A Modern Mobile Architecture

By Paul Madsen

Many enterprises today are actively pursuing mobile device initiatives—largely driven by the desire to support BYOD, which holds high potential for productivity gains as well as improved employee satisfaction.

Enterprise IT has a lot on their plate to support BYOD. They must secure the sensitive business data accessed and stored on mobile devices while enabling employees to do their job more efficiently. At the same time, IT must preserve employee privacy. In some regions, a right to privacy is encoded in legislation. A modern mobile architecture capable of supporting BYOD must therefore balance:

- **Application and data security**—protecting the sensitive business information accessed by and stored on mobile devices.
- **User enablement**—ensuring that employees can perform the duties of their role when and where they wish to, fundamentally allowing them to ‘get things done’.
- **User privacy**—acknowledging the employees’ rights to be ‘left alone’, such that the enterprise does not have complete visibility into their personal applications and data on the device, particularly for BYOD.

Historically, security has been seen as actively inhibiting user productivity. This is mostly seen as an acceptable price to pay to protect business data. Yet, today’s employees, accustomed to the ease and convenience of consumer applications, are less likely to accept such barriers. If they see IT as interfering with their ability to get their work done, they have options. For every locked down enterprise system, there is likely an equivalent ‘shadow IT’ third-party application that the employee can sign up for with a credit card (and subsequently expense). Similarly, earlier models for securing mobile devices didn’t adequately recognize the employee’s rights (or at least expectation) for some degree of privacy over how they used that device for non-business applications.

Balancing application and data security, user enablement and user privacy is not easy, but is achievable by building on the following four technology pillars.

- **Mobile-based authentication**—leveraging the capabilities of smart phones to provide secure and easy sign-on
- **Single sign-on across web and native applications**—giving employees a seamless user experience for both web and native mobile applications
- **APIs**—granting access for business data only to authorized applications and users
- **Work/personal separation**—isolating business applications and data from the applications that the employee installs for their personal use

By building on these pillars, an enterprise can find the right mix of security, user enablement and privacy.
1.1 Mobile-based Authentication

The old saying of ‘something you know, something you have and something you are’ has served as a useful model for distinguishing authentication mechanisms. More and more, we are seeing a trend of moving away from the ‘what you know’ of passwords to the ‘what you have’ of mobile phones. This trend is driven by both the increasingly apparent issues and limitations of passwords and the opportunities that mobile-based authentication provides for both increased security and usability (historically imagined to be mutually exclusive).

Modern mobile phones provide a useful ‘what you have’ authentication factor—either acting as a second factor to traditional password-based schemes, or replacing passwords completely.

Effectively, a smartphone is a powerful portable computer with the following important features that are relevant to authentication:

- **Connectivity.** By definition, mobile devices are connected, supporting authentication schemes in which an authentication challenge can be sent over the network to the device, for example, via an SMS message or through the mobile operating system’s (OS) notification infrastructures.

- **Processing power.** This allows for on-board computations in support of cryptography and so on.

- **User interface.** This interface happens by the user being prompted to enter credentials and so on, or shown one-time codes and so on.

- **Secure storage.** Secure storage allows for the storage of identifiers, secrets and credentials used in authentication schemes.

- **Biometrics.** Increasingly, devices have hardware that allows a verification of some biometric of the user, for example, a fingerprint or retina.

- **Single user.** Devices are typically associated with a single user. Consequently, authentication of the device can serve as a proxy for the user of that device.
Different mobile-based authentication schemes leverage the features in different combinations. For instance, PingID™ is a mobile based authentication scheme that authenticates users by sending a challenge to an application installed on that user’s previously registered device through the Google Cloud Messaging for Android™ or Apple Push Notification Services. Upon receipt, the user simply swipes their screen to answer the challenge.

The FIDO™ (Fast Identity Online) Alliance is defining an alternative mobile-based authentication model—leveraging the emerging biometric capabilities of devices. In the FIDO model, the user authenticates to the device through a biometric check—serving to unlock a cryptographic key that is then used to authenticate to the server.

Current mobile-based authentication mechanisms are periodic (in that the authentication of the user happens relatively infrequently and explicitly [in that the user must perform an action]). However, the phone (and other local sensors) can enable a more continuous and passive model for authentication—where the user’s actions and other context are continuously monitored and compared to previously established patterns. For instance, researchers are exploring the potential for passive biometrics, such as typing or walking stride to contribute to the overall confidence in the authentication of the user. Continuous authentication promises to make user authentication more passive, reserving explicit and active authentications for special circumstances (such as purchasing a stock versus just viewing a brokerage account).
1.2 Single Sign-On

Single sign-on (SSO) refers to mechanisms that can provide users with a seamless experience for application access. The user's authentication into the applications should be as invisible as possible (where ‘as possible’ is dictated by the nature and sensitivity of the different applications and their data). Minimizing overt and explicit sign-ons is a significant enablement mechanism—nothing slows down an employee from doing their role more than being unable to access the relevant applications that their role demands.

While mobile-based authentication schemes like those described above can significantly improve the authentication experience for users, performing such an explicit authentication for each and every application may still not be ideal. Consequently, there is value in combining a mobile-based authentication with SSO mechanisms because a user’s single mobile-based authentication can be leveraged across multiple applications.

