Making Everything Easier!™

Oracle Special Edition

Enterprise Mobility FOR DUMMIES®

A Wiley Brand

Learn to:

- Understand enterprise mobile trends
- Integrate enterprise to mobile devices
- Secure mobile devices, apps, and content

Brought to you by

ORACLE

Lawrence C. Miller, CISSP

Enterprise Mobility

FOR DUMMIES®

A Wiley Brand

Oracle Special Edition

by Lawrence C. Miller, CISSP

FOR DUMMIES®

A Wiley Brand

Enterprise Mobility For Dummies®, Oracle Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-118-93087-8 (pbk); ISBN 978-1-118-93355-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Senior Project Editor: Zoë Wykes

Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Karen L. Hattan

Project Coordinator: Melissa Cossell

Table of Contents

Introduction

Mobile technology has matured as organizations look for transformative new ways to use mobility in their business strategies. Mobile-savvy consumers expect to interact with businesses seamlessly, across multiple platforms, with powerful, innovative, and engaging new mobile apps. Inside the enterprise, Bring Your Own Device (BYOD) and Corporate Owned Personally Enabled (COPE) mobile device policies have already taken root in many organizations, demonstrating the power of consumer demand to shape enterprise mobility strategy. And enterprise users, influenced by their consumer experience, demand advanced apps that are ever more capable and sophisticated. Enterprise mobility means untethered productivity.

Organizations need an enterprise mobility strategy to ensure that they can reap the business benefits of mobility and effectively address its many challenges. Much needs to be considered: client architecture, integrations, security, scalability, ongoing development, and maintenance. What tools and resources are available to help you measure and analyze the effectiveness of your mobile strategy? Will you be ready?

About This Book

Enterprise Mobility For Dummies, Oracle Special Edition, consists of six chapters that explore the modern challenges and opportunities in enterprise mobility, including development, integration, and security issues.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I'll assume a few things nonetheless. I assume that you know a little something about mobility challenges in the enterprise. As such, this book is written primarily for executives and managers, such as Chief Information Officers (CIOs), functional line-of-business (LOB) managers, and technical managers.

Icons Used in This Book

In this book, you occasionally see these icons that call attention to information that's particularly worth noting:

This icon points out information that may well be worth committing to memory.

This icon points out useful nuggets of information.

These helpful alerts offer practical advice.

Beyond the Book

Oracle Mobile Platform is a unique enterprise mobility platform that complements and extends other products within the Oracle Fusion Middleware family. You can learn more about Oracle Mobile at `www.oracle.com/mobile`.

Chapter 1

The State of Enterprise Mobility

In This Chapter

- Recognizing the new normal
- Taking stock of the mobility trend
- Knowing your mobile audience

The rapid growth of the worldwide mobility trend over the past decade has been incredible. Mobile devices are spreading faster than any other consumer technology in history. Smartphones now outsell PCs, and touchscreens outnumber keyboards.

This chapter introduces some key mobile concepts and technologies, enterprise mobility challenges and opportunities, and some common mobility use cases in the enterprise.

The Mobile Status Quo

For many years, IT departments looked to the desktop as the only way to present information from their enterprise applications. Mobile computing has changed

everything. Applications are no longer tied to the desktop and users expect to transition seamlessly between desktops, tablets, and smartphones anytime and anywhere. Thus, the multichannel experience is evolving to an omnichannel experience and has become the new normal for all consumers.

Multichannel refers to the use of numerous, separate channels to interact with a customer such as in a retail store, an online store, a mobile store, a mobile app, or a telephone conversation. *Omnichannel* refers to the use of numerous integrated channels to interact with a customer in an holistic manner, seamlessly across all channels.

In addition to external customers, in many cases the mobility trend is driven from within the organization, as marketing departments, line-of-business (LOB) managers, and innovative users accelerate the need for a mobile strategy. Responding to pressure from the user community to get new mobile applications up and running quickly, many organizations have turned to third-party agencies to rapidly create tactical mobile apps. Internally, IT shops have turned to native, device-specific development frameworks simply to satisfy short-term needs without considering the impact and cost of integration, security, and ongoing maintenance and support of multiple platforms.

These conflicting demands have led to growing challenges within the IT department as it struggles to develop and maintain a growing set of mobile applications for various platforms and device types. This strategy is difficult to scale because supporting native applications across multiple current and growing mobile platforms can

quickly become overwhelming. IT pros need to implement effective and scalable strategies for the short term and over time.

Rather than continuing to develop applications for the desktop first and then making tactical mobile development choices, IT leaders want a consistent architecture that considers all channels — desktop, web, mobile, and otherwise — a true omnichannel strategy. IT needs to expose their enterprise data and applications in a secure and flexible manner to support the many ways that users choose to access those applications. Achieving this goal will require a flexible, unified platform for building and accessing corporate applications.

