WHITE PAPER

Securing Personal Mobile Device Access to Enterprise IT and Cloud Assets with Strong Authentication

Strong Authentication is the Foundation for Securing Mobile Access

Executive Summary

The consumerization of IT is forcing enterprises to take a second look at how they establish trust in users' identities and grant access to corporate resources and cloud applications, as an increasing number of users are bringing their own devices to work and demanding support from their IT departments. When looking at protecting access from these mobile devices, many of which are not owned or managed by the organization, enterprises must strike a balance between cost, convenience and security. With HID Global, organizations can establish trust in their users' identities when they are accessing resources from their mobile devices and then manage that access to protect their enterprise and cloud applications. HID Global has a long history of providing innovative, comprehensive identity assurance solutions to ensure organizations can meet their security and cost requirements, as well as their users' expectations.

A Mobile World – By the Numbers:

- An Accenture survey found 83% of companies believe mobility will significantly affect their business.
- Gartner predicts one billion smartphones will ship in 2013.
- Apple sold 67 million iPads in less than two years – it took Apple 24 years to sell an equivalent number of Macintosh computers.
- By 2016, it's estimated global mobile data traffic will reach an annual run rate of 130 exabytes a year.
- There will be seven billion new wireless devices on the network by 2015 – including machine-to-machine modules– which equates to almost one mobile device per person on the planet.
- 1-2% of all mobile phones are infected with malware at any given time.

Loss of Control – The Mobile, BYOD Phenomenon

In the world of enterprise security, what used to be a fairly contained universe – with the ability to put effective controls at critical physical and online entry points — is now an exploding, constantly moving target. The new landscape many enterprises and government organizations are facing is a mobile one, where employees, partners, customers and other constituents want to access resources from anywhere, at anytime, using the latest, smartest mobile devices they have on hand to conduct their business. While organizations recognize the opportunities and productivity gains that can be garnered from anywhere, anytime access, they are struggling to effectively support it.

A key reason this is so difficult is that organizations no longer own all the devices that enter their premises and connect to their networks. Employees are bringing their own devices (BYOD) to work and demanding IT support for them at an increasing rate because they want the same quick, easy and convenient access to resources at work, with the same devices and tools they are used to having in their personal lives. Since these personal mobile devices are being used to access enterprise resources and cloud applications, they become a highly attractive target for security threats. Against a backdrop of increasing mobile malware, advanced persistent threats (APTs) and highly motivated and sophisticated attackers, enterprises and government organizations must be able to secure mobile access – it cannot be the weak link. The consummate balance between convenience and security must be maintained to ensure the convenience that mobile access enables doesn't jeopardize the resources and ongoing operations of the business.

But how do organizations protect access from mobile devices when they don't own or control them? They can't standardize on a couple, even a handful, of platforms and operating systems to create a consistent environment or reduce support complexity; they can't tell users what to download or do with the device on their own time; and they certainly can't watch them to make sure they don't give it to someone else or leave it somewhere. While organizations and government agencies don't have a lot of control over the device, they can control the access they allow from that device to corporate resources, networks and cloud applications.

By deploying a complete identity assurance solution, the foundation of which is strong authentication, organizations can establish trust in their users' identities and their mobile device when they are accessing corporate resources and manage and control that access. In this way, organizations can enable users to access enterprise and cloud applications from their mobile devices, in a more secure, cost-effective way, while regaining control over their environment.

Strong Authentication is the Foundational Element to Securing Mobile Access

Strong authentication, which is sometimes referred to as advanced authentication (AA) or multi-factor authentication, serves as the foundation for an effective identity assurance solution that can be used to secure mobile access. By requiring additional factors, beyond a simple password, to validate a user is who they say they are, organizations are able to deploy a higher level of security and better control access to corporate resources, networks and cloud applications. To trust personal mobile devices and deploy strong authentication, organizations may use any combination of factors:

- Something the user knows, such as a unique password or personal identification number (PIN);
- Something the user has, such as a token, one-time password (OTP), short message service (SMS) message, or a secure element on a mobile device (such as a SIM card, embedded smart chip, smart MicroSD, etc.);
- Biometrics of the user, such as their fingerprint, Iris pattern, voice pattern or facial geometry;
- Or a collection of parameters the authentication system gathers with fraud or behavioral intelligence. It may consider characteristics of the device itself, such as type of phone, browser, etc., geographic location, or unique characteristics of the user, such as keystroke patterns, typing rhythm, etc.

