KCOM

The new face of digital identity

The trends redefining identity management

Re-imagine how.

Identity matters

Online, a person's identity is their key to the digital services they require. It is how businesses identify individuals and determine their access privileges. In short, if your name is not on the list, then you will not be allowed in.

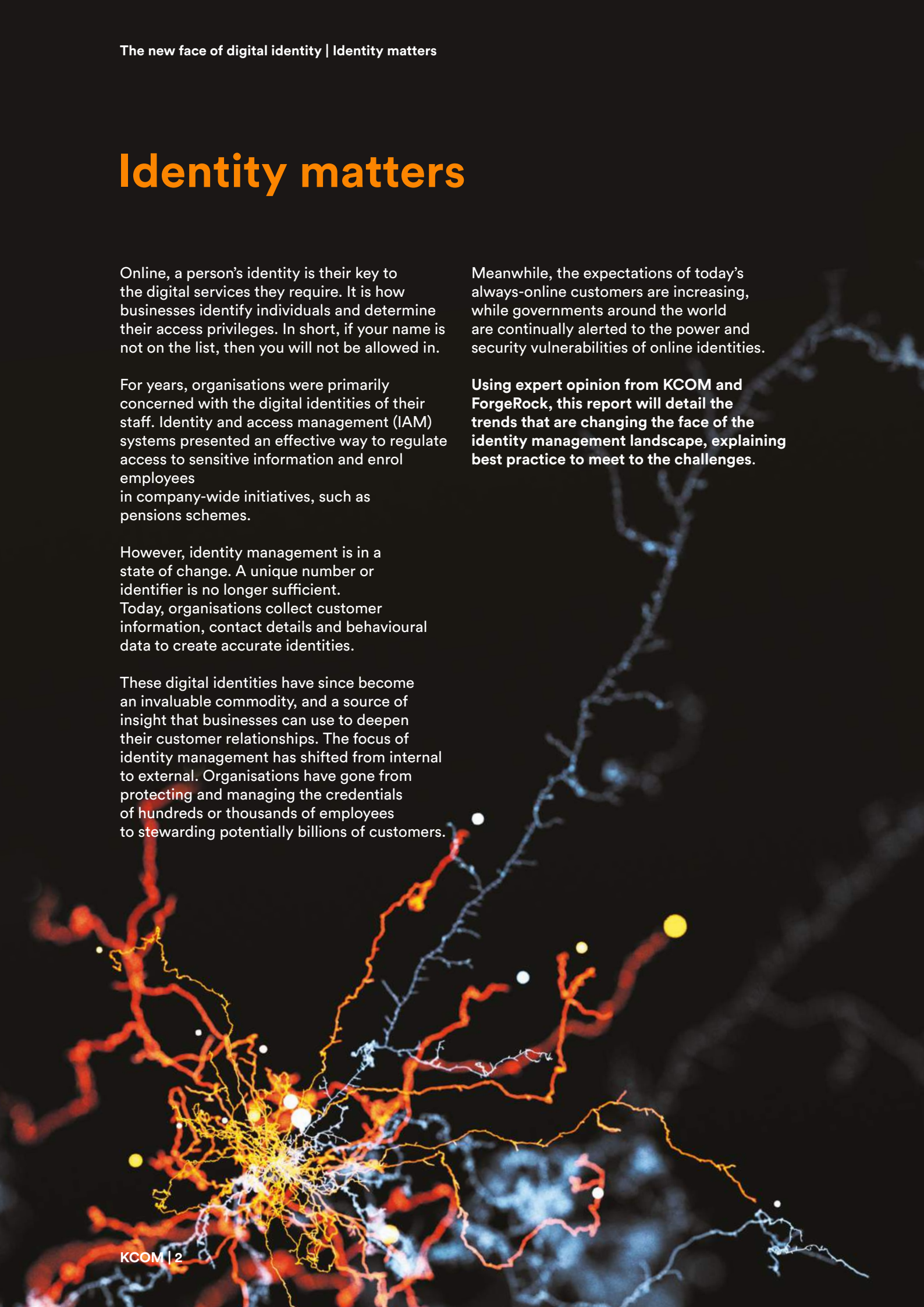
For years, organisations were primarily concerned with the digital identities of their staff. Identity and access management (IAM) systems presented an effective way to regulate access to sensitive information and enrol employees in company-wide initiatives, such as pensions schemes.

However, identity management is in a state of change. A unique number or identifier is no longer sufficient. Today, organisations collect customer information, contact details and behavioural data to create accurate identities.

These digital identities have since become an invaluable commodity, and a source of insight that businesses can use to deepen their customer relationships. The focus of identity management has shifted from internal to external. Organisations have gone from protecting and managing the credentials of hundreds or thousands of employees to stewarding potentially billions of customers.

Meanwhile, the expectations of today's always-online customers are increasing, while governments around the world are continually alerted to the power and security vulnerabilities of online identities.

Using expert opinion from KCOM and ForgeRock, this report will detail the trends that are changing the face of the identity management landscape, explaining best practice to meet to the challenges.



About the contributors

Andy Cory

Head of Identity & Access Management Practice

KCOM

Andy has 20 years of experience in IT. Having joined KCOM in 2006, he leads KCOM's Identity Practice, specialising in the architecture and delivery of Identity and Access Management solutions. Andy has worked with IAM products from vendors such as Oracle and Sun, and most recently with ForgeRock. Andy is a certified and accredited ForgeRock solutions architect, and has also been awarded ForgeRock Mentor status.

LinkedIn: linkedin.com/in/andycory

Gavin Brown

Head of Identity

KCOM

Gavin has over 15 years of industry experience. Working with his team of experts he provides consultancy, implementation and ongoing support services for the ForgeRock identity platform. Gavin is dedicated to improving customer experiences, increasing brand loyalty and reducing costs for the organisations that he works with.

LinkedIn: linkedin.com/in/gavin-brown-8b7a086

Carlos Scott

Digital Risk Consultant

FORGEROCK

Carlos has over 15 years of experience in the Information Security and Digital Banking industries. He works with Financial Services organisations globally to solve complex identity and regulatory challenges in the digital and cyber-security domains. Carlos has managed Data Loss Prevention operations and Information Protection controls at Barclays. He also led technical consulting at a number of high-growth cyber-security start-ups.

LinkedIn: linkedin.com/in/cscott-digital

KCOM | 3

From internal to external – **the customer matters most in identity management**

Identity management has grown into a crucial part of the customer experience. Consumers are all too familiar with sign-in pages and having to go through multiple stages of authentication when they want to access online services. Yet the tide is turning.

77%
of customers believe that security measures are unnecessarily complicated[1]

To be competitive, organisations must be able to keep up with changing expectations, and be able to capture and capitalise on customer information. Increasingly, this entails delivering an experience that is seamless, hyper-personalised and secure.

Identity management is no longer just a security matter. It has a direct impact on revenues and the growth of your organisation.

[1] FICO, July 2018

"Data collection is crucial for building an accurate view of the customer. However, it must be done in a progressive, transparent way. If a customer is faced with a three-page registration form the first time they use your services, there's no guarantee they will complete it.

Customers gravitate towards the easiest, fastest way of getting the products and services they want. In such a competitive environment, the goal should always be to make the authentication process as painless as possible."

Andy Cory
Head of Identity & Access Management Practice – KCOM

"Ultimately organisations look for the authentication process to be frictionless for their customers, but that does not mean it should also be invisible.

Different businesses will have different priorities, but trust is still crucial to the customer experience. Increasingly, consumers care about their personal data and want to be reassured that it is protected and will not be misused.

