IBM Security Systems
Identity and Access Management
October, 2013

GETTING STARTED WITH IDENTITY AND ACCESS MANAGEMENT FOR MOBILE SECURITY

Version 1.0

by
Patrick R Wardrop
Scott M Andrews

Table of Contents

Getting started with Identity and Access Management for Mobile Security

1 Executive Summary

Mobile computing is not new, but it is one of the most disruptive technologies in recent years. There are changes to form factors, increases in consumer use due to reduced costs and enhanced features, and shifts in social interaction and engagement. While it delivers productivity advancements, it also creates significant security challenges that change the traditional IT paradigm.

Devices for mobile computing include:

- Traditional notebook computers
- Smart phones
- Tablets
- Any portable WiFi or cellular device that provides data access

More mobile devices are in the hands of consumers. A *Internet Trends* article from 2012 reports that in May 2012 mobile internet usage in India surpassed the desktop internet usage[1]. In 2011, there was a 38% year-to-year growth of mobile internet usage in that country. In addition to this worldwide explosion of mobile-connected devices, companies now permit employees to connect personal mobile devices to the corporate network. This trend is commonly called *Bring Your Own Device* (BYOD).

Enterprises and their Chief Information Security Officer (CISO) face challenges in applying traditional enterprise controls to these devices. They require new security models, business policies, and controls to protect company assets and data. Protecting web and mobile applications requires IT groups to authenticate and authorize *both* the user *and* the device before they grant access. *Device authentication* associates the device with the owner and compares previous and current contexts of where and when the device accesses the resource. By authenticating the device and using a known context, an application owner can decrease the risk far beyond traditional access control practices.

Traditional access and authentication controls are no longer sufficient when employees and customers access the internet or intranet-facing resources with their mobile devices. Mitigating risk requires additional mobile security practices, such as risk-based access. *Risk-based access* can include device authentication, transactional context (including identity, device, location, time and so on), and user behavioral analysis.

This paper introduces common mobile security business scenarios. It also demonstrates how the IBM Security Access Manager family of products provides robust, enterprise-ready solutions to those scenarios.

---

[1] 2012 Internet Trends KPCB – Mary Meeker

2 Mobile Application Security with IBM Security Solutions

It is important to understand the various touch points of a mobile security engagement in your system architecture. Figure 1, IBM Mobile Security and Management Framework, outlines the various architectural components.

