# TRUSTED IDENTITIES IN
## Today's Connected Enterprise


Entrust Datacard™

# Contents

# Introduction: Identities are Critical to Our Digital Life

The proliferation of wireless networks combined with the rapid advancement in mobile device technology has radically transformed our world in ways even science fiction could never have imagined. As much as the computing age transformed the business world, and to a lesser extent society as a whole, mobile computing is having a far greater, and far reaching impact. From the third world to teenagers with smartphones, mobile devices are everywhere and are transforming everything we do.

The core concept of security in the enterprise, as well as elsewhere in society, is identity. Are you who you say you are and do you have a right to be here? When it comes to verifying identity in order to gain access to a physical location or digital account, the technology used 15 to 20 years ago is, by and large, what is still in place today. Usernames and passwords are universally used for online logins, and keycards are what most employees turn to in order to access their workspace.

There are other authentication schemes out there, including hardware tokens, grid cards, challenge questions and device fingerprinting which have been used regularly in enterprise settings.

These technologies are adequate in certain use cases but they increasingly become harder for users to manage and easier to circumvent by criminals. For the most part, however, passwords and keycards (or other forms of physical keys) are what we all use to access both personal and work information and locations.

It's not to say that these technologies don't add a measure of safety, but they leave something to be desired. After a while, even the best authentication schemes lose their effectiveness.

Identity underpins our personal life, our work life, and is a core part of how we interact with society. We have no shortage of identity markers, whether it's a government issued ID, website log-in, or access key card. But are we reaching a point of identity overload?

Instead of just relying on dated measures, organizations can make their authentication practices more robust by incorporating mobile devices into the mix. When smartphones (and maybe one day wearable devices) become a critical part of the equation, enterprises will find themselves one step closer to having truly trusted identities, while better guaranteeing physical and digital security across the board.

## Today's Enterprise

The main issue with trusted identities in the enterprise is that they are too complex, too easily compromised and too cumbersome. We have dozens of log-ins for a variety of different sites, services, networks, VPNs, servers, and even doors. Each one of these identities has a different password with different rules. Lowercase, uppercase, special characters, the name of your first family pet, it's very complicated.

Some expire every 30 days, some never expire, some, ok most, are forgotten. Users are in a constant battle with IT administrators to create a password just simple enough for them to remember but complex enough to please the password algorithm. In an effort to make passwords easier to remember, users often reuse passwords or variations of passwords which also increases their vulnerability.

What about physical access items like smartcards, hardware tokens and USB sticks? Sure they offer some level of added security but they bring a whole new set of logistical challenges in distributing the hardware, replacing lost hardware, and deactivating and retrieving the cards and USB sticks of former employees.

Regulation is increasingly making identities even more complex to manage as governments work to address privacy concerns and lock down personal data.

The problem with security in the enterprise is that no matter how comprehensively you lock down your systems, networks and data, the weak link is always your people. This isn't due to incompetence or nefarious intent, but simple human nature. We forget logins, lose cards, surf insecure websites and we are duped by sophisticated phishing attacks that can easily plant malware on our systems. Hackers know this and they are targeting your people in order to get at your network. Most major security breaches target password weakness and they don't have to hack your system administrator to get access. Sometimes a low level employee is an easier target. All industries are at risk and employees are becoming a weak link.

## The Most Common Problem with Your Current Identification Scheme

The most common problem with your current identification scheme is user passwords. While they were secure 20 years ago, today passwords are easily cracked, hacked and stolen. And because end users have had to deal with so many, hard to remember, passwords they try to circumnavigate security policy best practices by choosing easy to remember passwords that they then reuse over and over again.

The vast majority of people choose easy to remember passwords, which puts their accounts in trouble. According to the latest information from SplashData, "123456," "password," and "12345" were the three most commonly used passwords in 2014. This means it would not take a malicious actor much time or effort to guess the passwords people use to secure their email, online bank account and other critical assets.

Further compounding this problem is the fact that few people select and use unique, hard to guess passwords for all of their online accounts. Of the approximately 545 average apps that people use for business and pleasure, most of us rely on about 10 passwords to access all of them.

This means that by compromising one site, a hacker could theoretically gain credentials for hundreds more simply due to password repetition.

