NEXT GENERATION AUTHENTICATION FOR THE MOBILE READY ENTERPRISE

A Goode Intelligence white paper sponsored by RSA
CONTENTS

The changing face of IT – the twin challenges of mobile and service orientated IT .......... 2
Enterprise IT is changing ........................................................................................................... 2
How does security react to these changes? ............................................................................. 4
Meeting the demand of flexible IT provision ........................................................................ 4
Supporting strong authentication for BYOD .......................................................................... 4
One person, many devices – different authentication mechanisms ....................................... 6
The Password Pain .................................................................................................................. 7
Too many accounts too many passwords! ................................................................................ 7
Too many passwords results in password re-use ................................................................... 7
Poor protection for password files leads to widespread identity theft .................................... 7
Strong passwords are not suited to mobile use ..................................................................... 7
Password Service Management Costs .................................................................................... 8
Can organizations leverage existing authentication solutions across mobile endpoints? ... 8
Solutions .................................................................................................................................... 9
Introduction to mobile-based Multi-Factor Authentication (MFA) ........................................ 9
Key features of next-generation mobile-based MFA; Device trust and the benefit of leveraging other security services ........................................................... 11
Ensure the mobile device can be trusted ................................................................................. 11
Leverage other security services – don’t deploy authentication in isolation ......................... 12
Provide tools to enable developers and integrators to build multi-factor authentication into mobile Apps ...................................................................................................................... 13
Don’t forget your existing IT investment – why throw away solutions that work? .............. 14
Summary .................................................................................................................................. 14
About Goode Intelligence ......................................................................................................... 15
This white paper from mobile security research and consultancy specialist, Goode Intelligence (GI) explores how the changing face of IT is creating the need for flexible mobile-based authentication services that support the demands of accessing IT resources from a multitude of devices; next generation authentication to support agile IT service provision.

THE CHANGING FACE OF IT – THE TWIN CHALLENGES OF MOBILE AND SERVICE ORIENTATED IT

Enterprise IT is changing

Enterprise IT is moving away from centralized internal infrastructure to a more agile service orientated architecture. This change is not revolutionary however, but evolutionary with organizations changing at different rates.

Many organizations are still heavily dependent on an IT infrastructure where desktop computers are connected to enterprise IT resources and managed by a centralized in-house IT department. If an employee needs access to the enterprise IT infrastructure when they are out of the office then, if they can justify the business expense, they may be equipped with a laptop or a company issued smartphone.

In this scenario, security policy usually dictates that information either stored on the laptop/smartphone or transmitted back to the enterprise...
over a public network, is protected by a combination of data encryption and strong, usually two-factor (2FA), authentication.

There are also many organizations that are starting to change by embracing more agile service orientated IT provision. The new breed of IT services are varied and include virtualization, cloud-based services that include Software-as-a-Service (SaaS), Platform-as-a-Service etc. and Bring Your Own Device (BYOD) – part of the Consumerization of IT movement. These services are flexible and very often quick to turn on or off.

It is rare for organizations to migrate completely to these new IT services. More often, there are hybrid models with a combination of on premise and cloud-based services being accessed by a variety of enterprise-owned devices, desktop, laptop computers and smart mobile devices (SMD) and employee-owned devices (BYOD does not just mean bring your own smartphone).

Running simultaneously to this is the move to mobile computing. The smart mobile device (SMD), a term created by Goode Intelligence to include smartphones and tablet computers running mobile platforms, is becoming the primary method of consuming digital information, both for enterprise and consumer. Mobile is dominating email client usage market share with Apple iPhone being the most popular email client with 24 percent market share, Apple iPad with 12 percent and Google Android taking up 11 percent. Mobile accounts for nearly half (47 percent) of email client usage around the world.¹

Email and calendar services were part of the first wave of enterprise services to be deployed to mobile devices. Organizations are now looking to mobilize other services in the next waves of enterprise mobilization and they are turning to a combination of custom in-house development and off-the-shelf SaaS solutions to match their mobile strategy.

Services that are increasingly being delivered to mobile include mobile-optimized intranet access, emergency response, sales force automation and field service applications. In a survey of over 770 enterprise leaders, Appcelerator, a mobile platform provider, discovered that employee-facing mobile Apps are starting to take off.² The survey detailed what back-end data systems are being connected to mobile applications and 44.7 percent were connecting to ‘enterprise content management systems’, 39.1 percent to Microsoft databases, 29.2 percent to Oracle, 29.6 percent to Microsoft SharePoint, 19.8 percent to SAP and 17.9 percent to Salesforce.com.

¹ Email Client Market Share, Litmus Email Analytics, October 2013: http://emailclientmarketshare.com/
How does security react to these changes?

This change has created a number of crucial questions for organizations attempting to benefit from these new agile IT services:

- Do existing security products and services meet the needs for new agile IT services; some of which may not exist within an organization’s direct control?
- Are existing security products and services flexible enough to work on consumer mobile devices that are owned by the employee, and not the employer?
- What characteristics do new security products and services have that can effectively work with new IT services and can they balance security and convenience?
- Does an organization need to start again and dispose of existing security products and services?

This is at a time when security attacks are becoming more prolific, including a substantial increase in network breaches that can lead to identity theft and valuable corporate data being compromised.

MEETING THE DEMAND OF FLEXIBLE IT PROVISION

So how are organizations meeting the demands of flexible IT provision and what are the difficulties they face as they search for more convenient methods to secure and protect access to sensitive information; sometimes on infrastructure that they do not own or control?

Supporting strong authentication for BYOD

Organizations have been struggling to meet the demand of their employees who want to use their personal mobile devices for work purposes for a number of years. The Bring-Your-Own-Device (BYOD) trend has democratized mobile use within the workplace and opened up mobile working to millions of employees often denied the benefits of a corporate device. By 2017, half of employers will require employees to supply their own device for work purposes.³

Despite its benefits, BYOD has caused problems for IT functions. How can the security posture of an organization be maintained when company critical information is being accessed and stored on devices that they have limited control over? And how does an organization push out strong authentication to these employee-owned devices – the current policy will probably dictate that any employee accessing company IT resources from outside of the office must use a Virtual Private Network and must be authenticated by an approved 2FA solution.

Authentication on BYOD devices is problematic and, in many cases, the ability for an organization to extend its authentication policy out to BYOD mobile devices can be hampered by the inability of mobile device management (MDM) solutions to support effective two or multi-factor authentication (2FA/MFA).

Securing access to an MDM mobile app or mobile ‘container’ by using a PIN or password to lock down a device may not be secure or convenient. Potentially, it is a significant risk and one that could allow unauthorised access to sensitive enterprise information. Compromise the PIN and password on a device and an attacker could gain access to information and IT services that are available from the enterprise mobile container app. This could be locally stored information, including emails, or the ability to gain access directly into an enterprise infrastructure.

The PIN/Password can be the weakest link in preventing unauthorised access to sensitive enterprise information. Smartphones and other mobile devices such as tablets, are being stolen daily in the thousands around the world, so protecting valuable enterprise assets with strong authentication is vital.

The problem is heightened by the use of Single Sign On (SSO) to access business apps within the container. It is convenient to only authenticate once at the point of unlocking a secure container. By using a weak, inconvenient, authentication method to secure the container, the risk is that all the business-class apps are at risk of being accessed if the authentication is bypassed.
One person, many devices – different authentication mechanisms

In a survey entitled “How many devices do you carry” carried out by Lifehacker4 during November 2013; out of over 3100 respondents, one-third stated that they carried two devices with them. A further third carried either three (23.9 percent) or four (8.13 percent) devices with them. There were even just over five percent that carried five or more devices at one time – do they have enough pockets?

Smartphones are not the ‘one device to end all devices’ as originally anticipated by commentators. Instead, we use different devices for different purposes. A laptop to create information, a smartphone to consume information on the go (as a music player and to read and respond to emails) and tablets largely for media consumption – where the larger high-resolution screens make watching movies easier.

