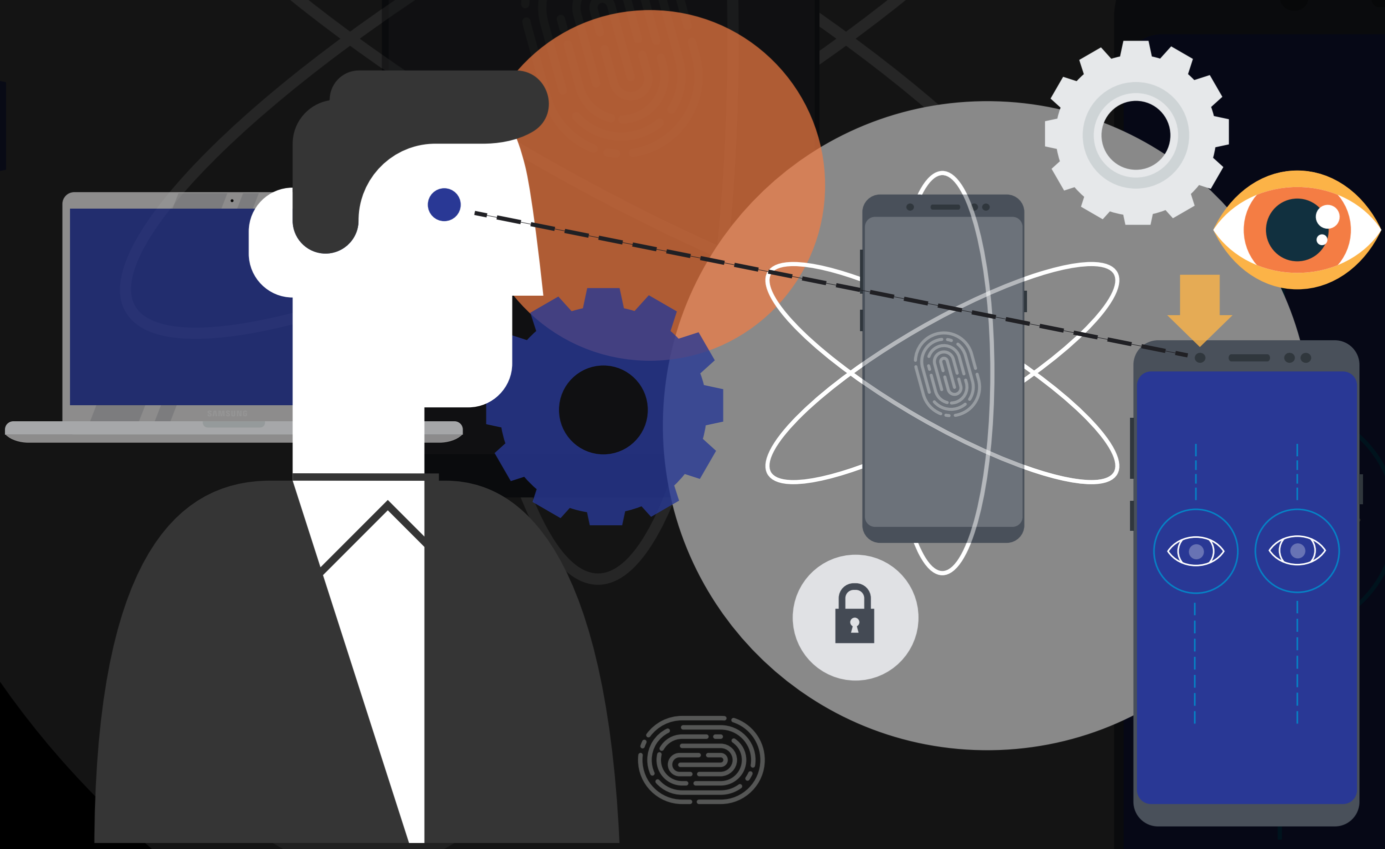
SAMSUNG

White Paper:

The Mobile Passport:

How Biometric Authentication Can Secure Your Business, Employees and Customers From Security Threats



Smartphones today are among the most powerful computing tools we use on a daily basis. The effective use of these devices in business can not only increase productivity and efficiency, they can also allow for more flexible work practices and free up employees to work remotely.

All of this means that the smartphone is quickly becoming not only our most used device but also our most important one, holding employees' most vital personal and professional data and giving them the ability to access critical business systems. It's clear why security has become one of the most important aspects to consider when purchasing new mobile devices for employees.

