A SEAMLESS EXPERIENCE FOR THE MOBILE DESKTOP

Frictionless Access Authentication

Table of contents

Today, mobility is no longer a trend. It's an established reality, reshaping the enterprise. This white paper is the second in a three-part series on enabling the mobile desktop while securing information and protecting your organization.

Part 1: Mobile as the New Desktop — Solution Overview
Part 2: A Seamless Experience for the Mobile Desktop
Part 3: Buyer's Guide to Mobile Identity Solutions

Agile Identity For The Evolving Mobile Desktop

The unstoppable momentum of mobility continues creates a new enterprise need for a mobile desktop solution that fully enables the benefits of mobility while protecting the enterprise from the complex risks of productivity outside the firewall. Forward-thinking businesses are increasingly deploying mobile-embedded identity solutions to meet this challenge. By embedding a virtual smart card directly on the mobile device, the enterprise creates a concurrently frictionless and secure mobile user experience: Secured by strong PKI credentials and biometrics-based authentication, mobile workers seamlessly access resources and navigate workflows with a simple touch — no problematic passwords or tokens required.

The Need For An Agile Mobile Identity Platform

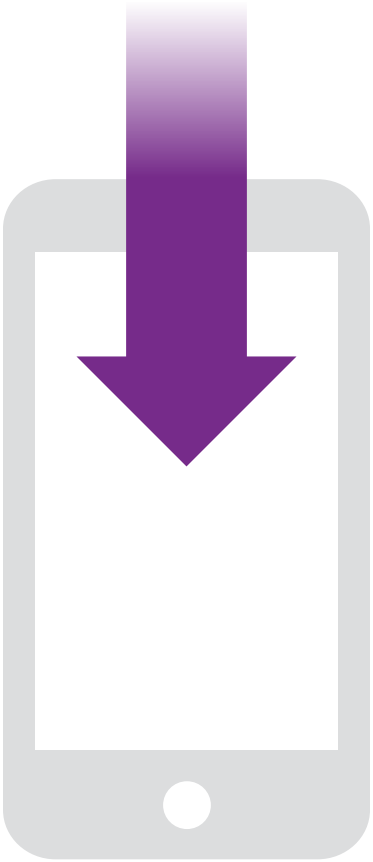
No two enterprises have identical IT infrastructures. And within each enterprise, there are multiple user communities, each with their own specific networks, applications and workflows. An effective mobile identity platform must deliver the agility to fit the unique architecture — legacy server-based resources, private cloud networks or public cloud applications. It must also adapt to provide frictionless access across the range of uses cases in each respective user community. This allows the enterprise to leverage a single trusted mobile identity across its entire mobile desktop environment — and ensures that this mobile identity can continue to drive frictionless, secure mobile productivity as applications and mobile workflows evolve.

Frictionless, High-Assurance Authentication — Inside Or Outside The Mobile Application

A comprehensive mobile-embedded identity solution, such as Entrust IdentityGuard™, delivers the flexibility to fit unique applications and workflows. This includes the critical capability to authenticate high-assurance mobile identity both inside an application — in a fully integrated approach — and outside of an application, as a third-party identity/authentication application on the mobile device.

MOBILE APPLICATION INTEGRATION	MOBILE ID MUST BE INTEGRATED VIA SDK/API	NONE
SERVER SIDE INTEGRATION	NONE	SAML OR IdentityGuard API
USER EXPERIENCE	TRANSPARENT	TAP/SWIPE TO AUTHENTICATE
SUPPORT FOR SSO/ID FEDERATION	☑	☑

In-Application Identity



Use Cases

A mobile identity solution such as Entrust IdentityGuard™ allows the enterprise to embed a virtual smart card within an application or application suite. This in-application identity is generally deployed in three different scenarios:

- **Enterprise Mobility Management Platforms**
  Entrust Datacard partners with several of the top enterprise mobility management (EMM) platforms, including Citrix Worx, Blackberry and Mobile Iron. This enables the Entrust IdentityGuard virtual smart card to be fully integrated within the EMM mobile client.
- **Internally Developed Applications**
  For custom applications developed by the enterprise, the Entrust IdentityGuard SDK enables the integration of the virtual smart card within the internal mobile client.
- **Extending access to Public Cloud Apps via SAML IDP**
  For access to Salesforce.com, Google Docs and other public cloud applications, Entrust IdentityGuard integrates with an established Identity Providers (IDP), such as Microsoft Active Directory Federation Services, enterprise SSO platforms or the Entrust IdentityGuard Federation Module. This approach extends secure mobile desktop access to virtually any browser-accessible SaaS application.