These devices may also be running a combination of platforms (operating systems). For instance; a laptop running Microsoft Windows, a smartphone running Android and a tablet running Apple’s iOS. Different platforms with different ecosystems and varying levels of security.

This creates a problem in how to manage authentication and access control across all of these devices. A person may start the day by checking their email and calendar from their smartphone on their way to a meeting. During a break at the meeting they then access an enterprise SaaS application on their laptop. Arriving back at home, after checking their social network account on their smartphone on the way home, they relax by viewing a movie on one of their home’s ‘pool’ of tablets whilst watching out for their Twitter feed.

We have the ability to access the same information across a variety of devices and in different contexts. Wouldn’t it be great if our authentication mechanisms could intelligently detect these different devices and contexts, and then apply appropriate authentication that ticks the boxes for security and convenience?

The Password Pain

Too many accounts too many passwords!

We have a password problem. Our digital lives have exploded resulting in multiple digital identities and multiple passwords. We cannot remember them so we either have to write down strong passwords or make them weaker so we can easily remember them.

Too many passwords results in password re-use

In having multiple accounts and multiple passwords there is also a tendency to re-use them on different accounts.

A person may use the same password on their social media account and then re-use it for internet banking. This is a serious security risk as the social network and the bank will have different security requirements and associated controls.

Poor protection for password files leads to widespread identity theft

A social network may make the wrong decisions in protecting their users’ passwords. This could either be a poor choice of hashing algorithms, used to help protect and conceal passwords, or insufficiently protecting them on their servers (vulnerabilities in web server or SQL deployments for instance).

The real risk is – and we are reminded of this on a weekly basis as hack after hack is revealed - that a social network may get hacked resulting in identity theft. This can be caused by inadequate protection of identity/password databases. A hacker will then attempt to try these stolen passwords on other accounts that may be associated with that person. They may get lucky and use a password that is associated with that person’s enterprise account.

Strong passwords are not suited to mobile use

A strong password containing more than 12 characters and including numbers and special characters may prevent unauthorised users from accessing accounts but does it work on mobile?

Anyone that has attempted to use a strong password on a small touch screen will know that the experience is not ideal. Passwords that may be easy to enter on a physical keyboard are difficult to enter into a five inch mobile touch screen – the problem is compounded if we have to switch between alpha, numeric and special character instances of the virtual keyboard. Mistakes are easily made that can leave legitimate authorised users locked out of their accounts, to unlock their accounts people may either reset their passwords automatically or by contacting their organization’s help desk.
Password Service Management Costs

This situation is inconvenient. It costs time, stops people from accessing the service and is a waste of valuable company resources. Although many organizations have implemented automated password reset solutions there are indications that calls to the help desk for password issues are still high. Forrester estimates that an average user calls the help desk to reset a password about 1.7 times a year.\(^5\)

Can organizations leverage existing authentication solutions across mobile endpoints?

They could, but would users accept a poor user experience and the possibility of frequently locked accounts/password resets?

We are in the midst of a transformation in how IT is created and consumed. Mobile devices are becoming the number one endpoint for much of our daily work and personal digital lives. We still use traditional IT services where the endpoint is a desktop/laptop and connect into an enterprise-managed infrastructure but this is changing.

As a result of these changes, how effective are traditional authentication solutions when a mobile device is being used to access company IT resources?

Two of the most popular 2FA solutions are hardware OTP tokens, e.g. RSA's SecurID, and digital certificates; often stored on a smart card.

How do these technologies fare for mobile use?

Hardware OTP tokens can be used as a method of providing 2FA on mobile devices but how convenient is it to reach for your token and enter in the OTP especially when you are out and about – mobile?

Soft tokens have been popular on mobile devices, running as an authentication app, but they are often used as a 2FA solution for non-mobile authentication, e.g. authenticating for laptop-based VPN access or for internet banking. How can it be classified as 2FA when the device that is the second factor is also the device that is accessing the IT service?

Smart cards that leverage securely stored digital certificates are another effective 2FA solution but you need a smart card reader to use them. There have been attempts to emulate smart cards within a mobile device, either software emulation or by replacing the smart card with a mobile-compatible SD card but not all mobile devices (iOS and some Android devices) have a SD slot.

This white paper has explored the challenges that a combination of mobile devices and cloud-based services, has given organizations and the pain that they are currently

\(^5\) Forrester: “Simplify Identity And Access Management Processes To Reduce Costs, Increase Business Efficiency, And Make Users Happy”, published April 2013
Next Generation Authentication for the Mobile Ready Enterprise

Goode Intelligence believes that there are solutions that allow organizations to effectively manage these challenges. Some of these solutions are available today whilst some will be available shortly as authentication providers introduce solutions that meet the needs for today’s IT requirements – balancing and maintaining existing IT infrastructure, with the future demands of agile IT provision.

SOLUTIONS

Introduction to mobile-based Multi-Factor Authentication (MFA)

Mobile-based 2FA is now an established technology with many organizations embracing the technology to enhance and extend their authentication provision.

One of the major drivers for the adoption of mobile 2FA has been the need to enhance the security and usability of large-user authentication services. Lapse security controls and deficiencies in existing, mainly password-based, authentication solutions has resulted in security breaches that has led to large-scale identity theft. Stronger alternatives were needed to restore trust and to prevent online fraud.

Mobile-based 2FA has enabled organisations to quickly scale stronger authentication solutions and to minimise the risk of further identity theft.

Common mobile 2FA technologies include:

- One-time-passwords (OTP) generated on the phone by a mobile App – similar to a hardware token generated OTP
- OTPs generated on an authentication server and then sent to mobile devices using SMS text message
- Smart card emulators running on mobile devices for certificate-based (PKI) authentication solutions (sometimes the certificates are stored in the SIM)

Goode Intelligence believes that we are entering the next phase of mobile-based authentication where the technology becomes a whole lot smarter – smart authentication for smart mobile devices.

Existing 2FA solutions (both mobile and non-mobile) have been effective in proving identity for both enterprise and consumer-facing technology services. They are extremely effective in providing scalable cost-effective authentication for people accessing technology services using desktop computers and laptops. They are not currently as effective for providing convenient authentication for mobile-initiated services – accessing enterprise IT resources or financial services from a mobile device.
Next Generation Authentication for the Mobile Ready Enterprise

What is desperately required are authentication mechanisms designed to work seamlessly for mobile services; services that provide convenient and secure authentication for applications accessed on all mobile devices.

Fortunately, these services are becoming available and what sets them apart from other solutions is how they are putting the mobile device, its in-built features, and the user at the heart of their design.

They are also leveraging an increasing range of in-built technology and sensors that are available in most smart mobile devices. Technology vendors are researching innovative ways in which the in-built technology can be used for identity verification purposes. These include:

- **Location** – Most smart mobile devices will have embedded GPS sensors that will usually work in combination with the cellular (radio) services to create an accurate picture of the location of the device. Location-based services are used in MFA solutions

- **Microphone** – every phone has one and can be used in MFA solutions that use the voice for identification/recognition

- **Camera** – another ubiquitous piece of mobile device hardware that is being used for facial and eye recognition biometric services

- **Touch-screen** – by analysing the touch and swipe input into a touch-screen enabled smart mobile device, behavioural analysis can correctly identify if the correct person is using the device

- **Embedded biometrics** – Apple’s iPhone 5S was launched with an embedded touch fingerprint sensor, **Touch ID**. Goode Intelligence believes that other mobile OEMs will follow-suit and integrate a range of biometric sensors within their mobile devices and that by 2018 they will become a common feature for most devices.

- **Short-range radio** – Either Bluetooth, found in nearly all mobile devices and Near Field Communications (NFC), found in an ever-increasing amount of mobile devices, excluding Apple iOS device. Enables mobile devices to interface with either a wearable/carry-able device or smart card to act as the second factor. There is a high level of innovation in the wearable technology market with a number of form factors that include glasses, bands, watches and rings

On their own these features can be effective in establishing identity; when combined they become even more powerful. By making use of a combination of sensors within the mobile device and linking these to context and environment, an extremely powerful method for establishing identity is created; **Mobile-based Multi-factor Authentication (MFA)**.

