Key Authentication Considerations for Your Mobile Strategy
The Need for Mobile Authentication Reaches Critical Mass

According to an old adage, consumers speak through their pocketbooks. While that saying still has merit, it may soon reference consumers’ mobile devices instead. The fact is, mobile device usage has been climbing at a phenomenal rate. According to Forrester Research, one billion consumers will have smartphones by 2016. U.S. consumers alone will own 257 million smartphones and 126 million tablets.¹

The related impact on buying habits is significant. Consider recent consumer statistics from Nielsen²:

- 79% of U.S. smartphone and tablet owners have used their mobile devices for a variety of shopping-related activities.
- Among these activities, 36% of smartphone users redeem mobile coupons, while between 29-42% of both mobile and tablet users purchase items via their devices. Performing research and locating stores ranks high among all users.

Given data like this, it’s no wonder that many consider mobile the new face of customer engagement.

Forrester estimates that mobile spend will reach $1.3 trillion as the mobile apps market reaches $55 billion in 2016.¹

Businesses Respond With More Mobile Apps

With customer loyalty at stake and competitive pressures on the rise, more and more businesses are increasing their mobile apps budgets and development efforts. By doing so, they hope to not only improve their ability to engage with customers, but also reap the benefit of a lower-cost business model.

¹“Mobile is the New Face of Engagement”, Forrester Research, Inc., Feb 13, 2012
The Need for Mobile Authentication Reaches Critical Mass continued

The “consumerization of IT” extends to the workplace, as well. Spurred by executives and remote employees seeking to work more productively, bring your own device (BYOD) initiatives are increasingly underway at companies of every size. However, properly supporting them takes a flexible authentication strategy given the types and number of devices involved.

52% of all information workers use three or more devices for work; 60% of devices reported are used for both work and personal purposes.³

---

<table>
<thead>
<tr>
<th>Security Concerns - % of “Very Significant”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device may be stolen and corporate data exposed</td>
</tr>
<tr>
<td>Malware could be introduced to corporate network</td>
</tr>
<tr>
<td>Compliance requirements</td>
</tr>
<tr>
<td>Data on device will go with employee to next employer</td>
</tr>
<tr>
<td>Legal data ownership issues</td>
</tr>
<tr>
<td>Lack of integration with traditional IT systems</td>
</tr>
<tr>
<td>Cost of providing technical support</td>
</tr>
</tbody>
</table>

| 61% | 58% | 48% | 41% | 35% | 29% | 26% |


Mobility Introduces Additional Security Concerns

From consumers to employees, the “Consumerization of IT” is here to stay.

Frankly, it’s making security very complicated. Huge numbers of people are now using a variety of mobile operating systems, devices and applications to access sensitive data and perform transactions. These activities have to be protected appropriately to guard against identity theft and the loss of organizational data.

However, as your organization increasingly promotes online customer engagement – and as workplace BYOD policies become more pervasive – risks to mobile security can rapidly escalate through the sheer volume of users and potential access points. These security concerns are compounded by the growing use of cloud-based services to perform work among employees and partners.

To protect your consumer and enterprise data under these conditions, you need a solid security strategy that addresses, and supplies effective mechanisms for, mobile authentication.

Traditional considerations such as security, convenience and cost have always played a role in authentication, but mobility makes user convenience more important than ever. And as the number of mobile users continues to spiral, access demands can reach all-time highs — making scalability extremely critical. Meanwhile, lost devices and related authentication issues have risen among the top considerations, as well.