User Experience

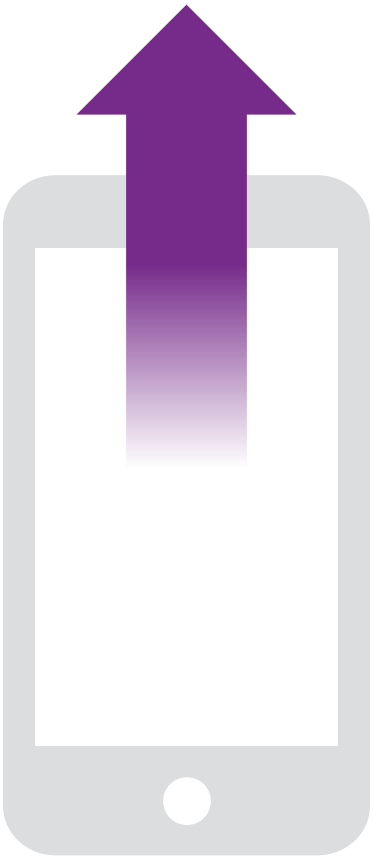
The mobile user experience is identical — and equally frictionless — for each of these in-application identity scenarios:

1. User opens mobile browser
2. User selects URL
3. User scans Touch ID/enters PIN to authenticate access

Once the mobile identity is authenticated, the user moves seamlessly through workflows — without the need to authenticate again and again, tediously entering passwords or fumbling with physical tokens. The user even has digital signing capabilities through the simple PIN or Touch ID.

This in-application identity use case is the most graceful and most frictionless solution. However, it does require a small amount of work upfront — whether it's a partnership or integration between the mobile identity solution and an EMM platform, integrating to internal apps with an SDK, or partnering with an IDP for public cloud access.

Outside-Of-Application Identity



Use Cases

A mobile identity solution can also be leveraged as a standalone application on the mobile device. In this deployment scenario, when a user accesses a SAML support application — such as a SaaS application or Skype for Business — the authentication server intermediates the authentication process. A push notification is sent to the user as an authentication challenge, via the standalone mobile identity application on their phone. The user acknowledges the push notification and confirms their identity with either biometrics or a PIN, and the authentication server then provides a SAML assertion to authenticate the user to the target application. This use case is not dependent on technical partnerships between the mobile identity provider and application provider, and requires minimal setup to deploy. This allows the enterprise to quickly adapt to new productivity applications, leveraging the same mobile identity application to enable easy, secure access. Because of this simplicity and flexibility — and because many enterprises have not yet adopted an EMM platform like Citrix Worx — the outside-of-application identity use case is likely to remain more common in the enterprise world.

The Entrust IdentityGuard™ mobile application accommodates a range of outside-of-application authentication scenarios:

- Entrust IdentityGuard app communicates with IDP for sign-on to specific server-side application
- Entrust IdentityGuard app communicates with SSO portal (such as Oracle Access Manager). Sign-on creates a secure web connection that enables seamless access to all web apps protected with the SSO portal.
- For server-side applications that don't support SAML/SSO, the Entrust IdentityGuard application can be directly integrated through the Entrust IdentityGuard API. This scenario does require additional setup, but ensures a seamless experience going forward in these unique situations.

User Experience

The user experience is identical across all of the outside-of-application use cases. Because the mobile identity is not fully integrated in the productivity application, the outside-of-application user experience involves a few more steps as the user authenticates access. However, this experience is still far more frictionless than authentication using passwords, tokens or smart cards.

1. User opens mobile browser
2. User selects URL
3. User enters username in application login (The in-application identity use case allows the embedded PKI certificate to auto-populate the username field, enabling the user to skip this step.)
4. User authenticates with push notification, using Touch ID or simple PIN
5. User confirms session with a click/swipe

Push Notifications Trump Soft Tokens

For the outside-of-application authentication use case, why not use a soft token (e.g. OTP) instead of a push notification? Because a soft token adds even more steps to the user authentication process, including the cumbersome task of copying and pasting an OTP from one application to another. For mobile users moving in and out of mobile applications frequently, this is an unacceptable burden.

A Single Identity For The Evolving Mobile Desktop

Just as the physical environment of every enterprise is unique, each organization has its own blend of legacy server, public and private cloud resources — as well as a range of user communities, each with their own use cases and workflows. These diverse mobile desktop environments are constantly evolving, as new mobile productivity applications are released every day. The right mobile identity solution must deliver the flexibility to fit to your organization's unique network and application architecture, and respective user community needs. This solution must also provide an agile framework that is ready to adapt as your users' mobile desktops evolve, empowering your mobile workers to use the best tools for the job. This flexibility and agility starts with the ability to ensure high-assurance authentication — inside and outside of applications — for internal, third-party and public-cloud based apps. With a single, trusted mobile identity in place, the enterprise can drive the secure and frictionless mobile user experiences that fully empower the benefits of the mobile desktop.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA