testing and evaluation: A lack of automated tools for efficient assessment and authorization of mobile applications
- Device sanitization: A lack of agency processes and tools to follow requirements on device sanitization

- ▶ Infrastructure challenged

The most common technical challenges to mGovernment development and dissemination involve a lack of infrastructure. This problem is evident in developing countries. The mGovernment infrastructure consists of wireless networks and mobile access devices, for example, mobile phones, notebooks, and personal digital assistants (PDAs), and accessing software services. However, many countries are struggling with connectivity problems.

- ▶ Accessibility

mGovernment applications must have a provision for equal services to all citizens, regardless of their physical, mental, or technical capabilities. The accessibility challenges that are associated with the use of mobile devices imply that certain services might not be suitable for consideration as part of the mGovernment agenda. MGovernment must ensure that services and benefits are available to all citizens equally.

- ▶ Integration and compatibility

The primary challenges for integration with existing mGovernment solutions are how to pull data from a server-side system and how to represent data on the mobile device. These challenges are compounded in older systems. Key considerations include the requirements for connectivity, security, data integrity, and devices.

- ▶ Payment infrastructures

A first obstacle for consumers to buy online is a feeling of mistrust in sending their credit card information over the mobile phone or the Internet. In developing countries, though, another problem, low credit card penetration, precedes that issue. The number of people with credit cards is too small in comparison to the number of potential users for mGovernment transactions.



- ▶ Interoperability and collaboration
 

Mobile technologies must not only be secure, but they must be compatible across many platforms. Interoperability, which allows an agency to share information with other agencies, is paramount. The benefits of interoperability include increased effectiveness, efficiency, and responsiveness. The ability of agencies to work together technologically can mean a reduction in the redundancy in the government. The implementation of mGovernment requires inter-governmental, inter-agency, and private sector collaboration.
- ▶ Timeliness (data freshness and service expediency)
 

The basis for mGovernment relies on how quickly relevant data can be shared within the various entities. *Data freshness* implies that the information that is seen by the citizens or government is new.
- ▶ Reliability
 

mGovernment must strive to maintain a constant level of availability and quality. Citizens must be able to obtain information and rely on fundamental services, even in dire circumstances, for example, natural disasters.
- ▶ Location-aware applications
 

The use of the Global Positioning System (GPS) and other technologies, for example, Bluetooth or radio beacons, is another challenge for mGovernment applications to tailor applications to a specific location. The citizen or government employee must be able to access specific information about the services, facilities, and requirements in the immediate area.
- ▶ Legal aspects and standardization
 

Many countries do not yet recognize the Law of Fair Information Practices, which defines the rights of data subjects (citizens) and the responsibilities of data holders (government). In specific cases, the law does not recognize mobile documents and transactions. No clear legal status exists for the government's online publications, and no regulations and laws exist for online filings, online signings, and online taxable transactions.

## 4.2 Reference architecture for mGovernment

This section addresses the reference for mGovernment in terms of the following types of views:

- ▶ 4.2.1, "Notional view" on page 59
- ▶ 4.2.2, "Functional view" on page 61
- ▶ 4.2.3, "Operational view" on page 62
- ▶ 4.2.4, "IBM technology view" on page 63

### 4.2.1 Notional view

The reference architecture for mGovernment depicts mGovernment as more than a channel for delivering citizen services and conducting the business of government. The reference architecture for mGovernment is also a platform for an entirely new set of government services. These services use the new features that are offered by mobile technologies, such as ease of access, ubiquity, location or context awareness, and digital recording functions.

The core government business objectives and the service delivery context remain the same for mGovernment as for traditional government services. Most of the government to citizen (G2C), government to employee (G2E), and government to government services that are conducted digitally via eGovernment can be converted as mobile apps for the mobile platform. For a description of G2C, G2E, and G2G, see 1.3, “mGovernment interactions” on page 10.

The constraints and requirements are also the same for mGovernment, such as compliance to regulations and standards. However, mGovernment uncovers a new set of opportunities that were not available on eGovernment or the traditional brick-and-mortar services. The following opportunities for mGovernment are new:

- ▶ Challenged environment. The ability to reach out to rural areas where IT infrastructure might be lacking.
- ▶ Responsiveness/emergency. The ability to establish real-time communications and deliver basic services quickly.
- ▶ Transparency. With the relatively low barrier of entry for developing mobile applications, the responsibility of the government shifts from owning the application to owning the data and exposing this data for mobile application consumption in a self-service model.
- ▶ Cost reduction. With employee mobility and ubiquitous access to the work environment, government business processes are accelerated and more efficient. Similarly, with mobile citizen participation and self-service access to government resources, backlogs are reduced significantly.

The infrastructure components for mGovernment are also the same as eGovernment, such as security, operational support, and DevOps. However, these infrastructure components might be carried out and implemented a bit differently:

- ▶ Security. Special attention is paid to data security and identity access management mainly for G2E applications. Security is supplemented by a strong mobile device management (MDM) component for policy enforcement.
- ▶ Support. Event tracking, monitoring, and reporting are key to responsiveness and continuous delivery in mGovernment.
- ▶ DevOps. Developing and testing for multi-platform devices can be daunting. Context awareness and security need to be incorporated into the application design.

Mobile services, the core infrastructure component in mGovernment, covers the following key aspects of mobility:

- ▶ Devices. These devices need to be managed in terms of provisioning/deprovisioning and usage policy.
- ▶ Users. Mobile analytics provide insights into the user experience.
- ▶ Data. Mobile application programming interfaces (APIs) expose government data to the mobile developers.
- ▶ Apps. These apps need to be managed during their lifecycles, consumption and download, and run time.

Figure 4-1 on page 61 depicts this notional or contextual architectural view of mGovernment.

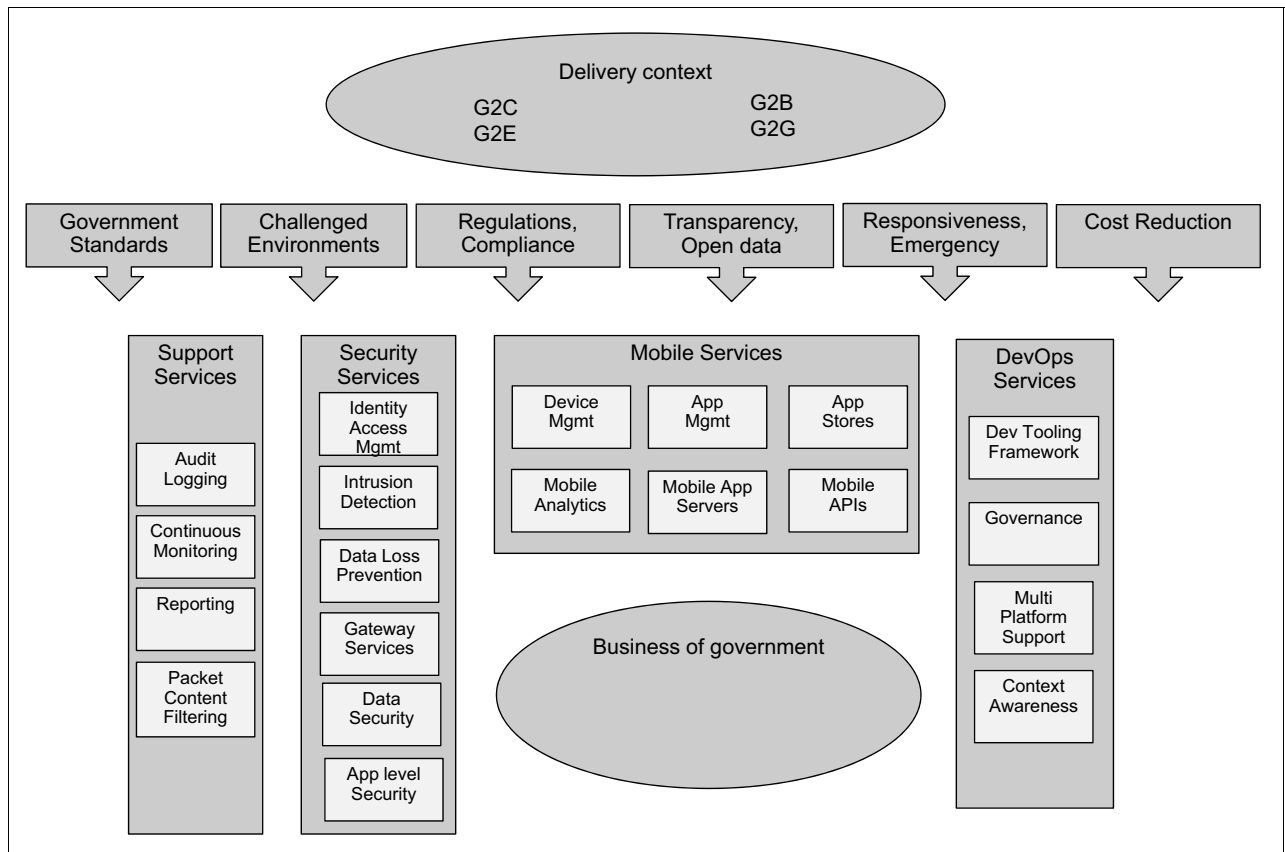


Figure 4-1 mGovernment notional reference architecture view

## 4.2.2 Functional view

Figure 4-2 on page 62 shows a functional view of a generic mGovernment environment. A broad set of functional capabilities for an mGovernment environment is required, including the following functional capabilities:

- ▶ Mobile application gateway (MAG)
- ▶ Identity and access management (IAM)
  - Public key infrastructure (PKI) certificate management
- ▶ Mobile device management (MDM)
- ▶ Mobile application management (MAM)
- ▶ Mobile application store (MAS)
- ▶ Mobile application server (MASvr)
  - API management (API)
- ▶ Data security
- ▶ Mobile application development (MAD)
- ▶ Analytics, security, and event management (SIEM)

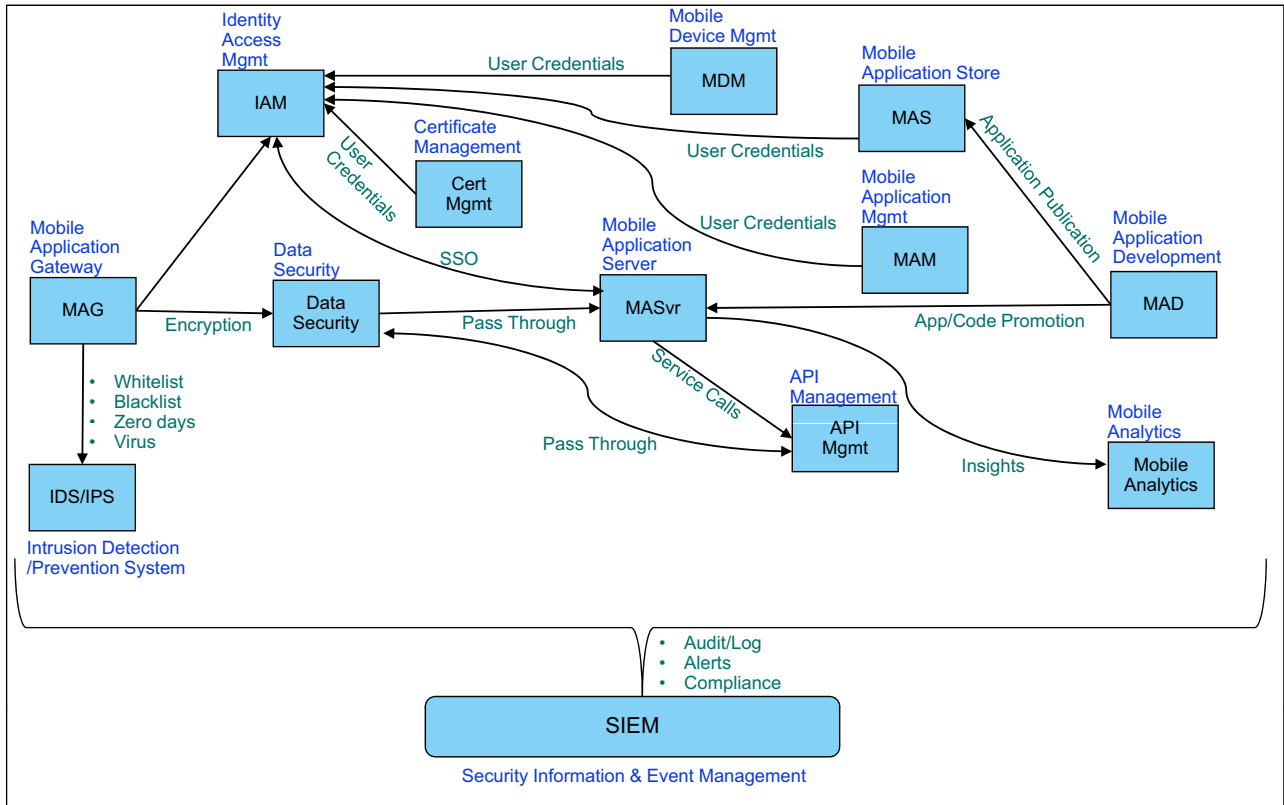


Figure 4-2 Functional view

As shown in Figure 4-2, many of these functional components have interdependencies with other functions:

- ▶ The mobile application gateway application provides specific network security for the mobile application infrastructure interfaces with the IAM, data security, and intrusion detection components.
- ▶ The IAM component provides services or uses services interfaces with the MDM, MAS, MAM, and the certificate management server.
- ▶ The MASvr uses services from the API management components and any other enterprise application infrastructure to provide services to the users.
- ▶ With in-house application development, the MAD components likely interface with MAS and MASvr.
- ▶ The SIEM components are used across various functional components by providing security, intrusion detection, and event management services.

### 4.2.3 Operational view

A typical mGovernment operational view is shown in Figure 4-3 on page 63.

This view is no different from many the typical eGovernment environments. Figure 4-3 on page 63 depicts the placement of functional components. Parts of several of the components, such as IAM and MAS, are often in the DMZ. In addition, isolation of the data in the data tier is suggested, although this isolation is not shown explicitly.

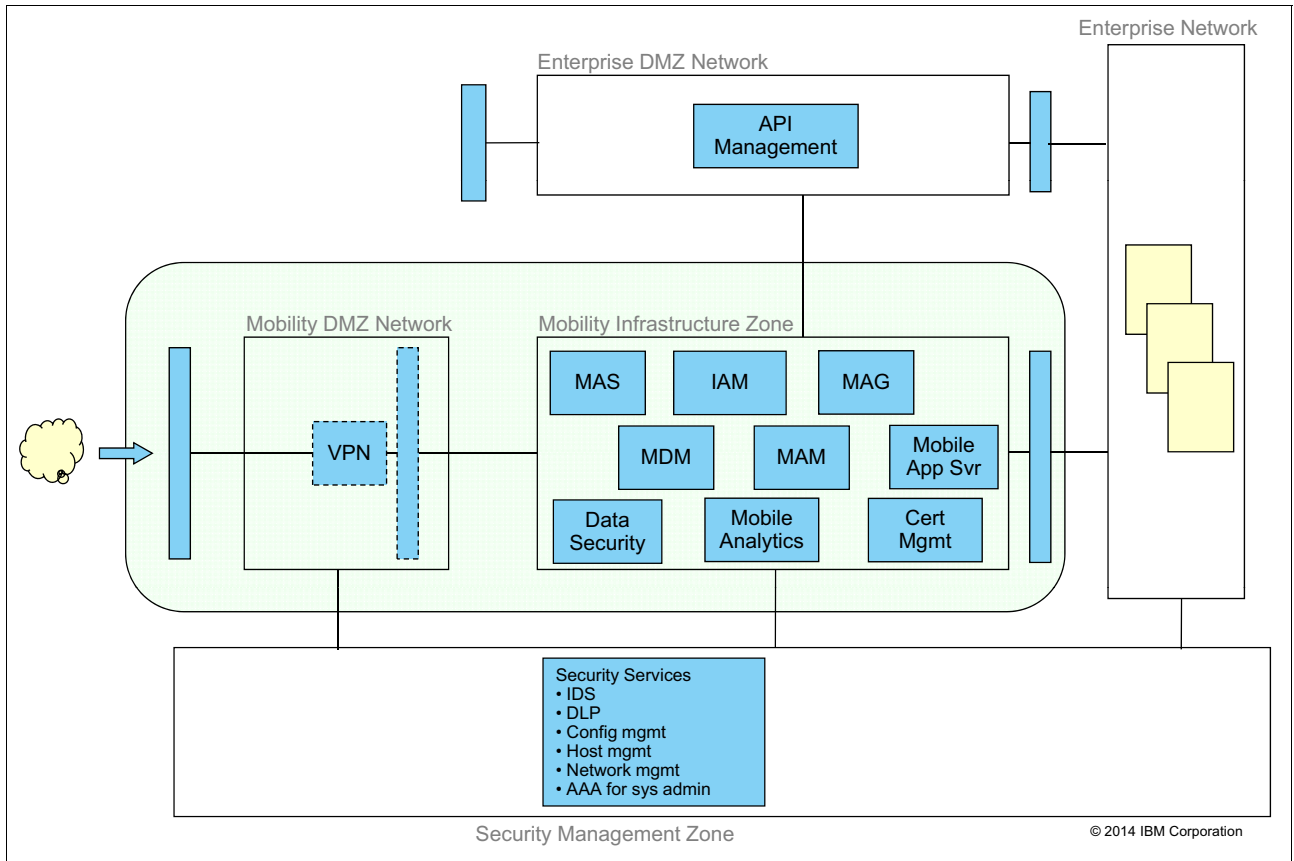


Figure 4-3 Physical view

#### 4.2.4 IBM technology view

Figure 4-4 on page 64 shows the IBM technology view that maps to the functional view.

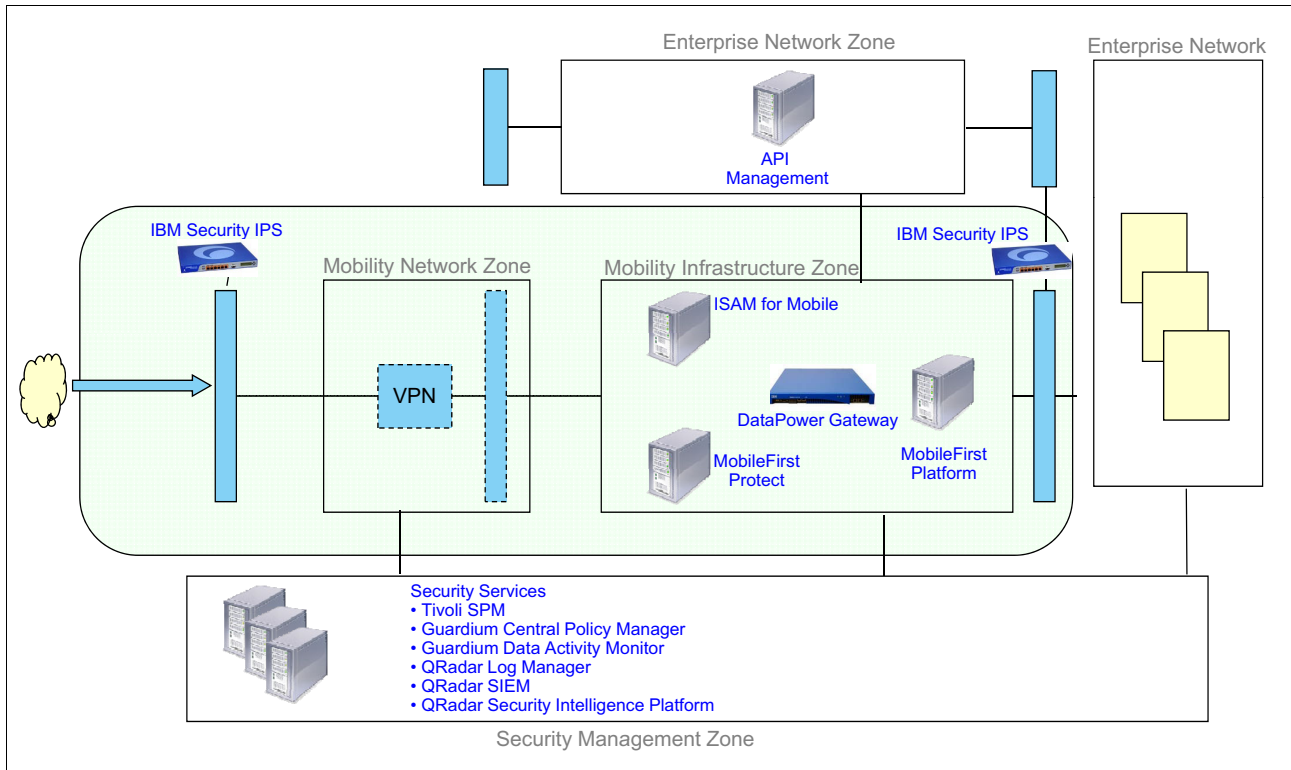


Figure 4-4 Technology view

A comprehensive array of IBM products is available to meet the needs of an mGovernment environment. At a high level, the following broad categories of products are used for a typical mGovernment environment:

- ▶ Mobile development
- ▶ Mobile application server
- ▶ Mobile device management
- ▶ Mobile application management
- ▶ Mobile application store
- ▶ Identity and access management
- ▶ Security

Because products evolve, up-to-date information about IBM products to meet the needs of mGovernment is available at the links that are listed in Table 4-1.

Table 4-1 Links to IBM mobile-related products and solutions

Functional category	URL
IBM product finder	<a href="http://www.ibm.com/software/products">http://www.ibm.com/software/products</a>
Mobile development and connectivity	<a href="http://www.ibm.com/software/products/en/category/mobile-application-development">http://www.ibm.com/software/products/en/category/mobile-application-development</a>
Mobile integration of data and applications	<a href="http://www.ibm.com/software/products/en/category/mobile-data-application">http://www.ibm.com/software/products/en/category/mobile-data-application</a>
API management	<a href="http://www.ibm.com/software/products/en/api-management">http://www.ibm.com/software/products/en/api-management</a>
Mobile management and security	<a href="http://www.ibm.com/software/products/en/category/SW500">http://www.ibm.com/software/products/en/category/SW500</a>

Functional category	URL
<b>Security</b>	
Mobile device management	<a href="http://www.ibm.com/marketplace/cloud/enterprise-mobility-management/us/en-us">http://www.ibm.com/marketplace/cloud/enterprise-mobility-management/us/en-us</a>
Identity and access management	<a href="http://www.ibm.com/software/products/en/category/identity-access-management">http://www.ibm.com/software/products/en/category/identity-access-management</a>
Mobile application security	<a href="http://www.ibm.com/software/products/en/category/application-security">http://www.ibm.com/software/products/en/category/application-security</a>
Data security and privacy	<a href="http://www.ibm.com/software/products/en/category/data-security">http://www.ibm.com/software/products/en/category/data-security</a>
Security intelligence and analytics	<a href="http://www.ibm.com/software/products/en/category/security-intelligence">http://www.ibm.com/software/products/en/category/security-intelligence</a>
Advanced fraud protection	<a href="http://www.ibm.com/software/products/en/category/advanced-fraud-protection">http://www.ibm.com/software/products/en/category/advanced-fraud-protection</a>
Advanced security and threat protection (not a product)	<a href="http://www.ibm.com/software/security/adv-security-threat-protection/">http://www.ibm.com/software/security/adv-security-threat-protection/</a>

## 4.3 Applying the reference architecture to mobile solutions

This section applies the mGovernment reference architecture to the following three mobile scenarios. We selected these use cases to cover a wide cross section of potential government mobile solutions:

- ▶ Use case 1 (4.3.1, “Use case 1: Car registration renewal” on page 650) is an interactive mobile solution that is transactional and illustrates a combination of G2C and G2E scenarios.
- ▶ Use case 2 (4.3.2, “Use case 2: Farming application” on page 70) is an interactive mobile solution that addresses the challenged environment and push capabilities. It illustrates a G2B scenario.
- ▶ Use case 3 (4.3.3, “Use case 3: First responder” on page 74) is a situational mobile solution that is collaborative in nature and set up to manage an emergency. It covers both the G2G and G2E scenarios.

