WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

Passwordless Authentication

The next breakthrough in secure digital transformation

In collaboration with the FIDO Alliance

January 2020

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Preface

Andrew Shikiar
Executive Director and
Chief Marketing Officer
FIDO Alliance
USA

Seven of the ten most valuable companies in the world are platform businesses.[1] Across industries, global companies have proven that digital platforms help us all participate in the connected economy, surfacing business opportunities and, ultimately, competitive advantages. It is no surprise that chief executive officers (CEOs) are either building or buying platforms to achieve their digital transformation objectives.

Authentication is the cornerstone of secure digital transformation for platform businesses, and beyond that, a pillar of the Fourth Industrial Revolution: from internet of things (IoT) devices that need authentication for machine-to-machine communication, to artificial intelligence (AI) that will be used both to secure and bypass authentication systems, and even blockchain, for which trustworthy authentication is the key to mass adoption.

However, one critical issue stands in the way of continued progress – the continued use of passwords as the principal means of authentication. The reliance on and use of passwords disrupt the customer experience, which is becoming one of the most important brand differentiators. Moreover, and paradoxically, passwords are actually very difficult to secure: on one hand, users keep on re-using them, on the other, companies struggle to process and store them securely. The vast majority of data breaches stem from weak or stolen authentication credentials. Today, credential stuffing attacks, i.e. attacks leveraging stolen credentials, are so common that over 90% of all login attempts on major retail sites are malicious, with average success rates around 1%.[2] For high-value targets, even manual fraud attacks using stolen credentials are on the rise. Passwords are not providing sufficient protection. And perhaps most importantly, passwords cost companies millions every year, not just in data breach mitigation but also in password management costs.

To enable the platform economy and, in parallel, to address increasing costs of password management, security and fraud risks, there is a need to incentivize new authentication methods that eliminate our reliance on password-only technology. But what will it take to do so? What are the risks, trade-offs, costs and challenges that await in the transition and beyond?

This white paper makes the case for passwordless authentication, for four main reasons. First, it considerably improves the user experience. Second, it substantially decreases the costs associated with password management and data breaches. Third, it favors interoperability, unlocking value within and across businesses and public services, while supporting the digital transformation efforts needed to reap the benefits of the platform economy. Last but not least, passwordless authentication is much more secure. It eliminates a long list of attack vectors, from credential stuffing to phishing attacks, and puts users back in control.[3]

Authentication is so much broader than passwords. It is the foundation of digital trust, an enabler of cybersecurity in the digital economy and of the Fourth Industrial Revolution: in short, authentication is a critical enabler of the future.

Introduction

The use of passwords for authentication purposes forces users to create and memorize complex amalgams of letters, numbers, symbols and cases; to change them frequently; and to try not to re-use them across accounts. Users have to manage anywhere from 25 to 85 passwords[4] and their information sources and tools are exploding exponentially. Wanting to sign on to digital tools simply and efficiently, they are increasingly challenged and consequently tend to re-use the same passwords repeatedly.

Passwords are indeed at the heart of the data breach problem. According to the 2019 Varizon Data Breach Investigations Report, 80% of hacking-related breaches involved compromised and weak credentials, and 29% of all breaches, regardless of attack type, involved the use of stolen credentials.[5] Such attacks participate in a thriving underground economy that further exacerbates the problem.

While company adoption of platform businesses[6] is increasingly driving business valuation and growth, the problem of digital trust is growing equally fast and eroding confidence across online communities. Individuals are wary about giving out too much personal information; partners fear the loss of confidential information and business processes; and global enterprises risk the loss of reputation and revenues when systems and customers are compromised.

Beyond the technological answers and in line with systems design thinking, authentication has to be an integral part of the experience lifecycle. User experience has become such a competitive differentiator that it is the main driver of the transition to passwordless technologies. Authentication ought to be designed holistically, leveraging open standards to ensure interoperability within and beyond a company and built upon adaptive, secure and privacy-minded building-blocks, to foster user trust, drive better adoption of services and thus successfully pass the test of time. Why? For prosperity and security to reinforce each other.

The first section of this paper sheds light on the importance of authentication in digital transformation efforts, to support government and commercial leaders structure their approach. The second introduces a framework for future authentication systems, and the third builds the case for passwordless authentication. The paper concludes with a shortlist of five key passwordless technologies available for use.

It is worth emphasizing once more the importance of adaptiveness: security enhancement is a continuous process, there is no magic bullet. Cyber criminals will adapt and develop new means of attack, but the alternative authentication mechanisms presented here provide greater challenge to them and greater security in the foreseeable future.

1. Why is authentication the cornerstone of digital transformation?

1.1 The evolution of authentication practices

Authentication has always been a crucial need of life. Animals and humans "authenticate" each other using their five senses.

In the digital world, authentication is the process by which it is determined that the authenticators presented to claim a digital identity belong to the same entity that initially established the identity.

It is closely related to and generally follows identification, the process of establishing or recognizing as being a particular person or thing in a given population or context. It often takes place through identity proofing, to verify and validate attributes such as name, birthdate, fingerprints or iris scans that the entity presents.[7] (See page 18 for an example of a passwordless technology using facial biometrics for user enrollment and identity proofing.)

While both identification and authentication are important, this white paper focuses on the latter.

As threats to humans grew in complexity, authentication schemes grew in complexity. Concerned that enemies could dress up as one of them, Roman guards were among the first to use a shared secret, a watchword, when changing shifts at night.[8] They actually used three types of such authentication factors, that still form the foundation of authentication today:

- Type 1: *Something we know*, such as a watchword, a password or a PIN
- Type 2: *Something we have*, such as a guard uniform, a credit card or a mobile phone
- Type 3: *Something we are*, an inherent feature such as our height, face, fingerprints or DNA

Increasingly today, security companies are introducing additional factors that can complement these three, but that cannot be used on their own. Behaviour-based information (See page 19), or geolocation, or even a user's personal relationships[9] can be leveraged to further increase result accuracy. This underlines

The long history of password security

11th century BC
Ephraimites test word

2nd century BC
Roman guard watchword

18th century AD
"Open Sesame" in Ali Baba and the Forty Thieves

1961
Passwords introduced to computer security

1974
First hashed password on Unix OS

1994
Data Encryption Standard

1998
Advanced Encryption Standard

1998
Hardware one-time passwords (OTP)

2000
Completely Automated Public Turing Test tells Computers and Humans Apart (CAPTCHAs)

2003
SMS 2nd factor authentication (2FA)

2011
Time-based OTP

2012
FIDO Alliance created

2013
Smartphone based fingerprint authentication

2016
SMS 2FA declared unfit for purpose

2017
Smartphone-based face recognition

2019
WebAuthn standard for passwordless authentication

an important consideration worth highlighting – authentication does not have to be absolute. It simply needs to be good enough for the authentication purpose. Sometimes the costs of authenticating correctly at 99.99% will be more cost-effective than authenticating at 100%, notably given that all biometrics have a false positive rate.

Securing the authentication process has also grown in complexity. Security is a continuously evolving process, a cat and mouse game in which attackers and defenders seek to outsmart one another. This paradigm has held true throughout thousands of years of military history and is unlikely to change, even with the ongoing advancements in information technology. If anything, technology will make these changes more frequent and disruptive. As a direct consequence, another conceptual approach emerged in military theories in the last centuries: defence-in-depth.