Standardized mechanisms for enabling SSO to mobile browser applications are well established. The security assertions markup language (SAML) enables SSO for a mobile browser in exactly the same form as a desktop browser. Other web browser SSO protocols exist, such as OpenID® and WS-Federation. More recently, OpenID Connect (Connect) has emerged as a protocol that, as it is built on top of OAuth, can enable both web browsers and native applications.

Both OAuth and Connect can be used to secure native mobile applications (unlike SAML and other web SSO protocols). But neither OAuth nor Connect can, out of the box, enable an SSO experience across native applications as both presume that the user must separately authenticate to, and authorize each, native application on its own.

The Native Applications (NAPPS) working group (WG) in the OpenID Foundation is defining a profile of OpenID Connect that will enable an SSO experience between and across both web and native mobile applications by the following method:

- SAML enables SSO across mobile web apps.
- OAuth individually enables mobile native apps.
- OpenID Connect enables individual mobile native apps and SSO for mobile web apps.
- NAPPS enables SSO across both mobile web and native apps.
1.3 Application Programming Interfaces

APIs are a key piece of modern mobile architectures. APIs separate application data from the application UI or delivery channel—and so provide an important abstraction layer. Increasingly, APIs are built in a so-called ‘RESTful’ model, a rejection of the relatively heavyweight SOAP architectures.

An important category of REST API clients are native mobile applications. The best practice for native applications to authenticate to their corresponding REST endpoints is to include an OAuth access token on the API calls.

Below is a diagram that shows the OAuth standardized flow by which a native application obtains a token from an authorization server (AS) and then uses that token on its calls to an API. It is by validating the token that the API is able to determine on which user’s behalf the native application is working, and so make an appropriate authorization decision.

Because the user is directly involved (via the mobile browser) in the issuance of the token to the native application, the above flow allows for (but does not mandate) a consent step, which is an important privacy enabling feature. Additionally, because the user is authenticated in the browser, it opens up the possibility of them being directed elsewhere for the actual sign-on step and then redirected back to the AS via a federated SSO flow.

The burden of validating the OAuth access token presented on the REST call is typically removed from the API itself, and placed on an API gateway that sits in front of the APIs. The gateway typically maps the incoming OAuth token into another token format (Kerberos ticket, X,509 certificate, etc.) when it proxies the original request onto the application.
1.4 Work / personal distinction
Native mobile applications pull data down from REST APIs and store that data on the device. Such device storage of business data enables offline access—the so-called ‘CEO on a plane’ use case. However, it also introduces a new security threat relative to browser applications which generally leave no data on the device. Therefore, it becomes paramount to protect that data against active attack, or merely a lost device.

Countering the enterprise’s desire to control the device in order to protect against sensitive data loss is the BYOD trend—with the implication that employees will have an expectation of some degree of autonomy over how they use their own devices for non-business usages.

The underlying mechanics of the division, and how it manifests for employees, differ. Mobile application management (MAM) modifies each business application (either by wrapping or via some SDK) to give the enterprise the necessary security controls without touching any of an employee’s personal apps. From the employee’s point of view, such MAM-enabled applications exist alongside their personal applications.

Dual persona solutions presume a different user experience—namely one where the employee explicitly switches between business and personal workspaces (a negative for some). To enter the business side of the phone, the employee will be expected to authenticate—typically by providing some PIN or similar locally validated credential. The fingerprint sensors on the latest iOS and Samsung phones (and the increasing availability of their functionality to third-party applications) makes possible a scenario where the employee would scan their fingerprint to enter the business side of the device.

Different technologies can enable a dual-persona model, including virtualization and containers. In the containerization model, the employee downloads and installs a mobile application which creates an isolated work-only environment. Business applications logically run inside this container, and consequently can run only under the policies set by the enterprise administrator for that container.
In addition to enforcing enterprise policy for the business applications, the containerization agent has a potential role to play in enabling the employee using those applications to be productive—specifically by enabling an SSO model across those applications. In the previously discussed NAPPS model, the role of the token agent (that by which obtains the OAuth access tokens for the business applications to use on API calls) can be assumed by the container agent. Once the employee is authenticated into the container, that container is able to use the NAPPS defined protocols to obtain the OAuth tokens that the business applications need. From the employee’s point of view, the business applications ‘just work’, not separately requiring an explicit authentication step.

This scenario is represented below:

In the above, note that the S1 native application does not directly interact with the user for authentication—it is the container that does so, logically on behalf of the business application.
1.5 Summary
A modern mobile architecture must balance the requirements of security, user enablement and privacy. In support of those requirements, we have presented four pillars:

- Mobile-based authentication
- SSO
- APIs
- Work / personal separation

All four of the pillars support security, mobile authentication and SSO support enablement, and dual persona is an important privacy enabler.

This balanced approach is the key to unlocking the potential of enterprise mobile initiatives. The value mobile devices represent to organizations continues to grow, with employee productivity and user satisfaction at the heart.

Visit pingidentity.com to find out more about how Ping Identity solutions can help with your BYOD initiatives.

About Ping Identity | The Identity Security Company
Ping Identity is The Identity Security Company. Ping Identity believes secure professional and personal identities underlie human progress in a connected world. Our identity and access management platform gives enterprise customers and employees one-click access to any application from any device. Over 1,200 companies, including half of the Fortune 100, rely on our award-winning products to make the digital world a better experience for hundreds of millions of people. Visit pingidentity.com for more information.