As devices that are frequently used outside of the office or place of business, smartphones are inherently more vulnerable to the threat of unauthorized access than traditional desktop or laptop computers. While common authentication methods such as passwords, pins and patterns provide some protection in the case of lost or stolen smartphones, they do not offer sufficient levels of assurance for regulated enterprises who increasingly allow employees full access to corporate information systems from their smartphones.

Fortunately, as smartphones have evolved, so too has the technology securing them. Today, the pinnacle of that technology is biometrics, which takes advantage of highly unique personal characteristics such as your iris pattern or fingerprint to secure the device.

> This white paper will address current challenges and vulnerabilities surrounding mobile device authentication and security, how Samsung's implementation of biometric authentication can address these issues, and how enterprises can leverage powerful services like Samsung Pass to take advantage of cutting-edge biometric technology. It will also explore how the role of biometric technology may extend beyond authentication in the future, presenting diverse new applications for enterprises requiring a reliable method for verifying the identity of employees and customers.

The Password Problem

The current system of utilizing passwords or pin numbers to secure our IT infrastructure – and indeed our digital lives – is inherently ineffective.

A recent survey of highly mobile workers, conducted by GfK Public Communications & Social Science on behalf of Samsung, revealed the extent of today's password problem:*

Poor Password Practices

32% tend to use variations of a single password for all accounts

28% have five or fewer passwords that they use interchangeably

only **26%** use unique passwords for each account

End User Frustrations

65% rate having different log-in credentials for each account as a frustration

66% find themselves needing to reset passwords a few times a year, if not on a monthly basis

In their personal lives, employees are already struggling to manage dozens of passwords for everything from personal email and social media, to banking, utilities and frequent fliers accounts. For IT and corporate security departments, requiring employees to remember unique passwords for each business system and application is not an effective long-term security strategy.

Beyond these management and memory challenges, hacked passwords and pins can also have a cascading effect due to the poor user practices highlighted above.

"It is clear passwords are the weakest link and more needs to be done by businesses to enable other forms of authentication to prevent cyber breaches," wrote Martijn Verbree, a partner in KPMG's cybersecurity practice, in a report on recent email account hacks.[1] "Though these hacks have wider implications than just what can happen to linked accounts. When an email account is breached, it opens up access to other non-linked accounts that often use emails to validate password reset requests."

*This Enterprise Mobility Trends Survey was conducted by GfK Public Communications & Social Science using a blend of online sample sources, including GfK KnowledgePanel. From April 6-25, 2017, a sample of 1,205 "mobile workers" across the US was interviewed. In order to qualify for this study, respondents were required to be working either full- or part-time at companies with at least 100 employees, own a smartphone, and spend at least one-third of their working day "on the go." Respondents were interviewed from six key industry groups.

Biometric Authentication Emerges to Address Unique Mobile Threats

Mobile devices by their very nature are more vulnerable to unauthorized access than computer systems that remain fixed within the place of business. And none more so than smartphones, which are frequently used for both personal and business purposes, and carried by employees virtually everywhere they go.

According to the GfK survey, as many as 23 percent of highly mobile workers have had a smartphone lost or stolen.

The mobile industry has responded to this through the development of advanced mobile device management (MDM) and security solutions. MDMs have allowed IT to enforce password requirements on enrolled employee devices and to wipe data and apps from lost or stolen devices. Data separation solutions allow IT to create work containers on the employee device, requiring additional layers of authentication to access even after the device is unlocked.

However, mobile devices are still only as secure as their authentication protocols. "A password and pin can easily be shared, whereas a biometric cannot. You can share your password with someone halfway around the world, but how are you going to share your fingerprint or your voice?" George Avetisov, CEO of biometric software company HYPR Corp, says.

Fingerprint scanners have been available on some smartphones since as early 2011, and on most flagship devices since 2015. Fingerprint scanning is quick and convenient for end-users, and false-acceptance rates are low in the latest implementations. However, reports of would-be hackers using synthetic replicas of fingerprints to dupe scanners have raised concerns about using fingerprints alone to protect highly confidential corporate or government information.

In 63 percent of confirmed data breaches, the attackers leveraged weak, default or stolen passwords.[2]

To further combat these issues, Samsung has introduced iris scanning on the Galaxy S8 smartphone. For consumers who purchase a Galaxy S8 device and S8+ smartphones, iris or fingerprint scanning can be used to replace their passwords and pins when unlocking the device, accessing the Secure Folder, or making payments using Samsung Pay.