Defence-in-depth builds upon the idea that multiple security measures are required either to thwart the most skilled attackers or give defenders enough time to respond. This approach was used in the Middle Ages to protect castles, and is still used today to protect computer networks and nuclear plants.

For the purposes of authentication, this translates into the need to combine multiple types of authentication factors. This is why several online payment systems require both a password and a temporary code sent by SMS: the password is a type 1 authentication factor, and the SMS a type 2, given that it is supposedly received by a mobile phone that belongs to the person to be authenticated.

Nevertheless, the concept of defence-in-depth relies on the premise that each security measure adds another degree of security, and experts have long pointed out the fact that SMS-based multi-factor authentication can easily be compromised.[10]

The exponential growth in the use of passwords has led to an exponential dilution of their robustness due to bulk password disclosure in data breaches, the increase in computational power allowing hashed passwords to be guessed, and the automation of password-guessing attempts.

Attackers are able to infer passwords, steal them, brute-force them, and consequently, type 1 authentication factors have become somewhat of a paper wall. The solution hence relies on combining factors, and most likely for years to come, i.e. type 2 + type 3 factors.

Passwordless authentication, i.e. type 2/3 authentication, has really only coalesced in the last few years.

1.2 Authentication is a key enabler for digital businesses

Cybersecurity ranks in the top five global risks according to the World Economic Forum *Global Risks Report 2019*, along with climate change.[11] Reducing cyber-risk exposure should hence be a foremost priority for business leaders. In the age of platforms, this starts with effective authentication.

An outdated authentication system is a source of complexity, a known enemy of security. Complexity results in blind spots and vulnerabilities that hackers leverage to gain access to core parts of company networks. Once inside, they can exfiltrate confidential company information and personal customer data, encrypt files and demand ransom, uncover details about the company and use them to blackmail C-suite executives or leverage illegitimate access to propagate nation-wide mistrust.

The very nature of platforms implies that one such blind spot can have consequences for millions of users.

Weak authentication is not just a matter of enterprise risk, it can have much wider consequences. An early example of this occurred in September 2008, when a college student leveraged Yahoo's email platform knowledge-based password recovery procedure, along with publicly available details concerning Republican vice-presidential candidate Sarah Palin, to access her email account. Although this incident did not directly impact the electoral process in the United States, it was an early example of cyber activity having potential societal consequence.

A modern authentication system is not merely a necessity from a security perspective, it is a key digital enabler. It makes mobility much more seamless, reduces user friction and thereby improves customer and employee experience. It drives operational efficiency and improves regulatory compliance. It is worth noting that authentication is one of the building blocks of an IAM (identity and access management) system. Silos increase the risk of identity theft and vulnerabilities.

1.3 Platform businesses have changed the authentication landscape

The platform economy is changing the way in which many companies are interacting with their customers. While businesses have historically operated "inside-out", i.e. developing products and services and then trying to market them, platform businesses are inherently "outside-in", listening first to the market and then developing products or solutions. Password-based consumer authentication is a legacy of the "inside-out" trend: authentication solutions were initially designed for employees in a context where user friction was not a prime concern. Today, it is consumer behaviour that is defining what authentication solutions should look like.

Passwords force users to create and memorize complex amalgams of letters, numbers, symbols and cases; to change them frequently; and to try not to re-use them across accounts. Discrepancies in password rules across online services further add to the confusion.

Numerous studies and cumulated company experience prove that individuals don't think or act this way.[12] As a result, they re-use the same passwords repeatedly, which is one reason why passwords are at the core of the data breach problem.

While the adoption of platform businesses is increasingly driving business valuation and growth, growing digital mistrust erodes confidence across online communities. Users are wary about disclosing too much personal information; platforms fear the loss of personally identifiable information, and global enterprises risk fines and the loss of reputation and revenues.

Major drivers for IAM investments

Regulatory compliance

360° view of user access and activity

Compliance-driven reporting and user access certifications

Protection of sensitive information assets

Operational efficiency

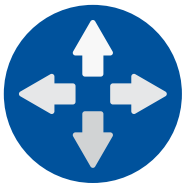
Automated provisioning and password management capabilities

Closed-loop attestation and remediation

Streamlined identity lifecycle processes (i.e. joiners, movers, leavers)

Cloud

Access governance of cloud resources



Mobility

Increase productivity and accessibility

Support BYO and CYO initiatives

Device independent, single user view

Digital transformation

Detective and preventative policy enforcement

Discovery and remediation of Rogue/Orphan/Privileged Accounts

Mitigation of risks associated with BYOD, Cloud and SaaS adoption

Mergers, acquisitions and divestitures

Improve access and reduce risk during times of high staff churn

Risk management

Improved customer experience

Security, preference and privacy management

Source: KPMG. 2018. Identity and Access Management

The service providers leading the platform economy are stuck in the proverbial middle. These include the creators of platforms for their own digital community ecosystems, as well as cloud, mobile and other technology and infrastructure providers.

These are the very organizations that are best placed to break the impasse and lead, not lag, the redesign of user authentication with stronger, simpler authentication for the platform economy.

Largest global companies in 2008 vs 2018

2008			
Rank	Company	Founded	USD (Billion)
1	PetroChina	1999	$728
2	Exxon	1870	$492
3	General Electric	1892	$358
4	China Mobile	1997	$344
5	ICBC	1984	$336
6	Gazprom	1989	$332
7	Microsoft	1975	$313
8	Shell	1907	$266
9	Sinopec	2000	$257
10	AT&T	1885	$238

2018			
Rank	Company	Founded	USD (Billion)
1	Apple	1976	$890
2	Alphabet	1998	$768
3	Microsoft	1975	$680
4	Amazon	1994	$592
5	Facebook	2004	$545
6	Tencent	1998	$526
7	Berkshire Hathaway	1955	$496
8	Alibaba Group	1999	$488
9	Johnson & Jonhnson	1886	$380
10	J.P. Morgan	1871	$375

Sources: Bloomberg, Google. In blue: Companies based on a platform model

2. What are the building blocks of a future-proof authentication framework?

Security technologies tend to be short-lived and evolve rapidly. Whether operational one year or 10 or more, cyber criminals are generally adept at finding ways to circumvent security controls. Authentication technologies are no exception. It is consequently critical to build out a long-term security strategy.

While transitioning away from knowledge-based authentication is long overdue, and passwordless authentication is the way forward for reasons explained in the following section, six principles are to be considered when building an authentication programme capable of passing the test of time: security, privacy, sustainability, inclusiveness, scalability and user experience.[13]

2.1 Security

Security logically comes first when building a strategy for an authentication system. Security in an authentication system will be based on multiple considerations, from its relative strength compared to other solutions, to its lifespan against known threats and the new threats to which it exposes the system, along with the hardware and software vulnerabilities that it solves and those that it introduces.

The security of an authentication system will also depend on its efficiency in reducing fraud and risk, and on the accountability that it allows through the logs it records.

