Ovum
TMT intelligence | informa

Managing and Leveraging Digital Identity in Financial Services

Identity verification and biometric authentication can streamline processes, increase security, and improve the customer experience

In partnership with

SAMSUNG

SAMSUNG SDS

CONTENTS

Summary

Catalyst

This report looks at the challenges for customer-facing financial services organizations in managing identities in the digital era. It goes on to consider how technology can help them address these challenges and, in doing so, present them with opportunities to streamline service delivery and improve the customer experience.

Ovum view

As ever more transactions move online, banks face a major challenge in managing the digital identities of their customers in order to verify their identity, authenticate them, and authorize access to their accounts. As they now engage with customers across multiple channels, the challenge is compounded by the need to guarantee security while at the same time providing a customer experience that is friction free. Technology can and should help address this issue, and in this context, biometrics has a growing role to play.

Biometric authentication provides strong security without the need for additional authentication methods such as one-time passwords (OTP), which the National Institute of Standards and Technology (NIST) says are inherently insecure. Biometric technology can also improve the user experience by making the authentication process frictionless and by decreasing the level of threat. It should be considered for granting access to basic services, and for the step-up authentication that is coming into play for operations that require even greater levels of security, such as fund transfers.

Samsung SDS is one vendor that offers technology to help address evolving market needs around identity and security; in addition to a discussion around market trends, an overview of Samsung SDS's offerings in this area will also be discussed in this report.

Key messages

- Friction in customer interactions must be minimized in modern omnichannel banking.
- Competition is more intense than ever, and open banking complicates matters further by greatly increasing the number of endpoints.
- Identity is at the heart of next-gen banking.
- Biometrics enable streamlined identification.

What challenges do banks face?

Modern banking is omnichannel

The days when a bank's interactions with its account holders were primarily carried out via face-to-face meetings in the branch, with occasional correspondence through the mail, are arguably long gone. In the UK, for instance, the British Bankers Association reported in 2016 that customer bank branch interactions declined from 476 million in 2011 to 278 million in 2016 – a 32% fall since 2011. At the same time, the total number of customer/bank interactions grew by 52%, largely through smartphone apps.

While this fuels an ongoing debate about the future of branch banking, there are some transactions – house purchases, for instance – for which customers will always prefer a face-to-face interaction with their bank, resulting in a need for multiple channels through which a customer can conduct business with their financial institution. As branch numbers decline, many institutions are experimenting with the use of remote video conferencing to provide a replacement for the branch interaction.

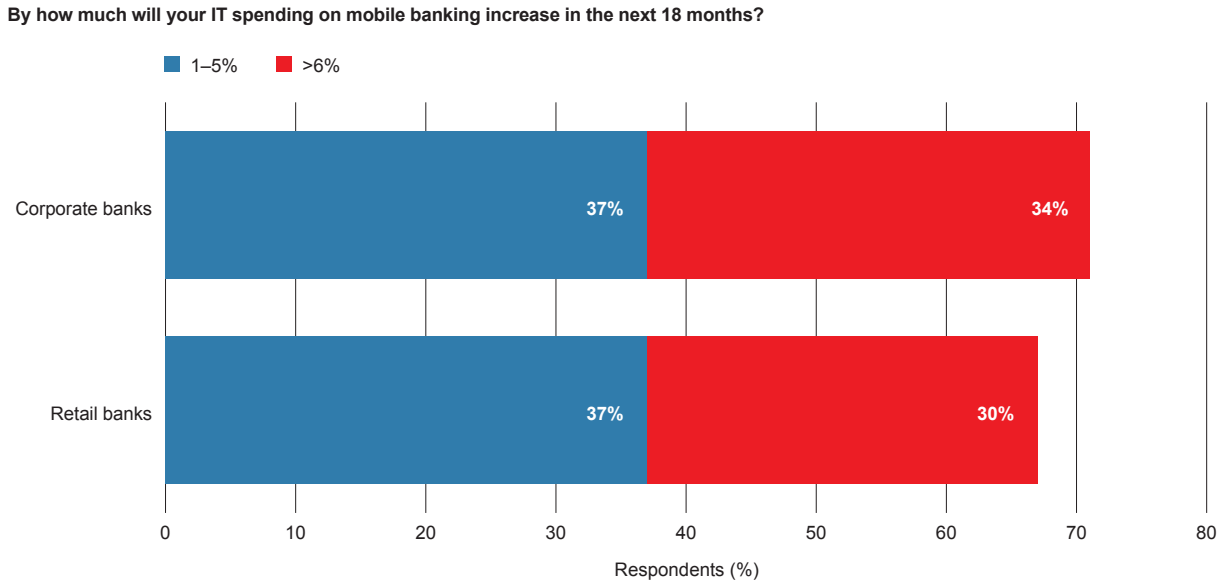
Contemporary consumers of retail financial services expect to be able to bank online (fixed and mobile), on the phone, and in some cases in the branch, presenting a challenge for the institutions in that they need to manage complex service chains across all these channels. For instance, a customer may have begun a loan application online, then made a call to a contact center (and perhaps been transferred to an account manager) for further clarification, then visited his or her branch to provide a document for identity verification.