Mobile Growth and Trends

Enterprise mobility is inevitable, and the challenges faced by IT are significant. According to a recent *CIO Insight* magazine survey, these are the top three mobility challenges cited by CIOs:

- Securing corporate information (41 percent)
- Integrating with other systems (31 percent)
- Supporting multiple devices (28 percent)

Mobility is an imperative for enterprises that want to compete effectively across any industry. According to *CIO Insight*, 67 percent of organizations are seeking increased productivity and 57 percent expect to improve customer service with their mobile investments. A recent *CIO Magazine* study found that only 10 percent of organizations polled have mobile apps in production enterprisewide, while another 23 percent have mobile apps in production within a business unit or division,

and another 52 percent are actively researching or piloting mobile apps. There's clearly strong interest and ample opportunity for a mobile enterprise, and the pace is quickening. A 2014 Triangle Research survey found that 87 percent of enterprises are updating or releasing mobile apps every six months or less.

IT has an opportunity to work with line-of-business leaders to define enterprise omnichannel mobile strategies that transform an organization. Although organizations used to be more concerned about how they were going to develop their apps, today's CIOs are realizing that enterprise mobility is expensive. According to a recent McKinsey report, 41 percent of CIOs cited mobility as an expensive-but-critical challenge with the annual cost per device being as much as $250, including the cost of connectivity, infrastructure, and support.

The Bring Your Own Device (BYOD) trend has taken hold in organizations, as employers increasingly recognize the benefits by allowing — even enabling — employees to use their personal mobile devices for work-related purposes.

When organizations adopt a permissive BYOD policy, they are better positioned to control and secure personal mobile devices in the organization while enjoying the BYOD productivity benefits. Rather than playing a cat-and-mouse game with each other, IT staff and end users can work together to define and implement workable strategies for securely and efficiently enabling BYOD.

An alternative to the traditional corporate-owned device policy that is gaining traction is the Corporate Owned, Personally Enabled (COPE) model. With COPE, the

organization provides its users with a choice of approved devices and apps but also allows the employee to use the device for personal use, such as installing third-party apps and games, personal calls, and storing personal information.

Whether the strategy is BYOD or COPE, the mix of personal and business apps in the organization adds a level of complexity to the environment that did not exist before, but that IT must address going forward.

Employees, Customers, or Both?

Mobile blurs the boundaries between the office and home for both your employees and your customers. Thus, your enterprise mobility strategy needs to consider both.

Connected workforce (B2E)

The modern workforce expects to be able to connect to the corporate network any time, and from varying devices. Your enterprise mobility strategy should address this reality with policies that safely enable employees to be productive, from a multitude of devices, anywhere, anytime.

Connected marketplace (B2C)

Consumers increasingly expect to engage businesses through multiple channels. Such interaction has to be convenient and seamless, enabling the customer, for example, to compare products on a desktop computer at the office, continue researching selected products and initiate a product inquiry through online chat on a tablet in a coffee shop, and call a contact center on a

smartphone at home. The organization must be able to track this entire interaction regardless of the devices or locations that the customer uses, in order to provide a seamless and exceptional customer experience.

As such, organizations need to have an enterprise mobility strategy that enables them to be responsive and adaptive, delivering an omnichannel experience to the consumer.

In the mobile world, it's all about convenience, speed, and ease of use to the consumer. Mobile apps offer the presence and convenience that increase sales.

Chapter 2

Mobile Apps

In This Chapter

- Considering mobile client architectures
- Going from Mobile-First to Mobile-Plus
- Integrating mobile features
- Developing and deploying apps
- Building for the future

How do you simplify your mobile application architecture and remove the need to code for unique devices and platforms? And how do you use your existing architecture and skill sets? In this chapter, you learn about mobile client architectures, mobile app design principles, developing and deploying mobile apps, and the need to future-proof applications.

Mobile Client Architectures

The mobile client architecture that your organization adopts has important considerations, such as:

- Development and maintenance costs
- Multiplatform support

- Performance requirements
- Integration to backend systems
- Native device services
- Offline capabilities
- Security
- Total cost of ownership (TCO)

Here are three mobile architectures to consider:

- **Web:** The application runs on a browser and is optimized for mobile devices using HTML5 (HyperText Markup Language version 5). This approach has relatively limited functionality (compared to native or hybrid architectures) but is simpler to support across multiple platforms. Two popular approaches to web design are M.dot and Responsive Web Design (RWD). M.dot requires organizations to develop and host separate websites that are specifically optimized for mobile devices. RWD automatically detects the type of device accessing a website and dynamically optimizes the content and layout for that device.
- **Native:** A mobile application is built for each mobile OS platform to be supported. Native offers the full functionality that the device platform offers, but the code is platform-specific to the device and thus more expensive to develop and support if you decide to support other platforms (for example, iOS and Android).
- **Hybrid:** Hybrid is a combination of the web and native architectures. With hybrid, a native container is installed on the device to help integrate with local device services and support offline

capabilities. For the interface, hybrid architectures leverage the device's browser-rendering engine (not the browser itself) to render HTML5 and process JavaScript. This approach provides easier cross-platform support offered by the web architecture with the benefits of on-device capabilities typical of a native app. A hybrid architecture combines the flexibility of web apps with the capabilities of native apps.