## The Most Common Password Workarounds

Most authentication systems have not evolved to take into account the extent to which we use digital applications today. This failure to innovate has driven enterprises to look for alternatives and created the reliance on passwords.

Many enterprises think that the best way to work around the password problem is to require users to manually, or through a password manager, create hard-to-guess, complex passwords for every enterprise account.

However, not only is it incredibly time consuming and difficult to develop and then remember 100 or so characters for every single online account, but some researchers have found that complex passwords can still easily be compromised today.

A single sign-on mechanism would seemingly help by allowing your users to use one solid password for all logins. But what happens when the password manager provider gets hacked, stolen or the one main password is compromised?

For proof of how current authentication schemes are failing enterprises every day, just take a quick peek at the headlines. Over 1 billion records were leaked or compromised in 2014, a 78 percent increase over 2013. This would be bad enough if data breach incidents were plateauing, but all signs show that subsequent months and years will be even worse. The situation is not just bad for financial institutions, government agencies and large enterprises, as organizations of all sizes and in all industries have seen their authentication schemes fail to protect them.

Industry regulations in healthcare, critical infrastructure, banking, defense and more continue to evolve to have stricter rules and requirements for stronger authentication. Hardware tokens, certificates, USB security keys and other security technologies are improving the situation considerably and go much farther to protect enterprises than typical passwords. But these technologies are not multi-purpose and typically tend to be difficult to replace.

Having one loose token or security key out there is dangerous because it can put an entire building and all its networks at risk. It can also be prohibitively expensive to issue a physical token to every employee - and then to replace everything when one is invariably misplaced.

## How Do We Move Towards Trusted Identities?

Faced with the need for better authentication solutions that are secure, simple for users and cost effective, organizations may not be sure where to turn for authentication. The answer may already be in arm's reach. Mobile provides the unique combination of security and usability that protects user identities ensures while ensuring they don't get frustrated, lose interest or find shortcuts that circumvent the system. By leveraging smartphones and other mobile devices as part of a more robust authentication scheme, organizations can feel more confident that they are blocking physical and digital access to their infrastructure and network.

**Pro Tip: Entrust Trusted Identities**

To find out more about Entrust Trusted Identities in Today's Connected Enterprise please visit.

http://www.entrust.com/enterprise/

# Mobile – The Foundation of Next Generation Identities

Mobile devices are ubiquitous in both enterprise and consumer organizations. Mobile devices provide a unique combination of security and usability that make them particularly well suited to be included as part of a robust authentication plan.

According to the latest statistics from the Pew Research Center, approximately 64 percent of all adults in the U.S. now own a smartphone - and that number is only going to rise in the coming years. The pervasiveness of mobile today ensures that any authentication scheme revolving around this technology can be widely used and relatively inexpensive to roll out.

And mobile devices are incredibly intuitive. We know how to use them and can easily download and update applications, reducing the learning curve and need for training—a benefit to IT support teams that often do not have the time or the budget to handle an increase in internal support.

## How Does Mobile Enhance Security?

In comparison to physical tokens, smartphones are less likely to be lost or misplaced because people have become so reliant on them (a recent poll found that around 90 percent of millennials never let their smartphone be out of reach).

So how exactly does mobile enhance enterprise security? Many of the native hardware and software features of mobile devices naturally enhance security:

- **Device & Location Attributes:** GPS lets you know if the person accessing your network is where they are supposed to be, or helps you find a lost or stolen device.
- **Application Sandbox:** Apps on mobile platforms are separate from each other, which ensures that any malware issues are isolated and cannot infect other apps on the device.

- **Cryptography:** mobile phones include native encryption to protect data and keep sensitive data private.
- **Biometrics:** Many modern devices feature easy-to-use biometrics like fingerprint or facial scanning. These methods are not only more secure, but are more user friendly ensuring greater compliance.
- **Trusted Execution Environment or Secure Element:** many devices feature a tamper-resistant microcontroller capable of securely hosting applications and cryptographic data. These elements are like small firewalls within a mobile device for processing secure transactions.

## What are the Risks with Using Mobile for Enterprise Authentication?

While mobile devices are proving to be infinitely more secure than PC's, they do come with their own set of risks. Smartphones can be compromised by malware, and people lose their mobile devices or have them stolen every day.

But, these issues can be easily mitigated.

With a quality mobile device management solution, for example, enterprise IT teams can easily roll out updates to everyone and effectively keep remote tabs on all mobile devices.

Furthermore, because authentication measures are sandboxed and set apart from other programs on a set device, organizations can make sure that a compromised app on a smartphone doesn't put the authentication scheme at jeopardy.

All of this, combined with a thorough and well-maintained smartphone use policy that dictates how phones must be utilized, which devices are allowed and how biometric authentication such as fingerprint scanning must be leveraged where applicable, can ensure mobile devices are only helping and not hurting physical or digital security.

# Practical Use Cases for Mobile Authentication

As far as *how* mobile devices can be used as part of a robust authentication scheme, the possibilities are seemingly endless.

But, one of the most popular use cases thus far is as an additional authentication factor on top of what might already be in place. In such a scenario, a one-time code or other form of notification is sent to a designated mobile device via an out-of-band channel after a password has been entered in or a keycard used. Only by using the code distributed to the smartphone, or by otherwise affirming an identity or action on a mobile device, will full access be granted.

Watch Entrust IdentityGuard Mobile Smart Credential Video

## VPN Authentication

Signing into an enterprise VPN can be a frustrating task. Whether you are using a hardware token, a complex password, or in most cases both, the systems are not typically user friendly.

Mobile Push Authentication simplifies the process by using the mobile device to verify identity and leverage transparent two-factor authentication to ensure your network can trust the identity of the person trying to access it. This ensures easier user provisioning and provides a secure authentication approach with a simple click of an “OK” button and without the use of complex passwords.

Watch Mobile VPN Access with Push Authentication Video

## Physical and Logical Access

Most of us have the need to access a physical environments such as a building, a door to a secured area, well as the ongoing task of logging into our workstations. Whereas smartcards are ubiquitous in enterprise environments, they are also expensive to deploy, easy to lose and can sometimes be skimmed.

Passwords and access codes on the other hand suffer from being difficult to use, easy to steal and complex to manage.

The solution is a Mobile Virtual Smart Card that securely and conveniently accesses doors, workstations and other secure areas. With a Mobile Virtual Smart Card, one device can become the access point for multiple resources eliminating the need to carry multiple cards or remember many passwords. A user's mobile device is always on hand, and by combining the Mobile Virtual Smart Card with biometric security on the device the system becomes even more user-friendly and secure.

A Mobile Virtual Smart Card can even auto-logout a user when they leave a secure area or workstation or auto-detect them when they arrive. This mean no more propping the door open for a quick run to the bathroom or forgetting to log out of our computer.

A Mobile Virtual Smart Card is PKI-certificate based, can't be skimmed or stolen, and is PIV / Derived Credential compliant.

## Mitigating the Risk of Fraud

When making an online transaction, the risk of attack is high, and the losses can be immediate and devastating. Fraud attacks are increasing in scope and sophistication, and customer data, enterprise systems, intellectual property and money are all at risk. According to Kapersky's 2014 consumer risk study, 62% of consumers are worried about financial fraud.

Hackers are using malware to "ride" on authenticated user sessions and most often the presence of these vulnerabilities goes completely undetected until it's too late.

How can you be sure your system isn't infected with malware ready to intercept the transaction?

With a mobile security solution, the transaction can be verified "out of band" on your the mobile device with transaction details retrieved and displayed over secure connection. Now you can know before a transaction is completed that a fraudulent transaction is in process.

Mobile devices can also be beneficial second authentication factors after a transaction has been started, to ensure the action taken on a desktop or laptop is indeed legitimate.

For example, before the accounting department is allowed to finalize a purchase, a notification of the transaction can be sent to a designated mobile device. That way, personnel can be quickly alerted if a fraudulent purchase was attempted.

Watch OTP TVS Transaction Confirmation Video

In situations when you may not have a data connection your mobile device can still be used to authenticate a transaction in real time with a quick scan of an encrypted QR code displayed on your banking application, using a secure passcode generator unique to the device. Only when the QR code is scanned by a pre-authorized device will everything be finalized. A second push notification can also allow someone to verify a transaction on the go, making digital signatures a reality.

Watch OTP QR Code Transaction Confirmation Video

## On-the-Go Approvals

People expect anywhere, anytime access—especially when doing business. Sometimes opportunities depend on the ability to get fast approvals before a window of time closes. Many business processes require formal, signed approvals to move to the next step, close the transaction or validate the information. Traditional digital signing is complex to deploy and has a very poor user experience.

Mobile devices can provide anytime, anywhere digital transaction signing, which provides a huge boost to productivity and can improve business processes greatly.

Whether it's a doctor writing a prescription, a banker offering a loan or an employee submitting a requisition, the ability to conveniently and securely sign a document, verifying both identity and authenticity directly from your own mobile device is tremendously powerful.

Digital mobile signatures are fast, convenient and user friendly ways to speed up day-to-day business operations, improve internal efficiency and provide better customer service.

# Mobile Security Best Practices

- **Don't click suspicious email links:** This is pretty straightforward advice, and it holds true as much for smartphones as it does for computing devices
- **Only download apps from trusted sources:** Sometimes a strain of malware will try to dress itself up as an app. But again, the signing/vetting employed by legit app repositories will weed such imposters out. So make sure to only download apps from trusted sources.
- **Don't choose easy PINs:** Make sure workers know that PINs should be as robust as possible or better yet take advantage of embedded biometrics to secure access to the phone.
- **Don't join just any Wi-Fi hotspot:** Be sure to confirm the legitimacy of any Wi-Fi network you're joining. This should be a relatively simple process - if you're at a cafe, for instance, just go up to the counter and ask an employee to identify the store's official Wi-Fi.
- **Authenticate Wi-Fi-connected devices:** If a mobile device wants to gain access to your corporate network, you must ensure that it's properly authenticated. The absence of an authentication platform could lead to malicious users gaining access to your Wi-Fi network.

# Summary

Smartphones are no longer peripheral elements of daily life - they're right in the center. They're helping to regulate our homes, open our doors, start our cars, and conduct payments. And fortunately for businesses, they offer tremendous transformative potential to improve how enterprise security is achieved as well.

*And enterprise security is needed*. Not only are data breaches and leaks becoming more common, but such incidents are increasingly costly too. According to the latest numbers from the Ponemon Institute, a breach typically sets an organization back about $3.8 million, with the price associated with just one stolen record now hovering around $150. When the reputational damage caused by a leak or breach is factored into the equation too - a 2014 survey from Semafone found that more than 86 percent of people polled said they were less likely to do business with an organization that had suffered a breach - the costs related to an incident rise even higher.

By relying just on outdated authentication schemes, organizations are assuredly putting themselves in harm's way. It's become more than a security issue—enterprises and consumer facing organizations are actually encumbering users and are often "getting in the way of business."

Identity is critical to today's connected enterprise, and managing them is clearly a complex task. Organizations need to consider authentication that addresses every digital reality while taking advantage of the technologies that make it more secure, easy to use and cost effective. While passwords, tokens and access cards may have worked in a world where every device wasn't in some way connected to the web, today a better solution is needed.

Dated authentication methods fall short not just due to technology, but because they are not user friendly enough to gain the compliance levels needed to maximize security. So why not move the trusted identity enclave to the device that everyone already carries and loves?

Mobile trusted identities allow you to move beyond passwords and transform business processes. Mobile devices are more secure, more convenient and are multi-purpose devices that users already have, love to carry, and don't feel burdened to use. By making the smartphone the center of the trusted identity, enterprise security can be stronger and more fully embraced by employees than ever before.

To learn more about your options, contact an Entrust Datacard representative today.


# 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, visit www.entrustdatacard.com

**Contact & Social Links**

www.entrust.com

Entrust@entrust.com

888.690.2424

**Connect with Entrust Datacard:**

# About Mike Byrnes

Mike Byrnes has more than 20 years' experience in product management and technology marketing with a focus on internet security and business communication systems. Mike drives product marketing for the Entrust IdentityGuard authentication platform with a significant focus on mobile solutions.

In addition to mobile, his background covers identity and access management, fraud detection, malware protection, and email encryption solutions. Mike serves as vertical market prime for Entrust financial services segment, working with large banks across the globe to roll out solutions to their consumer- and corporate-banking client base.