

# Biometric Authentication: The Future Is Now

**Challenges with password management lead financial firms to adopt biometric authentication solutions.**

It's a continuous balancing act: having simple and user-friendly authentication without increasing vulnerability. Historically, security has gone hand in hand with added complexity, which in turn leads to greater management overhead, increased costs, and dissatisfied end users. Fortunately, the growing availability of open standards-based biometric authentication capabilities embedded in mobile devices helps ease the conflict as customers and employees, particularly millennials, eagerly embrace a mobile-centric lifestyle.

In fact, a recent IDG Research Services survey of executives in the financial services and insurance industries finds that some firms are already adopting biometrics, and many are looking to make the transformation in relatively short order. This shift is not surprising, as users today are increasingly accustomed to using their phones to navigate highways, pay for everyday items using digital wallets like Samsung Pay, perform a variety of banking functions, and even withdraw cash from ATMs.<sup>i</sup>

## Biometrics breakout

Secure authentication has to keep pace with innovation and the needs of end users. Any organization that is unable to meet the mobile demands of its employees and customers risks losing them to more tech-savvy competitors.

Password management is a never-ending struggle for enterprises, and ever-more problematic, as companies race to provide mobile access to online accounts and services. Call centers are overburdened with requests for password resets, and IT security teams are constantly in fear that users will resort to oversimplified passwords that fail to protect them.

While implementing biometrics in the enterprise has been characterized as a future vision, most of the executives surveyed by IDG Research Services believe biometric-enhanced security is practical now, or will be in the near term. Fifty companies with a median workforce of 25,000 are represented

in the survey, with two-thirds serving at the level of director or above.

As The New York Times reported recently, "Some of the nation's largest banks are acknowledging that traditional passwords are either too cumbersome or no longer secure, therefore they are increasingly using fingerprints, facial scans, and other types of biometrics to safeguard accounts."<sup>ii</sup>

## Parting ways with tradition

The IDG survey provides compelling evidence that biometric adoption is underway, at least with the movers and shakers in the financial services industry. It also points out persistent, and perhaps unwarranted, confidence in existing security infrastructures.

Currently, server authentication is the most common method of corporate security, being used at 28% of companies included in the survey. Another 20% say they use one-time password tokens, 16% employ smart cards, and 14% rely on digital certificates. While survey respondents indicate they have a high degree of confidence in their current authentication technology, they continue to explore alternative technologies such as biometrics to improve the user experience while maintaining or increasing security.

"There is a tendency to think, 'If it isn't broken, don't fix it,'" says Shankar Saibabu, director of solutions architecture with Samsung SDS America, the U.S. subsidiary of Samsung SDS, a global IT solutions company. Even if IT and security teams are not motivated, they are being driven by marketing organizations and innovation teams that are urgently focused on making it seamless and more simple for customers to get connected in a secure fashion.

Traditional password authentication approaches have proven to be a persistent security risk. According to Verizon's annual Data Breach Incident Report, 63% of confirmed data breaches involve the use of weak, default, or stolen passwords.<sup>iii</sup> The reality is that passwords are too easy to



SPONSORED BY:




**SAMSUNG SDS AMERICA**

<sup>i</sup> "Samsung Pay rolls out ATM cash withdrawal capability," Mobile Payments Today, May 2, 2016.

<sup>ii</sup> Michael Corkery, "Goodbye, Password. Banks Opt to Scan Fingers and Faces Instead," The New York Times, June 21, 2016.

<sup>iii</sup> Kelly Jackson Higgins, "Verizon DBIR: Over Half Of Data Breaches Exploited Legitimate Passwords In 2015," Information Week Dark Reading, February 26, 2016.

## Perceptions of Biometric Authentication Use Cases

	Impossible	Sounds possible	Sounds interesting but doubt it will work for us	We could benefit from it if it were available	We are working on something similar	Already doing this	
<b>Mobile banking/payments:</b> Allowing retail banking customers to access and manage account information and make payments using biometric authentication such as fingerprint, voice or facial scan	6%	12%	16%	38%	16%	12%	Senior leaders are more likely to see this as something their company could benefit from 
<b>ATM Banking:</b> Banking customers can access all account information via biometric authentication eliminating the need for banking cards and reducing vulnerability to fraud.	4%	14%	20%	48%	8%	6%	
<b>Company Systems Access:</b> Employees can access emails, mobile apps, web apps and confidential documents via biometric authentication, eliminating the risk of a data breach by limiting access to internal documents.	2%	14%	16%	46%	18%	4%	

SOURCE: IDG Research Services, March 2016

circumvent or compromise, too costly, or too hard to manage; few companies, for example, want to provide customers with smart cards and one-time password (OTP) tokens.

### Biometrics capabilities readily at hand

Biometric authentication is becoming the premier option for enterprises to replace the complexity of tokens, passwords, and PINs. The reason: smartphones. According to comScore, as of January 2016, 198.5 million people in the U.S. owned smartphones, representing 79.1% of the mobile market.

Enterprises can rely on those devices to provide convenient, reliable, and secure access to corporate data using verifiable biometric data, such as a voice scan, iris recognition, facial recognition, or fingerprint scan. According to Acuity Market Intelligence, more than 200 biometric-equipped smartphones have been introduced since the first quarter of 2013.<sup>iv</sup>

About half of the participants in the IDG survey say they view biometric authentication as a viable option within the next 12 months for a range of applications; a significant portion indicate that one to two years is a realistic time frame. Currently, a minority say they are already using biometrics in some areas and others are working on implementation.

Respondents are most enthusiastic about biometric authentication for mobile banking and payments, which 24% say is an immediate reality and a total of 74% say is viable in two years or less. Given the speed with which survey respondents

see the onset of biometrics in security, businesses can't afford to be left behind. "The primary factor driving adoption is competition," says Saibabu. "If one bank gets on board, the others want to get on the bandwagon; they don't want to get left behind." Saibabu says Samsung has demonstrated scalability of its biometric solutions and compliance with security requirements, both of which are key for enterprise adoption.

### Bottom line

Financial institutions can't sit back and watch biometric use cases unfold. A number of banks have already implemented biometrics using embedded mobile device finger scans, and others are working on capabilities such as facial, voice, and iris recognition to bypass dependence on password security.<sup>v</sup> There's little doubt the competition is already testing the waters, if not in full-scale production. Customers, especially millennials, are eager for secure authentication that supports their mobile work and lifestyles.

### About Samsung SDS

As a leading provider of mobility and IoT solutions, Samsung SDS' vision is to deliver software and services that provide seamless biometric authentication with the highest levels of security to enable superior customer experiences. For more information, visit [www.samsungsdsa.com](http://www.samsungsdsa.com) or email [bd.sdsa@samsung.com](mailto:bd.sdsa@samsung.com).

<sup>iv</sup> "Biometric Smartphones Are Officially 'Mainstream.' More Than 200 Models Have Been Introduced Since 2013," Acuity Market Research. February 11, 2016.

<sup>v</sup> "More Banks Turn to Biometrics to Keep an Eye on Security," Nasdaq.com, NerdWallet. May 23, 2016.