Choosing between a web, native, or hybrid mobile architecture depends on user needs. Web mobile apps offer flexibility, but the trade-offs are that they require network connectivity to work and offer limited device integration functionality. Selecting a native or hybrid architecture enables you to integrate your mobile apps with device-specific features such as the camera, GPS (Global Positioning System), or accelerometer. An app that can access device features is more capable and enriches the user experience. Native is feature-rich but platform-specific, requiring more development and maintenance resources for each platform. Hybrid combines the best of both worlds, which is cross-device flexibility with native device capabilities under one framework.

Developing Mobile Apps

Mobile users set high expectations for mobile apps with regard to overall user experience, user interface, and user convenience — specifically, the appearance, ease of use, and behavior of mobile apps. When developing mobile apps, thought must be given to user context and mobile design guidelines such as touch first,

mobile gestures, simplicity, search, and voice interfaces. The mobile app experience should be intuitive to the user.

For developers, new UI design skills are required and the choice of tools to support cross-platform capabilities and Mobile Web must be weighed to support these mobile requirements.

When developing your mobile apps, you need to understand the use case and define the type of mobile app that you want to build and then use the appropriate mobile development framework. The customer experience is an increasingly mobile one thanks to the ubiquity of mobile phones and tablets. As usage has grown, a rich and engaging mobile experience has become a necessary component of an organization's digital strategy. The challenge, however, is in creating and managing mobile experiences that are optimized for delivery to the thousands of different devices.

Apache Cordova, based on Phone Gap, is an open-source framework for building hybrid mobile applications using a set of device APIs (application programming interfaces) that is commonly leveraged by hybrid frameworks to enable device features access across platforms. Cordova allows developers to build mobile apps using JavaScript, HTML5, and CSS3 (Cascading Style Sheets version 3) rather than native, device-specific programming languages.

Mobile-First to Mobile-Plus

Traditional enterprise apps are fully self-contained applications with no dependencies on other applications or software code. Customer relationship

management (CRM) and enterprise resource planning (ERP) software are examples of traditional enterprise applications that provide a full suite of functionality.

In contrast, mobile first apps are more focused in terms of functionality. Instead of a mobile CRM app, mobile first apps might provide separate contacts and sales order apps, both tied to the CRM server backend. Similarly, you might have a timesheet and an expenses app that share an ERP backend. Focusing the functionality of mobile first apps simplifies their design and shortens development cycles.

Today, having a Mobile-First strategy is expected, and we are now moving to the era of Mobile-Plus. The Plus is about the convergence of mobile, cloud, and the Internet of Things (IoT), and the need to consider the client, content, context, and cloud as core components of an enterprise mobile strategy.

Deploying Mobile Apps

You can deploy your consumer apps in a public apps store, such as the Google Play or Apple's App Store. For enterprise deployments, you may want to consider deploying your own enterprise app store. Having a centralized and automated management of device security, app management, and app deployment can offer great benefits integrated with user access rights, roles, and authorization policies. A robust Mobile Application Management (MAM) system offers the capability to host an enterprise app store to create internally managed groups to deploy, update, and manage corporate apps on employee devices.

14

Future-Proofing Your Mobile Architecture

You need to ensure that your mobile development strategy provides cross-platform support for different mobile OS platforms. Google Android and Apple iOS platforms have no code sharing — even the user interface needs to be customized because of diverse display requirements.

Today, Android and iOS are the dominant operating systems in the smartphone and tablet categories. However, the mobile industry continues to evolve, and there's no telling what the next big thing will be or who will dominate the market in the future.

Flexibility is key to future-proofing your mobile architecture. You should consider the costs of writing, supporting, and maintaining applications for different mobile platforms and form factors. A cross-platform architecture based on standards such as HTML5, JavaScript, and Java that can be deployed to multiple platforms while still meeting the needs of your customers helps ensure compatibility, as well as a large pool of developer resources that are familiar with these technologies.

Chapter 3

Mobile Integration

In This Chapter

- Looking at mobile styles and formats
- Integrating services
- Improving business processes
- Scaling up with an enterprise service bus
- Building for the future with MBaaS

This chapter discusses strategies for integration and creating or leveraging a services strategy designed for mobile but leveraged by other channels. It also explains some of the tools used for mobile integration, how to plan and build your mobile architecture for future scalability, and opportunities for mobile innovation.

Service Integration

Integration between applications is challenging in and of itself. Integrating the apps on a mobile device with your organization's backend systems — whether on premise or in the cloud — can make the integration challenge seem Herculean.

Mobile integration introduces challenges that differ from traditional integration issues. For example, mobile developers must consider issues associated with network connectivity, latency, bandwidth, carrier costs (data plans), and device battery life, among others, as they design an app to remotely consume organizational backend data and other external data sources.

From a scalability perspective, mobile developers and backend service developers must consider the impact of mobile traffic and load on backend systems that weren't originally designed for mobile apps.

Service integration is one possible solution. Mobile developers can integrate their client-side code with services exposed from the backend data sources via RESTful (Representational State Transfer) APIs (application programming interfaces), discussed in the next section, to help address some of these challenges.