- Does the authentication solution resist the most common cyberattacks?
- What is the risk exposure of the platform or the end-user when using it and how acceptable is the residual risk?
- What new vulnerabilities is this solution introducing that may be leveraged at some point in the future?
- Does the solution meet current standards for each of the authenticators?
- How effective is the solution at fraud detection?
- How complete is the solution?
- Does the solution provide continuous authentication through the lifecycle including after authorization?

2.2 Privacy

Passwords have been the source of numerous data breaches that have negatively impacted privacy globally. Acknowledging the various regulations and cultural aspects needed to ensure privacy, future-oriented authentication technologies should be mindful of these and, for global acceptance, ensure compatibility with the most stringent. While certain authentication solutions may fall within the category of Privacy-Enhancing Technologies, others will not.

- How is private data stored and transmitted? Is authentication performed on the user or server side?
- If private data is stored, is it stored in a central or distributed database?
- Does the solution integrate or have capabilities for consent management?
- Does the solution provide a choice for users with respect to how much data to share?
- Does the solution provide capabilities to enhance privacy?
- How will the privacy posture of the solution reflect on the reputation of the company?
- In case of breach, does the solution provide users with an opportunity to be informed in real-time?

2.3 Sustainability

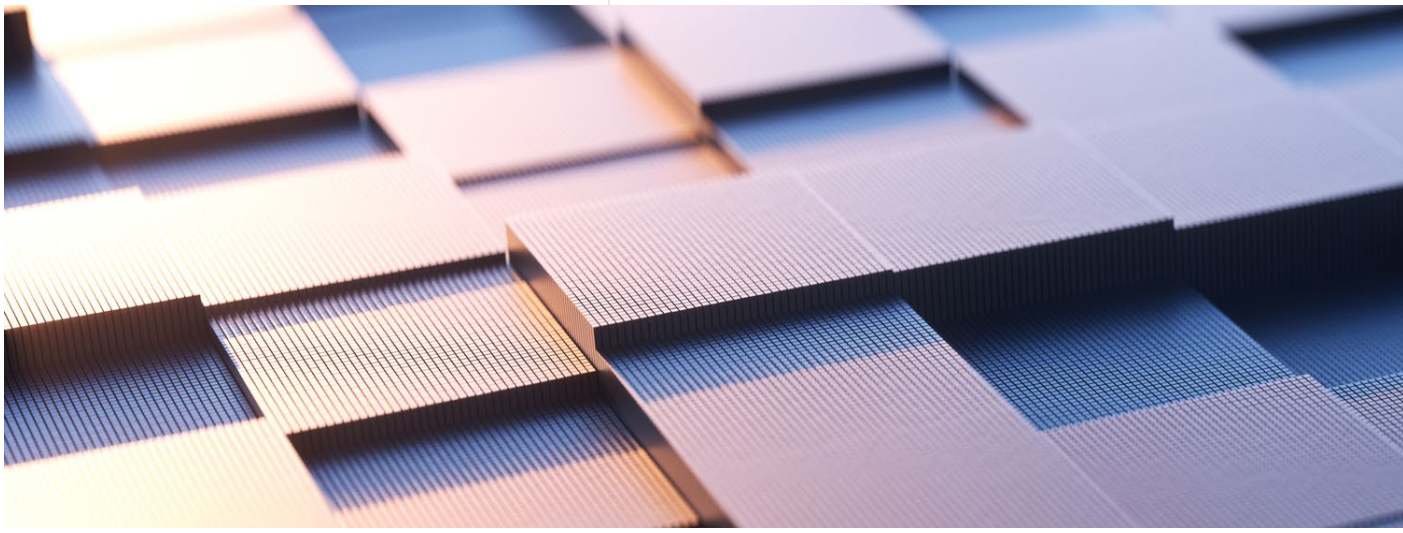
Sustainability is another key element to confirm that technological choices fit in a long-term vision strategy. Transitioning to passwordless authentication cuts costs and potentially increases revenues (See page 13), but what are the actual acquisition costs? For some companies, the sheer scale of their IT systems might call for a phased approach, which in turn requires new and legacy authentication solutions to coexist. Along the same line, authentication technologies are closely linked to identity and access management: ensuring that authentication and identification systems are compatible is also key to a sustained advantage. Finally, the externalities of the authentication system must be considered: What are the side effects, how much electricity and network activity does it generate compared to other solutions, etc.?

- How much does it cost to implement and maintain the solution?
- What is the actual return on investment?
- What is the compatibility of the solution with legacy systems?
- How does the solution integrate with the company's identity and access management framework?
- How does the solution integrate or allow for built-in fraud-detection capabilities?
- What are the secondary effects of the solution from an environmental perspective, for instance shipping thousands of security keys to employees?

2.4 Inclusiveness

Authentication systems are the entry points to digital services, so making sure that they are inclusive – as opposed to discriminatory – will be essential for platform businesses. Such systems should strive to avoid discrimination of any kind, whether due to age, culture, disability, language, name, nationality, medical condition, origin, religious belief, sexual orientation, skin color, among other factors. Case in point: Authentication technologies are increasingly using AI. What biases do machine-learning algorithms introduce that could discriminate against certain segments of the population when presenting authentication to an online service? The World Economic Forum leads several projects on these topics, notably Ethics in AI[14] and Responsible Limits on Facial Recognition Technology[15].

- How universally accessible is the authentication of users, regardless of their financial resources?
- To what degree does this authentication system discriminate against certain users?
- What biases, if any, does the potential use of AI introduce into the authentication solution?



2.5 Scalability

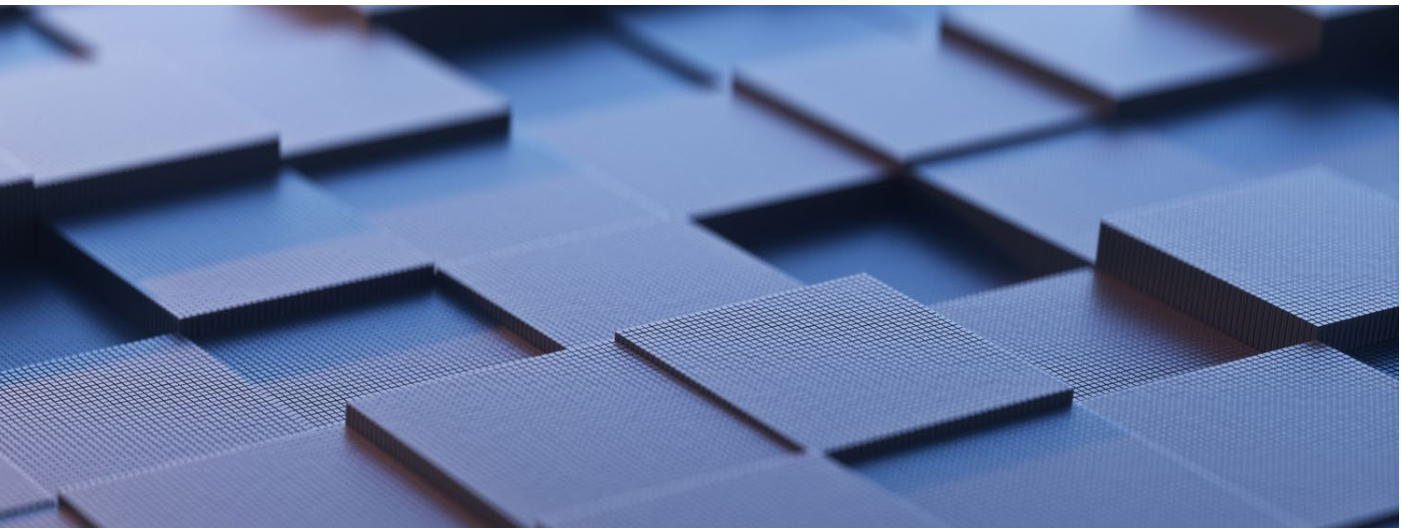
The platform economy calls for solutions that scale. Employees and end-users are increasingly going to authenticate across different platforms. It is therefore critical to consider authentication solutions from the perspective of scale: when a platform reaches critical mass and starts experiencing network effects, growth can be exponential. The performance targets of the authentication system need to be planned long in advance, notably around reliability and availability. Similarly, the "growth potential" of the solution will be important in subsequent phases: for instance, off-the-shelf solutions may not allow for the expected level of customization needed for a large company operating multiple IT environments.