From a mobile perspective, there are three possible elements to authentication. The first is authenticating to the device – for example, when a user turns on their phone and punches in a PIN to start using it; the second is authenticating to access the resources that are either on the mobile device or accessible by that device; and the third element is authenticating to the wallet/enterprise container.

The second element – authenticating to access resources – is where organizations can apply a point of control. They can ensure users authenticate before they can access enterprise resources via their personal phone, tablet, etc. Strong authentication enables organizations to gain higher trust in the identity of their users and then grant appropriate access to VPNs, virtual desktops, WiFi networks or individual enterprise and cloud-based applications, while addressing the potential security risks associated with users bringing their own devices into the corporate environment.

The Options for Authentication to Meet Different Security, Convenience and Cost Requirements

When looking at protecting access to resources and cloud applications with personal mobile devices, once again it comes down to a balance between cost, convenience and security. There are several approaches that add varying levels of security and introduce varying levels of complexity. Organizations should consider the users' needs, as well as the costs, both capital investments and ongoing operational expenses, to the organization.

One option may be that certain users or applications require additional levels of security and differing levels of access, so organizations may end up deploying a variety of authentication methods to appropriately control access. When combined, an organization can achieve a layered approach to mobile authentication that meets both their security and cost requirements and their user's expectations when using their own mobile device. Some of the authentication options organization can consider for securing access to corporate resources with personal devices include:

- **Static Passwords:** They simply aren't enough – they are vulnerable to keystroke loggers, phishing attacks, etc. and do nothing to protect against insider threats.

- **Hardware Token:** A device that can be used for multi-factor authentication. Hardware tokens offer strong security, however, the onus is on the user to carry and remember the token, which can negatively impact the user's experience. When they need to authenticate, they look at the token and plug in the OTP that it has generated to gain access (if the device has a reader, the user may instead put the token in the reader to authenticate). The tokens can increase overall costs for an organization, since they need to purchase, send out, manage and maintain the tokens. Note, sometimes these tokens are delivered as a USB drive, which some phones don't support.

- **Mobile Soft Token:** Delivered as either a standalone application or embedded into an application that someone develops, the soft token is downloaded by the user to act as an OTP for multi-factor authentication. This may not be as strong as having the keys of the OTP generated on a dedicated, tamper-proof certified chip, however, many have special anti-cloning technology built into them to prevent counterfeiting or cloning the token onto another device. When they need to authenticate to an enterprise resource or cloud application, users simply click on the mobile soft token (app), enter a pin and use the OTP that's good for approximately a minute to get access. It doesn't require any hardware, which makes it very simple to deploy and manage and easy for the user to incorporate into their existing workflow.

- **SMS Message**: Acts as an OTP that's sent over SMS. Similar to delivering the OTP via a mobile soft token, but instead of clicking on an application to get the OTP, the user makes a request and receives an OTP, via an SMS message, which they must then copy and paste into the application. This makes it slightly less convenient for the user than a soft token. It is also less secure, since SMS can be intercepted and doesn't always arrive at the destination. There is also an ongoing cost associated with sending the SMS messages.

- **Secure Element-based Security Tokens:** Security mechanism incorporated into the mobile device that enables users to leverage strong credentials. Note, mobile platforms, which have varying levels of maturity, have to be able to either have the secure element already on board (embedded) or have a place to hold the smart chip or microSD, so it can be leveraged for different uses, such as to authenticate, encrypt, decrypt, sign email, and provide secure physical access and cloud application access. This offers the highest level of security; it's also convenient for the user, since they can securely do everything they need. It can be costly to purchase, but innovative solutions are on the market that simplify the deployment and ongoing management of secure elements and the credentials they harbor. To date, it's used mainly by government organizations and regulated industries that need to adhere to standards and regulations.

BYOD – Strong Authentication Options

Option	Description	Security	Complexity	Cost	Convenience
Password	Simple password	Low	Low	Low	High
Hardware Token	OTP developed in hardware (or	High	High	High	Low
Mobile Soft Token	Acts as an OTP delivered via an application	Medium	Low	Low	Medium
SMS Message	Acts as an OTP delivered via an SMS message	Low/Medium	Low	Low	Medium
Secure Element	SIM, embedded Smart chip, or Smart microSD that's installed on the phone	High	High	High	High

How Authenticating to Cloud Applications Works
The organization can use HID Global's ActivID® solutions to deploy a variety of authentication methods, while keeping the user experience simple and limiting security risks associated with bring your own device (BYOD). For example, a user can go to the app store, download the soft token app (or the organization can push it out) to start the registration process with ActivID.