However, beyond these device-level features, a much larger opportunity exists for enterprises to leverage biometric authentication with the Samsung Pass platform to secure their data, their employees and their customers.

How Does Biometric Authentication Work?

Biometrics refers to a broad range of ways that users can verify their identity using unique personal characteristics. They include the likes of facial recognition and fingerprint scanning — which have become widely used thanks to their implementation on smartphones in recent years — to more advanced systems like iris scanning, hand geometry and vein structure, as well as voice, signature and keystroke recognition. You can even be identified by the way you walk or the shape of your ears.

Biometric authentication systems work by first capturing the necessary data and enrolling the user in a database. From there, the systems can be used for verification, where a person's name and identity is checked against their profile in the database; or identification, where the person's biometric data is scanned and checked against everything stored in the database to answer the question, "Who is this person?"

The benefits of using biometric authentication can be distilled down to the idea that traditional systems rely on something you **know** or **have**, such as a password or swipe card, whereas biometrics works off something you **are** in addition to something you **have** — your phone.

Iris Recognition: The Next Step in Biometric Security

Your iris is the thin, colored ring of the eye, which is used to regulate the amount of light that reaches the retina by opening and closing the pupil, in a similar way to how a camera shutter works. It has an extremely data-rich physical structure and contains a pattern that's unique to each individual and virtually impossible to replicate. While fingerprints may degrade over time as a result of manual labor, your iris pattern does not. Additionally, because eyes are self-cleaning and image capture is performed without physical contact with the reader, readings are more accurate and reliable.

While fingerprint scanning does offer a high level of security, iris scanning takes things one step further, offering a lower false acceptance rate than fingerprint scanning. A report by the Center for Global Development last year highlighted the benefits of iris capture over fingerprints in terms of "its recognized accuracy, reliability and security."[3] Similarly, a United Nations report on using iris scanning in the field found that iris capture beat fingerprint capture in terms of ease of use, speed and overall preference.[4]

Securing Biometric Data on the Device

The Samsung Galaxy S8 and Galaxy S8+ have dedicated infrared cameras just for capturing an image of your iris. The camera is directly connected to a secure area within the smartphone called TrustZone, which is isolated from other parts of the system and is secured by Samsung's defense-grade security platform, Knox. This ensures that from the second the data is captured, it never leaves this secure environment.

The dedicated camera utilizes a special image filter to receive and recognize the reflected images of the irises with a red infrared LED light, which provides the best range for iris scanning. Unlike RGB images, which can be affected by iris color or ambient light, infrared images display clear patterns and have low light reflection. Once captured, the biometrics are not kept in the raw form; instead, they're digitized and hashed, a process whereby an algorithm converts the relatively large biometric data into a much smaller string of characters.

By utilizing this system, even if the hash value gets stolen or leaked, an attacker can never come back to the original iris image, rendering it virtually useless for any would-be hackers. After the iris image is digitized and hashed, that data is kept in the TrustZone, and only secure applications within Samsung Pass have access to this item. The raw biometric data is never kept on the phone.

> **While fingerprint scanning does offer a high level of security, iris scanning takes things one step further, offering a lower false acceptance rate than fingerprint scanning.**

Samsung Pass – A New Way to Use Biometrics

Samsung Pass leverages the advances in biometrics to offer enterprises a convenient way to authenticate users, as well as offer greater protection for critical data and systems.

Utilizing the Samsung Pass platform, enterprises can integrate biometric authentication into their apps and services, offering a frictionless experience for their customers and employees.

Samsung Pass also incorporates cloud-based information that both an enterprise app and an enterprise server can check, allowing them to independently verify the integrity of the authentication information. The Samsung Pass solution uses a clever exchange of certificates, an opaque identifier, an authentication token and Fast Identification Online (FIDO) compliance in order to authenticate a user's identity without compromising privacy or gaining access to enterprise data.

> Utilizing the Samsung Pass platform, enterprises can integrate biometric authentication into their apps and services, offering a frictionless experience for their customers and employees.

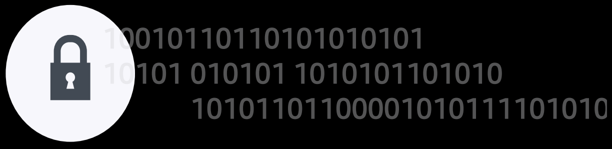
Creating a More Secure System With Samsung Pass

So what happens behind the scenes when a user accesses a Samsung Pass-enabled account using their biometrics?