- How flexible is this solution to scale across verticals, geographies and demographics?
- How flexible is it to integrate new types of authenticators?
- How easy is it for businesses to administer the solution?
- How optimal is the solution in a context of high demand?
- What is the error-rate of the solution?
- What continuity and recovery strategies work with this solution?
- How interoperable is the solution, for instance, to which extent does it build upon existing standards?

2.6 User experience

User experience is no longer a nice-to-have, it has become a key differentiator: the quality of the user experience determines user choice, preference and behaviour. As such, future authentication should strive to offer a seamless user experience to ensure adoption.

- How easy is it to install and operate the solution?
- How does the solution encourage user adoption?
- Does the solution offer choice of authenticators on the basis of user preference?
- Is the solution able to cover all customer channels consistently?
- How difficult is it to administer this solution?
- How convenient, ubiquitous and portable is the solution?



3. Why passwordless authentication now?

While it is critical to build out a long-term strategy for authentication, experts concur that the next digital breakthrough will be passwordless authentication, primarily for security reasons but not only.

Passwordless authentication offers four key advantages over traditional, knowledge-based authentication. First, it makes sense financially: it increases revenues and lowers costs. Second, it makes sense from a customer perspective, provides a better user experience. Third, from a strategic point of view, it can help redefine competition by unlocking value from interoperability. Fourth, as already mentioned, it greatly improves security.

3.1 Higher revenues, lower costs

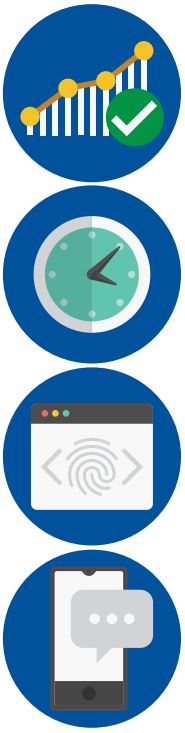
Cybersecurity has been traditionally perceived as a cost centre, so the financial consideration is perhaps the most notable reason why companies should consider transitioning to passwordless authentication. Not only does it lower costs associated with password management and data breaches, it actually improves revenues through increased productivity and customer ratings.

Higher revenues from employee productivity and customer ratings

According to a recent survey[16], employees worldwide spend an average of 11 hours each year entering or resetting their password. For a company of 15,000 employees, on average, this represents a direct productivity loss of $5.2 million. There will be costs associated with transitioning to a passwordless ecosystem but they are expected to be rapidly offset by the productivity boost alone.

With standards such as the ones developed by the FIDO Alliance, which allow for most of the authentication to be performed on the user side, password administration is significantly simplified. System administrators and call centre operators are going to have a much better experience liaising with employees and customers and this will indirectly improve company reputation and customer ratings.

The financial sevices industry is at the forefront of adoption of next-generation authentication technology, driven by user experience improvement and security. An example of the benefits was a recent mid-sized US retail bank. The bank had recognized that password authentication was a source of consumer dissatifaction, impacting use of their digital services and driving increasing operating costs. With millions of consumers, even a minor improvement would have a significant impact on ROI.



92%

Increased authentication success rate from 80% to 92%, because there is no SMS timeout, no input inconvenience

30%

Compared with traditional authentication methods, users can finish payments within 1 second saving up to 30% in time

65%

The development costs for fingerprint payment were reduced by 65%. Previously it took over 3 months for a financial institution to develop a fingerprint function with a manufacturer in only one device

2.9 Million

Reduced SMS costs by over 10%, saving more than $2.9 Million annually

Source: Nok Nok Labs

A US financial software company has been able to bring its authentication success rate to 99.9% and reduce sign-in time by 78%. Because of its simpler user experience, the company was also able to introduce other security features, shortening the life of the authentication tokens and dramatically reducing the potential attack surface.

Source: Intuit

Lower costs in case of data breach

80% of all data breaches involve weak or stolen passwords, and 29% of all attacks leverage the latter. The average global cost of a data breach in 2019 is $3.92 million – a 1.5% increase from the year before. When there are no passwords to infer or to steal, this seriously hinders the ability of criminals to access and exfiltrate data. Even password hashes are useful to criminals who can brute force them without any limitation imposed by the authentication server. From a risk management perspective, this implies that transitioning to passwordless authentication allows companies to cut the budgets associated with their breach risk exposure by 4/5. This translates immediately into lower cyber insurance premiums.

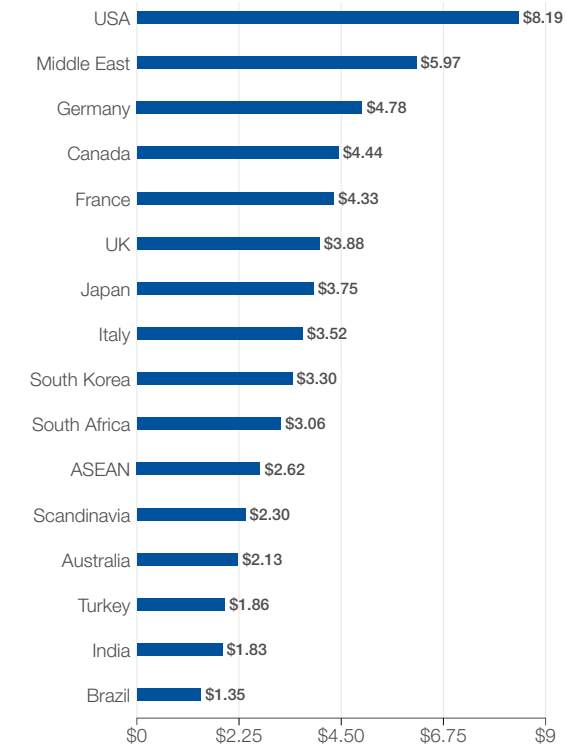
Password reset overhead savings

When it comes to IT departments and call centres, companies spend on average 2.5 months resetting internal passwords.[17] 20% to 50% of all calls to the IT helpdesk concern password resets, and the estimated cost of a single reset ranges from $30 to $70.[18] LastPass, a well-known password-safe company, estimates that companies spend on average $1 million per year in staffing helpdesks alone to deal with password resets.[19]