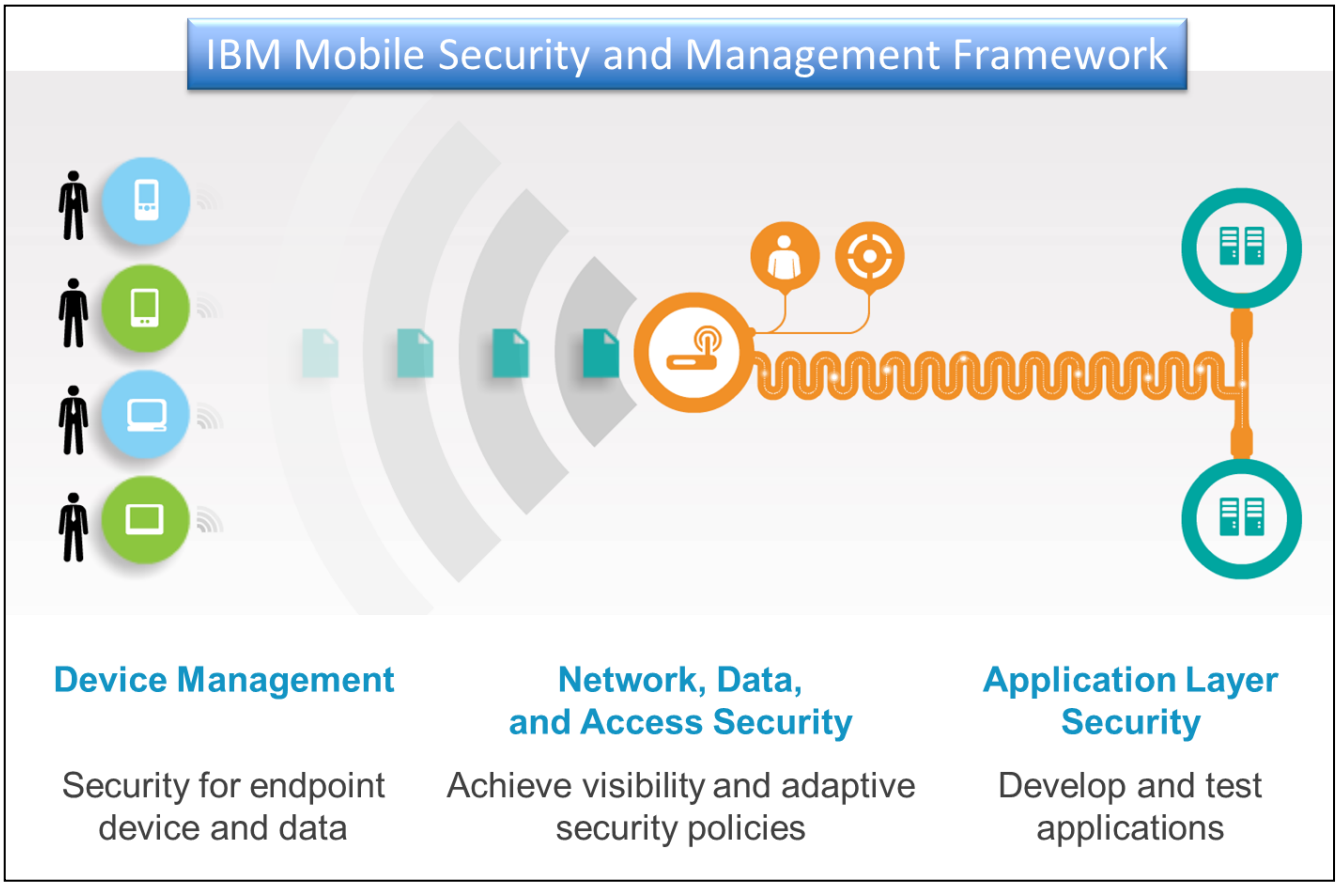

Figure 1: IBM Mobile Security and Management Framework

The three components include:

- Device management
- Network, data, and access security
- Application layer security

IBM Security Access Manager for Web and *Tivoli Federated Identity Manager* are industry-leading products that secure the access points into the network and enforce context-based access policies that define who and what can access protected resources.

Figure 2 illustrates the IBM Security Access Manager mobile security reference architecture, which is cited throughout this paper. It is important to understand the capabilities and role that IBM Security Access Manager for Web and Tivoli Federated Identity Manager play in the solution architecture for each business scenario.