REST and JSON

REST (Representational State Transfer) is a software architectural style for distributed systems. REST uses standard HyperText Transfer Protocol (HTTP) methods to return content to the browser. Because REST uses the standard HTTP protocol, it is a widely accepted means of connectivity. JSON (JavaScript Object Notation) is a popular format, considered lightweight compared to XML (Extensible Markup Language) or SOAP (Simple Object Access Protocol) and easier to use.

You can learn more about JSON at `www.json.org`.

You can easily call REST from JavaScript and return JSON for a very powerful result. Given the ubiquity of HTTP and the simplicity of REST/JSON, they have largely become the de facto standards for mobile apps to connect to backend servers.

Business Process Management

Business process management (BPM) represents a strategy of managing and improving business performance by continuously optimizing business processes in a closed-loop cycle of modeling, execution, and measurement. BPM makes mobile apps richer, going beyond relatively simple applications.

Most organizations maintain information in separate systems, such as prospect data in Sales Force Automation (SFA), order information in Enterprise Resource Planning (ERP), and customer issues in Customer Resource Management (CRM). To best serve the customers, organizations must pull information scattered across these systems. BPM helps you deliver these experiences and design customer experiences that integrate the underlining channels, systems, and applications to make sure that accurate, consistent information is delivered to the right people at the right time across any channel of interaction.

Enterprise Service Bus

To achieve scalability and mobile enablement, consider using an enterprise service bus (ESB) in your mobile architecture. An ESB acts as a mediation, integration, and interface layer between your existing systems and your mobile and cloud technologies.

For example, you may have one or more ERP systems installed, and some of these systems may support SOAP and REST interfaces. But you should think twice before simply publishing these interfaces as your mobile service layer. Publishing application-specific interfaces directly to mobile devices tightly couples them to each other. Using an ESB as a service mediation layer helps to loosely couple your mobile clients from your enterprise IT systems, resulting in greater flexibility and agility. An ESB offers a flexible, common interface over your backend systems, quickly enabling them to participate in the mobile world.

Mobile Backend as a Service

Mobile Backend as a Service (MBaaS) is a model for providing web and mobile app developers with a way to link their mobile applications to integrate with server-side enterprise services and data through a cloud-based environment. A complete MBaaS offering should include the following:

- Cloud-based data storage
- Automatic RESTful API generation
- Optimized access to data (for example, JSON)
- User authentication
- Push notifications
- Analytics

Chapter 4

Mobile Security

In This Chapter

- Protecting smartphones and tablets
- Securing apps and data
- Taking a look at backend security

According to a recent *Forbes* magazine article, 65 percent of organizations allow personal devices to connect to the organization's network and 78 percent say that more than twice as many personal devices are connected to organizational networks now than just two years ago. These sobering Bring Your Own Device (BYOD) statistics necessitate an enterprise security strategy that allows employees to continue to leverage mobile devices productively while protecting access to organizational applications and data.

This chapter delves into the different mobile security issues to consider in your mobile security strategy.

Securing Mobile Devices

With the proliferation of mobile devices and increased BYOD adoption, organizations have an increased

requirement to secure access to information and applications from these less secure personal devices. When an employee's personal smartphone or tablet is lost or stolen, or an employee leaves the organization, sensitive systems and data may be at risk.

Securing Mobile Applications

BYOD adoption has resulted in IT no longer having traditional control over mobile devices in an organization. IT has the following key security challenges in managing mobile apps:

- Integrating with organizational access and governance policies
- Separating business apps from personal apps
- Securing business apps to create trusted apps, regardless of where they came from or how they were developed
- Encrypting data stored on the device and sent over the Internet
- Securing communication of data from apps to the organization without requiring a VPN
- Ensuring data leakage prevention policies are implemented in the app
- Wiping the business container remotely and preventing access when employees leave

Business apps must be developed in a secure framework that provides proper authentication and authorization to protect sensitive data.

The use of secure application containers provides application management and security while enabling the

organization to deploy approved mobile apps. Mobile application management (MAM) also may include the ability to whitelist, or approve, authorized apps and blacklist, or block/quarantine, unauthorized apps.

Securing Mobile Content

Sensitive corporate and/or customer data that are stored or accessed on personal devices must also be addressed in your enterprise mobile security strategy.

Content management software secures mobile content stored or accessed on the mobile device through a number of capabilities, including the following:

- **Antivirus/anti-malware:** Protects mobile devices from infection or propagation of malicious code — often referred to as malware.
- **Data loss/leak prevention:** A system designed to detect/prevent sensitive data, such as financial or personal information, from being accidentally or maliciously copied or distributed (for example, via email or text).
- **Mobile user identity:** Protects user credentials (such as usernames, passwords, and security certifications) from unauthorized disclosure if the device is lost, stolen, or compromised.
- **Encryption:** Data that is stored or processed on the device, as well as data that is sent over the air and encrypted to prevent unauthorized access if the device is lost, stolen, or otherwise compromised.

Server-Side Security

If business apps that access backend systems are installed on a mobile device that is lost or stolen, these systems and data may be compromised. User and device authentication should be enabled and required on mobile devices that access organizational systems and data.