<table>
<thead>
<tr>
<th>Traditional Focus</th>
<th>New Dynamics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>USER CONVEIENCE</td>
</tr>
<tr>
<td>Convenience</td>
<td>SCALABILITY</td>
</tr>
<tr>
<td>Cost</td>
<td>Lost devices</td>
</tr>
<tr>
<td></td>
<td>Limited or no control over devices</td>
</tr>
<tr>
<td></td>
<td>Credential protection</td>
</tr>
<tr>
<td></td>
<td>Support costs</td>
</tr>
<tr>
<td></td>
<td>Flexibility/time to market</td>
</tr>
<tr>
<td></td>
<td>Business intelligence</td>
</tr>
</tbody>
</table>
Toward a Unified Mobile Security Strategy

A comprehensive mobile security strategy must address numerous challenges to protect data. But a focus on authentication and access management is a good place to start. As you look to mitigate risks in these areas, it’s important to get a comprehensive view of all of the mobile initiatives in play within your organization. For example:

- What current mobile apps are under development, who are the intended users and how will they access them?
- How are mobile app development teams across different business units or geographies solving their security and authentication problems?

Will you need to enable secure authentication for non-traditional devices in the future, such as kiosks or cars?

Once you’ve captured these details around current operations and future-state requirements, you’ll be able to identify security gaps or obstacles that must be addressed as you move forward.

Knowing what requirements lie ahead is essential to building a mobile authentication strategy that provides long-term protection for mobile applications and services accessed by both internal and external parties.
Fragmented Security Practices Present Additional Challenges

Some of today’s development practices can hinder, rather than help, the delivery of secure mobile apps.

For starters, your organization may be on the hook to quickly develop and deploy new apps. And if you’re working apart from other development groups, you may be lacking a coordinated enterprise approach in the rush to meet deadlines. This can create several problems:

- Different authentication and security policies are employed for mobile, Web and non-traditional devices (e.g., vending machines) – leading to separate maintenance, support and governance requirements.
- Developing identity and access management security uniquely into each new application and service is highly inefficient and delays time-to-market, which can be critical in competitive situations.
- Uncoordinated development efforts result in an inconsistent user experience in terms of authentication across various interaction methods, including Web, mobile Web and native mobile applications.

These fragmented approaches make it difficult or impossible to track user activity across interaction methods for security and business intelligence/marketing.

A coordinated approach to authentication and access should include all your mobile and other online user interaction methods so that sensitive data is protected no matter how or where it is accessed.
Deploying an Effective Mobile Authentication Approach

Conversely, when you standardize and unify mobile authentication processes within your overall security strategy, you build the end-to-end capability to securely engage with customers and employees.

Deploying access policies that can be applied to multiple interaction methods provides a more user-friendly and consistent experience, while simplifying their administration and reducing support costs.

### Capabilities
- Common access management security policy
- Ability to leverage existing identity store
- Single security policy for all access, big browsers (desktop), small browsers (mobile browser) and native apps
- Multiple session management methods to support a variety of access channels

### Benefits
- Deploy new applications faster
- Gain a common audit trail across all access points
- Do not have to write unique security per platform
- Supports corporate or personally owned devices
As you move forward with mobility initiatives to extend enterprise app access, you can start by incorporating mobile users into your existing identity and access management (IAM) solution. This gives you a quick way to leverage centralized management capabilities, while also delivering a common user experience.

Determining which authentication approach to take from this point hinges on the specific app, and how and where you expect it to be used. For example:

- What mobile (and non-mobile) device platforms will you need to accommodate to enable customer or employee access to the app?
- Is the application a native mobile app or a Web-based app? Each one will have unique support requirements.
- How will users be interacting with the app – will it require the user to access another app in order to complete a specific transaction?
- How sensitive are the data and transactions related to the app in question?

Once you’ve addressed these issues, along with convenience factors and the predicted volume of users, you can map them to an authentication approach best suited to handling app-related security concerns.
Methods for Mobile Authentication

The use of a basic username and password, or even no authentication, may be sufficient to enable access to your low-risk mobile applications. However, when an application contains more sensitive customer or company data, a stronger form of authentication information is warranted. A layered approach, which allows you to evaluate multiple risk factors and then require the appropriate level of authentication, provides greater security to protect more sensitive data and transactions.

Let’s look at the various tactics you can employ to support your strong authentication requirements.