---

Additionally, solutions that can automatically adjust to users’ environments by using the embedded technology, readily available on smart mobile devices, will naturally be adapted by more people.

Professor Steven Furnell, Head of School, School of Computing and Mathematics, Plymouth University, United Kingdom, and his team have coined the phrase “Authentication Aura” to describe this adaptive approach to user identification and authentication on mobile devices.7

By moving away from a single technology that acts as the second factor to multiple factors, and by linking the factor to context and appropriateness, stronger, more adaptive, authentication solutions can be built.

Mobile-based MFA has the ability to provide convenient agile authentication for flexible, anywhere, anytime secure access.

**Key features of next-generation mobile-based MFA; Device trust and the benefit of leveraging other security services**

Security should never be designed and deployed in isolation. If authentication services on mobile devices are to be trusted, we must ensure that the platform is secure and that they leverage other associated security services as far as possible. By doing so, we ensure that strong mobile-based authentication services can be trusted to secure access to important digital services.

**Ensure the mobile device can be trusted**

It is vital that mobile-based services can be trusted (including mobile Apps and the cloud-services that they interface into). This is especially so when they are being used for high-risk purposes; accessing an enterprise IT resource or application, paying for goods and services and for interfacing into a government or healthcare service.

There is no point delivering strong authentication services to devices that are insecure and within apps that have weak security protection.

Trust can be built into mobile-based services through a combination of factors that include:

- Constant improvements to the security of the mobile platform (OS) and patching vulnerabilities as soon as possible
- Leveraging available hardware-based security environments built into the mobile device. This includes such technologies as **ARM’s TrustZone** (linked to a Trusted Execution Environment (TEE) where processing can be protected from unauthorised interference)
- Constant threat monitoring and assessment that can provide early warning of vulnerabilities in the mobile and cloud ecosystem

---

Ensuring that mobile Apps are developed securely and in accordance to security policy. This includes security testing the mobile App and how it interfaces with both enterprise back-ends and cloud services.

**Leverage other security services – don’t deploy authentication in isolation**

There is an opportunity to take a more holistic approach to authentication through tighter integration with other connected security services.

Advanced security threats necessitate a change in the way we approach authentication and access control. The rise of mobile-based authentication has reduced the cost of entry for new technology vendors delivering largely one-time-password (OTP) 2FA services to the mobile device.

There are plenty of simple mobile-based 2FA solutions that allow an OTP to be generated (either on the device itself or by an authentication network service, with delivery to the mobile device through SMS) and then used as part of an authentication session. These services have become ubiquitous and are offered by all the major global information services including Google and Twitter. They can be effective in raising the security bar and can improve the security posture for services wanting to strengthen their authentication solution.

There is a risk in this approach; by relying on one technology for the second factor, usually a one-time-password, and by isolating authentication from other security services, there is a risk that these authentication solutions will not be adequate in proving identity.

Two important questions must be asked; are existing authentication services good enough to prove identity and are they robust enough to deter the latest advanced threats?

There is a way forward; design and deploy agile authentication services that leverage other security services to ensure the service is trusted and robust.

Other security services that are complimentary to the next generation of authentication services include:

- **Risk-Based Authentication (RBA)** – a solution that transparently assigns a risk level to each authentication request. Contextual analysis evaluates each attempted login and activity in real time. There can be hundreds of risk indicators that determine the risk associated with each access request. Risk indicators include date and time for request, geographic location of person requesting authentication request and what action the person is requesting to perform. The mobile device can be utilised to create unique risk indicators that can be fed into the risk engine.

- **Single-Sign On (SSO)** – a solution that allows a person to access multiple IT services (all with their own unique authentication requests) by using a single login (sign-on). The person signs in once and gains access to all authorised systems without having to sign-in for each individual system. SSO is associated with other enabling technologies such as Security Assertion Markup Language (SAML) and
Identity Federation These SSO solutions could integrate with MFA solutions to provide policy driven authentication.