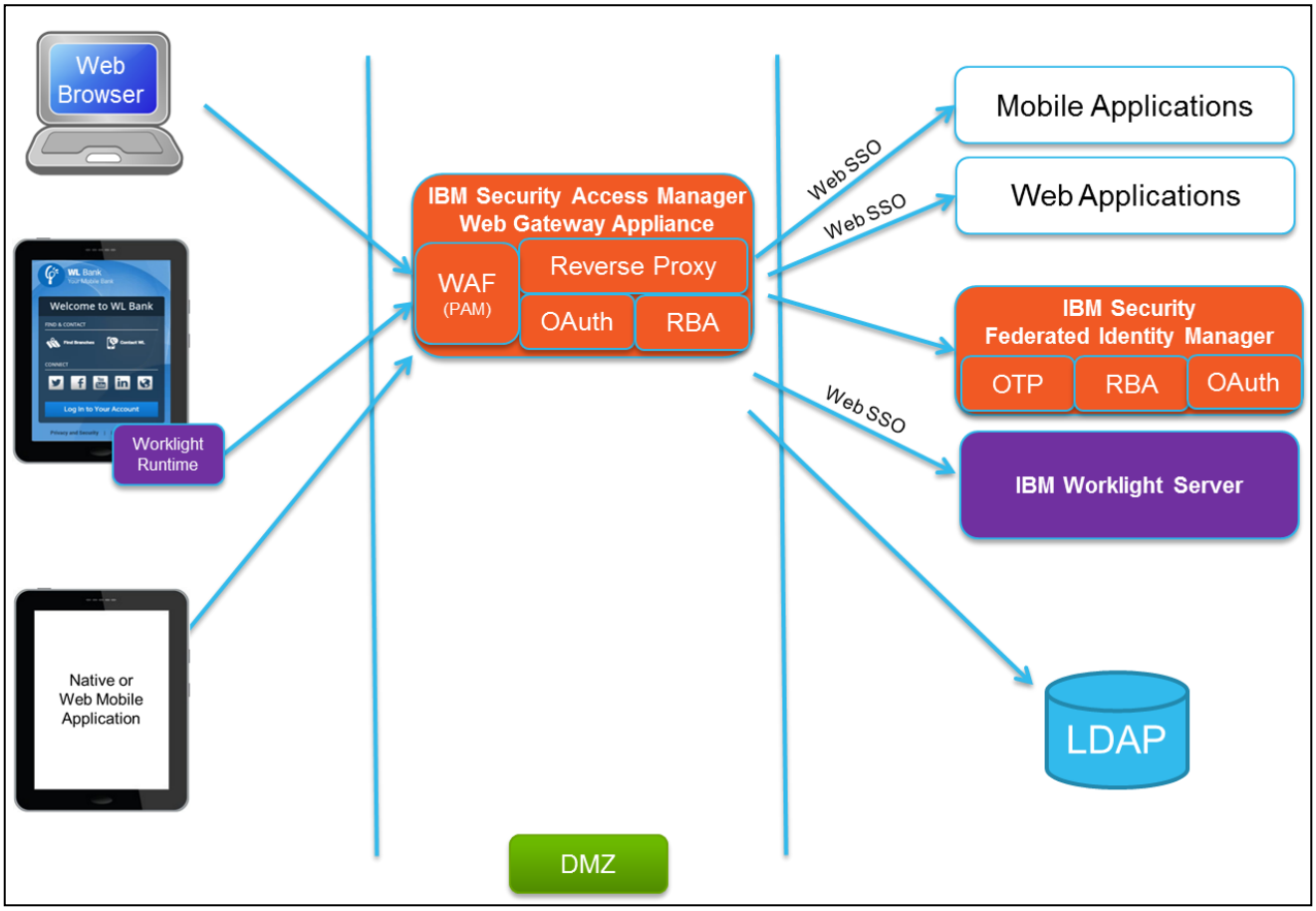

Figure 2: IBM Access manager mobile security reference architecture

2.1 Mobile Application Types

There are three main types of mobile applications:

Mobile web application

Typically, web applications have a touch-enabled interface and navigation, which is easy to use, but it might be slower and less reliable than native or hybrid applications. Mobile applications can be platform and device agnostic. They are more cost effective to implement, but they work only if the device is connected to the Internet.

Native application

This type of application uses only native widgets and interfaces, which are typically coded in the native language of the device. Examples include Java for Android and Objective C for iOS. This

type typically is more expensive to implement, has a fast user interface, and does not require Internet connectivity (offline).

Hybrid application

This type of application has a mix of native and web interfaces. It is cross-platform, has access to the device hardware, and can be used offline, although doing so might reduce functionality.

2.2 Identity and Access Maturity model for Mobile Security

The Identity and Access Maturity Model for Mobile Security can assist in the evaluation of solution offerings and mappings to business requirements. The model outlines the capabilities of an Identity and Access Management solution to determine the effectiveness of the offering.

Maturity Level	Capabilities
Basic	• Browser-based Federated Single Sign-On • Server-side Single Sign-On • Server-side application protection (Authentication, Authorization, Audit, Session Management)
Proficient	• Application access management • Device registration, authentication, and revocation (such as, OAuth) • Strong authentication (OTP, Device authentication, ...) • Application Virtual Private Networking (VPN) • Application threat protection (Web Application Firewall) • Connecting client's reputation
Optimized	• Access Monitoring and Reporting • Content Filtering/Prevent loss or leakage of sensitive information • Access governance / certification to mobile applications • Integration with SaaS and BaaS • Context / risk based access • Advanced and multi-factor authentication (Bio-metrics, behavior, analytics, ...)

3 Scenarios

The following scenarios examine typical mobile access. The use cases identify which components from the IBM Mobile Security and Management Framework can achieve different proficiency levels of the Identity and Access Maturity Model for Mobile Security.

3.1 Providing the basic mobile security architecture

This scenario focuses on securing a basic mobile application. It maps *to Server-side application protection* for the *Basic* maturity level.

Providing a basic level of security for any of the mobile applications requires:

Authentication
Identifies the user. The simplest way to authenticate is a user ID and password. Authentication typically challenges the users to enter their credentials either before the application launches or before they can access a protected resource.

Authorization
Permits or denies the user access to data or resources if they are a member of a specific group or role by using basic permission checks.

Audit
Tracks what the user did, when they did it, and to which resources or data they were granted or denied access by using various mechanisms and request gathering.

Session Management
Avoids passing the user's credentials on every request, but forces an authentication challenge if the user has been inactive for a period of time. Mobile data, especially roaming, can be expensive, which adds an additional business driver to the efficiency of mobile applications.

Protection against HTTP attacks
Provides entry-level protection against common HTTP attacks, such as SQL Injection, cross-site forgery, and cross-site scripting.

IBM Security Access Manager for Web can meet the preceding basic security requirements. Web Application Gateway, the out-of-the-box IBM Security Access Manager appliance offering, provides:

- Several authentication mechanisms
- Centralized coarse-grained authorization
- Authentication, audit, session management, and basic web application firewall protection

In Figure 3, Web Application Gateway is overlaid into the reference architecture. Using a combination of the Web Application Firewall (WAF) and web reverse proxy, the basic security requirements are met to achieve a ***basic*** maturity of the deployed solution.

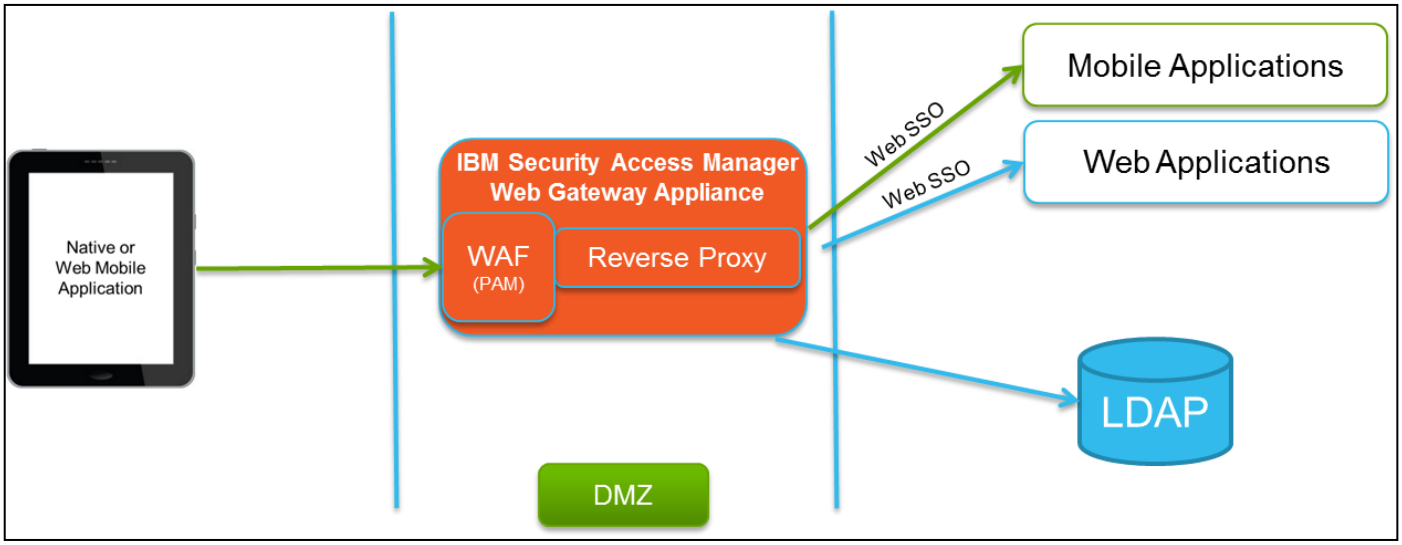

Figure 3: Basic mobile security Architecture

3.2 Making mobile applications identity aware at start-up

This scenario focuses on making a mobile application identity-aware at start-up. Due to the requirements of this scenario, only native and hybrid applications can achieve full identity awareness.

The “Providing the basic mobile security architecture” section introduced the concept of authentication. Mobile applications that provide basic authentication typically require users to enter their primary credentials when they log in. This method is not ideal on a touch-enabled mobile device because the user must enter long user IDs and passwords every time the application is started or when an inactivity timeout occurs. This requirement introduces several attack vectors, such as weak passwords, denial of service through account lockout as a result of multiple incorrect logon attempts, and so on. One solution is to store the user ID and password on the device. Although it improves the user experience, it can introduce even more attack vectors.

The OAuth standard offers an alternative, secure solution that removes most attack vectors and improves the usability of the application. With OAuth, the mobile application:

- Never stores or requires entry of the primary credential on the device.
- Does not require long password (or no password), but provides an application launch with optional PIN protection.
- Provides user or administrator-managed device revocation.

Using a combination IBM Security Access Manager for Web and Tivoli Federated Identity Manager, you can implement a mobile OAuth solution that increases user satisfaction, manages access management, and increases overall security. Figure 4 shows this solution.