Each use case uses the base MobileFirst reference architecture for public sector and adds or removes capabilities.

### 4.3.1 Use case 1: Car registration renewal

Table 4-2 on page 66 provides the details for reference use case 1, which is a mobile application for car registration renewal.

Table 4-2 Reference use case 1 description for the car registration renewal

<b>Use case name</b>	Renewal of registration or re-registration of a non-commercial vehicle.
<b>Brief description/scope</b>	The Department of Transportation decided to support mobile devices for non-commercial vehicle registration and renewals.
<b>Actors</b>	<ul style="list-style-type: none"> <li>▶ Citizen</li> <li>▶ Regional Transportation Office - Manager (Government employee)</li> <li>▶ Regional Transportation Office - Field agent (Government employee)</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>▶ Reduces operating costs and improves customer satisfaction</li> <li>▶ Increases on-time responses and job completions</li> <li>▶ Reduces travel distance, vehicle emissions, and missed appointments</li> <li>▶ Improves productivity and decreases field agent hours and overhead</li> </ul>
<b>Normal flow</b>	<ol style="list-style-type: none"> <li>1. The citizen completes the reregistration form by using a mobile app, pays the registration fee, and submits the form.</li> <li>2. The citizen uploads scanned copies of their registration certificate, emission certificate, and valid insurance by using the upload documents feature in the mobile app. Note: Documents are uploaded only when a Wi-Fi signal is available; otherwise, the documents reside on the mobile device.</li> <li>3. The submission of the documents invokes a business process that appoints a field supervisor. The Short Message Service (SMS) notification is sent to both the citizen and field inspector.</li> <li>4. Field inspector logs in to the mobile task map app and checks the citizen locality and other details, visits the citizen location, monitors the vehicle's condition, and updates the data on the central Department of Transportation server.</li> <li>5. The business process for approval/rejection is invoked after the data submission by the field agent. The business process applies certain rules based on the information that is provided by the citizen and the field agent. The business process provides the approval for registration and notifies the citizen via SMS.</li> <li>6. The citizen, upon the receipt of the SMS, logs in to the mobile app and can view the registration certificate. The transportation department sends the registration certification sticker within seven working days after the approval.</li> </ol>
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>▶ A citizen needs to have a smartphone with a data connection.</li> <li>▶ A citizen needs to have a valid credit or debit card.</li> <li>▶ The inspection of the vehicle is carried out on working days between 10:30 am and 3:30 pm.</li> <li>▶ The government uses the "bring your own device" (BYOD) policy for its employees.</li> <li>▶ The device that is used by the government employee needs to be a smartphone with camera capabilities.</li> </ul>
<b>Post condition</b>	<ul style="list-style-type: none"> <li>▶ A citizen's vehicle is registered. The citizen can view the registration certificate on the mobile app.</li> <li>▶ The citizen receives a registration certification sticker within seven working days after the approval.</li> </ul>

### Implementation architecture

This use case implementation uses two mobile applications:

- ▶ G2C. Bidirectional communication between the government and the citizen (transactional services). This application is a mobile wrapper over the existing eservice for online form submission and registration fee payment.
- ▶ G2E. Bidirectional communication between the government and the employee (connected). This hybrid application is used by the employee to check for appointments, a schedule, the form for the inspection of the vehicle, and a route finder.



Figure 4-5 shows the physical operational view for this use case. This view is derived from the convergence of the reference architecture for mGovernment (see 4.2.3, “Operational view” on page 62) and this use case’s requirements.

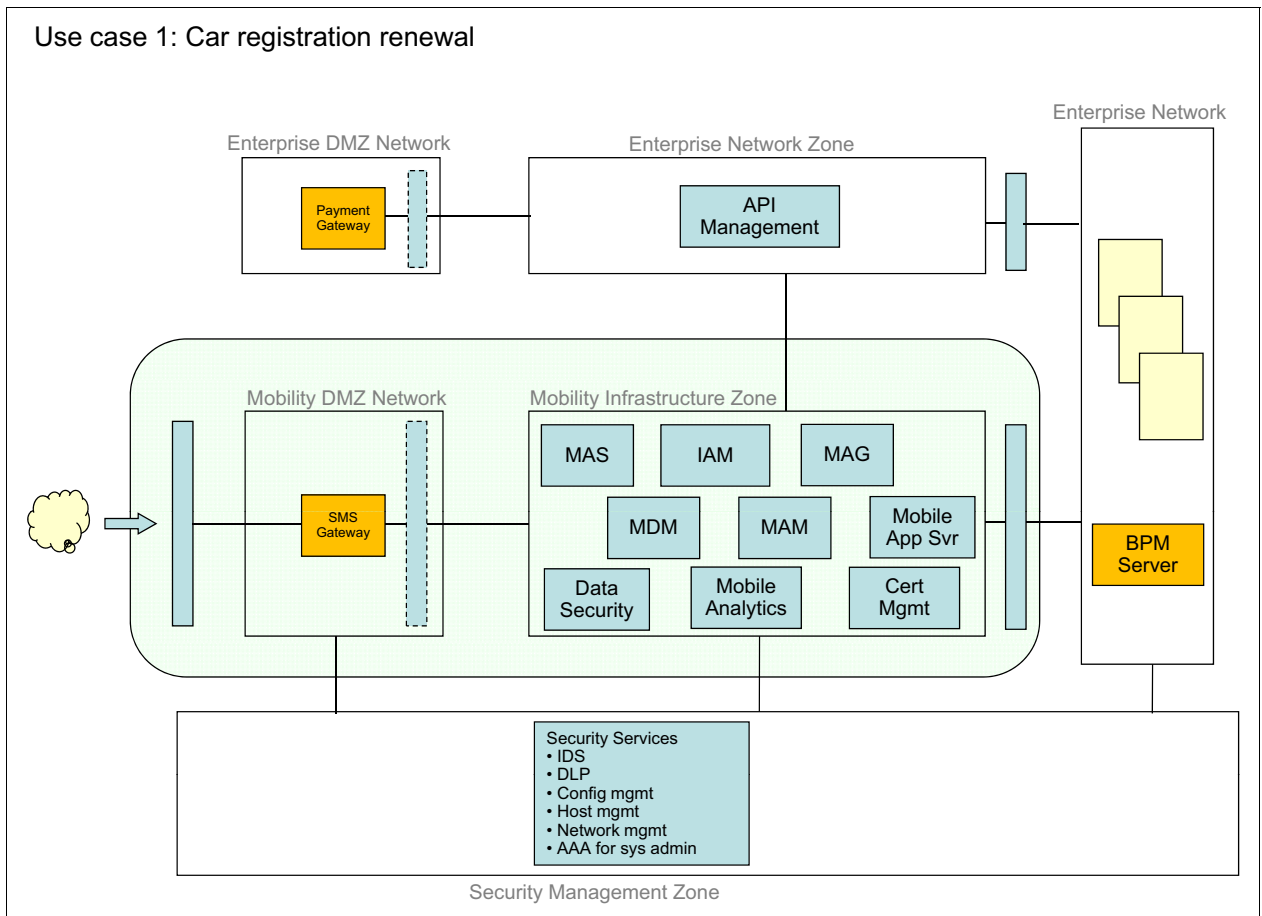


Figure 4-5 Use case 1 operational view

Figure 4-6 shows the application flow and components that are used for the vehicle registration renewal scenario.

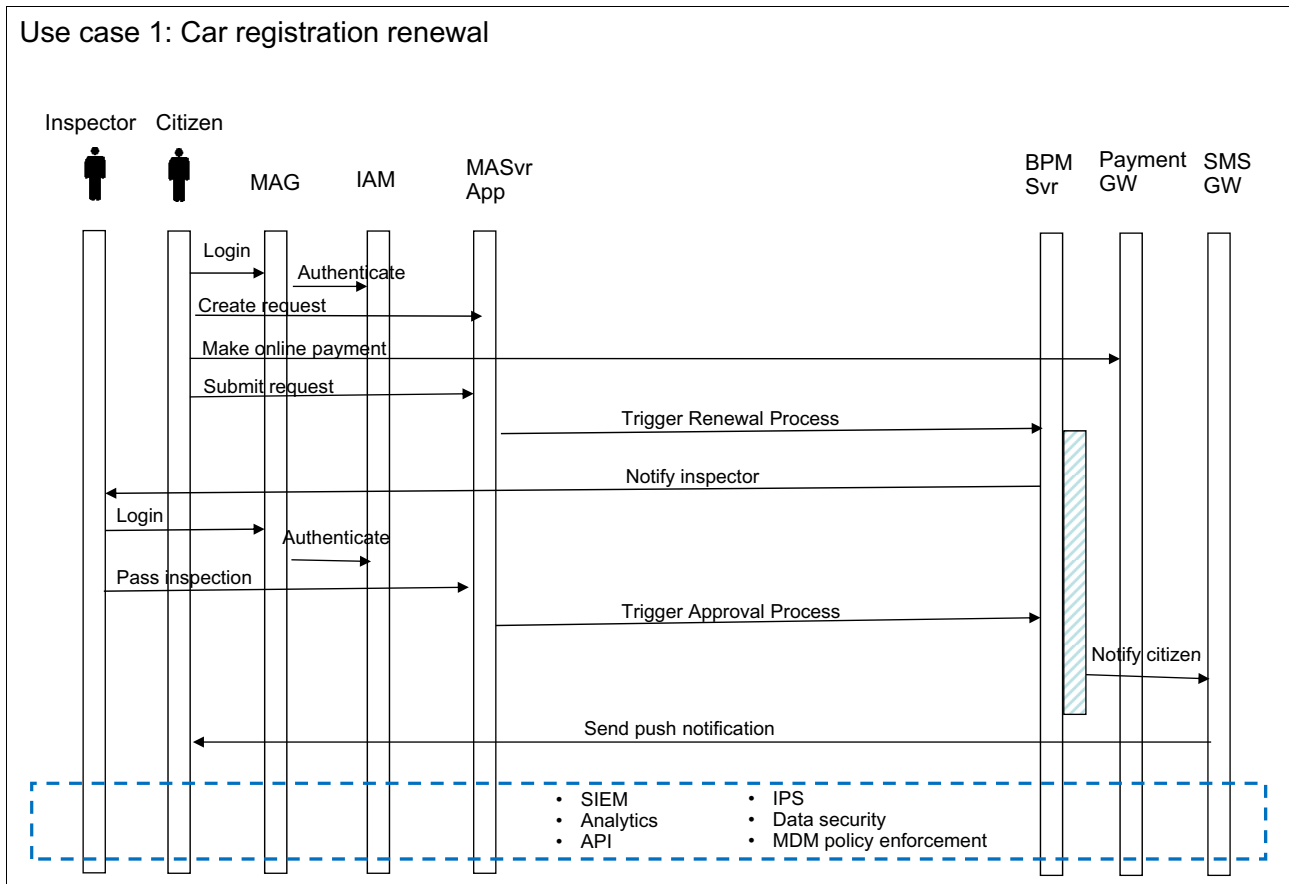


Figure 4-6 Use case 1 application flow and components used

The steps that are listed in Table 4-3 describe the basic flow of this use case as shown in Figure 4-6. These steps depict the mobile components that interact to provide the required services for the actors in this scenario.