As with retail banking, corporate banking users are increasingly using mobile devices, typically for final payment authorization, which further complicates the management of access rights.

Internationally, banks are increasing their IT budgets for projects relating to mobile banking services more than in any area other than cybersecurity. According to Ovum data, 71% of corporate banks will be increasing their spending on mobile, with 34% saying they will increase budgets by more than 6%.

Among retail banks – which have been investing in mobile for longer than corporate banks – the figures are similar, with 67% increasing budgets, of which 30% are increasing them by more than 6%.

Figure 1: Banks continue to increase their investment in mobile banking



Note: Sample sizes: Corporate 207; Retail 427

Source: Ovum ICT Enterprise Insights 2017/18

Friction in customer interactions must be minimized

Ideally, a bank should enable a user to conduct business by seamlessly moving between channels if necessary to complete a transaction. This seamless operation is critical to avoid the need for a customer to give duplicative information or re-verify their identity in one channel when this has already been completed in another channel. This is the gold standard that financial institutions try to achieve, but it requires a degree of sophistication within banking systems that is not yet commonplace.

This matter is complicated by the fact that banks often have a siloed structure in which the current checking account information resides in one database while credit card details are held in another, and contact center agents may not have access to information across all channels and services currently provided to a given account. It is, however, of paramount importance that the bank has this single view of the customer across all channels to minimize friction and deliver the best possible customer experience.

In business/corporate banking the complexity of corporate clients' account structures compounds the difficulties of having a single view of account status, for both the bank and the customer. A large multinational corporation can have relationships with dozens of banks involving hundreds of accounts.

Competition is more intense than ever

Friction needs to be kept to a minimum as a matter of course and as good business practice. This is made even more critical, however, by the growing competition in financial services of late. In recent years, innumerable non-banking institutions such as supermarkets, online payments, and money transfer platforms have all entered the market for traditional banking services such as loans, mortgages, and insurance, and by applying focus and new technology they are more efficient (Quicken Loans, Rocket Mortgage, etc.).

Other than in lending, few of these non-banking institutions have yet taken significant market share from the incumbents. The Financial Times reported in November 2017 that, for the first time, fintech lender Funding Circle lent more new money to UK small businesses than the major banks. In the three months to September, Funding Circle reported £114m of net new lending, compared to £95m by the main established retail bank lenders.

The internet, and more latterly smartphones, made it easy for banks to service their customers without operating huge branch networks. After a period when they were on the back foot while they revamped their infrastructure to support mobile banking, the banks' apps have rapidly improved in terms of user experience and breadth of service capability. The arrival of API-based open banking from 2018 will likely only accelerate this for those banks that choose to see it as an opportunity rather than a threat, and several major banking groups, including HSBC in the UK and Nordea in Scandinavia, have indicated that this is their intention.

In theory, the same technology will also make it much easier for the customer to switch banks if they are not satisfied with the products and services of their provider, but this is proving to be less attractive to consumers: although the UK's five-day automatic account switching service saw the number of customers switching accounts grow by 82% in the first 11 months of 2017, at 107,934 this is still only 0.02% of the number of active current accounts in use.

Friction in interactions increases the propensity for customers to try another financial institution, and the high abandonment rates for e-banking and e-commerce transactions indicate that there is still much work to be done to improve the customer experience. Customers require better identity verification and application process experiences, and they are showing it by taking their business elsewhere.

