EMPOWERING eGOVERNMENT
With Mobile Identity

Entrust Datacard™

Contents

Growing Complexity in eGovernment Ecosystems

Just as the proliferation of mobile devices, the Internet of Things and other elements of increasing connectivity have impacted our everyday lives, these trends are rapidly changing the landscape for government agencies. More agencies than ever before leverage advanced eGovernment applications to deliver citizen services. Government workers are at the forefront of the mobile workforce growth, with around 90 percent of government employees using at least one mobile device for their daily work. Collaboration among agencies and between states is increasing interoperability of eGovernment systems and networks.

All of these elements of growing connectivity have the potential to significantly increase productivity, streamline operations and enhance service levels to citizens and stakeholders. But these benefits are only one side of the story. The added complexity of the new eGovernment environment also creates many new challenges, as government agencies search for effective ways to secure and control access to the rapidly growing number and variety of gateways to their ecosystems.

Learn more about Entrust Datacard Connected Government Solutions

See what Entrust Datacard has to offer at http://www.entrust.com/government/

Connectivity Creating New Challenges

This new world of innumerable interconnected devices, apps and networks also creates significant new security challenges.

- Increasing Threat of Cybercrime — Increasing Cost of Breaches
- BYOD & Shadow IT
- Poor Mobile Security
- Rigid Regulations

Increasing Threat of Cybercrime — Increasing Cost of Breaches

It seems you can hardly go one week without reading of another major data breach or cyber attack in the headlines. The numbers don't lie: 2014 saw cybercrime and data breaches reach an all-time high — an estimated 1 in 4 Americans received a breach notice in the last 12 months — and forecasts suggest that growth will continue in the coming years.

Government agencies are attractive targets for cybercriminals, as they tend to hold particularly sensitive (read: valuable) information. The Pentagon reports around 10 million attempted cyber attacks each day, and some state governments face nearly 200,000 daily attacks. Since 2009, more than 94 million — or about 1 in 3 — U.S. citizens' records have been exposed in breaches.

Not only are breaches becoming more frequent — they are becoming more costly. According to the Ponemon Institute, the cost of the average data breach has increased 23 percent over the last two years. For the organization recovering from a breach, each compromised record now costs an average of $194. Multiply that by the 94 million records lost since 2009, and breaches have cost the U.S. government over $18 billion.

It's no wonder, then, that the recent Office of Personnel Management (OPM) breach led the government agency to sign a contract for identity protection services worth more than $20 million.

Why the increase in breaches? One side of the problem is the growing complexity of cyber attacks, aided by increased computing power and advanced algorithms. Sixty percent of U.S. state CISOs reported a notable increase in the sophistication of the cyberthreats they face. The other side of the problem?

The so-called "human-factor" challenges that are amplified by the connected workforce. Human errors — from weak passwords to workarounds — account for almost half (49%) of all government breaches.

BYOD & Shadow IT

Today, we are all tethered to our mobile devices. So it follows naturally that we want to use the mobile device of our choosing in our work lives. Many government agencies are embracing a BYOD environment as part of the overall productivity boosting goals of empowering the mobile workforce.

Along with using their own devices, mobile workers are also used to finding a specialized app for everything, and they take the same approach to their mobile productivity on the job. A recent survey found that 80 percent of U.S. workers admit to using non-approved applications in their jobs, creating an entire "Shadow IT" world of unsanctioned app use and data exchange that blurs the lines of a government agency's digital ecosystem.

Poor User Security

Whether accessing sanctioned or unsanctioned applications, many government employees fail to maintain strong security controls on their devices. A recent study found that 41 percent of government employees admitted to regularly practicing "potentially harmful behaviors."

These included:

- 25% fail to use passwords to secure their mobile devices
- 33% admit to using passwords that are easy to guess
- 31% regularly use public WiFi networks
- 52% fail to use multi-factor authentication or data encryption

Evolving Regulations

As they maintain particularly sensitive information, government agencies have always been subject to strict data security regulations. But the increased risk — and increasingly successful attacks — in the government world are leading to more demanding standards, tougher regulations and harsher sanctions and fines for non-compliance. From the new NIST Cybersecurity Framework 1.0 to IRS 1075 regulations, to new requirements from CMS and the Office of Child Support Enforcement, agencies in every field are facing tougher standards that require more complex and comprehensive data security solutions.

Budget Struggles

While all agencies feel the growing pressure of security threats, there is not matching growth in funding for these projects. In fact, more than half of state governments have a security budget that accounts for less than 5 percent of total state spending. The challenge, then, is finding a security solution that enables government organizations to do more with less.

Identity at the Core

Identity is the core element of all of these trends shaping the connected government ecosystem. Government employees access eGovernment systems and mobile applications with identity credentials — and cybercriminals gain unauthorized access through hacking, stealing or otherwise subverting these identity credentials. To position themselves for success in this new landscape, government agencies need to focus on making trusted identity the core of their security strategy. With the ability to quickly and effectively authenticate the identity of both the user and the device, an agency can fend off sophisticated threats while empowering the streamlined productivity and enhanced service levels of a fully connected, anytime-anywhere workforce.