Table 4-3 Reference use case 1 detailed steps

Mobile component	Step 1: The citizen logs in, creates the request, makes the payment, and submits the request.	Step 2: The back end processes the request and detects the need for inspection.	Step 3: The inspector logs in, gets the task, inspects the vehicle, and submits a passing report.	Step 4: The back end processes the request that is granted and gets the final approval.	Step 5: The push notification is sent to the citizen.
IAM	Authenticate.		Authenticate.		
Mobile GW	Challenge and authenticate.		Challenge and authenticate.		
Mobile app on app server	Request user interface and payment handoff.	Trigger request approval process.	Inspection user interface.		

<b>Mobile component</b>	<b>Step 1: The citizen logs in, creates the request, makes the payment, and submits the request.</b>	<b>Step 2: The back end processes the request and detects the need for inspection.</b>	<b>Step 3: The inspector logs in, gets the task, inspects the vehicle, and submits a passing report.</b>	<b>Step 4: The back end processes the request that is granted and gets the final approval.</b>	<b>Step 5: The push notification is sent to the citizen.</b>
Business Process Manager (BPM) engine		Run request processing flow.	Detect need for inspection and send email notification to inspector.	Run request granted flow and final approval flow.	Prepare a push notification message for requesting citizen.
Payment GW	Process online payment.				
SMS GW					Send push notification message.
MAM	Citizen downloads vehicle registration app.		Inspector downloads car inspection app.		
MAD	Code, test, and deploy vehicle registration renewal app.		Code, test, and deploy car inspection app.		
MDM	Enforce device policies during user session.		Enforce device policies during user session.		
Certification management	Validate credentials.		Validate credentials.		
Mobile APIs	Calling payment GW APIs.		Calling email APIs.		Calling SMS GW APIs.
Mobile analytics	Collect user experience data.		Collect user experience data.		
SIEM	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.
Intrusion prevention	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.
Data security	Encrypt data in transit.		Encrypt data in transit.		

Table 4-4 on page 70 lists the interactions among the mobile device, IBM MobileFirst, and Business Process Manager (BPM) for this use case.

Table 4-4 Interaction patterns for use case 1

<b>Interaction pattern (with flow type)</b>	Mobile device <-> IBM MobileFirst	BPM <-> IBM MobileFirst
<b>Interaction patterns between BPM and MobileFirst</b>	HTTP/S call from the mobile device to the IBM MobileFirst server.	Use of Java Message Service (JMS) to initiate the process from IBM MobileFirst to BPM.
<b>Interaction pattern (with flow type)</b>	IBM MobileFirst notifies the mobile device by using an available push notification scheme.	BPM triggers a notification event to IBM MobileFirst over HTTP.
<b>Inbound: Invoking a long-running process</b>	HTTP/S call from the mobile device to the IBM MobileFirst server.	HTTP/S call from the mobile device to the IBM MobileFirst server.
<b>Outbound: Updating user of status of a long-running process</b>	HTTP/S call from the mobile device to the IBM MobileFirst server.	Use of JMS to initiate the process from MobileFirst to BPM.

### 4.3.2 Use case 2: Farming application

Table 4-5 provides the details for reference use case 2, which is a farming application.

Table 4-5 Reference use case 2 description for the farming application

<b>Use case name</b>	Mobile farming registration program.
<b>Brief description/scope</b>	The government established an agriculture (farming and breeding) program. A farmer, breeder, or business owner can participate in the government agriculture program.
<b>Actors</b>	<ul style="list-style-type: none"> <li>▶ Farmers and breeders</li> <li>▶ Agriculture department</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>▶ Infrastructure-challenged mobility access</li> <li>▶ Information dissemination</li> <li>▶ Transactions between government and businesses or citizens and vice versa</li> </ul>
<b>Normal flow</b>	<ol style="list-style-type: none"> <li>1. To participate in the program, the citizen or business needs to register first. After the participants are registered, they provide the program with the details of how they want to participate in the program, for example, farming rice or breeding chickens.</li> <li>2. After the participants provide the information, the government agency provides the participants with guidance about how best to farm vegetables or breed animals. The agriculture department also advises the participants to update their activities and send any issues to the agriculture department.</li> <li>3. The agriculture department also provides alerts and notifications about issues and information that relates to the participants, for example, viruses, epidemics, vaccines, and weather.</li> <li>4. The participants submit their generated crop or breeding program outcomes. The agriculture department then provides the necessary incentives for the participants based on their outcomes.</li> </ol>
<b>Preconditions</b>	The geographical area of the farmers and breeders offers cellular coverage only. Mobile data coverage is unavailable. All information that is passed between the farmers and breeders to the agriculture department is by Unstructured Supplementary Service Data (USSD), Short Message Service (SMS), or Multimedia Messaging Service (MMS).

### Implementation architecture

Figure 4-7 on page 71 depicts the suggested implementation architecture for this use case. The key differences are the inclusion of the gateways to support the telecommunication protocols, which are USSD, SMS, and MMS.

The following gateways are required:

- ▶ SMS gateway
- ▶ MMS gateway
- ▶ USSD gateway

In this particular implementation, the following components are not required because the application is based on USSD, MMS, and SMS:

- ▶ Mobile application store (MAS)
- ▶ Mobile device management (MDM)
- ▶ Mobile application management (MAM)
- ▶ Certificate management

Because the application is based on USSD, MMS, and SSM, gateways that are specialized in these protocols are required. This implementation assumes that these gateways are owned by and within the government's data centers. The gateways are then linked to the telecommunications providers.

Figure 4-7 shows the physical operational view for this use case. This view is derived from the convergence of the reference architecture for mGovernment (see 4.2.3, "Operational view" on page 62) and the requirements of this use case.

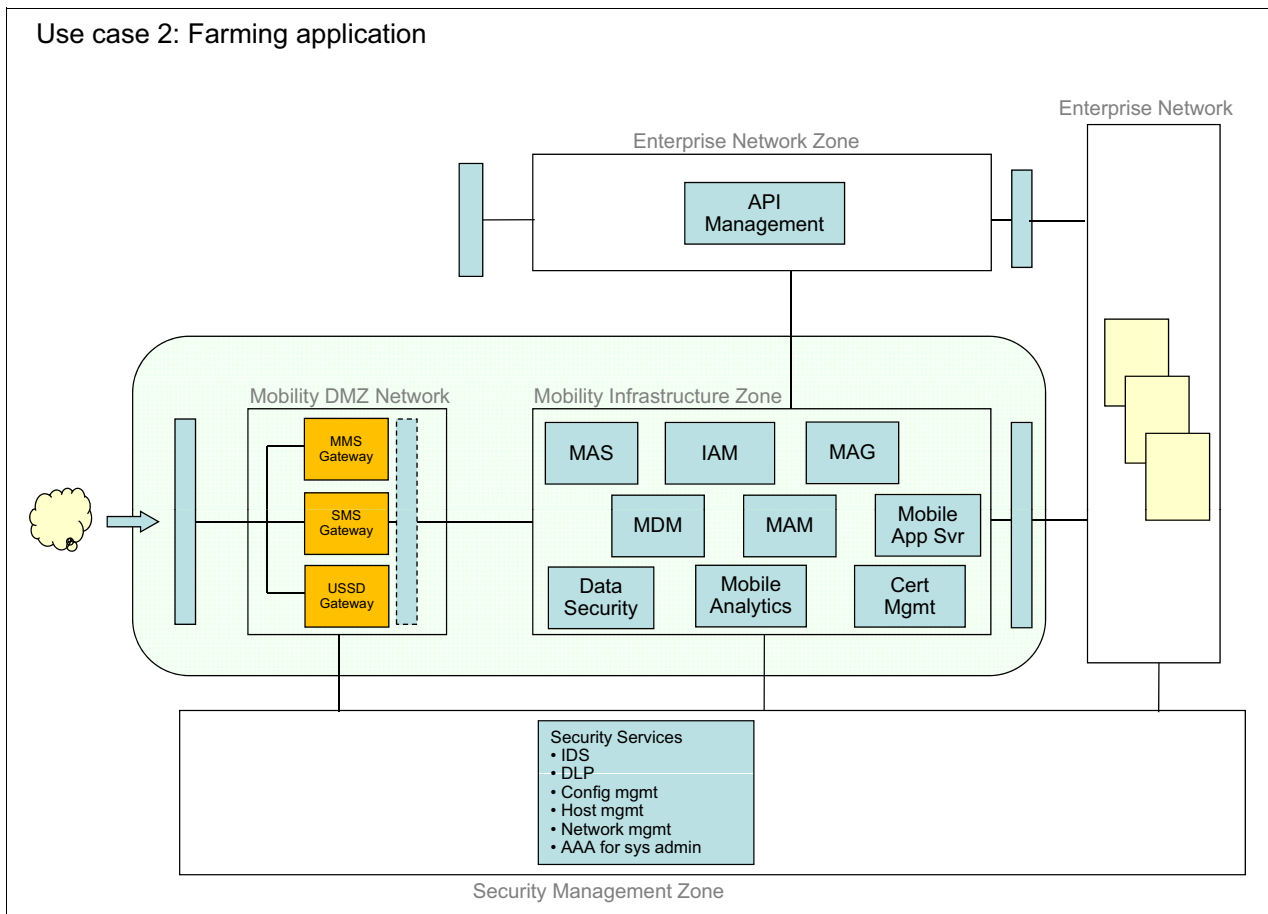


Figure 4-7 Use case 2 operational view

Figure 4-8 shows the application flow and the components that are used for this farming application scenario.

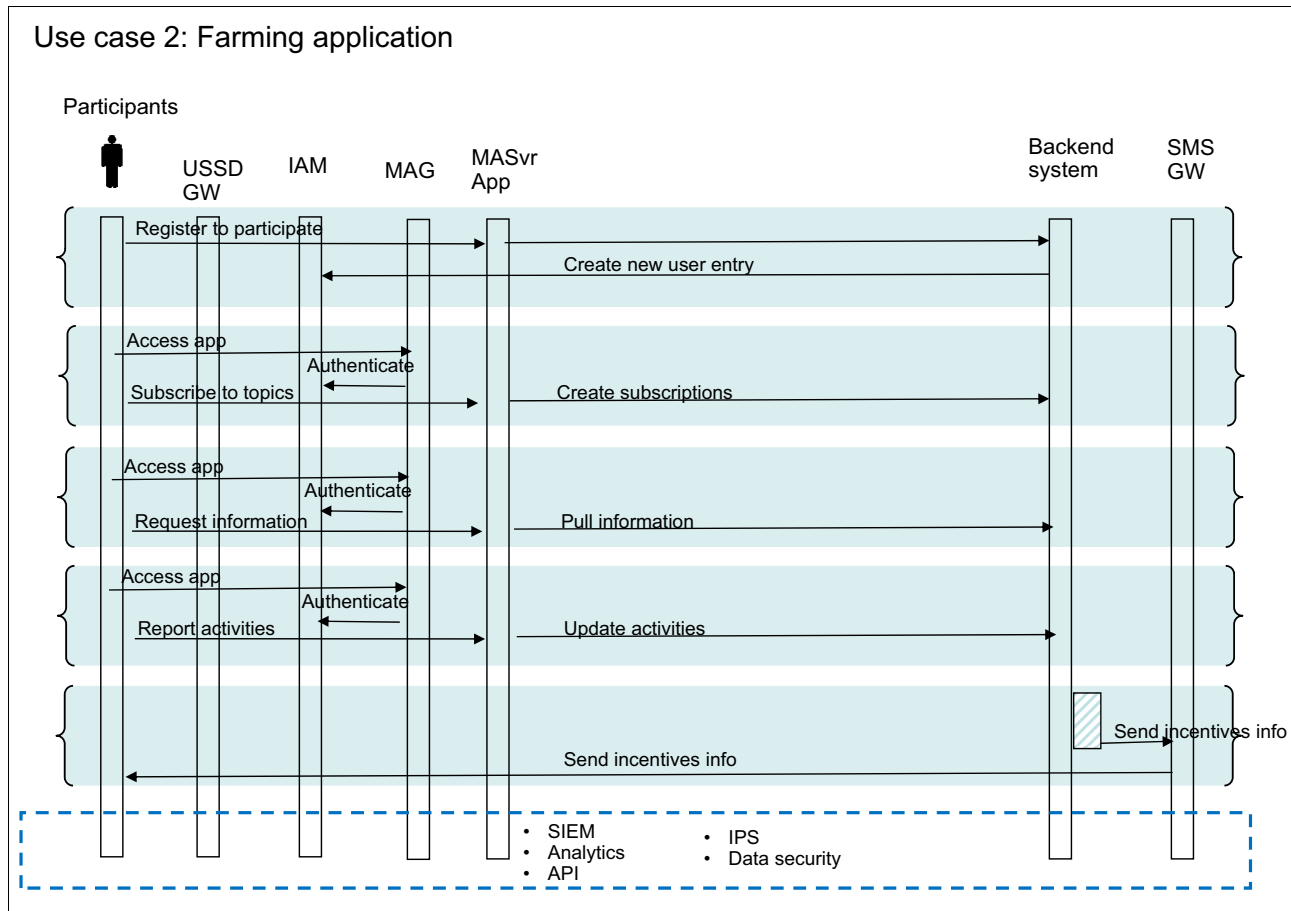


Figure 4-8 Use case 2 application flow and components that are used

The steps that are listed in Table 4-6 describe the basic flow of this use case as depicted in Figure 4-8. These steps depict the mobile components that interact to provide the required services for the actors.

