A BUYER'S GUIDE TO MOBILE IDENTITY SOLUTIONS

Discover the Right Solution for Your Organization

Entrust Datacard™

+1-888-690-2424 | entrust.com

Table of contents

Today, mobility is no longer a trend. It's an established reality reshaping the enterprise. This white paper is the third in a three-part series on enabling the mobile enterprise 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

The increasingly mobile world of work presents the complex challenge of enabling the upside of the mobile desktop while protecting the enterprise that now extends far beyond traditional security boundaries. A mobile-centric approach to trusted identity is emerging as a powerful solution to safeguarding information while providing frictionless experiences for authorized users. Identity solution providers are rushing to fill this need, but not all offerings deliver the same level of functionality — some even lack the agility to evolve with changing technologies, uses cases and standards.

This buyer's guide is designed to help the enterprise identify the key functionalities and best-in-class technologies that comprise an enterprise-grade solution — as well as the flexible features that identify both a quality solution and a future-proof investment.

Key Functionalities Of An Enterprise-Grade Solution

Simple, Self-Enrollment

Many technologies that seem sufficient fall apart at the implementation stage. For a mobile identity solution, enrollment/user provisioning is an essential hurdle for effective deployment. If enrollment is difficult for end users, deployment is slow and painful. And if enrollment places big burdens on IT, the costs add up quickly.

What to look for: The mobile-empowered enterprise should insist on a solution that enables users to conveniently self-enroll. This speeds adoption and greatly reduces IT burden and related costs. But effective self-enrollment also means offering more than just a single self-enrollment kiosk. To fit with the overall goal of empowering frictionless, anytime-anywhere productivity, self-enrollment should allow users to enroll from wherever they are, whenever they choose.

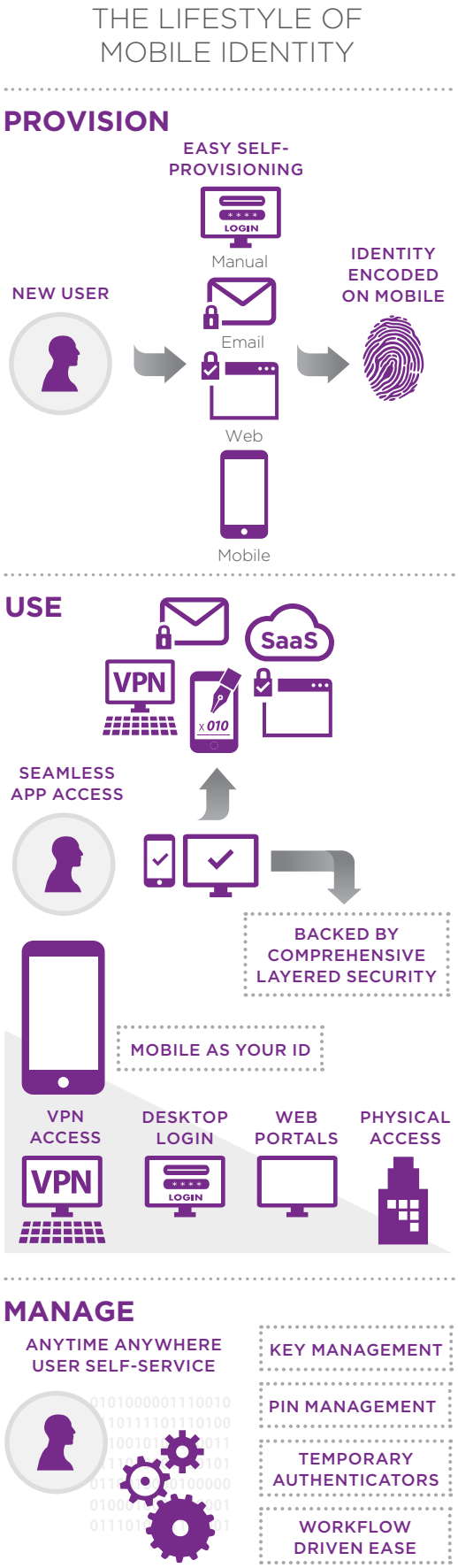
For example, IT should be able to offer users a range of options for accessing self-enrollment, based on both user needs and security policy, such as:

1. Email with direct, secure link to self-enrollment
2. Email with QR code that directs to self-enrollment
3. Email containing secure activation codes; users visit self-enrollment and manually enter codes for access

Fallback Authentication

The ability to use a trusted mobile device as an authenticator drives convenient, frictionless and secure access for users. But what happens when a mobile device is lost, stolen, or destroyed by a spilled cup of coffee?

What to look for: The mobile-empowered enterprise should focus on solutions that offer fallback authenticators to accommodate such circumstances. A robust mobile identity solution should already offer a range of tokens to enable step-up multi-factor authentication where necessary. IT and/or users should have the ability to designate which of these additional tokens will serve as fallback authenticators. This ensures that mobile device failure doesn't lock out users or impede productivity. It also prevents these common occurrences from placing an undue burden on IT staff.



Adaptive Authentication

Your organization has a range of user communities, each with its own use cases and needs. Not all users and use cases pose the same risk, however, and a one-size-fits-all approach to secure authentication either leaves security lacking or creates unnecessary friction. The enterprise must have the ability to step up security where it's needed most — in the most high-risk use cases — while minimizing friction where it's not.

What to look for: The mobile-empowered enterprise must deploy a solution that supports a range of authentication needs and approaches. The solution should offer robust multi-factor authentication capabilities that leverage sophisticated tokens, such as the biometric capabilities of a mobile device, for high-risk access. Another key is the ability to provide simple, two-factor authentication for use cases not requiring top-level security.