The Problem with Traditional Identities

Passwords are Predictable

Passwords secure access to 99 percent of all digital resources. But "secure" isn't exactly the right word. Given enough time, sophisticated cybercriminals can hack even the strongest of user-generated passwords — because passwords fall victim to two key human-factor flaws:

People are Predictable

Every year, security experts publish lists of the most common passwords, demonstrating a troubling truth: The majority of user-generated passwords fall on a list of just 100 or so. Even when users try to be clever and complex, they are unknowingly predictable. Half of all passwords follow one of 13 common (hackable) patterns.

People Find Work-Arounds

The average U.S. worker now uses 19 different usernames and passwords to access the digital resources in their jobs. We prize innovative approaches to overcoming obstacles and increasing productivity in the workplace. So it's no surprise that, given the task of juggling 19 different identities — and the expectation of regular password refreshes — government employees find creative ways to work around these cumbersome security requirements.

73% of online accounts are guarded by duplicated passwords *(Source: TeleSign)*	**1 in 2 people** use passwords that are at least **5 years old**	**72%** of people record their passwords somewhere (e.g. on paper or in a spreadsheet) *(Source: Meldium)*

Sophisticated Cybercrime Threatens Even the Strongest Passwords

The password flaws above are susceptible to "brute force" cyberattacks — directly guessing or cracking the plain-text password. But today's advanced hacking techniques can find side doors for gaining access. Techniques such as rainbow tables enable hackers to "pass the hash" — cracking the underlying encryption of a password system. This method is faster than brute force hacking, and even long, complex and truly random passwords are still susceptible, since the hackers no longer need to crack the plain-text password.

Hard Tokens & Stronger Controls Impede Productivity

Faced with weak passwords and frequent work-arounds, many government agencies fall victim to assuming that stronger, more complex access controls equal better security. This means implementing password complexity requirements, mandating frequent password refreshes, and adding hard tokens — such as smart cards or OTPs — to authentication protocol. In practice, this adds up to even more cumbersome workflows and end-user burdens that hamper productivity. A survey of government workers found 69 percent agreed that security protocol reduced their productivity by slowing workflows.

Mobile Identity Emerging as an Empowering Solution

Rather than looking to add complexity to authentication protocol, government agencies must look for ways to simplify. In looking for an identity solution for empowering a workforce tethered to and driven by their mobile devices, the simple answer is built into the challenge. Modern mobile devices have powerful built-in security capabilities that can assist in establishing a trusted identity for each unique user and secure access to the entire digital ecosystem. Just as importantly, users already carry their mobile devices with them at all times and already love their convenience and usability.

The Security of Mobile Identity

A mobile identity solution provides a much more secure authentication platform than traditional credentials like usernames and passwords or hard tokens, enhancing digital security by leveraging the inherent security capabilities of today's mobile devices:

- **Device Location & Attributes:** GPS lets you identify the location of the individual authenticating for access and flag unexpected or suspicious locations for further investigation. GPS also helps locate lost or stolen mobile devices.
- **Application Sandbox:** Applications on mobile platforms run separately from the core operating systems. Hackers cannot gain unauthorized access to the entire mobile device (and the mobile identity) via a single compromised app. This also prevents malware located on one app from corrupting other apps.
- **Cryptography:** Mobile devices include native encryption to secure data and protect sensitive information as it moves throughout a digital ecosystem.
- **Biometrics:** Many mobile devices feature easy-to-use biometrics capabilities such as fingerprint or facial scanning. These capabilities enable enhanced, multi-factor identity authentication that establishes the true physical presence of the individual authenticating for access. Because the user-friendly biometric reader is built into the mobile device, they drive greater compliance and fewer high-risk "work-arounds."
- **Trusted Execution Environment or Secure Element:** Many mobile devices feature a tamper-resistant micro-controller capable of securely hosting applications and cryptographic data. These elements are like small firewalls within a mobile device, enabling secure transaction processing.

Mobile Security Best Practices

While the mobile device provides a trusted platform for identities and transactions, there are a number of best practices that should always be considered when designing mobile applications:

- **Force PIN/Biometric Access:** For devices that support it, require the use of the most secure access restrictions possible on the device.
- **Find My Phone Apps:** Most mobile platforms have apps and services to help track down lost or stolen phones.
- **Block Jail Broken Phones:** Restrict the ability for users to jailbreak their phones bypassing manufacturer security.
- **Mobile Device Authentication:** Ensure you know and authorize each unique device connecting to you network and only allow authorized users in.
- **Mobile Device Management:** Provide the ability to provision security policies and remotely manage devices to mitigate risk.
- **Use Secure Work Partitions:** Mobile Device Management (MDM) platforms are helpful to segregate "work" and "personal" data on the device.
- **Signed/Vetted Applications:** Legitimate applications downloaded onto a mobile device will have been signed and vetted before they are loaded onto your system. So long as they are from an official store — such as the Apple App Store — they have gone through a rigorous process to enhance their security and stability.