**Out-of-band two-factor authentication:** This method is useful when users are attempting to access your Web applications via a laptop, tablet or workstation, and you want to authenticate their identity beyond their username and password. It involves utilizing a separate device (mobile phone) in the authentication process to provide additional security. For example, you could send a one-time passcode (OTP) to users’ smartphones via email, voice mail or SMS after they’ve already supplied their initial credentials to serve as a secondary confirmation when elevated risks have been identified or when they need to reset their password.

One-time-password (OTP) can be sent to the user’s phone to provide additional security when the user is accessing Web applications from any other device.

1. User begins the login
2. OTP is sent to user’s phone via SMS, email or voicemail
3. User enter the OTP to complete the login and
4. Accesses the application
Methods for Mobile Authentication continued

**Strong authentication embedded in native mobile apps:**
The first line of defense against potential security threats begins during mobile application development. Wherever development efforts are taking place in your enterprise, you can leverage a common strong authentication SDK and embed the required software libraries to build a consistent level of security into your native mobile applications.

**Risk-based authentication, including device identification:**
Transparent to the user, this form of authentication does a real-time, behind-the-scenes evaluation of contextual factors such as device identification, geolocation, transaction details and select historical data to assess risk. If suspicious activity is indicated, you can prompt the user to provide additional authentication, have an alert issued or simply deny the activity.

**Transaction signing:**
Transaction signing adds another layer of security on top of two-factor authentication methods, requiring a user to digitally sign a transaction for additional protection against new forms of Web fraud. In this scenario, the customer is asked to confirm the online transaction by entering (on their mobile device) their PIN and other transaction details such as the amount, account number or payee. Once these items are verified the customer is given a dynamic one-time-passcode to confirm the transaction. This process helps to prevent man-in-the-middle and man-in-the-browser attacks in which hackers attempt to change the amount and payee information to commit fraud.
A Coordinated Authentication Approach is Required to Support Your Mobile Strategy

Mobile devices are widely used by both customers and employees, providing your organization with an opportunity to leverage them as a key element of strong authentication. The rapidly increasing number of native mobile applications and mobile-Web applications also calls for new, user-friendly forms of strong authentication for access directly from the mobile device. To be effective, your mobile strategy requires a coordinated approach to authentication across all of these scenarios.

A comprehensive authentication strategy positions you to:

- Seamlessly extend convenient access to mobile apps and a range of mobile devices
- Get a cross-channel view of your customers, so you can improve customer engagement
- Boost employee productivity through anywhere, anytime access to critical apps
- Safely scale to support higher device and app volumes
- Bolster security, prevent fraud and improve compliance
CA Technologies Mobile Authentication Solutions

Working with CA Technologies, you can address a wide range of mobile authentication challenges by applying unified solutions to help reduce potential exposure from any malicious activities in your traditional or cloud-based IT environments.

Our mobile authentication solutions support a multilayered security approach. They include:

- **CA Strong Authentication**: offers a wide range of strong authentication credentials and out-of-band methods for more secure online interactions. This gives you the ability to incorporate multi-factor protection through out-of-band methods, OTP credentials or PKI-based credentials for additional protection against brute force or man-in-the-middle security attacks. Transaction-signing capabilities are also available to help secure purchase, transfer or payment activities.

- **CA Risk Authentication**: enables transparent multi-channel risk assessment and fraud detection using risk-based rules and statistical analysis to detect and block fraud in real-time. You can use these capabilities to create an adaptive risk analysis process that calculates the fraud potential of every online login and transaction based on the level of risk, user and device profiles, and organizational policies.

- **CA Single Sign-On**: features single-sign on, flexible authentication, policy-based authorization, session management and auditing to provide a consistent security solution across multiple access channels and platforms.

- **CA Advanced Authentication SaaS**: provides authentication-as-a-service (AaaS) offering a quick, cost-effective way for you to deploy and manage a variety of strong authentication methods to secure both logins and transactions.
Learn More, So You Can Move Forward With Confidence

Visit ca.com/securecenter for more information.