In industries like banking and financial services, it is important that customers know there is still a gateway that must be passed. That process will improve the perception of security and will provide an improved customer experience knowing there is a level of security protecting their account. For general access, however, such a gateway is not needed. After an initial sign-in on a retail mobile app, for example, you shouldn't have to resubmit your data every time you wish to use it."

Gavin Brown
Head of Identity – KCOM

"The task for organisations is two-fold. In the crowded marketplace, they must differentiate themselves by providing seamless, uninterrupted, highly-personalised customer experiences. Yet, they must also keep pace with the rising expectations of consumers around security and privacy.

For those able to achieve this, the rewards are immense. If you can make your online customer experience easier, simpler and more convenient to use, then the customer will be back. Not only will this mean more sales in the long term, but more data generated on that customer.

The more they use your platform, the better you will know their habits and preferences and the greater your ability will be to upsell and entice them with more relevant deals."

Carlos Scott
Digital Risk Consultant – ForgeRock

There is a clear need for quality and secure employee identity management. However, the focus has shifted. Organisations have woken up to the fact that identity management can have a huge impact on the customer experience. To remain competitive, businesses should always strive to deliver the fastest, most seamless experience every time.

Identity management platforms can also feed into efforts to hyper-personalise the user experience, but they need to be fully integrated to support this. From data collection to content delivery, the identity management platform should form the foundation of any customer lifecycle. Correct management of the system then puts the customer at the heart of digital transformation.

The data privacy debate. **Be agile, stay compliant.**

Regulation is rapidly catching up with technology. Digital identity fraud is a growing concern that can permanently damage customer relationships and ruin livelihoods.

80-90%
of login attempts on retailer websites are from hackers using compromised credentials[2]

While directives like GDPR have started to focus minds around the need to protect and respect user data, further seismic changes are on the way.

Compliance is only a baseline. It is the duty of organisations to ensure they have systems in place that are responsive enough to deliver both the letter and spirit of the law. Users must also be included, with organisations prepared to give them visibility and control over how their data is being used.

"GDPR may have come into effect, but it certainly isn't over. With looming fines and risks against corporate reputation for failure, companies need to respect GDPR and ensure they can deliver on its promises. This means having the infrastructure ready to comply with the right to be forgotten. If a customer confirms that they no longer want to be contacted by a vendor then this has to be respected. Their data should be wiped from all databases and no longer used in marketing campaigns.

The *right to request* is equally important. Organisations must have the capabilities to retrieve and display customer data on request and in a format that that is easy for the customer to understand. We are already seeing some innovative identity management solutions helping with this. GDPR dashboards can display to the user the data that is held on them clearly and simply. Additionally, it is more efficient to have this feature running on your identity management platform, where this data is collected and stored."

Andy Cory
Head of Identity & Access Management Practice – KCOM

[2] Shape, 2018 Credential Spill Report, 2018

"In the financial sector, many organisations are still getting to grips with the complexities of PSD2 and open banking implementation. This directive obliges financial institutions to release the data they hold on their customers to other third parties, providing they have the permission of the end user. This gives consumers more control over how their data is used and removes power from the data owning organisations. Organisations are being forced to adapt to retain their own customers.

While the directive is intended only for financial services, we should not assume that similar regulations will not appear in other industries. Preparation is key. Many of the applications of PSD2 and Open Banking compliance generate applicable user cases in other sectors. Regulation can drive innovation, with the right approach."

Gavin Brown
Head of Identity – KCOM

"GDPR is only the beginning. The EU has been very proactive in pioneering data management rights for its citizens. They are now the owners of their personal data rather than the companies they share it with. Already, many countries around the world - including Singapore, Australia and Canada – are enacting their own regulations to replicate or expand on it.

While GDPR established a legal baseline for data ownership, the EU ePrivacy Regulation will stipulate the need to capture consent. Organisations must ensure they have the infrastructure in place to provide customers with transparent, streamlined opportunities for opt-outs. They will, henceforth, also need systems that request customer consent for valuable metadata."