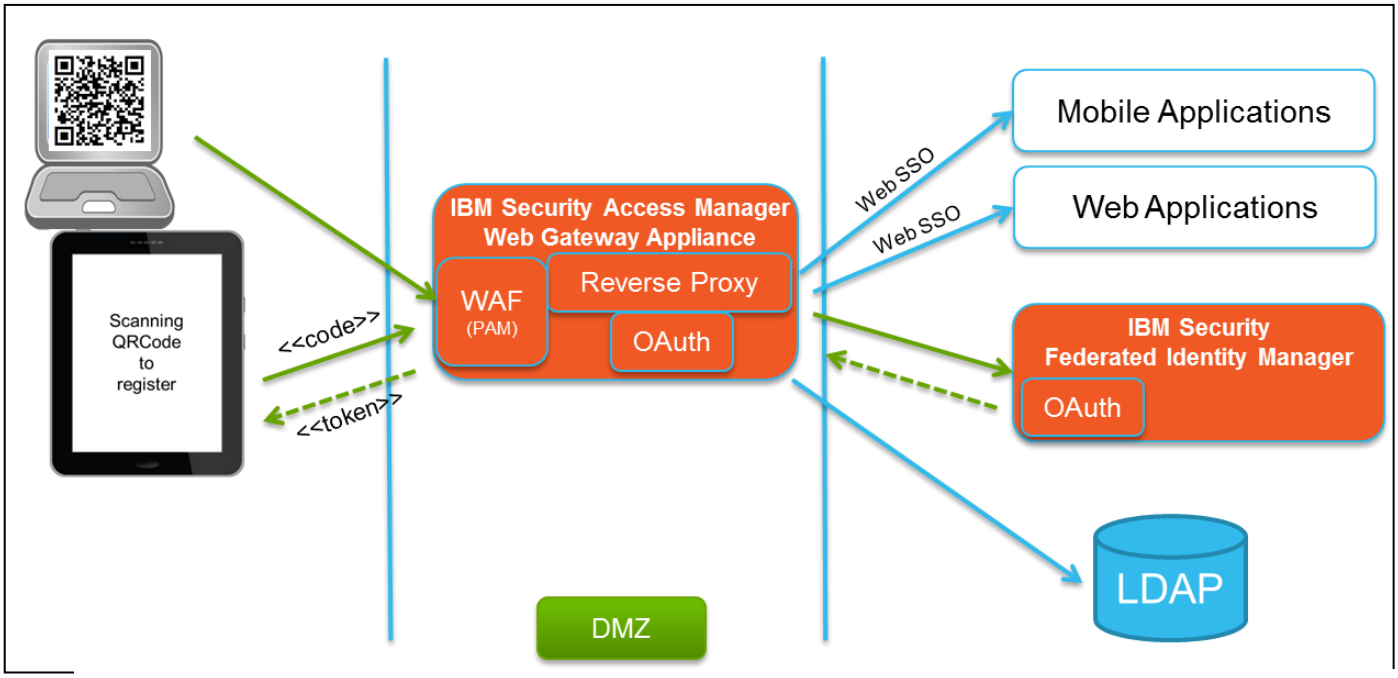

Figure 4: OAuth application instance registration process (Authorization code grant-type)

IBM Tivoli Federated Identity Manager adds support for OAuth 1.0 and 2.0 to the environment. OAuth 1.0 and 2.0 provides identity aware mobile applications. Instead of users supplying user names and passwords, a defined OAuth registration process is followed:

1. The user obtains a one-time authorization code from an OAuth server.
   Ideally, the user logs on to a computer with a keyboard, receives a QR code, and scans it with the camera mobile of the mobile device.

2. The mobile device uses the authorization code (a single use, limited time token) to obtain multiple-use tokens directly from the OAuth server (an access token and a refresh token).

3. The application stores the multiple-use tokens in secure storage on the device.
   OAuth does not support mobile web applications that do not have secure, on-device storage.

4. Each time the application is launched, authentication is seamless with the device.
   It sends the refresh token on the user's behalf to authenticate and establish the session. After successful authentication with the refresh token, Tivoli Federated Identity Manager provides the application with a new refresh token. The new toke is again stored on the device and overwrites both the original and a time sensitive access token, which is used for authentication during additional requests in the same session.

Using the OAuth pattern, no personal information about the user is ever stored on the device. The tokens stored on the device can be invalidated temporarily or permanently to prevent access from that device. Adding an optional Personal Identification Number (PIN) during authentication with a refresh token can also strengthen security.

Using IBM Security Access Manager for Web and Tivoli Federated Identity Manager to implement the OAuth pattern enhances the solution and provides a ***proficient*** maturity of the deployed solution.

3.3 Multi-factor authentication using a mobile device

When a higher authentication level is required to access a protected resource, the client typically must step up their authentication level. Two-factor (or multi-factor) authentication is a commonly used form of step-up authentication. In an access-based policy context, it is called *permit with obligations* or *step-up*.

In this scenario, a mobile device provides two or more of the four authentication factors. A mobile device can collect all four of the following factors:

Knowledge — *Something the user knows*
Passwords, PINs, and knowledge questions are common. The most appropriate for a mobile touch interface is something quick and simple, such as a PIN.

Possession — *Something the user has*
A shared secret that is stored on the device can generate a soft token.

Inherence — *Something the user is*
Biometric authentication using the camera or voice recognition of a mobile device are two emerging techniques.

Social network — *Somebody the user knows*[2].
Connecting to someone's social network and presenting a collection of profile pictures and challenging the user to select which ones are their friends is one technique.

Figure 5 shows examples of the four possible factors in a mobile access context.