- **Malware protection** – can ensure that both the endpoint (mobile device) and connected enterprise services are protected against malware. Mobile malware is rising and there have been targeted attacks on mobile-based authentication solutions, especially those that use SMS messaging.

- **Identity and Access Management (IAM)** – these solutions define what a person is allowed to do and access after the authentication process. Intelligent IAM solutions incorporate business context.

- **Threat intelligence** – allows an organization to leverage the collective intelligence and analytical skills of the global security community. It ensures that an organization has access to the most current intelligence into attack vectors. As new threats emerge on a daily basis an organization must have visibility from a network of trusted partners.

- **Policy (risk) management** – often called Governance, Risk and Compliance (GRC) is a term applied to how an organization manages security risk. Tools are available that enable organizations to manage and demonstrate their security risks. This is imperative in those organizations that are regulated.

- **Mobile Device Management (MDM)** – a term that refers to solutions that manage mobile devices. MDM enables organizations to manage both company-owned and employee-owned (BYOD) mobile devices. MDM allows organizations to enrol, configure, update and secure mobile devices using Over-The-Air (OTA) transmission.

- **Mobile Application Management (MAM)** – allows an organization to acquire, distribute, secure and track mobile applications. MAM provides a method for mobile App lifecycle management. Authentication services can be linked to MAM by allowing all mobile Apps within an enterprise to share a single authentication session. MAM can be associated with an Enterprise App Store (EAS).

**Provide tools to enable developers and integrators to build multi-factor authentication into mobile Apps**

By giving the necessary support to developers and integrators MFA can be added to mobile Apps to ensure that strong mobile-centric authentication becomes an integrated component.

Goode Intelligence recommends that development and integration tools are easily accessible and available for all popular mobile platforms. Supporting a cloud-based model for development support simplifies application MFA enablement and reduces the cost and complexity.

App developers and integrators should not deliver single-platform solutions as this will limit its use and adoption. It is important that developers and integrators choose solutions that work with multiple mobile operating systems and are not tied to a single vendor or hardware manufacturer. MFA SDKs and APIs must be available for all popular mobile operating systems to ensure that as many mobile devices are supported.
Don’t forget your existing IT investment – why throw away solutions that work?

Organizations have invested millions of dollars and significant time in their IT and security infrastructure and do not want to have to throw this investment away.

IT architects and managers design and deploy technology solutions that are scalable, cost effective, meet the needs of the business and are as future proof as possible.

New and emerging technology trends test those resources that are responsible for IT service provision. They are being particularly tested at the moment with the proliferation of mobile devices combined with service orientated IT provision; increased virtualization and cloud-based services.

This white paper has explored how next generation authentication services can embrace these technology trends to create solutions that are agile, convenient and intelligent.

Goode Intelligence believes that next generation authentication services can be integrated into existing core IT infrastructure; infrastructure that is proven.

Organizations have invested time, resource and money in deploying core IT and security infrastructure such as Microsoft’s Active Directory (AD) and on-premise authentication solutions such as RSA’s SecurID and Authentication Manager.

Next-generation mobile based authentication services can be leveraged to work seamlessly with existing IT infrastructure; realising the benefits of new user-centric authentication and identity management solutions in combination with core IT infrastructure that is proven.

SUMMARY

This white paper explored how a combination of factors, including the move to mobile and the introduction of service orientated IT provision, is demanding for the next generation of authentication services.

Authentication services that can leverage the in-built capabilities of the smart mobile device and can work to prove the identity of people to a variety of IT services, some managed by an organization and some outside the perimeter of their control.

Goode Intelligence believes that the industry has an opportunity to design next generation authentication services that are not isolated from other connected security services. **Flexible smart identity to meet the demands of smart agile IT.**
Next Generation Authentication for the Mobile Ready Enterprise

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consultancy services in mobile security, identity and biometrics.

For more information on this or any other research please visit www.goodeintelligence.com.

This document is the copyright of Goode Intelligence and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Goode Intelligence.