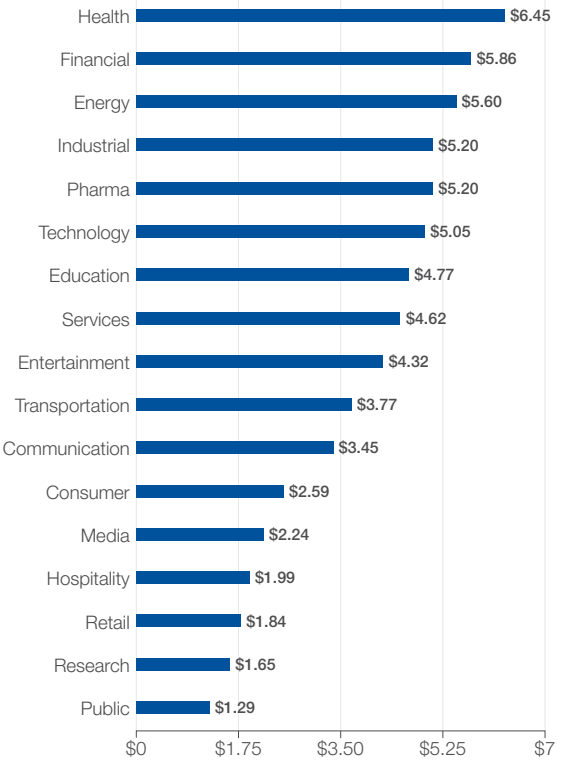
A Fortune 500 US health insurance company transitioned to passwordless authentication in 2018. In this type of sector, users log into key services intermittedly. Consequently, password resets and helpdesk congestion are common around the time of customer re-enrollment. This type of business model and user experience incurs spikes in costs and lowers overall authentication frequency for the customer.

Source: HYPR

Cost of a data breach by country or region ($ Millions)



Average total cost of a data breach by industry ($ Millions)



Source: IBM Security. 2019. Cost of Data Breach Report[20]

3.2 Better user experience

A convenient, seamless user experience is essential to widespread acceptance and use of authentication.

The experience economy

Increasingly, experience will be more important than price.[21] 86% of customers are indeed ready to pay a premium for more user-friendly experience.[22] This means that if a platform's authentication experience is subpar, some customers will prefer a platform with inferior services but a better authentication experience.

Passwordless authentication is seamless. It emulates the way in which human beings have recognized each other for millennia: by looking for either identifying belongings or personal traits, such as uniforms, height or body shape.

In other words, passwordless authentication is becoming a competitive differentiator, and a key consideration for digital transformation leaders. It is the entry door to an online service.

Google employees use FIDO-based security keys to authenticate internally. Total time spent authenticating with security keys dropped nearly two-thirds. Most importantly, there were zero authentication failures. In their examination of the time period studied, the failure rate for OTP-based authentications was 3%.

There were numerous additional benefits from a user experience perspective, the most notable impact being that no employee accounts suffered a phishing-attack since they switched to security keys.

Users are less likely to try to circumvent security measures

When users are asked to remember over 100 credentials and passwords, they naturally look for ways to reduce their burden and re-use passwords, choose weak ones, or note them down on their phone, email account or below their keyboard. A better user experience means that users are more likely to use the authentication system as it is meant to be: reducing the number of rules improves user endorsement which in turn, improves security.

The most frequently used passwords

1.	**123456**	2.	**123456789**
3.	**qwerty**	4.	**password**
5.	**111111**	6.	**12345678**
7.	**abc123**	8.	**1234567**
9.	**password1**	10.	**12345**

Source: UK NCSC[23]

Ubiquity

Passwordless authentication is customer-centric. Passwordless authentication technologies leverage fast and convenient solutions that work everywhere, relying on the same devices that many people use every day such as smartphones.

3.3 Interoperability unlocks value

Interoperability allows for scalability

Interoperability is made possible by standards. The FIDO Alliance[24], an open industry association and a prominent passwordless advocate, has created open standards for passwordless authentication to online and mobile services. Its most prevalent standard, FIDO2, was developed with the World Wide Web Consortium (W3C) and became a web standard in March 2019.

This type of authentication leverages public-key cryptography, i.e. a public key that can be shared with anyone. The associated private key that is held by the owner securely within the 'authenticator' on their device such as a mobile phone, a computer or a security key.

When users authenticate to a site supporting FIDO, their identity or presence is verified with a simple action, such as scanning a fingerprint or touching a security device. The website and the user's authenticator conduct a challenge-response to verify that the user is in possession of the correct private key. Each service uses a unique key pair, and the private key never leaves the user's device.

FIDO2 is supported by all leading web browsers, making its reach nearly ubiquitous on modern devices.

Login steps:

1. *Online service challenges the user to login with a previously registered device*
2. *User unlocks the FIDO authenticator using the same method as at Registration time*
3. *Device uses the user's account identifier provided by the service to select the correct key and sign the service's challenge*
4. *Client device sends the signed challenge back to the service, which verifies it with the stored public key and logs in the user*

Interoperability gives options

Taking a standards-based approach means that the implementation work is largely done and service providers can get started faster on their path to passwordless. Service and technology providers can develop solutions to a common standard - including a public API that web developers can easily leverage that eliminates dependence on passwords alone. FIDO interoperability is validated through an established certification programme that has seen over 650 products complete conformance and interoperability testing.

While standards can provide a scalable framework for adoption of password free technology, there are a number of additional process that can aiding with rapid implementation within enterprise environments. These include processes such as evaluation of vendors, building of user experiences, education of internal users, road mapping and migration from existing solutions and adjustments to improving sign-in flow.

The public sector is also heavily investing in digital programmes as online services become a principal source of interaction between citizens and their governments. The security of government digital services is a prime concern that is driving many public bodies to revisit their national authentication schemes. GOV.UK Verify is the way that UK citizens and residents access government services online. It builds upon a trust framework underpinned by standards and guidance documents which set the rules for participation in the framework. The good practice guide on authentication and credential management outlines the requirements for GOV.UK Verify identity providers regarding the authentication of users. It includes recommendations on the use of the industry standards that are applied to protect access to online services including, for example, FIDO technical specifications and certification. Such guidance is designed to both meet national requirements and to be interoperable internationally.

Interoperability unlocks access to new markets

Interoperability allows new users to access certain services, it allows existing users to transact more, and it allows digital services to offer their users new ways to transact. Open standards greatly reduce development time and unlock access to new markets that are adopting certified solutions. It allows for international compatibility and expansion.

Regulations such as GDPR impact businesses serving European users, regardless of where the businesses themselves are registered. Passwordless authentication makes it easier to comply with such international regulations, which is key to expanding digital businesses across geographies.[25]

3.4 Fewer passwords, greater security

Enterprises often struggle with balancing security and ease-of-use trade-offs. As explained previously, passwordless solutions enhance the user experience, but do they do so at the expense of security?

Reduced attack surface for businesses

When companies transition to passwordless solutions, they considerably reduce their exposure to data breaches. Contrary to companies that store their customers' passwords on their servers, passwordless solutions require no personal information to be stored for authentication purposes.

When authentication is performed on the user side, no personal information is transmitted over the internet, making man-in-the-middle attacks virtually impossible.