Open banking further complicates matters

Open banking using application programming interfaces (APIs) becomes a reality in Europe from January 2018 when the European Union's Second Payment Services Directive (PSD2) comes into force. It is likely to be followed by other countries such as Australia, which has announced its intentions to follow this route.

PSD2 creates new categories of non-bank payment service providers who will be able to access customer accounts (with the account holder's permission). These so-called "trusted third parties" (TTPs) will be able to retrieve account information, perhaps for accountancy purposes, and in some cases to initiate a payment directly from the account.

This poses enormous challenges for the banks. While TTPs will be registered with the appropriate financial regulatory authorities, the process of ensuring that a customer has given permission to a TTP creates a new onboarding process that will have to be followed by continuous checking for each transaction – is the TTP still authorized, both by the regulator and the account holder?

How banks approach this problem will vary, but automation and biometrics will both play a part here. Many banks already use biometrics for mobile banking services, and it is highly likely that they will use it for confirmation of authorization of TTP activity, but the underlying business process is not yet clear. Does the TTP tell the bank that customer A has authorized it to initiate payments from their account and then the bank asks customer A, or vice versa?

How can technology help?

Identity is at the heart of next-gen banking

The ability to verify a person's identity has always been an essential part of financial services. Now, however, it gains even greater importance as retail banking moves ever more online, while at the same time the friction in customer interactions needs to be kept to a minimum.

Technology is available to manage digital identities by providing a common back end from which customers can engage with a financial institution across its multiple channels. As well as executing identification, authentication, and authorization functions, it can hold data on the status of transactions such as loan applications, credit card issuance, and payments, and on how they have progressed. And by simplifying and streamlining the log-in process, it can help reduce friction levels.

An overview of third-wave/advanced authentication methods

Log-in processes requiring user name and password have proven increasingly easy to compromise in recent years, demonstrating a need for strengthening the authentication process. Best practice now dictates that an additional factor (or factors) be introduced to the authentication process to achieve this strengthening and increase security, a process referred to variously as two-factor or multifactor authentication (2FA and MFA). The password counts as the first factor.

There are multiple approaches to delivering additional factors, including the following:

- Smart cards: these cards contain hardware-based PKI-based digital certificates and cryptographic keys for a challenge/response-based authentication.
- Browser certificates: the software-based PKI-based digital certificates are installed in a browser – leverage cryptographic keys protected by a password.
- Hardware tokens: these are hardware devices that generate a one-time password (OTP) and are generally used in conjunction with a traditional password.
- Software tokens: typically this takes the form of either SMS-based OTPs or an OTP generator implemented as an app on a mobile phone.

Such approaches have their shortcomings, however:

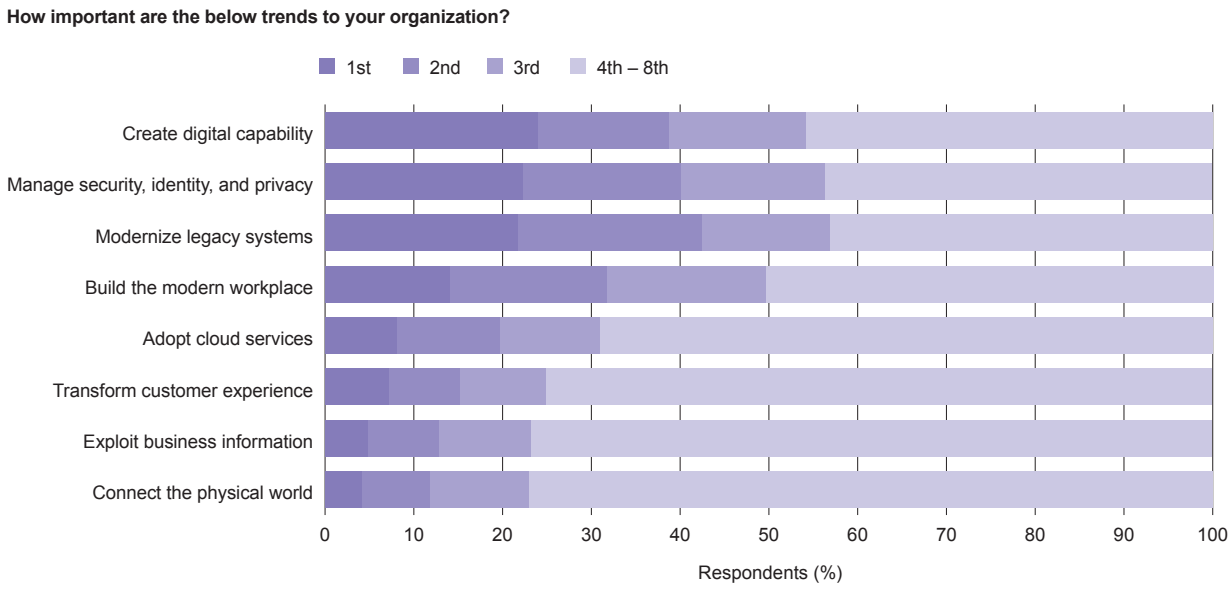
- Smart cards are expensive and require readers or drivers to be installed on a laptop machine, for instance.
- Browser certificates are not, in fact, a true multifactor solution, as the private key and password are not independent, and they are subject to brute-force attacks.
- Hardware tokens are expensive and can be inconvenient for the end user, requiring an extra log-in step as well as being a separate item to carry that can be lost or stolen. They also create questions about chain of custody.
- Software tokens present security issues related to various threats. They do not count as 2FA if the transaction is done on the same platform. For SMS the delivery mechanism is not secure.