The organization's administrator then sends an email with multiple codes that the user inputs to receive validation they have been bound to that device in the system. The user can then authenticate to secure access from that device to the enterprise network and/or cloud applications.

For example, the ActivID Appliance will use security assertion markup language (SAML) to work with Salesforce.com; when the user wants to access Salesforce.com they automatically get rerouted to the appliance, where they must use their credential to authenticate in and get access. That SAML ticket can be used by other cloud or enterprise applications to grant access – the applications accept the ticket because they know the user has been validated. This authentication federation is a secure, simple mechanism that makes it easy and convenient for users to access resources via their mobile devices as needed.

The Requirements for an Effective Authentication Solution to Secure Mobile Access (BYOD)

The mobile landscape is changing every day; new devices are introduced and mobile platforms are evolving at such a rapid pace that it is virtually impossible for organizations to keep up. Users are quick to adopt the latest device and bring it into the corporate environment and request access to resources. To effectively enable access via these personal mobile devices, without opening up the organization to unnecessary risks or costs, solutions must deliver:

- **Risk Reduction** – Nothing is going to eliminate the danger posed by the ever-changing, ever-progressing threat landscape; what's needed is a way to minimize the organization's exposure to risks introduced by mobile access. The solution should offer:

- **Strong authentication** – two-factor or more, to increase the confidence organizations have in their users' identity and their ability to grant appropriate access from their mobile devices.

- **Differing levels of access** – based on the risks associated with different types of users and the sensitivity of the enterprise resources and cloud applications being accessed via that mobile device.

- **Platform control** – to accommodate the available mobile platforms, organizations may have in their environment. Organizations should be able to enforce which platforms and what specific version of each platform is allowed to access their networks and applications. For example, an organization might know a specific version of a mobile OS is vulnerable to attacks and could decide not to allow devices with that specific OS version to access network/resources.

- **Rapid and targeted response** – In the event a security incident occurs, organizations must have the tools and means to quickly and easily respond to that incident in a targeted fashion that does not impact the users unaffected by the incident. For instance, they should be able to bar access from a particular device or version of applications/software that have been deemed a high risk, perhaps from a specific vulnerability.

- **Manageability** – the solution should be easy to get up and running, without adding unnecessary complexity or costs. Ideally, it would enable organizations to have a consolidated view that simplifies the credential issuance and on-going management to support a consistent security stance. For example, it should be easy to identify and revoke credentials so the organization doesn't have an active credential for an employee who has left the company.

Versatility – The solution should be versatile and scalable, so organizations can satisfy their different requirements. It should support:

- **Multiple Authentication Methods** – To balance an organization's cost and security requirements, the solution should be flexible enough to support different authentication methods for different users, resources and cloud-based applications.

- **Best-of-Breed Standards-based Technology** – In the quickly evolving mobile landscape, organizations want a solution from a vendor that has a history of innovating to find solutions to tough problems. The solution should embrace standards so organizations can deploy technologies as they are available, without having to rely on the timeline of any one vendor.

- **Wide Platform Support** – With BYOD, it's a wide open field; users can be using all sorts of devices, with different operating systems and different versions of those operating systems, from a variety of vendors. What organizations need is a solution that can be applied across the spectrum of mobile devices to ensure access controls can be consistently applied in a way that's simple to manage.

- **User Convenience** – the solution shouldn't disrupt workflows or cause undue delay to the enterprise and cloud-based applications users need to conduct their business.

HID Global's Approach to Mobile Authentication – Comprehensive, Flexible and Secure Options

With HID Global, organizations can establish trust in their users' identities when they are accessing resources from their mobile devices and then manage that access to protect their enterprise and cloud applications. HID Global, worldwide leader in secure identity solutions,, has a long history of providing innovative, comprehensive identity assurance solutions that meet an organization's security and cost requirements, as well as their users' expectations. Depending on the organization's business needs, the solution offering could be one or a combination of products from HID Global's Identity Assurance portfolio. HID Global offers a breadth of authentication and credential management products and have issued more than 20 million credentials worldwide. The portfolio includes:

HID Global's ActivID Versatility At-a-Glance

- **Device support**: smartphones, tablets, laptops, and other devices
- **Authentication methods:** OTP hard tokens and soft tokens, smart cards (PKI), device IDs, adaptive authentication, fraud detection mechanisms, and Out-of-Band SMS, or email OTP mechanisms for transaction level authentication
- **Applications:** Business, Cloud, etc. – such as Windows, Salesforce.com, SAP, Oracle, and Google Apps

- **HID Global's Mobile Soft Tokens and SDK (HID Global's ActivID® Tokens)** – the soft tokens can be pushed out over the network and quickly downloaded by users (or downloaded from an app store). Users can simply generate a one-time password (OTP) when they want to connect via their mobile device to corporate resources. HID Global's Mobile Soft Tokens are available on leading handset operating systems, including RIM BlackBerry®, Apple® iOS (for iPhone® and iPad), Google Android, Windows Mobile, and many other Java 2 Platform, Micro Edition (J2ME) enabled devices, and come with replacement for life with a current maintenance contract. Organizations can also use HID Global's Mobile Soft Token SDK, which can be embedded directly into the mobile application, such as a mobile banking app offered by a retail bank.

- **HID Global's ActivClient™ Mobile** – Middleware that leverages a local phone secure element, which can be a Smart microSD, embedded smart chip or even the SIM or an existing issued smart card (e.g. PIV, PIV-I, CIV cards), inserted into the phone, via an attached reader (for example in form of a sleeve), to provide the highest Levels of Assurance (LoA 4) for security services, from strong authentication and non-repudiation to digital signature and encryption services. Supports HID Global's FIPS-certified applets that provide trusted government grade components of a PIV card "on the phone."

  For example, users can have secure, digitally signed email on their phone –the ActivClient acts as middleware, enabling the organization to exploit the security functionality on the secure element. It interfaces with HID Global's Applets on the secure element to leverage public-private key credentials, making it easy to use public key infrastructure (PKI) for secure email. Because the mechanism is within the phone, there is no need to tether or pair a smart card reader with the device, making it far more convenient for the user and less complicated for the organization.

- **Strategic Alliance with Good Technology** – delivers an array of new government-strength, mobile enterprise collaboration, messaging and management solutions for the iOS and Android platforms. The solutions couple the existing government-grade security capabilities of Good for Enterprise™ and Good for Government™ with the strong authentication technology of HID Global's ActivClient® Mobile middleware. They make it easier for regulated industries, government employees and the companies that support them to gain access to pertinent applications using their mobile device, while maintaining the necessary security levels required by the organization. The solution helps compartmentalize access to resources from the mobile phone, specifically for BOYD scenarios, to mitigate risk.

ActivID CMS At-a-Glance

- **Authentication Devices**: from smart cards and USB tokens to secure elements on mobile phones
- **Data**: static passwords, biometrics and demographic data
- **Applets:** OTP applications and PIV applets
- **Digital Credentials**: including PKI certificates throughout their entire lifecycle

- **HID Global's ActivID Credential Management System (CMS)** – provides a complete, flexible solution to enable organizations to easily manage the issuance and administration requirements of successful authentication deployments. Organizations can issue and manage secure elements, smart cards, smart USB tokens, etc. that can be used to authenticate to applications from mobile devices. The ActivID system provides over-the-air lifecycle management capabilities to enable locking the secure element (and all related certificates and keys) while the phone is in the field; self-service capabilities enable a user to unlock a locked PIN or receive a new credential (for example a new PKI certificate and related private key) while in the field, without having to return to a service desk.

It delivers full, tamper-evident audit features that log all event activities for reporting, with unique, patented secure post-issuance update capabilities to help keep the organization's authentication solution in force. Web-based self-service and help desk administration reduce the operational costs associated with the ongoing management and maintenance of the solution.

- **HID Global's ActivID Authentication Appliance** – provides versatile strong authentication, including out-of-band SMS Message Authentication, for users accessing a wide range of applications, such as VPN remote access, virtual desktops, terminal services, and private and public clouds. Through a single appliance, HID Global supports a multitude of authentication methods to protect the organization's data, network and reputation assets.

  ActivID allows the organization to tailor authentication methods to the needs of specific groups of users, providing each the right balance of security, cost and convenience to meet business objectives. Templates and easy-to-define policies enable organizations to be as specific as they want, limiting access to particular devices within a particular area or looking at the role of the user (such as whether they are a CEO or a marketing manager) and determining what credential to provision and how to handle their access.