With the authentication data, such as the biometrics of the user, kept on the user device, there is no single collection point for cyber criminals to get access to a customer biometric dataset: this dataset does not exist. As a result, the risk probability of online fraud and identity theft is greatly reduced. There are down-sides, too: should users lose their authenticator, for instance if it is tied to a physical device, resetting access can be more cumbersome than a password reset.

Better end-user security

As criminals and computers have become more effective at stealing and guessing passwords, password hygiene rules have developed exponentially. Recognizing that these rules were difficult to enforce, an inflexion point was reached recently with experts calling to simplify password management protocols. When using passwordless solutions to authenticate, there are no passwords for cyber criminals to steal out of a platform server. There is no information stored by companies that could be leveraged by hackers to infer or bruteforce a password. Users are hence better protected.

Implicit multi-factor authentication

Most passwordless authentication leverages both a particular device or app – the authenticator, that is tied to the user, and a biometric feature: those are two distinct authentication factors that provide much stronger guarantees than a single shared secret. Unlike a one-time-password sent by SMS for instance after a password is entered, a passwordless authentication solution is frictionless, hence fostering the adoption of multi-factor authentication more rapidly than ever.

It is an impediment to the cybercrime economy

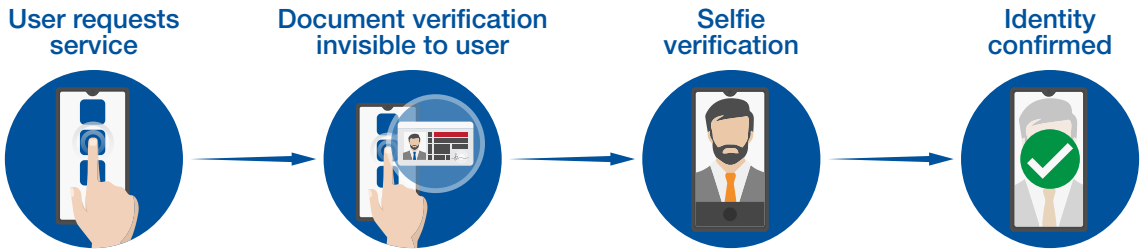
Login credentials to bank or Uber accounts are on sale on the dark web for $7 or even less.[26] This is a problem for the user whose credentials are up for sale, yet another concern is that the income generated by such transactions fuels cybercrime and terrorist activities. Replacing passwords therefore impacts the underground cybercrime economy by increasing the cost of doing business for organized crime groups, which will reduce their profits and incentives to commit cybercrime.

4. How to transition to passwordless authentication today

There are numerous technologies available to replace passwords. Each of them presents advantages and disadvantages depending on an organization's context, legacy systems, objectives, and so on. Below is a list of some technologies with which the World Economic Forum has worked over the past years.

4.1 Authentication with facial biometric technology

Recent technological advances in smartphone cameras and machine-learning models mean facial recognition and document scanning can now be used to verify people remotely and at scale. In short, when creating a new account on an online service, users take a picture of their government ID and the application compares the picture with that of the person taking the picture. By using facial biometric authentication, users no longer need to associate a password with their account.

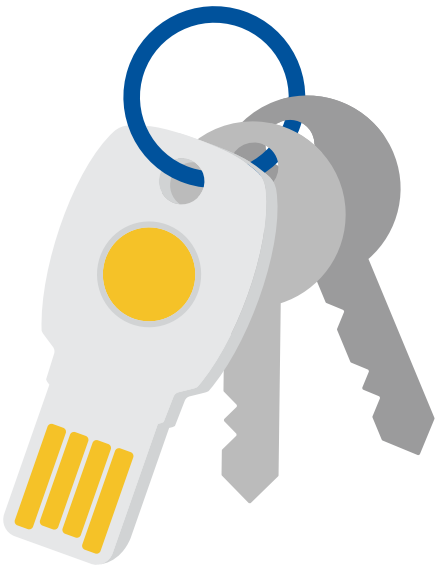


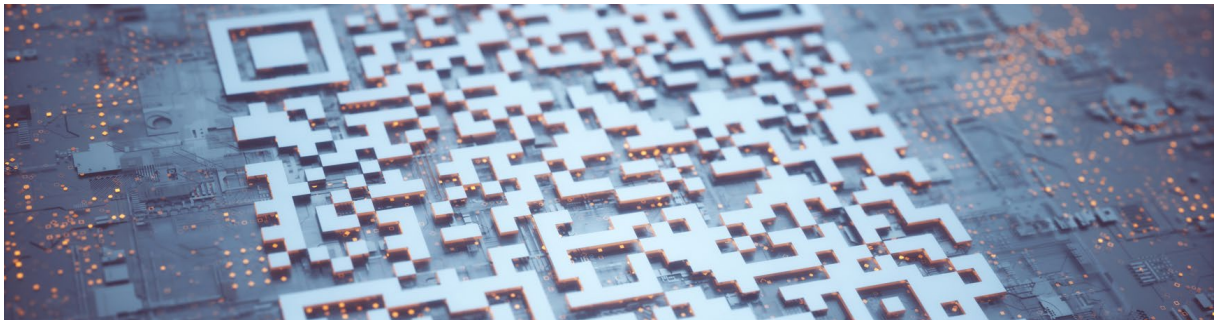
Source: Onfido

4.2 Extra security with hardware keys

In a recent research assessment, Google compared the standard baseline of password authentication with security keys, smartphone-based one-time password (OTP) generators, and two-step verification (2SV) over SMS. While no option is perfect and any form of 2SV is better than none, Google found that security keys provide the strongest security while also offering the best mix of usability and deployability.

Security keys come in a variety of form factors ranging from a small USB, NFC or Bluetooth device that can live on a user's keychain to something built into a user's mobile phone that can securely authenticate when they need to sign into a new device. The common factor here is that the device must be physically and locally present when authentication happens.

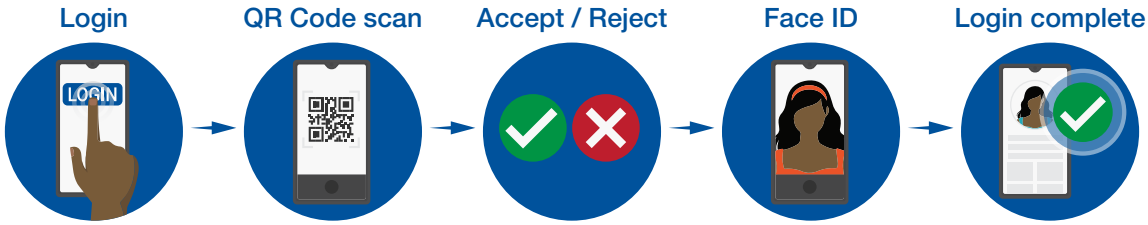




4.3 User experience first with QR code authentication

Complex animated QR codes can also be used to authenticate without passwords. Users logging in scan a QR code with a smart device to bind the session to their user identity. A confirmation message is then displayed in an app on the device verifying the authentication which triggers a biometric scan confirming that the users are who they say they are. Then, an authenticated session is passed to the relying party and the user is logged in.