Table 4-6 Reference use case 2 detailed steps

Mobile component	Step 1: Participant requests an application and registration.	Step 2: Participant subscribes to farming or breeding topics.	Step 3: Participant requests dynamic information about the location.	Step 4: Participant reports updates about their activities.	Step 5: Government agency notifies the participant of the participant's results and incentives.
IAM	Create new user entry.	Authenticate.	Authenticate.	Authenticate.	

Mobile component	Step 1: Participant requests an application and registration.	Step 2: Participant subscribes to farming or breeding topics.	Step 3: Participant requests dynamic information about the location.	Step 4: Participant reports updates about their activities.	Step 5: Government agency notifies the participant of the participant's results and incentives.
Mobile GW	Inspect URL calls from USSD GW for vulnerabilities and mediate calls to the actual service endpoints. Authorize authenticated access to protected resources.	Inspect URL calls from USSD GW for vulnerabilities and mediate calls to the actual service endpoints. Authorize authenticated access to protected resources.	Inspect URL calls from USSD GW for vulnerabilities and mediate calls to the actual service endpoints. Authorize authenticated access to protected resources.	Inspect URL calls from USSD GW for vulnerabilities and mediate calls to the actual service endpoints. Authorize authenticated access to protected resources.	
USSD GW	Maps the short code to a known URL that is provided by the mobile app server. Creates the USSD session and forwards the request to the URL.	Maps the short code to a known URL that is provided by the mobile app server. Creates the USSD session and forwards the request to the URL.	Maps the short code to a known URL that is provided by the mobile app server. Creates the USSD session and forwards the request to the URL.	Maps the short code to a known URL that is provided by the mobile app server. Creates the USSD session and forwards the request to the URL.	
Mobile app on app server	Respond to USSD GW request with USSD menu and simple text.	Capture participant details. Invoke the corresponding back-end service. Targeted information is gathered. Respond to the gateway request with USSD menu and simple text.	Capture participant details. Invoke the corresponding back-end service. Targeted information is gathered. Respond to the gateway request with USSD menu and simple text.	Capture participant information updates. Invoke the corresponding back-end service. Respond to the gateway request with USSD menu and simple text.	

<b>Mobile component</b>	<b>Step 1: Participant requests an application and registration.</b>	<b>Step 2: Participant subscribes to farming or breeding topics.</b>	<b>Step 3: Participant requests dynamic information about the location.</b>	<b>Step 4: Participant reports updates about their activities.</b>	<b>Step 5: Government agency notifies the participant of the participant's results and incentives.</b>
Back-end system	Profile creation.	Perform participant triage. Provide targeted information.	Identify participant information request. Gather relevant information from various repositories. Provide targeted information.	Update participant information with their activities. Reply acknowledgment.	Tabulate participant activities, updates, and outcomes. Update participant profile. Provide targeted information about results and incentives for participant.
SMS GW					Sends summarized updates about the participants' results and incentives.
MAD		Code, test, and deploy farming app.			Code, test, and deploy farming app.
Mobile analytics	Collect user interaction data.	Collect user interaction data.	Collect user interaction data.	Collect user interaction data.	
SIEM	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	
Intrusion prevention	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	

### 4.3.3 Use case 3: First responder

Table 4-7 on page 75 provides the details for reference use case 3, which is a first responder mobile application for a government at the time of a disaster.



Table 4-7 Reference use case 3 description for first responder

<b>Use case name</b>	First responder mobile application for a government at the time of a disaster.
<b>Brief description/scope</b>	At the time of a disaster or any major incident, a government wants their employees to use a mobile application to report about the incident. Reporting helps to pass the message to the other entities of government that are responsible to handle the situation.
<b>Actors</b>	<ul style="list-style-type: none"> <li>▶ Government employee or entity</li> <li>▶ Different government organizations</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>▶ Reduces operating costs and improves customer satisfaction.</li> <li>▶ Increases on-time responses and job completions.</li> <li>▶ Reduces operational time and ensures that help is on the way.</li> <li>▶ Improves productivity and decreases field agent hours and overhead.</li> <li>▶ Provides complete analysis of the disaster.</li> </ul>
<b>Normal flow</b>	<ol style="list-style-type: none"> <li>1. Government employees need to install the application on the government-issued mobile device or devices that are secured by an additional application on the mobile device.</li> <li>2. The mobile application needs to be provisioned.</li> <li>3. The government employees need to be registered.</li> <li>4. Government employees report about the incident. They can reach the incident location and upload images and videos of the current situation at the incident's location. They can also notify various government entities for help and support.</li> <li>5. The back-end system notifies a different government entity that needs to be present at the incident's location to provide help and support.</li> <li>6. Government entities or employees respond to their particular assigned tasks. After the completion of their work, they can also upload images and videos about the work that was performed at the incident's location for final reporting.</li> </ol>

This application is based on G2G bidirectional communication among G2G entities.

### Implementation architecture

The architectural implementation for this use case requires the following components:

- ▶ Mobile device management (MDM)
- ▶ Mobile application management (MAM)
- ▶ Identity and access management (IAM)
- ▶ Certificate management
- ▶ Security information
- ▶ Event management for the government devices, applications, and security management

The connection between the mobile application and the back-end system needs a mobile gateway and intrusion prevention system (IPS) for data security over the network. The application requires back-end services for the distribution of data or work to the various government entities according to the requirements. A notification system contacts government employees so that they can also respond back to the onsite team. API management is used to maintain the data over the back-end system for distribution. Later, the government can use analytics to track the work progress.

Figure 4-9 on page 76 shows the physical operational view for this use case. This view is derived from the convergence of the reference architecture for mGovernment (see 4.2.3, "Operational view" on page 62) and the requirements of this use case.

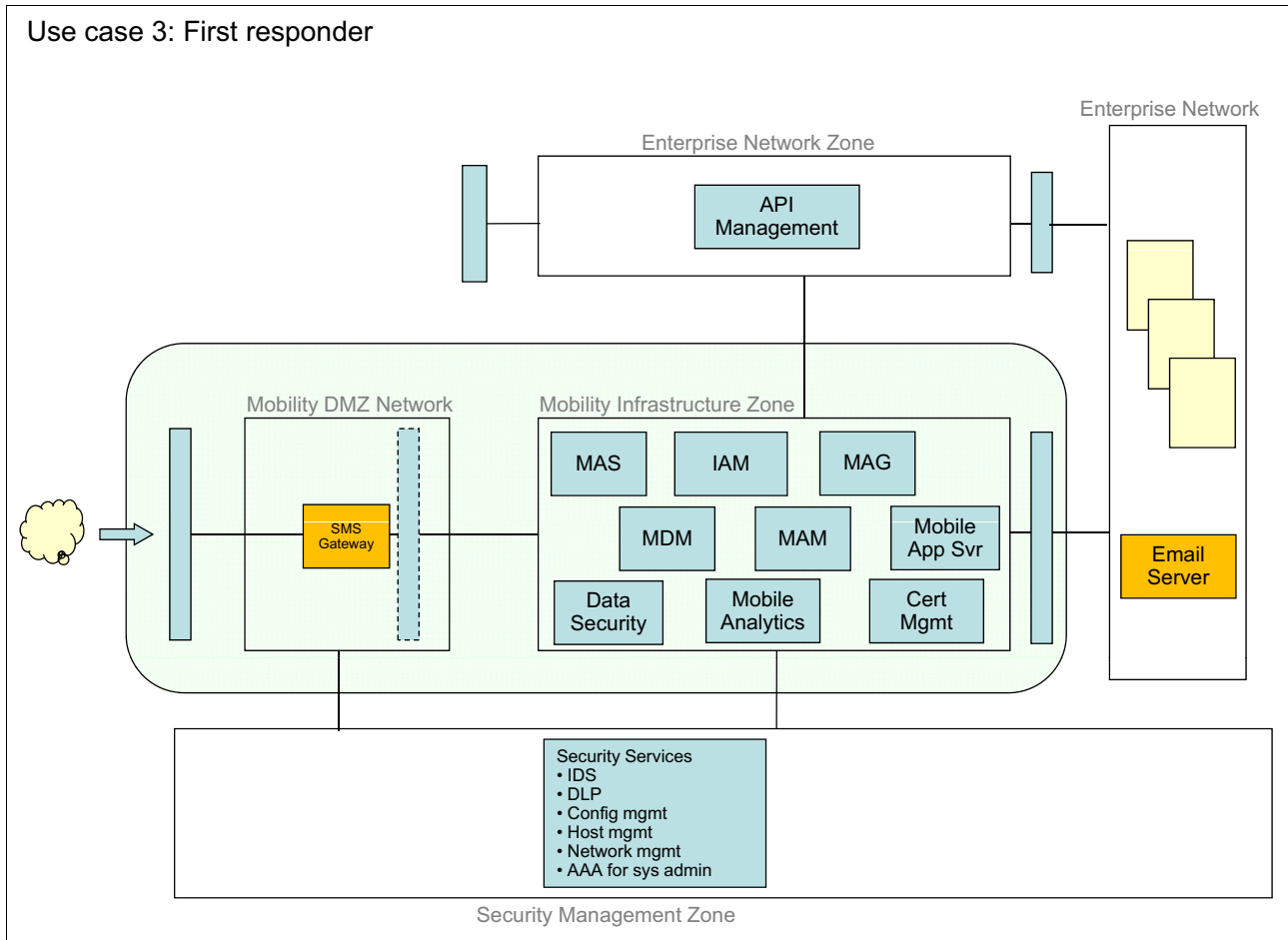


Figure 4-9 Use case 3 operational flow

Figure 4-10 shows the application flow and the components that are used for this first responder scenario.