Your mobile application framework and reference architecture needs to address traditional server-side security risks, such as denial-of-service attacks, buffer overflows, and cross-site scripting.

Beyond exposing RESTful (Representational State Transfer) APIs (application programming interfaces) for integration, organizations must also look at securing access to the APIs themselves. This access should be integrated with the user authentication and authorization policies. Use of location services further enhances security access to corporate data via these APIs, such as preventing access to certain APIs based on user location or if the same user is trying to access data from two different locations at the same time.

Chapter 5

Exploring the Oracle Mobile Platform

In This Chapter

- Looking at Oracle Mobile Suite
- Learning about Oracle Mobile Security Suite
- Discovering Oracle WebCenter
- Getting to know Oracle Mobile Cloud Service

Oracle Mobile is about simplifying enterprise mobility, giving organizations a complete mobile solution and the choice and flexibility to develop a strategy that suits varying situations. Whether you prefer turnkey mobile applications or decide to develop and extend your existing enterprise applications, Oracle provides the platform, security, and tools to meet your needs.

This chapter talks about Oracle's complete mobile solution for the enterprise.

24

Oracle Mobile Suite

The Oracle Mobile Suite is an integrated suite of products that enables organizations to build all the layers of their mobile applications in a simpler way, targeting multiple client devices and backend sources of data, based on a scalable and robust architecture. The suite provides support for the development of both the front-end client and the backend integration layer of a mobile system. Key features of Oracle Mobile Suite include the following:

- Productivity-boosting mobile development framework
- Cross device/operating system deployment
- Lightweight and robust enterprise service bus
- Extensive connectivity through adapters
- Integrated security and governance

Benefits of Oracle Mobile Suite include these:

- Reduce integration complexity and cost
- Develop once and deploy to various devices and operating systems
- Build a scalable and robust shared services infrastructure
- Create a mobile optimized service layer for applications
- Simplify mobile application development
- Achieve extremely high performance and scalability for mobile services

Oracle Mobile Application Framework

The Oracle Mobile Application Framework (MAF) is a Java and HTML5 hybrid mobile framework that enables developers to build single-source applications that install and run on multiple devices, including phones and tablets running both iOS and Android operating systems. The framework provides a robust architecture for mobile applications and leverages a model-view-controller design to deliver applications that are easier to develop and maintain (see Figure 5-1).

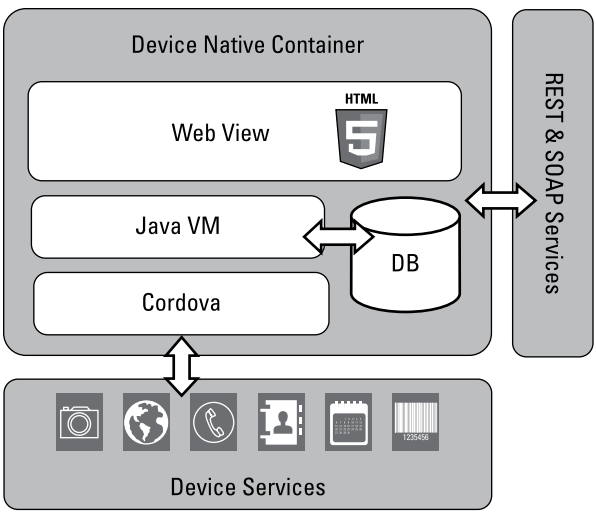

Figure 5-1: Oracle Mobile Application Framework.

Developers build a single application, using a visual and declarative development approach, which is then packaged and installed as a native application on these devices. A library of more than eighty professionally developed components simplifies the development of rich user interfaces (UIs), providing native-like user experience, touch gestures, and animation.

Developers can leverage the power of the Java language, both for the data model and the controller layer, to define the business logic of their applications. For the user interfaces, the framework uses HTML5 to deliver a native-like experience across devices with support for touch gestures and animations. The Java logic and HTML5 user interface execute inside a native container that is able to interface with local device features, as well as receive push notification events on multiple platforms.

For developers who prefer to code with JavaScript, the framework provides a set of JavaScript-based application programming interfaces (APIs) to integrate with the container and the Java features that they can use in their mobile HTML5 pages. Developers can also code HTML5/JavaScript pages with popular third-party JavaScript libraries (such as Sencha, Dojo, Backbone.js, and JQuery Mobile) — that would run on the device as well. HTML pages generated by remote servers can also be incorporated into the same application. The mobile container used by the framework enables each of these solutions to easily access device features.

Applications built with the framework can connect easily to backend services using either Representational State Transfer (REST) or Simple Object Access Protocol (SOAP) web services. For local persistence, a SQLite

database is included for storing data locally to increase application performance and enable offline operation in a secured way. Encryption capabilities are also included to protect the data if the device is compromised.

The Oracle JDeveloper IDE and Oracle Enterprise Pack for Eclipse provide visual tools that further simplify development. Oracle development tools integrate with both the iOS and the Android Software Developer Kits (SDKs) to enable direct deployment and test/debug capabilities to devices and emulators.