The dynamic QR code scan has many advantages such as preventing session hijacking or session replay attacks. Since the code is animated, unique and has a very short life span, it provides a secure way for binding sessions to identities while at the same time providing a seamless experience that doesn't require complex pairing between devices.

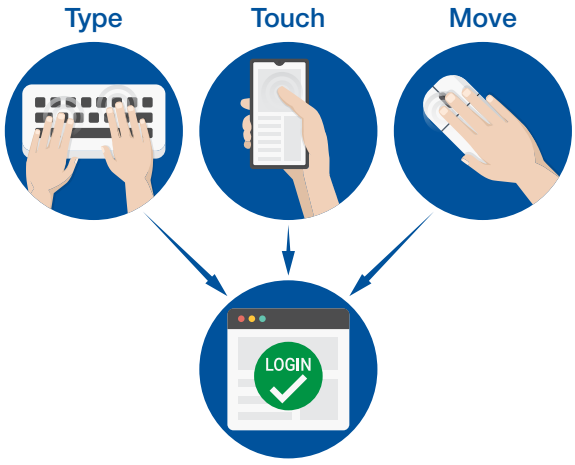


Source: Trusona

4.4 Seamless authentication with behavioural analysis

Behavioural authentication uses non-identifiable but individually unique factors to confirm identity. Users may not see a password login, but their identity will be authenticated in the background using factors such as non-identifiable behaviour attributes from mouse movements to typing speed and habits, login history, network details like IP address, browser used, etc. While each of these non-identifiable factors is not enough on its own, when they combine as a single-security mesh, authentication becomes both secure and invisible.

All these factors can be brought together in a big data set and apply artificial intelligence and machine learning to analyse and accurately differentiate legitimate users from criminals and fraudulent authentication – regardless of the credentials presented.

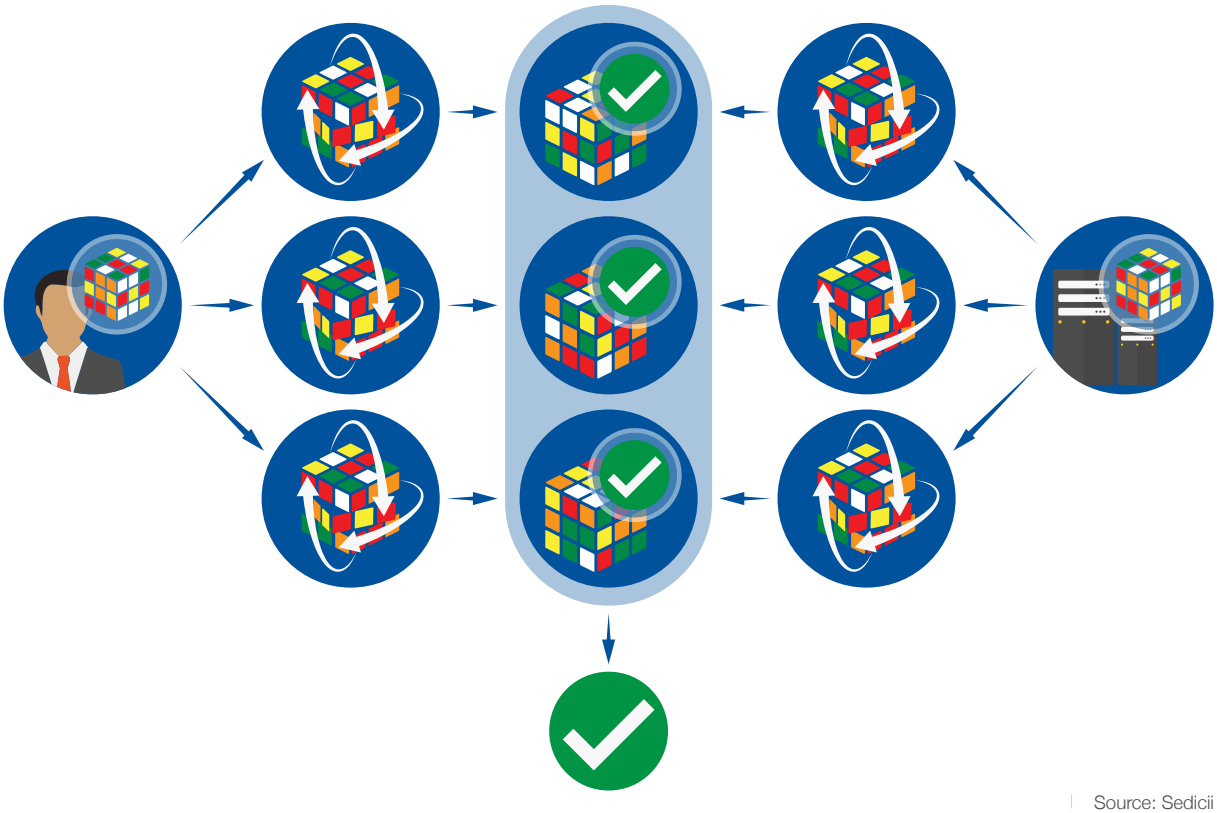


Source: Shape Security

4.5 Fewer passwords with zero-knowledge proofs

Zero-knowledge proofs (ZKP) are a challenge/response authentication protocol in which parties are required to provide the correctness of their secrets, without revealing these secrets. It allows authentication of users in such a way that a password never leaves the user's device or browser. In simple terms, a ZKP authentication process can transform a password into a complex and unique abstract string, like a Rubik's cube with a completely random pattern. The abstraction is transferred to a server and stored. The challenge is to prove that the Rubik's cube pattern on the client is the same as the one on the server by generating a series of random permutations that match both the Rubik's patterns. In this way, the entire pattern is never transferred but you can still prove, to a very high probability, that the two patterns are the same. One of the main advantages is that the verifier cannot learn anything from the authentication procedure.

ZKP technology can eliminate the exposure of private user data during authentication or identity verification. It can even be used beyond authentication, allowing users to reclaim and control the use of their digital identity.



Source: Sedicii

Conclusion

Authentication solutions to date have been predominantly knowledge-based, single-factor and have resulted in countless issues from customer and reputation loss to high costs in help-desk staffing and data breaches. For companies eager to transition into the new digital era, moving beyond passwords should be a short-term objective.

Enterprises seeking to capitalize on the platform economy opportunity are recognizing that authentication is one of the first steps to take. As the first contact with customers, it is a key to experience, and the competitive differentiator in the Fourth Industrial Revolution.

But user experience is not all that passwordless authentication has to offer. New internet standards are giving platform businesses ubiquitous authentication at a fraction of the cost, allowing for cross-platform interoperability and multinational expansion, all while faring much better on the security front.

If passwordless authentication is indeed the next step, it is not an end unto itself. Criminals adapt and security controls tend to be short lived. This is why a sound authentication system should build upon a long-term vision to foster security, privacy, sustainability, user experience, scalability and inclusiveness.

The future of authentication will lead take many paths, some that we are only starting to explore like blockchain-based self-sovereign identities and zero trust networks.[27] But the immediate journey for platform businesses to embark on leaves passwords behind.