The Productivity-Boosting Convenience of Mobile Identity

Embedding trusted identity within an already-popular device puts a convenient identity authentication solution at your users' fingertips, eliminating the need to manage myriad complex passwords and tote additional credentials or tokens along with them. Users authenticate faster and move through workflows more efficiently, boosting productivity and helping to enhance citizen service levels. And with mobile productivity becoming essential to efficient operations and services, trusted mobile identity creates a seamless experience as mobile workers move from authenticating to accessing mobile apps to carrying out their daily work functions, anytime and anywhere, via their mobile devices.

Cost-Effective Deployment

Though most IT administrators know the security and customer-usability flaws of traditional identity authentication methods, budget constraints keep many from examining alternatives. Ripping out a government agency's entire authentication architecture would be a costly, time-consuming affair — and could impact interoperability between agencies and states. Instead, mobile identity provides a solution that is easily implemented within the existing authentication architecture of most government agencies. Advanced mobile identity solutions enable the mobile credential to replace username/password authentication, serve as a hard token, and even provide biometrics-based proof-of-presence — all within the same front-end log-in framework and back-end authentication architecture that an agency is currently using for application and network access. And because most users already carry compatible mobile devices, the deployment of a mobile identity solution is fast and cost-effective, with minimal downtime.

Envisioning the Mobile-Enhanced eGovernment Work Experience

To provide a better understanding of the full power and potential of a mobile identity solution, here is a look at real-world ways in which mobile identity enhances security and empowers productive eGovernment:

- VPN Authentication
- Transaction Signing
- Transaction Verification
- Mobile Derived Credentials

VPN Authentication

Signing into a VPN can be a frustrating task. Government employees generally must manage a complex password and an additional hardware token. With mobile push authentication, a mobile push notification is automatically sent to the verified, secure mobile device. The user simply simply clicks "OK" to confirm the authenticity of the VPN session — no password required and no searching for a single-purpose token lost at the bottom of their work bag.

Transaction Signing

Many government processes and workflows 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 often has poor user experience that slows workflows. A mobile identity platform can leverage the built-in biometrics capabilities of a mobile device to allow fast, easy and secure digital signing. A push notification alerts the user that a digital signature is required, and the user simply scans a fingerprint or puts in their password to enable a cryptographic signature of the data. Whether it's an inspector submitting a report, a law enforcement officer obtaining a warrant, or an employee submitting a requisition, the ability to conveniently and securely sign a document, verifying both identity and authenticity, can speed operations, provide better customer service and dramatically boost productivity.

Transaction Verification

When transferring government funds between agencies, making payment to citizens or even accessing sensitive data, how can you be sure your system isn't infected with malware ready to intercept the transaction? Online transactions bring an even greater risk of cyber attack and other fraud that can bring high costs and exposes sensitive citizen data. Hackers use sophisticated malware to "ride" on authenticated user sessions — and these vulnerabilities most often go undetected until it's too late.

With a mobile identity platform, users can receive push notifications with key transaction details. Users quickly and easily verify transactions "out of band" and can immediately identify suspicious activity to defeat account takeovers before they are executed on the server side.

Meeting Regulations for Derived Credentials

As the shift away from the "static" workforce continues, government agencies are working toward meeting the heightened standards — and avoiding the harsh fines — of new regulatory policies, including:

- SP800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials
- FIPS201 PIV Authentication
- Common Policy Certificate Policy

The Entrust Mobile Smart Credential solution provides an HSPD-12 compliant credential within the mobile device, as well as secure, over-the-air, automated provisioning in order to meet specific requirements within an organization. This mobile smart credential uses the employee's existing government-issued credential to bootstrap the deployment process, greatly simplifying deployment.

Additionally, Entrust has partnered with mobile application developers to provide critical applications:

- SMIME email client, which can leverage the mobile credential for signing, encrypting and decrypting emails on a mobile device
- Secure web browser, which can perform mutual SSL, web single-sign-on and OWA
- File encryption for files stored on the device
- Digitally signing of documents
- Secure VPN access to resources from the mobile device

With the SP800-157 compliant mobile PIV derived credential, the employee can securely access computers, applications, cloud services and even physical doors. It can also be used to authenticate transactions initiated from the Windows web browser of your choice.

Leveraging Mobile Identity to Drive eGovernment Service Delivery

With eGovernment ecosystems growing more complex thanks to increased connectivity, mobile productivity and interoperability initiatives, traditional credentials — passwords, tokens and access cards — simply can't keep up. Government agencies need a better solution to protect their ecosystems while empowering the productivity benefits of the connected workforce.

Today, the anytime-anywhere connectivity of the smartphone makes it the center of our personal professional lives — and make it a natural, user-friendly and cost-effective answer to this identity challenge. Leveraging the built-in security capabilities of the mobile device — from push notifications and advanced encryption to biometrics — government agencies can effectively establish user and device identity, mitigate the risk of cyber attacks, and protect sensitive data and citizen information. At the same time, mobile identity gives government employees streamlined authentication workflows that simplify their work lives, boosting productivity, increasing operational efficiency and enhancing the level of service delivered to the citizens you serve.

Entrust Datacard™

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.

Headquarters
Three Lincoln Centre
5430 LBJ Freeway,
Suite 1250
Dallas, TX 75240 USA

www.entrsutdatacard.com

Entrust Datacard™