Oracle Service Bus

Oracle Service Bus (OSB) provides performance and scalability for all dimensions of your architecture. Applications need to scale in many dimensions — vertically, horizontally, with user numbers, and with message size. Scalability with an increasing number of services is an important and often ignored dimension of mobile architectures. OSB is designed to mediate, integrate, and interface heterogeneous services, legacy applications, and multiple enterprise service bus instances across an expanding service network, with built-in support for high-performance and low-risk cloud services incorporation. Simply put, OSB is a powerful tool for mobile-enablement of enterprise applications to participate in a mobile environment.

Your organization must be able to support emerging and future trends in mobile computing. Rewriting your existing enterprise systems to support mobile, cloud, and future technologies just isn't practical.

The service bus uniquely combines service integration, messaging, caching, operational service management, and security-enforcement capabilities. It offers unparalleled quality of service (QoS) through unique policy-based service virtualization, service pooling, and throttling capabilities that meet the demands of high-volume mobile projects (see Figure 5-2).

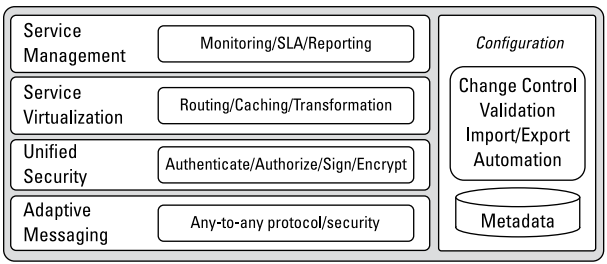

Figure 5-2: Oracle Service Bus components and architecture.

OSB provides the following capabilities and benefits:

- **Mediation:** Provides a rich environment for content-based routing, message transformations, and lightweight orchestrations. Using OSB as a service mediation layer helps to loosely couple your mobile clients from your enterprise IT systems, resulting in greater flexibility and agility.
- **Security:** Provides a rapid service configuration and integration environment that abstracts policies associated with routing rules, security, and service endpoint access. OSB supports a wide

variety of security protocols and applications including Oracle Access Manager, Oracle Identity Manager, Active Directory, and custom security protocols.

- **Service Level Agreements (SLAs) and metrics:** An SLA gives you the visibility you need to make guarantees, such as performance and availability, to your internal and external customers. When you create an SLA, you define the rules that define service performance.
- **Caching:** OSB comes complete with a networkable cache that can significantly boost the performance of your services. Presenting relatively static data, such as a product catalog, provides a simple example of this caching capability. Your customers may make thousands of requests daily to view your product catalog and the details of each product. It's likely that your product catalog doesn't change during the day. Caching results offloads additional requests to your backend catalog system. This is all done through a simple interface that can be quickly configured.
- **Reporting:** OSB comes with built-in reporting capabilities that give you access to the information you need most. Whether you're reporting for Sarbanes-Oxley (SOX) compliance purposes, mining data, creating dashboards, archiving data, or for any other reason, the powerful reporting capabilities of OSB make it simple, and you can generate report entries for an entire service, or at any point within a service's processing logic.

Oracle Mobile Security Suite

Solutions such as mobile application management (MAM) require mobile devices and apps to be locked down in accordance with an organizational policy to provide security. This creates privacy and usability issues because consumer devices are required to always adhere to corporate policies — even for personal use.

Oracle Mobile Security Suite (OMSS) overcomes these challenges by isolating corporate from personal data on consumers' personal mobile devices without needing to lock down the entire device. Oracle's Mobile Security Container technology protects corporate apps and data and enables a Secure Enterprise Workspace (see Figure 5-3) that meets enterprise security requirements without compromising user experience. This technology offers the most integrated solution with Windows authentication infrastructure for secure single sign-on (SSO) to corporate applications.

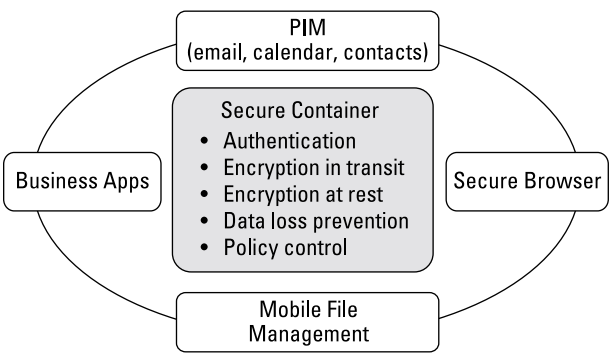

Figure 5-3: Oracle's Secure Enterprise Workspace.