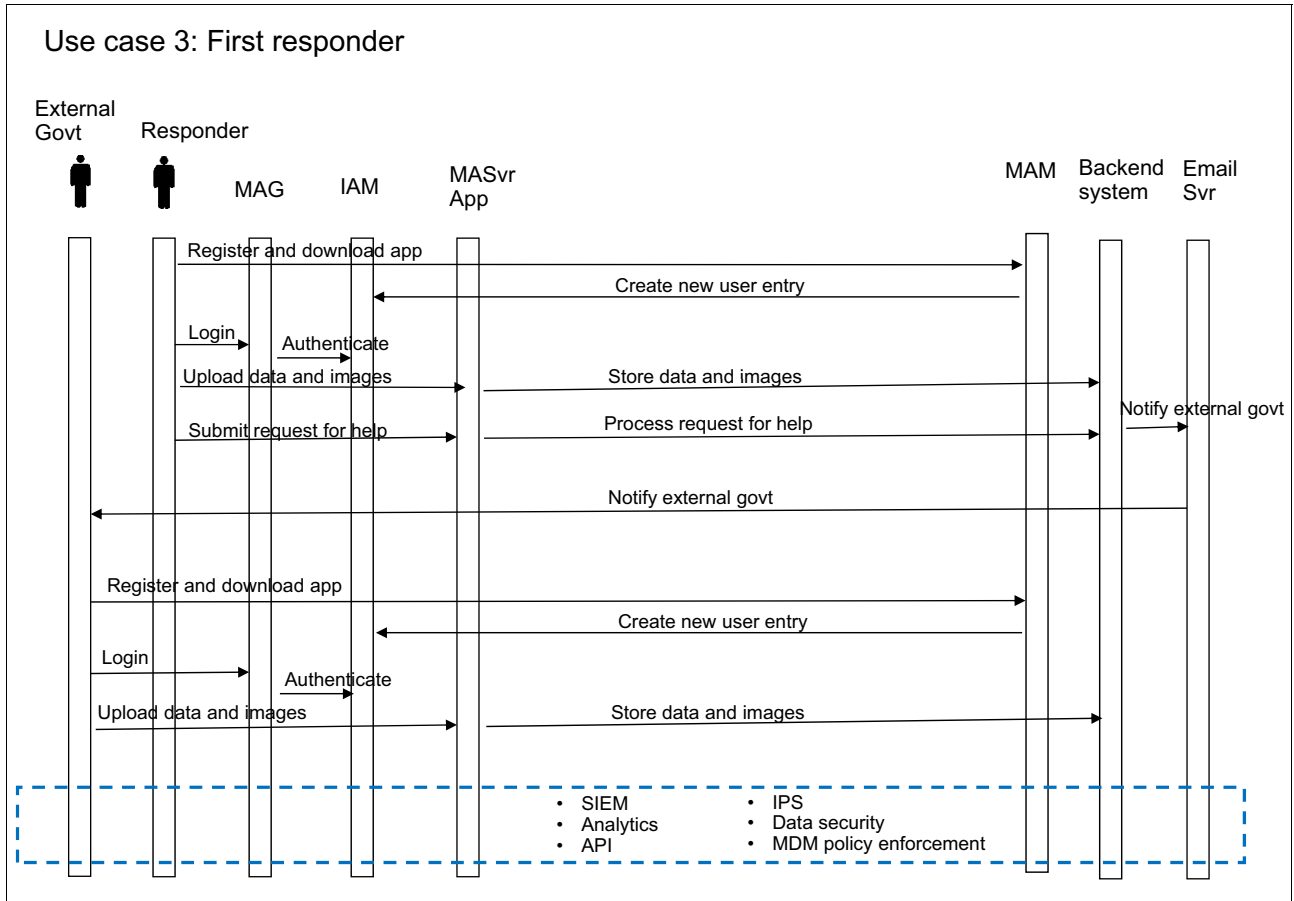


Figure 4-10 Use case 3 application flow and the components that are used

The steps that are listed in Table 4-8 describe the basic flow of this use case as shown in Figure 4-10. These steps depict the mobile components that interact to provide the required services for the actors in this scenario.

Table 4-8 Reference use case 3 detailed steps

Mobile Component	Step 1: First responder registers and downloads the first responder app.	Step 2: First responder assesses, reports with photos or videos, and requests external government agencies for onsite support.	Step 3: External government agencies are notified.	Step 4: External government agencies register and download the first responder app.	Step 5: External government agencies provide onsite support and report the situation with photos or videos.
IAM	Create new user entry.	Authentication.		Create new user entry.	Authentication.

<b>Mobile Component</b>	<b>Step 1: First responder registers and downloads the first responder app.</b>	<b>Step 2: First responder assesses, reports with photos or videos, and requests external government agencies for onsite support.</b>	<b>Step 3: External government agencies are notified.</b>	<b>Step 4: External government agencies register and download the first responder app.</b>	<b>Step 5: External government agencies provide onsite support and report the situation with photos or videos.</b>
Mobile GW		Challenge and authenticate.			Challenge and authenticate.
Mobile app on app server		First responder user interface (UI).	Process the request for help.		First responder UI.
Back-end system		Store reported data and images.	Prepare notification message.		Store reported data and images.
Email server			Send notification messages.		
MAM	First responder downloads first responder app.			External government employee downloads first responder app.	
MAD		Code, test, and deploy first responder app.			Code, test, and deploy first responder app.
MDM	Enforce device policies during app download.	Enforce device policies during app download.		Enforce device policies during app download.	Enforce device policies during app download.
Certification management		Validate credentials.			
Mobile APIs		Calling external government APIs.	Calling email APIs.		Calling external government APIs.
Mobile analytics		Collect user experience data.			Collect user experience data.
SIEM	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.
Intrusion prevention	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.	Track, monitor, and alert.
Data security		Encrypt data in transit.			Encrypt data in transit.



## Points of view in mGovernment

This chapter demonstrates the relevance of several architectural components in the IBM MobileFirst for mGovernment reference model that relate to issues that governments struggle with during their implementation of an enterprise mobile strategy.

This chapter formulates many points of view about mGovernment based on a bottom-up approach. This approach focuses on observations and requirement patterns that derive from specific requests for proposal (RFPs) or requests for information (RFIs) that were issued recently by various government agencies in the pursuit of their own mobile enterprise strategies. This chapter is not a statement of fact but rather an observational perspective.

This chapter helps you to understand the notional aspect of a mGovernment reference architecture when you compare it with the requirements patterns in the field.

The following topics are covered in this chapter:

- ▶ 5.1, “Striving for commonality and uniformity” on page 80
- ▶ 5.2, “Standards, standards, and standards” on page 80
- ▶ 5.3, “Balancing cost, function, and security” on page 80
- ▶ 5.4, “Data protection” on page 81
- ▶ 5.5, “Lifecycle and governance” on page 82
- ▶ 5.6, “Third-party application management and control” on page 82
- ▶ 5.7, “Risk management” on page 83
- ▶ 5.8, “Assessing the value of the develop-once-deploy-many approach in application development” on page 84

## 5.1 Striving for commonality and uniformity

The mobile technology landscape is still fragmented. Therefore, governments conscientiously try to be proactive in preventing fragmentation in their enterprise mobility implementations. Fragmentation across many agencies results in an inability to pursue the further vision of a digital government for open data and shared services.

The creation of frameworks, reference architecture, guidelines, and standards with expansive cross-agency collaboration is a catalyst for implementing a common baseline in government mobile enterprise deployment. This approach reduces costs, prevents project silos, and benefits from the “lessons learned” by many agencies.

**Talking points:** Use the mGovernment reference architecture as a starting point to implement common capabilities and identify shared services that can be provided across government agencies.

## 5.2 Standards, standards, and standards

As the technology in enterprise mobility evolves from infancy to prime maturity, governments constantly update their existing standards for security and privacy to account for the new ecosystem. Governments develop new standards to include guidelines and recommendations for adoption across all agencies. Solution vendors also update their products to ensure compliance with the new standards. Because the technology continues to emerge, the stability of the standards’ requirements is not optimal. Certain standards are stable but encounter challenges in the mobile environment, for example, Common Access Card (CAC)/Personal Identity Verification (PIV) authentication.

Governments must stay aware of the latest updates to standards in mobile security and quickly ensure that they comply or that compliance is in the strategy implementation roadmap. Governments strive for commonality. Therefore, after a technology or app component complies and is deployed in one part of the government, the probability of deployment elsewhere in the government is higher.

**Talking points:** Although the components in the mGovernment reference architecture are built based on standards, integrated, and communicating by using standards-based protocols, each component’s function must be evaluated. Before each component is implemented, it must be evaluated for specific local government standards, compliance requirements, and security processes.

## 5.3 Balancing cost, function, and security

Because enterprise mobility is a strategy that augments the existing IT fabric of an agency to accelerate the delivery of government services and advance the agency’s mission-critical objectives beyond what is possible in the traditional IT infrastructure, the level of adoption differs from agency to agency. Each agency has a unique mission focus. Agencies need to balance the gain in mission support with the financial costs and the security exposure, not unlike their existing return on investment (ROI) studies and risk management processes.

The challenges are in forecasting and stabilizing the cost of deployment and the cost of maintaining and enforcing data security based on the level of maturity in the mobile solutions market.

**Talking points:** The components in the mGovernment reference architecture are loosely coupled and meant to be substituted with existing government infrastructure components.

## 5.4 Data protection

Although the RFPs included extensive requirements for securing devices and applications, those requirements were merely a means to an end, which is the protection of government and personal data. Requirements for granular data access management, authorization, and encryption were common across individual RFPs and as published standards and guidelines. Unlike commercial enterprises, the focus in government is not to grow product markets but to enable the secure usage of government data to provide more efficient and expedient services.

Commercial mobile apps are scrutinized for the design of security and data protection policies that are based on the degree of their reach into core enterprise data. Depending on the enterprise data reach and the mission criticality, specific data protection policies govern the apps and also possibly a separate IT architecture framework.

The following examples show data reach for mobile applications:

- ▶ Read-only enterprise-owned public information, for example, brochure-ware, marketing, and reference information (the nearest office locations on maps and customer support frequently asked questions (FAQs))
- ▶ Read-only enterprise data and content, for example, dashboards and business intelligence (BI) apps
- ▶ Read/write enterprise data and content, for example, field workforce, field investigations, collaboration, photo uploads, expense submissions, and live customer feedback
- ▶ Transactional, for example, ordering, reservations, and e-payments
- ▶ Extra-enterprise data reach, for example, navigation, airline trip management, currency converters, and weather
- ▶ Data on device only, for example, calculators, viewers, and notepads

Beyond merely ensuring that apps support mandated standards for encryption, security, and privacy, governments must evaluate using their middleware stacks in the areas of data management and classification to consolidate data sources into a single mobile view of the enterprise data. Addressing mobile security then becomes more of a data-centric approach than a device-centric approach.

**Talking points:** The mGovernment reference architecture provides a separation of the mobile infrastructure, including run time, gateway, devices, applications, and network, from the user management and data management layers. The user management and data management layers are shared across mobile and non-mobile channels. This separation facilitates the implementation of data access control policies to include rules for mobile and non-mobile access.

## 5.5 Lifecycle and governance

From device management to application management to data management, government emphasizes the role of security controls throughout the entire lifecycle to ensure the continuous integrity of the device, application, and enterprise information. This role is exacerbated by the rapid rate of change and upgrade to devices, OS levels, and applications throughout their lifecycles, which are compounded with the requirements to audit, track, and monitor that are inherent in many government processes.

Governments also rely on commercial off the shelf (COTS) mobility tooling platforms that provide a wide range of flexibility in administration and management so that they can accommodate the various degrees of enterprise control in delivery models. Governments constantly balance between the placement of security control and the enablement of enterprise innovation and productivity. Depending on usage scenarios, governments want the agility to design and update policies as necessary.

Technology vendors incorporate lifecycle and governance into their device management, application management, and application development products. The added value for mGovernment is in providing a single view into those three aspects of mobile enterprise for ease and comprehensiveness of governance and control. Integrating a view of mobile data management is also a significant added value.

**Talking points:** Even with a comprehensive single point of administration and management, it might be more productive at each point of administration to segregate based on roles and domains (application governance, device governance, and data governance). Governments might also evaluate dual or multiple role use cases.