[2] Wikipedia.com https://en.wikipedia.org/wiki/Multi-factor_authentication

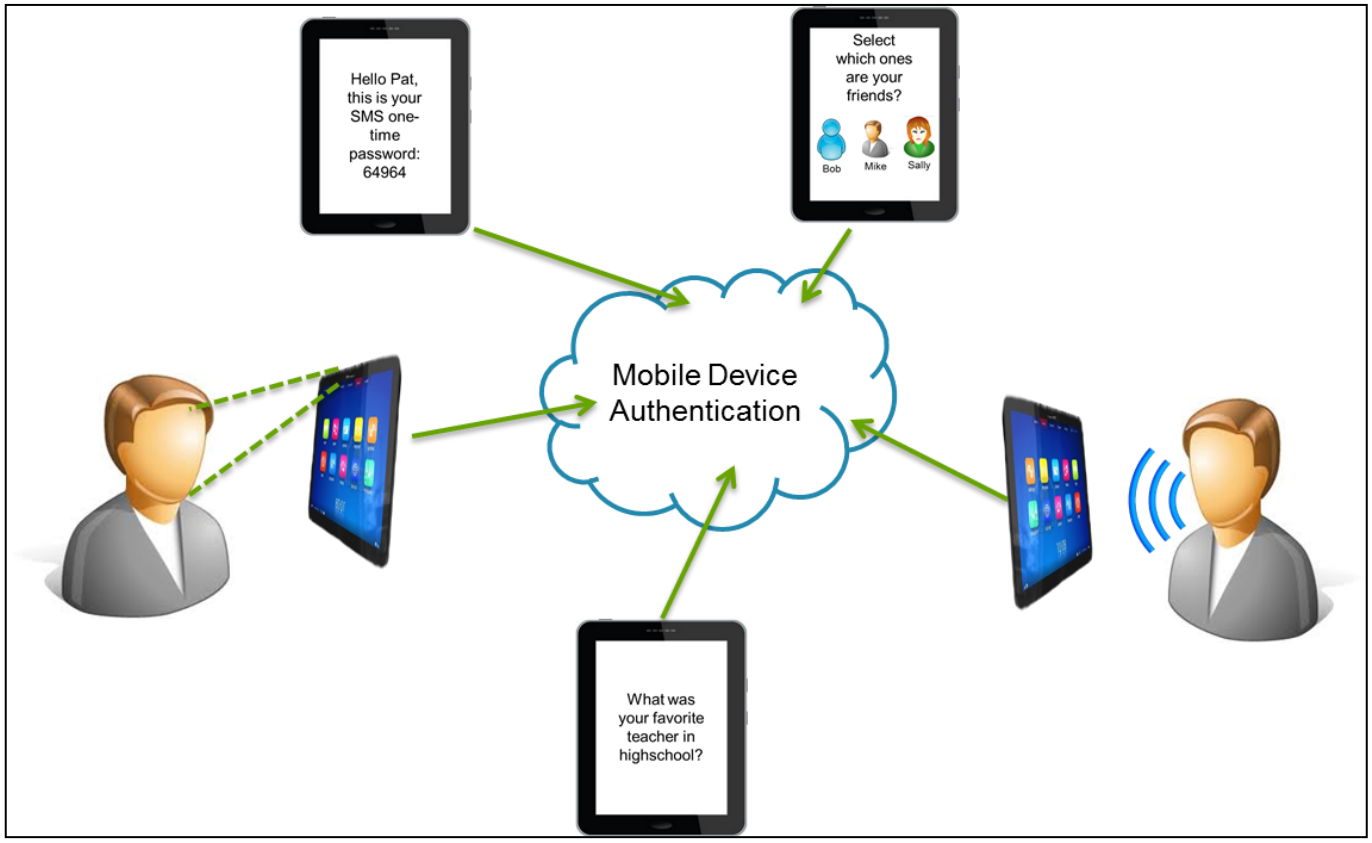

Figure 5: Multi-factor mobile device authentication

IBM Security Access Manager for Web and Tivoli Federated Identity Manager can achieve both the knowledge and possession factors. Depending on the Tivoli Federated Identity Manager configuration, there are a number of mechanisms, such as SMS and email, for delivering the one-time password (OTP) to the user. OTP mechanisms, such as time-based HMAC OTP (TOTP) and Sequence HMAC OTP (HOTP), require no delivery. Ideally, the OTP is not delivered to the same device that makes the transaction. If the same device is the only option for OTP delivery, the *something the user knows* factor, such as a user PIN that is also known to the server, is appended to the OTP entered by the user. Then, the OPT and additional known value is validated by the server before authentication is successful.

By using a combination of a device that is registered to the user and a PIN, you can achieve two-factor authentication. Figure 6 shows a deployment of IBM Security Access Manager for Web and Tivoli Federated Identity Manager that implements the OTP pattern. With this architecture, the security aspect of the solution is considered an ***optimized*** maturity level.

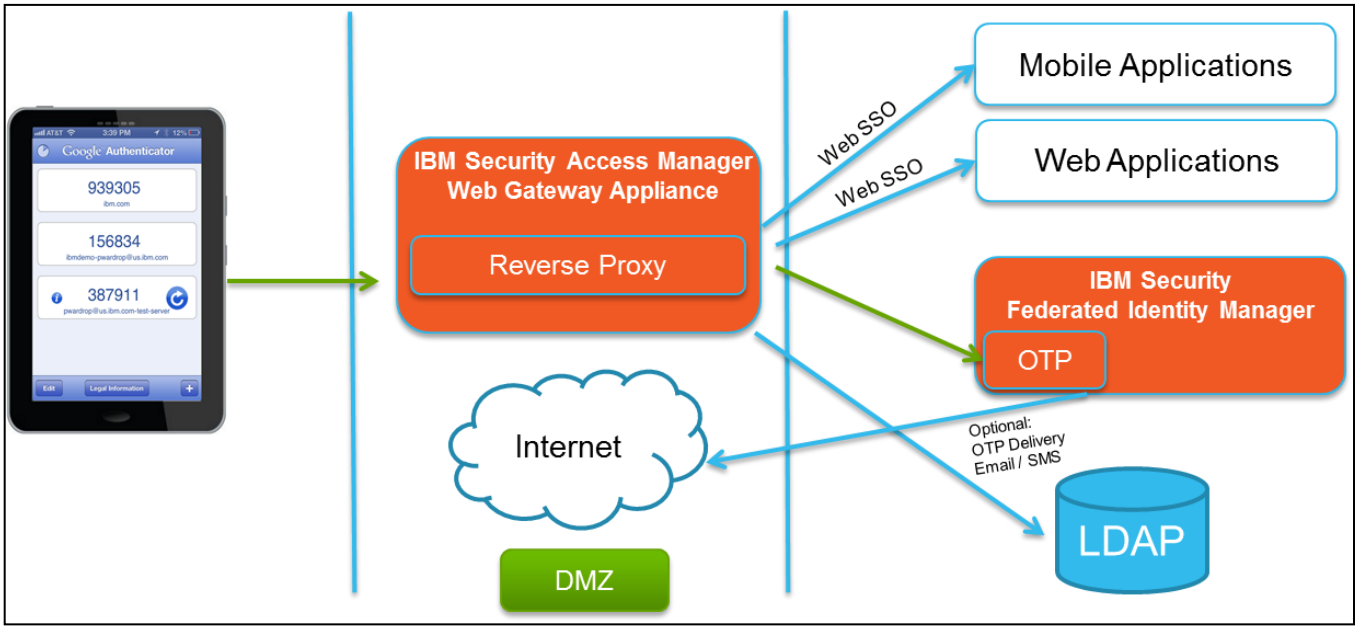

Figure 6: One-time password with Tivoli Federated Identity Manager

3.4 Context-based authorization and how it fits in the mobile space

Mobile applications are designed to be accessible from anywhere and at any time. This design introduces new security scenarios. You can no longer rely on physical device ownership or location. The mobile applications, along with their supporting infrastructure, must provide the additional security controls to overcome the security challenge.

Traditional web-based access controls typically rely on user authentication and a URI to determine what access controls and authorization policies to satisfy before granting access. Successfully launching the mobile application does not prove that the owner of the device is the person using it. A device can be misplaced, or the account details can be compromised.

Companies can safeguard high value transactions, such as a funds transfer in a mobile banking application, by using the available context to determine a risk factor and then requiring a stronger form of authentication to confirm that it is really the intended user.

This scenario shows how to use context-based information to:

- Authorize a transaction
- Determine a risk score
- Determine if step-up authentication is required

Risk-based access (RBA) uses contexts that include device, environment, identity, and behavior patterns.

Adding RBA capability to a mobile application deployment enhances security. It:

- Provides access decision and enforcement that is based on a dynamic risk assessment or confidence level of a transaction.
- Uses behavioral and contextual data analytics to calculate risk.
- Is a pluggable and configurable component for Tivoli Federated Identity Manager. It can also be integrated with IBM Security Access Manager for Web to protect web based transactions through the Web Gateway Appliance.

Figure 7 shows this architecture.