Here are the key steps for Samsung Pass to securely associate the device user with their specific device:

- The Samsung Pass Authentication Framework asks Knox to create an asymmetric signing key in the Knox TrustZone.
- The Knox TrustZone uses the private portion of the key to generate a certificate chain.
- The certificate chain includes the asymmetric signing key and the public portion of the device root key, which is unique to each device and is set at the point of manufacture.
- Finally, Knox passes the certification chain to the Samsung Pass Authentication Framework which uploads it to the Samsung Pass Cloud.
- Once this is complete, the Samsung Pass Cloud checks that the certificate chain is rooted by a legitimate Samsung Root Key, and if this passes, the Samsung Pass Cloud considers the device secure and authentic.

Sending any data from your smartphone to the cloud carries risks, but Samsung mitigates those risks by utilizing the FIDO protocol. This is a standard protocol for converting biometric authentication information on a device to user authentication information on a server without compromising the user's privacy.



Five Security Risks Facing Enterprises:

1. Focus on mobile

Hackers are increasingly focusing on smartphones as enterprises and end-users rely more and more on the portable devices for everything from accessing sensitive work data to online banking.

2. Cracking the cloud

As more and more of our services rely on cloud computing to offer access from anywhere, criminals are now building malware specifically to crack corporate cloud-based systems.

3. Ransomware

One of the biggest trends in cybersecurity today, ransomware can be devastating for a company, as it gives criminals leverage over compromised employees, meaning not only financial loss but potentially the loss of valuable data.

4. IoT

With everything from the kettle in your canteen to the thermostats in your offices now connected to the internet, hackers have a much greater range of attack options, and as they are typically lacking in security, hackers can use these devices as entry points to your network.

5. The human factor

Despite everything we know, the weakest link in the security chain today remains people. Sophisticated social engineering techniques make it ever harder to spot hackers attempts to get you to reveal your passwords.

Who Should Be Using Samsung Pass?

Samsung Pass offers the bleeding edge of security for enterprises who are seeking to secure their most valuable data. Government agencies, financial companies and healthcare providers are among the likely early adopters of this technology, but any business requiring employees to access highly sensitive data on their mobile devices should consider its benefits.

Today Samsung Pass offers a huge opportunity for B2C companies to offer their customers greater security and convenience when they engage with their online service or app. By integrating Samsung Pass, companies in areas such as e-commerce and banking can reassure their customers that they have adopted the latest technology in order to secure their transactions.

But Samsung Pass can be used by many different types of companies. An airline could leverage biometrics and Samsung Pass to allow frequent flyers to easily sign in when they open the app to check in for a flight safely and securely. Indeed, any company that wants to streamline the customer experience and offer a safe and secure way to log into their service can easily leverage the power of biometric authentication provided by Samsung Pass today.

The Future of Biometrics

As a technology on consumer devices, biometrics is very much in its nascent form, with Samsung's implementation of Samsung Pass and the Galaxy S8's iris scanner driving recognition as well as the adoption of this technology. As more and more enterprises look to secure their data with the latest technology, we'll begin to see more areas where this super-secure authentication and identification system can be implemented.

Here are just a few of the areas in which companies are already looking to exploit biometric solutions to offer enhanced features as well as easier-to-use systems:

- **Digital signing:** Signing documents for legal purposes typically means doing it the old-fashioned way, using a paper and pen and requiring someone else to verify your identity. With a biometric-based solution, we could see legal documents signed remotely on your smartphone using iris scanning as a way to verify your identity.

- **Secure e-commerce transactions:** Last year, smartphones drove more traffic to e-commerce sites than desktop PCs, and studies expect phones will reach 60 percent of traffic by end of 2017.[5] Therefore, making sure mobile transactions are verified will become increasingly important, and biometrics offers a perfect solution to this problem.

- **Tackling fraud online:** Because online interactions are by their very nature remote, verifying who is doing what can be difficult. For example, tax fraud is a huge problem for the IRS, but implementing a system that utilizes biometrics to authenticate who is filing the return would cut out a major portion of the problem.

Evolving to Mobile Passports and Beyond

Samsung Pass works by verifying that the person who owns the device and set up the account is the same person who is trying to gain access. While leveraging this technology as a form of personal identification is still a few years away, this is an area that offers huge possibilities. Here are just some of the areas where using biometric security solutions could transform our lives in the coming years.