Secure mobile container apps

OMSS comes with a set of enterprise-ready productivity apps that ensure that organizational data is always protected, including the following:

- **Secure Web Browser**
  - Access Intranet sites secured with Kerberos or NTLM
  - Run HTML5 applications including offline support
  - Download files into file manager (if your security policy allows it)
- **Secure File Manager**
  - Access network files on Windows File System or Microsoft SharePoint
  - Move or copy files to/from local file store (if your security policy allows it)
- **Secure Email, Calendar, Contacts, Tasks, Notes**
  - Supports any ActiveSync mail server in a native client, including Microsoft Exchange, Google Apps, and Lotus Notes
  - Can restrict attachments to the container

Here's a list of solution components:

- **Mobile Security Container:** Ensures security by isolating personal information from corporate data and apps. Provides authentication, SSO, and FIPS 140-2 encryption.
- **Mobile Security Access Server:** Offers secure Intranet access from mobile devices with zero programming, simple deployment, and low overhead

cost. This component typically sits in a DMZ and provides an app-level SSL tunnel from the Mobile Security Container only, which eliminates the need for device-level VPNs and the risk of rogue apps. Supports SSO authentication via Kerberos or NTLM protocols utilizing username/password or PIN-protected, PKI (Public Key Infrastructure) certificates.

- **Mobile Security Administrative Console:** Provides remote management of containers, logging, policy enforcement, application management, application store, and remote container lock/wipe. Can easily be integrated with Active Directory to manage users/groups. Provides detailed usage statistics and reports.
- **Mobile Security File Manager:** A component of the Mobile Security Administrative console that provides a WebDAV front end to internal SMB/CIFS file shares so that they can be exposed in a consistent fashion over HTTP/HTTPS.
- **Mobile Security Application Wrapping Tool:** Provides a toolset to inject security functionality into apps running on iOS devices, thereby linking them to the iOS Container.

Oracle WebCenter and Business Process Management

For organizations with an existing Oracle WebCenter implementation, out-of-the box mobile options are available with Oracle WebCenter Portal, Oracle

WebCenter Sites, and Oracle WebCenter Content. This suite of products combined with Oracle Business Process Management enables organizations to easily extend their traditional web presence to the mobile channel and to deliver highly personalized and relevant multichannel experiences, while also saving significant time and effort in managing mobile sites, portals, and content. By reusing existing web content, site plans, and navigation for mobile delivery, organizations can deliver an engaging mobile web experience that meets the needs of today's demanding customers.

Oracle Mobile Cloud Service

Oracle Mobile Cloud Service (MCS) is an enterprise-grade Mobile Backend as a Service (MBaaS) that reduces the complexities of mobile application development and integration. Oracle MCS provides ready-to-integrate features, backend templates, and a standard mobile backend to deal with complex server-side programming, thereby reducing redundancy and complexity in backend code blocks. It provides a set of rich RESTful interfaces for all the operations required by the mobile app and abstracts the backend from the mobile developer. This abstraction enables mobile developers to focus on the front-end apps, using their choice of mobile client development tools for cross-platform hybrid apps, native development, and other JavaScript tools, and simplifies development by integrating with mobile-ready APIs exposed in the cloud.

MCS takes a unique, persona-based approach to provide tools and services to all of the organization's stakeholders, developers, and administrators. MCS comes with built-in, mobile-specific features including

- SDKs, APIs, and services to integrate with custom and third-party APIs
- Containers to build, shape, and orchestrate services in Java or JavaScript (Node.JS)
- Service scaffolding via RESTful API Modeling Language (RAML), integrated security, analytics, monitoring, and management

Chapter 6

Five Key Considerations for Defining Your Mobile Strategy

In This Chapter

- Looking at issues to consider in your mobile strategy

This chapter covers some things you need to consider when defining your enterprise mobile strategy.

Think about the Business Case

Mobility is impacting how we look at nearly everything, so having a clear vision of what the business is hoping to achieve with mobility is important. You should identify one or more expected business outcomes, either quantified or qualitative. For example, the business goals might include

- Improve customer service
- Increase employee productivity
- Deliver a more differentiated service
- Reduce operational costs

Mobile development is an important component of your overall mobile strategy. Here are some questions to consider:

- Should you use in-house teams or an external agency?
- What frameworks and tools are available?
- What existing skills and resources do you have, and what training is needed?

Remember, it's not just about a slick client app. Integration to internal and external systems, and delivery of relevant and related information is a necessity. Having a standardized platform to support the execution of your mobile strategy is important.

You should incorporate service-oriented architecture (SOA) principles and industry best practices tailored to your organization's specific needs. Also consider

- What enterprise apps and data sources need to be integrated?
- What existing infrastructure needs to be incorporated?
- What are the required updates and maintenance of the application's lifecycle and continuous improvements over time?

Address Mobile Security

You need to address how you will secure devices, apps, content, and backend systems. Consider the following:

- For B2E (business-to-employee), BYOD (Bring Your Own Device) and COPE (Corporate Owned, Personally Enabled), you should consider a

Mobile Application Management (MAM) solution linked to existing enterprise identity management.

- For B2C (business-to-consumer), will authentication be provided through user registrations or social logins?

Your mobile security policy should be aligned with your existing organizational security policies. Mobile security policies have implications for your company's employees and customers.

Important considerations include these:

- For B2E, will you adopt a BYOD or COPE policy?
- For B2C, you need to support many different mobile platforms, or you risk alienating some customers.