## 5.6 Third-party application management and control

Whether a government is in a “bring your own device” (BYOD) or “corporate-owned personally enabled” (COPE) environment, it is struggling with the deployment and management of third-party commercial applications that are not developed in-house. Many of these applications are required or integral parts of enterprise mobility. Other applications are necessary to support enterprise staff productivity, and other applications are more personal than enterprise in a BYOD environment. The commercial third-party apps are enterprise-centric, for example:

- ▶ MDM agent
- ▶ Virtual private network (VPN) apps
- ▶ Virtual Network Computing (VNC)/Remote Desktop Protocol (RDP) apps
- ▶ Virtual desktop apps
- ▶ Printing agent
- ▶ Voice over Internet Protocol (VoIP) apps

Other commercial third-party apps are user-centric, for example:

- ▶ Content viewers
- ▶ Expense trackers
- ▶ Knowledge discovery
- ▶ Presentation tools
- ▶ Games



Governments place special focus in the area of managing acquired COTS applications. Governments want to extend existing capabilities, such as policy wrapping, containerization, application vetting, security testing, and licensing compliance.

With commercial mobile apps, governments keenly focus on data protection and security. Therefore, commercial mobile applications join in the same governance, security, and distribution management policies as any mobile apps in the enterprise regardless of authorship.

Similar to their traditional IT projects, governments face the same classic “build versus buy” dilemma in mobile application development. The decision criteria are also similar:

- ▶ Mission criticality
- ▶ Budget and finances
- ▶ Schedules and deadlines
- ▶ In-house skills
- ▶ Support infrastructure

On the consumption side, government agencies apply different degrees of tolerance to the use of commercial mobile apps for enterprise purposes. Certain commercial applications are required or integrated into enterprise mobility. Other apps are necessary to support enterprise staff productivity. And, other apps are more of a personal than enterprise nature in a BYOD environment. The apps are listed along a maturity continuum, for example:

- ▶ Commercial applications that are bundled with the device (maps, browsers, cloud sync, notepads, and calculators)
- ▶ Commercial applications purely for personal non-enterprise use (games and hobby-based)
- ▶ Commercial applications for personal productivity (content managers and viewers, expense trackers, knowledge discovery, and presentations)
- ▶ Commercial applications for mobile IT (MDM agent, VPN apps, VNC/RDP apps, virtual desktop apps, printing agent, and VoIP apps)
- ▶ Commercial applications for business productivity (file managers, document viewers, expense trackers, knowledge discovery, and presentations)
- ▶ Enterprise mobile applications (stand-alone)
- ▶ Mobile client extensions to commercial enterprise back-end systems (enterprise resource management (ERP) mobile extensions, email, and collaboration apps)

**Talking points:** The loose integration of mobile device management (MDM) and mobile application management (MAM) in the mGovernment reference architecture provides for policies and processes that support the granularity of a commercial versus an in-house mix.

## 5.7 Risk management

The risk management challenge refers more to user behavior control than to device capability control.

Mobile security is mostly mobile data security. The input and classification of the data that is created in a mobile environment depend on the user that follows the policies. The exposure of data that is retrieved on the devices outside of secure government premises also depends on the user providing the required level of physical security.

Government faces the challenge of determining which policies can be detected and enforced by the system and which policies summarily limit the release of data to a mobile device.

Certain security risks are more prone in mobile apps on the device that can benefit from tighter enterprise control during their lifecycles, for example:

- ▶ Malicious application behavior, which can affect the integrity of the device, other applications on the device, and back-end systems. These risks can be mitigated with strong monitoring and malware detection on the MDM side and rigorous vetting and testing from the MAM side.
- ▶ User behavior, which includes entering sensitive corporate data, unauthorized downloading of app features, and incorrectly configuring (for example, allowing cloud auto sync). These risks are again mitigated with strong monitoring and policy enforcement with blacklisting and whitelisting approaches.

Governments turn to a combination of technology and consulting services for risk management. Mobile technology allows policy management and enforcement at the device level, application level, data access level, and network level. Professional consulting services can help agencies mitigate risk with training and sound data classification and management practices. Although analytics products are not exactly intended for monitoring risk, government can also use analytics products to discover trends and patterns of risky user behavior and create data security policies in response.

**Talking points:** The mGovernment reference architecture is meant to serve as a model to start the discussion about professional consulting for various mobile strategy aspects and how the tooling can support the process. The mobile analytics component serves as a feedback mechanism to surface needed corrective measures.

## 5.8 Assessing the value of the develop-once-deploy-many approach in application development

At the time of this writing, the BYOD approach in government as a cost-saving measure for deploying enterprise mobility is still an unstable value proposition for most governments because of the fragmentation of the device market and associated mobile OS levels. COTS solutions to provide security and controls in a BYOD environment are not at a peak maturity level, therefore threatening to void the savings in procuring devices with the cost in securing them. After the BYOD approach solidifies in an mGovernment environment, the value of the develop-once-deploy-many approach in most Mobile Enterprise Application Platform (MEAP) solutions becomes more obvious.

However, in another perspective, public-facing mobile applications that access publicly available government data will likely soon be replaced by mobile application programming interfaces (APIs) that are exposed for third-party applications and mashups to consume. In this model, application development is less a responsibility of the government if the government exposes publicly available government data for private and commercial mobile applications to access. Presentation layer and device compatibility is no longer a key concern in in-house app development, at least for the government to citizen (G2C) domain.

Governments seek among their choices of commercial MEAP solutions a value proposition that transcends application development and encompasses back-end integration, runtime security, API management, and data lifecycle management.

**Talking points:** The mGovernment reference architecture separates data access from mobile application development by using an API management component and a tooling platform for the develop-once-deploy-many approach. This approach allows third-party applications that cater to certain specific UI requirements to access the same data and data policies as the in-house-developed application.





## mGovernment trends and directions

Because the mobile enterprise technology field evolves at a rapid pace with cloud and analytics capabilities, the mGovernment reference architecture needs to be expanded to accommodate mobile trends and patterns in the public sector in the near future.

The following discussion items highlight the direction of mobile enterprise in government:

- ▶ Common tools for app vetting, security standards, and evolved public key infrastructure (PKI) for issuance of derived credentials. Moving beyond Common Access Cards (CACs).
- ▶ Bring your own device (BYOD) security: Finding the right balance between security within context and dynamic security.
- ▶ Built-in security: Inside-out pre-deployment with apps software development kit (SDK) and outside-in post-deployment with app wrapping.
- ▶ Mobile user experience is key: User engagement that enables a federal employee or stakeholder to access the information and resources that they need so that they can be fully productive where they are.
- ▶ Moving from informational to transactional for citizen services and mobile workforce. A mobilized transaction is not an app; it is part of an extended enterprise system.
- ▶ Native apps and crowdsourcing: Engage the user to provide information and data, including offline scenarios.
- ▶ Open data: Expanding access, functionality, design, and trustworthiness of government data to the mobile application developer ecosystem.
- ▶ Adaptive content: Ability to publish content as modular, discrete pieces of information that are tagged with machine-readable descriptions. Structure within content has the potential to transform how people find, understand, share, and use government information.
- ▶ Process conscious: Extending mission-critical processes to field workers and field devices.
- ▶ Cloud integration that connects mobility, open data, and the cloud.

Because the mobile and cloud landscape is still shifting, government agencies want more effective cloud synchronization and to move from one commercial cloud provider to another without interruption. Government agencies want to know how to introduce new cloud and mobility capabilities that do not introduce new environments that must be maintained.

Although the intersection of mobile with cloud and analytics provides an opportunity to expand customer reach for the commercial world, this intersection poses an interesting dilemma for mGovernment in relation to security and privacy. Several of the concerns are listed:

- ▶ Addressing security concerns in the cloud and supporting government-specific cloud services models, such as the military cloud
- ▶ Designing cloud-based services to empower disconnected user issues
- ▶ Researching and developing field new technologies for improved information access
- ▶ Facilitating cloud interoperability standards and increasing the trust of third-party providers
- ▶ Collecting and retaining mobile user data and behavior
- ▶ Using location analytics

For more information, see the following website:

<http://fedscoop.com/takai-lays-dods-mobility-cloud-forecast/>



# Examples of mGovernment applications

This appendix provides some examples of actual mobile government applications that are being implemented today and highlights the different types of mobile government interactions that are involved in these various examples.

The following examples are described:

- ▶ “mHealth: Blood bank” on page 90
- ▶ “mWrapper: The Mobile portal - Kingdom of Bahrain” on page 90
- ▶ “mEducation: M4girls” on page 90
- ▶ “mEmergency: SMS broadcasting system” on page 91
- ▶ “mEmergency: Emergency service” on page 91
- ▶ “mPayment: NFC mobile payment” on page 91
- ▶ “mPolicing: Mobile field inspection system” on page 92
- ▶ “mTransportation: MOBESE” on page 92
- ▶ “mAdministration: Florida Keys mosquito control” on page 92
- ▶ “mBusiness: Agroportal” on page 93
- ▶ “mBusiness: Uganda Google Trader” on page 93
- ▶ “mBusiness: Gateway Sweden” on page 93
- ▶ “mBanking: Mobile Money 2.0” on page 94
- ▶ “Crowdsourcing: uRep” on page 94
- ▶ “Crowdsourcing: MyGov” on page 94
- ▶ “Context aware: Mobile emergency alert service” on page 95

For a description of the types of mobile government applications and services that are explained in this appendix, see Chapter 1, “Mobile government overview” on page 1.

## **mHealth: Blood bank**

The availability of sufficient amounts of blood for transfusions is crucial for any hospital. In Kenya, several centralized blood banks are responsible for supplying district hospitals with blood. To guarantee an adequate supply, these hospitals must frequently report the current status of their local blood repository. In Eastern Kenya, a program called SMS Blood Bank was created to allow healthcare workers from remote hospitals to report on the current status of their blood repository by using Short Message Service (SMS). Incoming status updates are collected at the central blood bank and graphically visualized through a web-based interface. SMS-based alerts are triggered automatically when blood repositories at district hospitals fall below a predefined threshold.

Channel used: SMS

Types of applications: Employee to government (E2G) and government to government (G2G)

Category of service: Information service

Country: Kenya

## **mWrapper: The Mobile portal - Kingdom of Bahrain**

The Mobile Portal - Kingdom of Bahrain application is used as a new channel in the delivery of eGovernment services to the citizens and residents of Bahrain. The portal includes over 45 eGovernment services. All services are made available in Arabic and English. The key services are listed:

- ▶ eWeather
- ▶ Doctor search
- ▶ Embassy contacts
- ▶ Mobile blogs or mobile polls
- ▶ Payments for electricity, water bills, or traffic contraventions

Channel used: Wireless Application Protocol (WAP) and SMS

Types of applications: Citizen to government (C2G) and bidirectional C2G

Category of service: Information, Interactive, and Transaction services

Country: Bahrain

## **mEducation: M4girls**

The M4girls project is a partnership between Nokia, Mindset Network, and the Department of Education (North West Province) to test the provision of educational content on a mobile phone platform to girl learners. The project targeted the development of mathematics competencies in grade ten girl learners. The project recognizes the active use of mobile phones by young people to access the Internet and network with peers, and the project uses their preferred channel to expand education.

Channel used: 2G/Data Network

Types of applications: C2G



Category of service: Interactive service

Country: North West Province, Africa

## **mEmergency: SMS broadcasting system**

An SMS broadcasting system is used in Mexico City, Mexico, to send alert messages to citizens in the district about meteorological and high rain risks, low temperatures, potential disasters, emergency locations, and contact numbers.

Channel used: SMS

Types of applications: Government to citizen (G2C)

Category of service: Information services

Country: Mexico

## **mEmergency: Emergency service**

The Italian Ministry of Foreign Affairs, during the aftermath of the Asian quake, sent an SMS to Italians in the affected area. The message was “Answer indicating your identity, health status, and place where you are”. The Italian Government obtained the list of people who were in the affected area from phone companies that provided the information based on the international roaming services.

Channel used: SMS

Types of applications: Bidirectional G2C

Category of service: Interactive service

Country: Italy

## **mPayment: NFC mobile payment**

In Poland, the mobile operator PTC launched a mobile payment pilot in 2010. Trial participants were enabled to make payments with their near field communication (NFC)-enabled smartphones in various stores, restaurants, gas stations, and other retail outlets.