Carlos Scott
Digital Risk Consultant – ForgeRock

Perhaps the only sure thing in business is regulation. New responsibilities are constantly being placed on organisations, especially as the data privacy debate gathers pace.

While integration across your data management and identity management is crucial for achieving compliance, so is agility. Regulation is changing constantly, so your identity management platform must be able to keep up. To do this, you need a platform that is easy to update, along with relevant expertise and experience.

Ultimately, prevention is better than the cure. With an advanced identity and access management system, businesses can detect security gaps and prevent malicious access to employee and customer data.

Survival of the fittest. **Innovate to compete.**

Technology continues to push the boundaries of what is possible in identity management.

A new generation of businesses has emerged that is shaking up their sectors with innovative approaches to digital identity. Multi-stage authentication, born of poorly-integrated legacy technology, is becoming a thing of the past.

The pace of change is quickening, with AI, enhanced biometrics and single sign-on driving a better, more competitive user experience. Established players must innovate to survive.

"If your objective is to provide the least intrusive customer experience possible, continuous authentication is the way forward. More organisations are moving away from the standard username and password method to a system where customers are only asked for their details if their behaviour changes significantly. This is much more sophisticated than detecting when a user is using an unfamiliar device.

The granular nature of data collection means organisations can build highly detailed profiles for their customers. Data such as how fast they scroll, how long on average they spend on a page and even how they swipe or how much pressure they put on their phone touchscreen. While the solution relies heavily on the data available, there are opportunities to deliver reliable authentication and a seamless experience.

For the future, AI is the one to watch. As GDPR has shown, many companies are responding to consent requirements by forcing customers through page after page of consent agreements. Not willing to impinge on customers too much, some organisations are starting to experiment with AI solutions that use preference data to make privacy and consent decisions on the customer's behalf. We will have to wait to see how the law responds. The jury is still out on whether 'intelligent consent' is actual consent."

Carlos Scott
Digital Risk Consultant – ForgeRock

"Fintech companies and so-called *neobanks* have had some success in displacing traditional banks. Such organisations don't suffer from the same resistance to change as incumbent brands, not because they're less risk-averse, but because their IT systems don't have the technical debt inherent in the legacy systems of established banks.

In the identity management sphere, this allows them to take advantage of the functionality of newer platforms. By adopting the most sophisticated of authentication methods, progressive and non-onerous methods of building up customer profiles, you can provide a modern customer experience. This will ultimately drive customer engagement."

Andy Cory
Head of Identity & Access Management Practice – KCOM

"The area where we are seeing the fastest movement and most immediate adoption is biometrics. The ability to sign in with only a fingerprint or face scan is game-changing, and consumers are already using these authentication methods.

Organisations are also really starting to embrace external sign-on solutions. These allow customers to access services across all their devices after only signing in once to a single device. The advantage here is that it allows customers to quickly pick up where they left off and at any time they want. For example, in media, this functionality creates the next level of customised and personalised streaming on-demand. Consumers can choose what they want to watch, when they want to watch, seamlessly across multiple devices."

Gavin Brown
Head of Identity – KCOM

To ensure they are at the forefront of innovation, companies need to seek out specialist partners. These organisations should have the experience and insight to re-imagine approaches to IAM. Working together, the partnership should address the implementation and running of the system, through to the integration of new technologies as they emerge.

This strategy will not only benefit customers, but also add value to the enterprise. The key is to have a single, dynamic platform that enables you to make changes rapidly and efficiently, while being supported by a team of experts that can take your resiliency and competitiveness to the next level.

Re-imagine how.

By combining ingenuity, agility and integrity, KCOM goes beyond the mandate: shaping solutions to meet the demands of emerging and future business challenges.

KCOM believes that the greatest opportunities lie in the unknown. That there is always an alternative, smarter way to achieve business goals.

To re-imagine how.

Get in touch:
Call: 0800 138 3525
Email: IAM@kcom.com
Twitter: @KCOMBusiness

www.kcom.com