An enterprise-grade mobile identity solution should also offer adaptive or contextual authentication capabilities. This feature should begin with automatic background analysis of every access attempt, considering everything from device ID to geolocation. This analysis should quickly detect anything that falls outside typical use patterns, such as access from an unfamiliar location, via an unfamiliar network or via an unfamiliar device. The best solutions can even detect if users are requesting access from a "jailbroken" mobile device that is more likely to contain malware.

IT and InfoSec administrators should be able to manage contextual authentication policies based on background analysis, leveraging a broad range of tokens to provide users with the most convenient experience while stepping up security where it's most needed.

Card Management System (CMS)

Managing smart cards — physical or virtual — is a complex task. Whether deploying smart card-based authentication for the first time, or leveraging an existing smart card program as part of a mobile identity solution, the burden on IT can extend well beyond initial deployment.

What to look for: The mobile-empowered enterprise should look for a solution that simplifies and streamlines smart card management for IT or InfoSec staff. Leading solutions offer a robust Card Management System (CMS), which enables IT to manage all smart card identities in the enterprise ecosystem from a single, intuitive platform. This powerful back-end feature can significantly reduce IT burden and costs.

Agile Features Of A Future-Proof Investment

Wide Range of Application Integrations

Every organization has its own broad range of applications, with each respective user community using its own critical and preferred apps. A mobile identity solution that doesn't integrate with your organization's essential apps, or that only accommodates legacy or cloud-based applications can create costly problems. Asking your users to switch to a compatible app is the definition of adding end-user friction. Asking your IT staff to develop custom integrations for unsupported apps is neither efficient nor cost-effective.

What to look for: The mobile-empowered enterprise identify an established mobile identity solution that comes with built-in integrations. It should accommodate the majority of your organization's essential applications — both legacy and cloud-based — without requiring extensive custom development. Moreover, it's important to choose a reputable solution provider with the established connections to leading providers of applications for critical enterprise functions such as single-sign-on, VPN, SaaS access via SAML, mobile device management (MDM) and enterprise mobility management (EMM) platforms.

Because new enterprise productivity apps seem to emerge every day, the enterprise should also look beyond the existing integrations for a solution. A trusted solutions provider should demonstrate a commitment to future-proof agility — continually expanding its integrations to accommodate new applications, new use cases and new technologies.

Finally, an enterprise-grade solution should also accommodate the proprietary applications that many enterprises custom-develop to fit their needs. This means offering robust and easy-to-use software development kits (SDKs) that enable streamlined integration of the mobile identity solution with a custom-developed legacy, mobile or web app.

Transaction Signing

Most people are familiar with mobile transaction signing or approval functionality in their consumer lives: confirming online purchases, approving online bank transfers, and even signing loan paperwork or other forms. In the enterprise world, mobile transaction signing promises to significantly streamline workflows that traditionally require approval, such as purchase, travel and vacation requisitions, or other approval-based workflows specific to an organization

What to look for: The mobile-empowered enterprise should look for a solution that provides mobile transaction signing capabilities that allows the enterprise to move from paper or email-based to streamlined digital workflows. The transaction signing functionality should enable users to easily make requests, automatically route these requests to the proper manager for approval, and enable managers to make one-click approvals on their mobile devices, anytime, anywhere.

By leveraging trusted mobile identities, these mobile-empowered approval workflows are not only faster — they reduce human errors and fraud, and create a digital trail for complete accountability.

Constant Security Innovation

The threats in today's digital world are evolving faster than ever. Nearly a half-million new pieces of sophisticated malware are released every day, outwitting even the best anti-virus products and contributing to the rapidly growing frequency and cost of enterprise data breaches. A mobile identity provider that isn't constantly adapting its security will quickly become a vulnerability — and soon become completely obsolete.

What to look for: The mobile-empowered enterprise should seek out a mobile identity solution provider with a proven commitment to constant security innovation. This should include demonstrated leadership with new security technologies and capabilities, a flexible mobile identity platform that can quickly integrate with the latest security technologies, as well as the organizational structure to drive the development of new security technologies to fit emerging use cases and stay ahead of evolving threats.

One emerging security innovation is the use of a mobile device's secure element, or trusted execution environment (TEE), to insulate a mobile-embedded identity from malware and other attacks. The TEE is an extremely secure area within the mobile device, designed specifically for the storage of sensitive information. Because the TEE is tied to the hardware of the device — and thus isolated from the operating system — malware and many other attacks cannot penetrate to compromise or steal this information. The forward-thinking enterprise should look to the leading mobile identity solution providers that are now working directly with top mobile device manufacturers to develop this new security capability and maximize the potential of the TEE.

Looking Deeper To Choose The Right Mobile Identity Solution

Mobile devices are now as ubiquitous in the enterprise world as they are in our personal lives. In fact, they are often the very same devices. A mobile-centric approach to identity has emerged as the solution to enabling mobile as the new desktop, allowing frictionless mobile access and productivity while securing a borderless mobile enterprise. Plenty of providers have jumped on this trend, developing basic mobile identity products that "talk the talk." But organizations looking to maximize the business impacts of the mobile desktop — and mitigate the growing, evolving threats in the mobile landscape — should look deeper.

A truly enterprise-grade mobile identity solution should come ready-built with robust capabilities to meet a range of enterprise needs today. Equally important: the right solution should provide the flexible framework — and the support of a solution provider with proven commitment to constant innovation — to grow with the enterprise, adapting to fit new mobile uses cases and technologies while securing the enterprise against evolving threats.

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

Twitter Facebook Youtube LinkedIn Google+ RSS