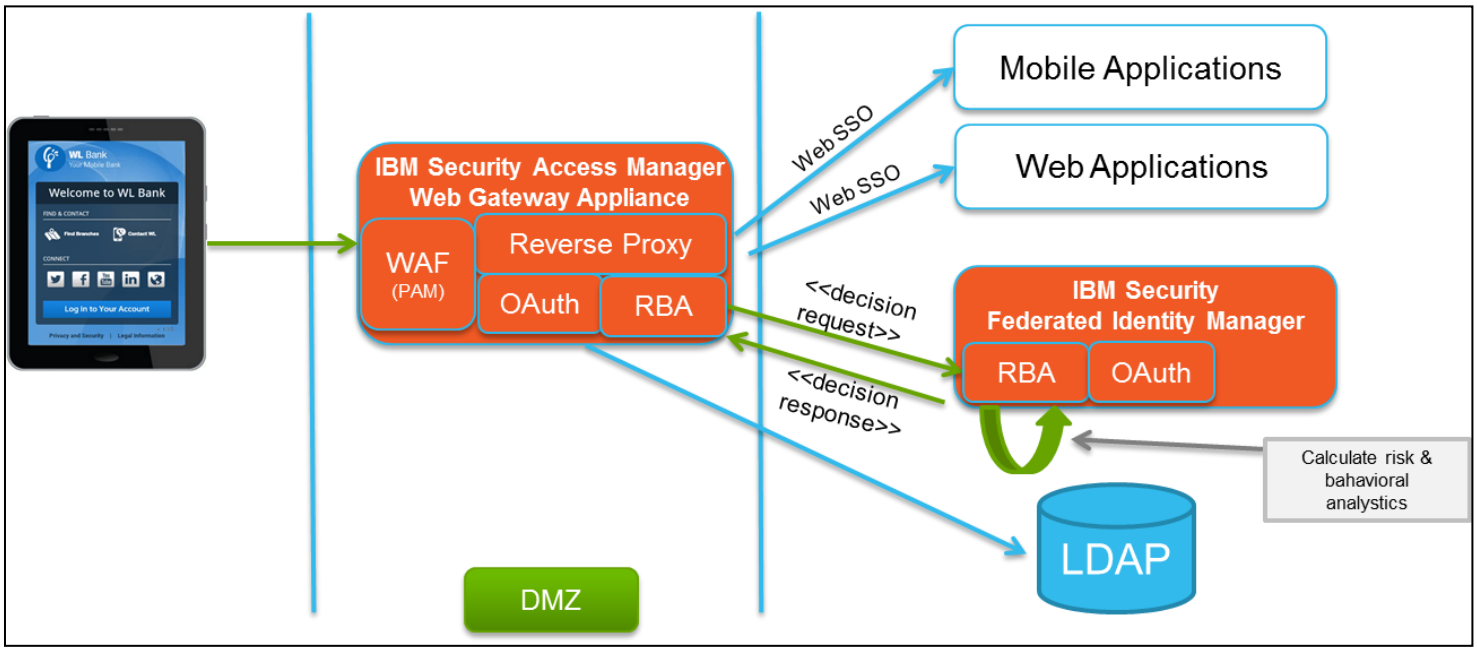

Figure 7: Risk-based access architecture

In this scenario, a mobile banking application is enabled for identity awareness. It uses the OAuth pattern where the application and device are already registered. When the application is launched, the user is prompted for their PIN and is therefore authenticated to a base level. Base-level authentication is sufficient to perform basic banking tasks, such as retrieving balances and transaction history.

Using traditional business rules, the financial institution might impose restrictions on transfer amounts or transfers to external parties. It also might require a multi-factor authentication, or step-up, before permitting these actions. These rules might not accommodate normal trends and behavior for a customer. For example, some customers might transfer $100 to a savings account every month after they are paid; they might not like stepping up their authentication each time to do this.

A middle of the night transfer of $100 to an external account that originates from a foreign country, even after a payday, appears suspicious. The institution should require a step-up before allowing the transaction. Traditional business rules might rely only on the transfer amount and allow the transfer when it is in fact fraudulent. A significant advantage of RBA is to apply all of the context and known behavior to calculate a risk score and determine an appropriate action: permit, deny or permit with obligations (step-up).

With IBM Security Access Manager for Web and Tivoli Federated Identity Manager, companies can implement risk-based access that discovers and mitigates hard-to-detect fraud on low value transactions without modifying the application code or logic. They can use business rules to author context-based access policies that provide assurance and strong authentication for an ***optimized*** maturity level.

4 Summary

As shown in Figure 2, the reference architecture integrates IBM Security Access Manager for Web and Federated Identity Manager to provide an integrated security solution for mobile applications. The combination of IBM Security Access Manager for Web and Tivoli Federated Identity Manager offers basic to optimized maturity levels for securing mobile and web applications.

Remember: IBM has many different products and solutions in the IBM Mobile Security Framework. They address different touch points in mobile security architectures. This paper focuses on the access points into the network.

5 Acknowledgements

Ori Pomerantz — IBM Software Group, Security Systems, Technical Enablement Specialist

6 For more information

To learn more about IBM Security Access Manager for Web, contact your IBM representative, IBM Business Partner, or visit **ibm.com**/security.

References

Rebook: *Securing Your Mobile Business with IBM Worklight*
http://www.redbooks.ibm.com/abstracts/sg248179.html?Open

IBM Security Access Manager Information Center
http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/welcome.htm

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 give 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.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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 might 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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 measurement 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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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. 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 IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at ibm.com/legal/copytrade.shtml.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

International Business Machines Corporation
New Orchard Road Armonk, NY 10504

Produced in the United States and Australia 08-2013