  HID Global increases productivity by securely authenticating users remotely via their preferred smartphone, browser or computer through a variety of devices and authentication methods. The ActivID Appliance supports the broadest choice of authentication methods, from strong passwords to certificate-based authentication, including two-factor, OATH-standards-based hardware tokens, soft tokens, and SMS Out-of-Band OTP options. The ActivID Appliance reduces costs with easy installation, worry-free tokens that last up to eight years, and simple integration into the existing network infrastructure.

  HID Global's advanced ActivID Threat Detection Service is a unique cloud-based device identification and global fraud network intelligence service that enables organizations to effectively add fraud-preventative measures to their existing authentication systems. The real-time device profiling and mobile location services can be used to provide an added confidence factor. With more than 300 live customers, 1.2 million new devices and 1.3 million transactions profiled daily, organizations have visibility into significant changes in the threat landscape to combat sophisticated cyber criminals and prevent online fraud. The ActivID Threat Detection Service gives them the ability to detect and block access from compromised or fraudulent computers; instantly identify stolen passwords, lock accounts and notify legitimate users of the need to change their password; and prevent fraudulent and other potentially high risk access.

With HID Global, Organizations Can Reap the Benefits of Secure Mobile Access, including Access from Personal Devices

With a long history in the identity and credentialing space, HID Global is able to provide organizations all the pieces they need to secure mobile access – from the credential management system and validation platform to the soft tokens and chips (and even on the phone or readers, if needed). HID Global protects the online banking and access to sensitive corporate and cloud applications of millions of users, across financial institutions, healthcare organizations, enterprises and government agencies; HID global is the partner of choice for the full range of customers' identity assurance and strong authentication needs. The company brings this experience to the nascent, ever-evolving mobile landscape to can help organizations embrace mobility in a successful manner. With HID Global, companies can:

- **Decrease Risk** – enable users to securely connect with their mobile devices, via robust multi-factor authentication that inhibits breaches and protect enterprise resources and cloud applications. Meet mandates to use strong authentication for mobile access and ensure it is not the weak link in the organization's security stance.

- **Reduce Costs** – with versatile, multi-layered authentication technologies, organizations have what they need to secure smartphone, iPad, laptop and other mobile access to VPNs, Web portals and cloud applications. Centralized management simplifies processes, reduces paperwork and streamlines the overall operations associated with the organization's identity assurance solution. The broad range of options enables organizations to choose the best solution for their different needs, eliminating the unnecessary costs associated with a "one size fits all" solution. Organizations can choose the level of security they need for their different users, enterprise resources and applications and easily scale their deployments as their needs change.

- **Improve Control** – employ a fully interoperable OATH-standards-based authentication solution to ensure users can securely access what they need to conduct business via their mobile devices. Easy to define security policies and business processes make is simple for organizations to issue and manage credentials and deliver varying levels of authentication for different resources and cloud applications to match the cost, security and complexity requirements of the business.

- **Deliver User Convenience** – ensure users have the access they need, when they need it from wherever they are to maximize productivity. The easy to use solutions add security in a seamless way, without unnecessary disruptions to workflows.

Summary

As smartphones get smarter and tablets and other devices are used to do more and more, they will become an increasingly attractive target for attackers. Smartphones are accessing not only email, but also an increasing amount of sensitive corporate data and systems, both directly and via cloud applications. It's important to minimize exposure to these new threats and dangers, while still enabling users to leverage their mobile devices to conduct business and maintain compliance with relevant regulations. Organizations need security measures that can work with a wide variety of device types (platforms and operating systems) and implement the security and convenience that different applications require.

HID Global applies a long history of identity assurance and authentication experience to the ever-changing mobility market to deliver solutions that enable organizations to effectively secure mobile access to enterprise resources, networks and cloud applications. With a broad, comprehensive portfolio that includes everything from secure, no-hardware solutions (with soft tokens and fraud detection) to LoA4 secure element solutions, organizations can achieve the level of identity assurance they require from a single trusted vendor. Organizations have the ability to apply the security they need for their mobile access, in a way that reduces their risks and costs, while offering convenience for their users. With HID Global, organizations can regain control over their environments and support mobile access in a convenient, secure manner to be able to seize opportunities and drive productivity.

hidglobal.com

2014-03-28-MobileAuthentication-wp-en PLT-01685