Google Android and Apple iOS are the two primary mobile OS platforms today, but what's coming next? What specific devices and mobile operating systems will your apps be tested on?

Focus on Innovation and Business Agility

Your mobile strategy will be largely defined by where you are with regard to your apps, where you're going, and how you plan to get there. Consider the following questions:

- What apps does the organization already have?
- What apps are you planning to deploy?
- How often do you plan to update the app?

- Are your mobile apps commercial off-the-shelf (COTS) or custom developed?

Remember the "There's an app for that!" mantra but don't lose sight of the customer. It's all about user convenience and driving productivity.

Be Proactive with Support

Ensure that you have the infrastructure to deploy, monitor, and support the apps you develop. Your apps don't have to be perfect. Users expect regular and frequent updates to their mobile apps, but be sure that you're able to proactively support your internal and external customers.

Important questions and issues to consider include the following:

- How will you deploy your apps and how often? Through a public app store or a private enterprise app store?
- If customers can use the app 24/7, what do you need to do to ensure that the backend infrastructure is available and reliable?
- App analytics monitor feature usage and help the business understand whether its mobile strategy is effective and transformative; you need to continually look for ways to improve the end-user experience. Keep in mind that you need to deliver continuous improvements over time.
- With a myriad of apps, a common API to the backend needs to keep up with the speed of mobile advancements.

- Cloud and mobile technologies are converging. Your architecture must be ready for this trend.
- What is your architectural roadmap for the next three to five years?

Establish Effective Governance

Executing your mobile strategy requires effective governance, including the following:

- How will the organization ensure that strategy is properly implemented and enforced?
- Do you have executive sponsorship and authority?
- Will you establish a corporate program office?

You have many important issues to consider, but ultimately the goal of your organization's mobile strategy should be to drive innovation and ongoing business agility, not to achieve perfection.

Glossary

API (application programming interface): A set of routines, protocols, and tools that specify how certain software components interact with each other.

CX (customer experience): A customer's total experience with a business.

DMZ (demilitarized zone): An area of a corporate network where services are exposed to an external network, such as the Internet.

FIPS (Federal Information Processing Standards) Publication 140-2: Defines the security requirements for cryptographic modules specified by the U.S. National Institute of Standards and Technology (NIST).

HTML (HyperText Markup Language) and HTML5: The primary language used for creating web pages that can be displayed in a web browser.

HTTP (HyperText Transfer Protocol): The application protocol that is the foundation for data communication over the Internet. HTTPS is a secure communication protocol layered on top of SSL. See ***SSL***

JSON (JavaScript Object Notation): An open standard format that uses human-readable text to transmit data objects.

Kerberos: A ticket-based computer network authentication protocol.

MAM (Mobile Application Management): Software used to provision and control access to mobile apps across an organization.

MDM (Mobile Device Management): Software used to secure, monitor, manage, and support mobile devices, such as smartphones and tablets, across an organization.

NTLM (NT LAN Manager): A suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users.

QoS (quality of service): Control mechanisms used to affect the overall performance of a network.

RAML (RESTful API Modeling Language): A non-proprietary, vendor-neutral, open specification that describes RESTful APIs in language that is both human and computer readable.

RWD (Responsive Web Design): A web design approach that optimizes websites for display on a variety of devices, particularly smartphones and tablets.

SLA (service-level agreement): A formally defined contract for performance of a service.

SMB/CIFS (Server Message Block/Common Internet File System): An application-layer network protocol used primarily for sharing files and printers over a network.

SOAP (Simple Object Access Protocol): A protocol specification for exchanging structured information in the implementation of web services in computer networks.

SQLite: A relational database management system.

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Asymmetric cryptographic protocols designed to provide communication security over the Internet.

SSO (Single Sign-On): A form of access control that allows a user to log in to a single system in order to gain access to multiple independent systems.

VM (virtual machine): A software-based emulation of a physical computer.

VPN (virtual private network): A tunneling or encryption protocol that extends a private network across a public network, such as the Internet.

web service: As defined by the World Wide Web Consortium (W3C), a software system designed to support interoperable machine-to-machine interaction over a network.

XML (EXtensible Markup Language): A markup language specification that is both human- and machine-readable.

Notes

Transform your business by engaging all with mobile

The Bring Your Own Device (BYOD) mobility trend has transformed businesses — and the way that customers interact with businesses — everywhere. An enterprise mobility strategy is a must-have for businesses to compete effectively.

- ***Understand mobile trends — and how they impact your enterprise***
- ***Define your Mobile-Plus strategy — move beyond Mobile-First***
- ***Develop and deploy mobile apps — securely and efficiently in a highly scalable manner***

Open the book and find:

- **What to consider before defining your enterprise mobile architecture**
- **How to build a scalable architecture geared for the end user**
- **What Mobile Backend as a Service (MBaaS) is**
- **How to secure users, apps, content, and systems**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Oracle engineers hardware and software to work together in the cloud and in your data center. For more information about Oracle (NYSE:ORCL), visit oracle.com.

FOR DUMMIES®
A Wiley Brand

ISBN 978-1-118-93087-8
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.