- **Mobile passport:** We can already use our smartphone as our boarding pass when traveling, so why not also use it as our passport or driver's license?
- **Online voting:** Smartphone users could soon log into an election app and vote online using biometrics to confirm their identity.
- **Bank accounts:** The pain of having to physically travel to the bank in order to open up a new account before presenting government-issued identification could all be alleviated by using a biometric identification system online.
- **Pharmacies:** Buying the medicine you need online is a difficult proposition today because you are required to verify your identity, which is another pain point biometrics could solve.

Five Benefits of Biometrics:

1. Security

Because of the inherently personal nature of biometric information, combined with the difficulty in replicating the data, these systems are simply more secure than traditional password/username systems.

2. Efficiency

Because scanning your iris or reading your fingerprint takes a fraction of a second, biometric security systems are much less time-consuming than having to input a username and password.

3. Accountability

Because you cannot give your biometric data to someone else, it allows businesses to know that the person who should be doing a particular task is the person doing it.

4. Frictionless

As well as saving time, using biometric authentication is much easier on the end-user who no longer has to remember a password or a swipe card to gain access to a building or an app.

5. Accessible

With biometric sensors increasingly incorporated into smartphones and tablets, enterprises can leverage this technology, together with solutions like Samsung Pass to easily and quickly implement biometrics into their workflow.

Biometrics and Education Are Key to Optimal Security

It's clear that the system of usernames and passwords that we use dozens of times every day to log into accounts, apps and services is broken. Humans are not wired to remember complex combinations of numbers and letters, and certainly not many different such passwords. The result is that people default to a single password that they can re-use over and over for different accounts. This leads to the situation where, if your password for one account is compromised, hackers have access to all your information. While this can be quite the hassle for an individual, for enterprises who are trying to protect valuable data, it can be catastrophic.

The way we currently manage mobile security needs to change, and biometrics can provide the answer. Changing the password dynamic from "something you know" to "something you are" not only makes it easier on the end user but also offers much greater security and prevents hackers from accessing personal accounts. Biometric data is incredibly hard for hackers to replicate, and because iris patterns don't degrade with age, the system is inherently more reliable. As well as being more secure, biometric systems free users from having to remember dozens of long, complex passwords. Samsung's additional features offer even more layers of security, as developers can use Samsung Pass to leverage the power of biometrics in their own apps, and Samsung's biometric security system is backed up by the company's defense-grade security platform Knox.

As well as the major security benefits of using biometric systems, which have been outlined above, these systems are also much easier to use, given that users no longer need to remember long and complex passwords and usernames.

Venki Vajja, a lead enterprise product manager for Samsung Pass, says that the ease and convenience of biometrics can give enterprise decision makers the impression that it is not highly secure. "Even though authentication via iris scanning is fast, it is secure too. That is the beauty of the technology, but more education needs to happen so that businesses understand it really is much safer for them and their customers," Vajja says.

With biometric scanning and the public key cryptography-based protocol of Samsung Pass, Samsung is helping to drive adoption of biometric authentication technology for the enterprise. As developers and enterprises begin to explore their power and the added security benefits they bring, people will quickly realize that biometrics offers a solution to today's broken system of passwords and PINs.

For more mobile solutions that combine productivity with security, click here:
http://www.samsung.com/us/business/discover/enterprise-mobility/

Learn more: samsung.com/business | insights.samsung.com | 1-866-SAM4BIZ
Follow us: youtube.com/samsungbizusa | @samsungsecure

SAMSUNG

End Notes

1. Passwords Continue to Remain the Weakest Link. KPMG. December 15, 2016. https://home.kpmg.com/uk/en/home/media/press-releases/2016/12/passwords-continue-to-remain-the-weakest-link.html.

2. 2016 Data Breach Investigations Report. Verizon Enterprise. 2016. http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf.

3. Iris Recognition: Better Than Fingerprints and Falling in Price, Alan Gelb, Anit Mukherjee and Anna Diofasi. Center for Global Development. August 1, 2016. https://www.cgdev.org/blog/iris-recognition-better-fingerprints-and-falling-price.

4. Biometrics in a Humanitarian Context, Andrew Hopkins and Justin Hughes. The UN Refugee Agency. 2014. http://www.connectidexpo.com/creo_files/expo2014-slides/1700_Hopkins_Hughs.pdf.

5. Smartphones Overtake Computers as Top E-Commerce Traffic Source, Declan Harty. Bloomberg Technology. July 25, 2016. https://www.bloomberg.com/news/articles/2016-07-25/smartphones-overtake-computers-as-top-e-commerce-traffic-source.