Channel used: Data network

Types of applications: C2G

Category of service: Transactional service

Country: Poland

## **mPolicing: Mobile field inspection system**

In Hong Kong, China's Mobile Field Inspection System enables inspectors to use touchscreen personal digital assistants (PDAs) to enter inspection information at the scene and to review the results of past inspections. Inspectors can send their reports through their mobile phones without going to the office. The PDAs were designed for easy use, so the training time was short.

Channel used: Data network

Types of applications: E2G

Category of service: Interactive service

Country: China

## **mTransportation: MOBESE**

Turkey's traffic information system, Mobile Electronic System (MOBESE), equips mobile traffic units with tablet personal computers to conduct queries on the licenses and vehicle information of offending drivers quickly. This capability increases the efficiency of the mobile traffic units. In addition, each mobile traffic unit can be located and dispatched to a particular location, such as a traffic incident. Vehicle information is cross-checked with several government agencies for road tax expiration, criminal suspicion, and owner validation.

Channel used: Data network

Types of applications: G2G

Category of service: Interactive service

Country: Turkey

## **mAdministration: Florida Keys mosquito control**

In Florida, the challenge was to effectively and efficiently use their 61 vehicles that were engaged in insecticide control to prevent the spread of the West Nile virus and other mosquito-borne diseases in over a million acres of coastal marshland. They are now using a wireless fleet management solution that monitors the locations, heading, speed, and insecticide applications of all their vehicles in real time. The information that is wirelessly provided by their vehicles is displayed on a digital map screen at district headquarters in Key West. The digital map monitors what each vehicle is doing, where it is spraying (or dropping) chemicals, and the vehicle rates of speed. This information allows supervisory staff at headquarters to monitor vehicle progress and instruct personnel as necessary. The systems also allow them to generate reports both in real time and on a historical basis (for example, to demonstrate spraying activity over a period of time or to calculate cost analysis information).

Channel used: Data network

Types of applications: Bidirectional G2E

Category of service: Transactional service

Country: United States

## **mBusiness: Agroportal**

A one-stop shop for the provision of mGovernment services for the Greek agricultural sector was introduced. The service is called Agroportal and its objective is to supply its target group with recent related news, frequently asked questions, and a list of useful links. Agroportal also enables the electronic submission of applications by users, the processing of the submitted applications by the responsible public authority, and the delivery of the application response back to the user. In general, Agroportal attempts to improve and facilitate the communication between users and between users and governmental authorities.

Channel used: Data network

Types of applications: Bidirectional business to government (B2G)

Category of service: Transactional service

Country: Greece

## **mBusiness: Uganda Google Trader**

Google Trader is a marketplace application that allows you to buy and sell goods and services on your phone by using SMS. Google Trader is a simple market system for buyers and sellers to find one another with fewer transaction costs by using the mobile phone to list their offerings and search for those with whom they are likely to transact business.

Channel used: SMS

Types of applications: B2G

Category of service: Informational services

Country: Uganda

## **mBusiness: Gateway Sweden**

The Gateway Sweden project aims to improve the customs clearance process in Sweden. Lorry drivers receive an SMS as soon as their cargo is cleared. The SMS includes a reference number that can be shown in case the drivers are stopped for checking.

Channel used: SMS

Types of applications: Unidirectional G2B

Category of service: Informational service

Country: Sweden

## **mBanking: Mobile Money 2.0**

In Uganda, up to 90 percent of the 5 million households do not have a bank account. The lack of area-wide banking infrastructures, especially in rural communities, impedes even simple financial transactions for the majority of the population. Alternatively, Uganda has a well-developed mobile phone infrastructure. The Mobile Money 2.0 project provides citizens with financial services through their mobile phones. This way, well-developed mobile infrastructures try to compensate for missing banking infrastructures.

Channel used: Data network

Types of applications: C2G

Category of service: Transactional service

Country: Uganda

## **Crowdsourcing: uRep**

An Android app, which is code named uRep, allows users to report a problem by snapping a picture and geo-tagging it by using the GPS functionality that is built into their mobile devices. uRep allows users to report power outages and see the location of other reports. Utility companies can also log in and set priorities to reported issues, all while outage reporters track their progress in addressing issues.

Channel used: Data network

Types of applications: Bidirectional C2G

Category of service: Interactive service

Country: United States

## **Crowdsourcing: MyGov**

The Indian government launched a new online platform that is called MyGov to encourage citizen participation in governance. This platform allows citizens to volunteer for specific projects and also invites suggestions about various policy decisions. The Indian government is also developing a mobile app that allows citizens to take pictures and report public problems on the forum.

Channel used: Data network

Types of applications: Bidirectional C2G

Category of service: Informational service

Country: India

## Context aware: Mobile emergency alert service

This location-based mobile emergency alert service sends warnings to mobile phones that are physically in an emergency zone when a disaster strikes. Australia's emergency warnings are currently limited to using a residential address that is associated with individual subscribers, as a result relying on outdated emergency notifications, such as radio warnings. The upgraded mobile emergency alert uses location-based mobile communications services to send anywhere, anytime warnings directly to mobile phones by using SMS.

Channel used: SMS

Types of applications: Unidirectional G2C

Category of service: Informational services

Country: Australia



# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

## IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- ▶ *IBM MobileFirst Strategy Software Approach*, SG24-8191
- ▶ *Securing Your Mobile Business with IBM Worklight*, SG24-8179

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

[ibm.com/redbooks](http://ibm.com/redbooks)

## Other publications

These publications are also relevant as further information sources:

- ▶ *US Federal Mobile Security Reference Architecture*:  
<https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf>
- ▶ US Department of Commerce, National Institute of Standards and Technology, *Guidelines for Media Sanitization*, NIST SP800-88:  
<http://dx.doi.org/10.6028/NIST.SP.800-88r1>
- ▶ Australian Government Department of Defence, *iOS Hardening Configuration Guide*, which is available at the following link:  
<https://itunes.apple.com/us/book/asd-ios-hardening-configuration/id881697251?mt=11>
- ▶ *Adoption of Commercial Mobile Applications within the US Federal Government*:  
<https://cio.gov/wp-content/uploads/downloads/2013/05/Commercial-Mobile-Application-Adoption-DGS-Milestone-5.4.pdf>
- ▶ US Department of Commerce, National Institute of Standards and Technology, *Guide to Storage Encryption Technologies for End User Devices*:  
<http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf>
- ▶ US Department of Commerce, National Institute of Standards and Technology, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 800-124:  
<http://dx.doi.org/10.6028/NIST.SP.800-124r1>

- ▶ US Department of Commerce, National Institute of Standards and Technology, *Technical Considerations for Vetting 3rd Party Mobile Applications*, publication 800-163:  
[http://csrc.nist.gov/publications/drafts/800-163/sp800\\_163\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf)
- ▶ US Department of Commerce, National Institute of Standards and Technology, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*:  
<http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>
- ▶ US Department of Commerce, National Institute of Standards and Technology, *Guide to Bluetooth Security*:  
[http://csrc.nist.gov/publications/drafts/800-121r1/Draft-SP800-121\\_Rev1.pdf](http://csrc.nist.gov/publications/drafts/800-121r1/Draft-SP800-121_Rev1.pdf)
- ▶ US Department of Commerce, National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*:  
<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
- ▶ US Department of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information*:  
[http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_guide\\_sp11\\_handbook.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_sp11_handbook.pdf)

## Online resources

These websites are also relevant as further information sources:

- ▶ IBM MobileFirst:  
<http://www.ibm.com/mobilefirst/us/en/>
- ▶ IBM product finder:  
<http://www.ibm.com/software/products>
- ▶ Mobile development and connectivity:  
<http://www.ibm.com/software/products/en/category/mobile-application-development>
- ▶ Mobile integration of data and applications:  
<http://www.ibm.com/software/products/en/category/mobile-data-application>
- ▶ API management:  
<http://www.ibm.com/software/products/en/api-management>
- ▶ Mobile management and security:  
<http://www.ibm.com/software/products/en/category/SW500>
- ▶ Mobile device management:  
<http://www.ibm.com/marketplace/cloud/enterprise-mobility-management/us/en-us>
- ▶ Identity and access management:  
<http://www.ibm.com/software/products/en/category/identity-access-management>
- ▶ Mobile application security:  
<http://www.ibm.com/software/products/en/category/application-security>
- ▶ Data security and privacy:  
<http://www.ibm.com/software/products/en/category/data-security>



- ▶ Security intelligence and analytics:  
<http://www.ibm.com/software/products/en/category/security-intelligence>
- ▶ Advanced fraud protection:  
<http://www.ibm.com/software/products/en/category/advanced-fraud-protection>
- ▶ Advanced security and threat protection:  
<http://www.ibm.com/software/security/adv-security-threat-protection/>
- ▶ UK Centre for the Protection of National Infrastructure documentation on best practice security for mobile devices:  
<https://www.cpni.gov.uk/advice/cyber/mobile-devices/>
- ▶ U.S. General Services Administration, *Mobile Device & Application Management*:  
<http://www.gsa.gov/portal/content/177475>
- ▶ *End User Devices Security Guidance: Apple iOS Application Security Guidance* at GOV.UK:  
<http://bit.ly/10TEE0P>
- ▶ Data protection laws of the world:  
<http://www.dlapiperdataprotection.com>
- ▶ Cryptographic policies of various countries:  
<http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/cryptographic-policies-countries.htm>
- ▶ “International Cryptography Regulations and the Global Information Economy” by Nathan Saper in *Northwestern Journal of Technology and Intellectual Property*, September 2013:  
<http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1205&context=njtip>
- ▶ Professor Bert-Jaap Koops’ Crypto Law:  
<http://www.cryptolaw.org/>
- ▶ W3C Web Accessibility Initiative:  
<http://www.w3.org/WAI/>
- ▶ BBC’s Mobile Accessibility Guidelines:  
<http://www.bbc.co.uk/guidelines/futuremedia/accessibility/mobile/about>
- ▶ Wassenaar Arrangement:  
<http://www.wassenaar.org/controllists/index.html>
- ▶ mobiForge:  
<http://mobiforge.com/>

## Help from IBM

IBM Support and downloads

[ibm.com/support](http://ibm.com/support)

IBM Global Services

[ibm.com/services](http://ibm.com/services)





**IBM MobileFirst in Action for mGovernment and Citizen Mobile Services**

(0.2"spine)  
0.17"->0.473"  
90->249 pages







# IBM MobileFirst in Action for mGovernment and Citizen Mobile Services



**Understand key focus areas for implementing a successful mobile government**

**Learn about IBM MobileFirst products to support an mGovernment solution**

**Review practical use cases and scenarios**

Mobile technology is changing the way government interacts with the public anytime and anywhere. mGovernment is the evolution of eGovernment. Like the evolution of web applications, mobile applications require a process transformation, and not by simply creating wrappers to mobile-enable existing web applications.

This IBM Redpaper publication explains what the key focus areas are for implementing a successful mobile government, how to address these focus areas with capabilities from IBM MobileFirst enterprise software, and what guidance and preferred practices to offer the IT practitioner in the public sector.

This paper explains the key focus areas specific to governments and public sector clients worldwide in terms of enterprise mobility and describes the typical reference architecture for the adoption and implementation of mobile government solutions. This paper provides practical examples through typical use cases and usage scenarios for using the capabilities of the IBM MobileFirst products in the overall solution and provides guidance, preferred practices, and lessons learned to IT consultants and architects working in public sector engagements.

The intended audience of this paper includes client decision makers and solution architects leading mobile enterprise adoption projects, IBM services and sales professionals selling IBM software and designing public sector client solutions that include the IBM MobileFirst product suite, and solution architects, consultants, and IBM Business Partners responsible for designing and deploying solutions that include the integration of the IBM MobileFirst product suite.

## **INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION**

### **BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:**  
[ibm.com/redbooks](http://ibm.com/redbooks)