Contributors

Lead Authors

Andrew Shikiar	Executive Director and Chief Marketing Officer, FIDO Alliance, USA
Adrien Ogee	Project Lead, Platform for Shaping the Future of Cybersecurity and Digital Trust, World Economic Forum

Contributors

Christine Leong	Global Lead, Blockchain Identity & Biometrics, Accenture, USA
Daniel Bachenheimer	Senior Manager, Accenture, USA
Douglas Lagore	Global Digital Identity Lead, Accenture, USA
Stefan Ulbrich	Principal Research Scientist, Acceptto, Germany
Jeremy Grant	Coordinator, Better Identity Coalition, USA
Abbie Barbir	Senior Security Architect, CVSHealth, USA
Cisa Kurian	Senior Security Architect, CVSHealth, USA
Alastair Treharne	Digital Identity Advisor, Government Digital Service, UK
Christina Hulka	Executive Director & Chief Operating Officer, FIDO Alliance, USA
Megan Shamas	Director of Marketing, FIDO Alliance, USA
Christiaan Brand	Product Manager, Identity and Security, Google, USA
Alex Consilvio	Regional Sales Director, HYPR, USA
Bojan Simic	Chief Technology Officer, HYPR, USA
Marcio Mello	Head of Product for Identity and Profile Platform and Solutions, Intuit, USA
David Ferbrache	Global Head of Cyber Futures, KPMG, UK
Ravi Jayanti	Associate, Cyber Futures, KPMG, UK
Alan Meeus	Product Manager, Microsoft, USA
Jackie Comp	Vice President, Worldwide Sales and Business Development, Nok Nok Labs, USA
Parker Crockford	Director of Policy & Strategic Accounts, Onfido, UK
Rob Leslie	Chief Executive Officer, Sedicii, Ireland
Michael Plante	Chief Marketing Officer, Shape Security, USA
Shuman Ghosemajumder	Chief Technology Officer, Shape Security, USA
Ori Eisen	Founder and Chief Executive Officer, Trusona, USA
Ronnie Manning	Chief Marketing Officer, Yubico, USA

From the World Economic Forum

Will Dixon	Head of Future Networks and Technologies, Platform for Shaping the Future of Cybersecurity and Digital Trust
Cristian Duda	Lead, Digital Identity, Platform for Shaping the Future of Digital Economy and New Value Creation
Monika Glowacki	Research and Analysis Specialist, Platform for Shaping the Future of Digital Economy and New Value Creation
Marco Pineda	Head of Security and Innovation, Platform for Shaping the Future of Cybersecurity and Digital Trust

Endnotes

1. Schenken, Jennifer L. 2019. The Platform Economy. The Innovator. https://innovator.news/the-platform-economy-3c09439b56 (link as of 14/01/2020)
2. Hay Newman, Lily. 2019. Hacker Lexicon: What Is Credential Stuffing? Wired. https://www.wired.com/story/what-is-credential-stuffing/ (link as of 14/01/2020)
3. O'Connor, Fred. 2019. The top six reasons to use passwordless authentication. https://www.veridiumid.com/blog/top-reasons-passwordless-authentication-phishing/ (link as of 14/01/2020)
4. 2019. Password habits still key obstacle to business' security. SecurityBrief. https://securitybrief.com.au/story/password-habits-still-key-obstacle-to-business-security-logmein (link as of 14/01/2020)
5. Steel, Amber. 2019. Passwords Are Still a Problem According to the 2019 Verizon Data Breach Investigations Report. https://blog.lastpass.com/2019/05/passwords-still-problem-according-2019-verizon-data-breach-investigations-report.html/ (link as of 14/01/2020)
6. Moazed, Alex. 2016. Platform Business Model. https://www.applicoinc.com/blog/what-is-a-platform-business-model/ (link as of 14/01/2020)
7. World Economic Forum. 2018. Identity in a Digital World: A new chapter in the social contract. https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract (link as of 14/01/2020)
8. The Roman Military System. https://web.archive.org/web/20080207011711/http:/ancienthistory.about.com/library/bl/bl_text_polybius6.htm (link as of 14/01/2020)
9. Kearns, Dave. 2007. RSA introduces the fourth-factor authentication. Network World. https://www.networkworld.com/article/2303112/rsa-introduces-the-fourth-factor-authentication.html (link as of 14/01/2020)
10. Meyer, David. 2016. Time Is Running Out For This Popular Online Security Technique. Fortune. https://fortune.com/2016/07/26/nist-sms-two-factor/ (link as of 14/01/2020)
11. World Economic Forum. Global Risks Report 2019. https://www.weforum.org/reports/the-global-risks-report-2019 (link as of 14/01/2020)
12. Ranghetti Pilar, Denise; Jaeger, Antonio; Milnitsky Stein, Lilian. Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3515440/ (link as of 14/01/2020)
13. This list of principles builds upon the following list of influencing factors developed for multi-factor authentication: usability, deployment, utility, financial, security and performance. Source: Accenture and Payments Council, Multi-Factor Authentication Security Review 2010.
14. World Economic Forum. Teaching AI Ethics (TAIE). https://www.weforum.org/projects/teaching-ai-ethics (link as of 14/01/2020)
15. World Economic Forum. Responsible Limits on Facial Recognition Technology. https://www.weforum.org/projects/responsible-limits-on-facial-recognition-technology (link as of 14/01/2020)
16. The 2019 State of Password and Authentication Security Behaviors Report. https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf (link as of 14/01/2020)
17. Barker, Ian. 2019. US companies waste over two months a year resetting passwords. Betanews. https://betanews.com/2019/05/02/password-reset-waste/ (link as of 14/01/2020)
18. Telesign. https://www.telesign.com/enable-secure-account-recovery/ (link as of 14/01/2020)
19. Petrillo, Katie. 2018. New Forrester Report: The Real Cost of Password Risks. https://blog.lastpass.com/2018/05/new-forrester-report-real-cost-password-risks.html/ (link as of 14/01/2020)

20. Cost of a Data Breach Report 2019. IBM Security. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.179928934.399179535.1576226359-1623201060.1572538493 (link as of 14/01/2020)

21. Mitchell, Vanessa. 2019. Lenovo: Experience more important than price or product. CMO. https://www.cmo.com.au/article/665537/lenovo-experience-more-important-than-price-product/ (link as of 14/01/2020)

22. Newman, Daniel. 2018. Want Better Customer Experience? Combine CRM And Customer Feedback. Forbes. https://www.forbes.com/sites/danielnewman/2018/04/10/want-better-customer-experience-combine-crm-and-customer-feedback/#7b289f723fbb (link as of 14/01/2020)

23. 2019. Passwords, passwords everywhere. UK NCSC. https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere (link as of 14/01/2020)

24. FIDO Alliance overview. https://fidoalliance.org/overview/ (link as of 14/01/2020)

25. McMillan, Robert. 2017. The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!. The Wall Street Journal. https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118 (link as of 14/01/2020)

26. Newcomb, Alyssa. 2018. Your identity is for sale on the dark web for less than $1,200. NBC news. https://www.nbcnews.com/tech/security/your-identity-sale-dark-web-less-1-200-n855366 (link as of 14/01/2020)

27. Data Breaches and IAM Trends. Identity Management Institute. https://www.identitymanagementinstitute.org/data-breaches-and-iam-trends/ (link as of 14/01/2020)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744

contact@weforum.org
www.weforum.org