Justifying the replacement of OTP with biometrics

Risks associated with new technologies mean that security is at the forefront of the strategic technology planning that most organizations are undertaking. Ovum's 2017/18 ICT Enterprise Insights survey showed that 40% of ICT decision-makers ranked the management of security, identity, and privacy as being a top priority (see Figure 2). The exceptional value of biometrics is that the technology can add a significant extra layer of protection without interfering with the user experience, and would in fact improve the experience.

Biometric technology has long been spoken of as another alternative to these approaches, representing the easiest and most frictionless way to add another factor, but it is only in recent years that it has matured sufficiently to be a mainstream alternative to OTP, in terms of both efficacy and cost. The FIDO (Fast IDentity Online) Alliance's specifications for a "Passwordless Experience" are strongly promoting the use of biometrics for authentication.

Figure 2: The importance that organizations are attaching to IT trends



Note: Sample size: 4,798
Vertical: All. Subvertical: All. Country: All. Enterprise size: All
Source: Ovum ICT Enterprise Insights 2017/18

False negative and positive rates have been reduced significantly, enrolment processes are now frequently passive (i.e. they require no action on the part of the end user), and costs have been brought down to more acceptable levels. For these reasons, it is now feasible to propose biometrics as a better alternative than any other two-factor authentication method.

Authentication support

Biometrics provides an evolved approach to user authentication, where instead of a password, users can authenticate using their voice, a fingerprint, or their eyes (iris). E-commerce companies and major insurance and banking institutions with an online presence are increasingly exploring how behavioral biometrics can offer an additional layer of security.

Working in tandem with step-up authentication

Particularly attractive, in the context of financial services, is biometrics' ability to serve as the additional factor for a basic level of authentication, enabling an institution to escalate the requirement – for further information or verification documents, for example – as the transaction requires additional security.

A customer may be able to get into their account to check their balance using entry-level MFA with biometrics, for instance, then if they want to carry out a fund transfer, the system can trigger a further challenge, which may require a knowledge-based answer or even an OTP sent to the customer's mobile.

Continuous authentication

Looking forward, Ovum sees biometrics being increasingly used in a more continuous, always-on fashion that takes it beyond authentication support at the point of access. This practice is referred to as continuous authentication and essentially constitutes a next wave of security around identity. It involves using behavioral biometrics to track the way people interact within a session to see if this behavior is consistent with appropriate human interaction or with the previous response patterns of that individual.

In addition, the use of digital identity verification prior to authentication will help the financial institutions streamline the process of verifying a customer's identity at the beginning of the onboarding process. Finally,

digital collaboration in customer onboarding will help to greatly reduce the friction that financial institutions experience when onboarding new customers and improve the overall customer experience.

Biometrics in corporate banking

Biometrics presents a greater challenge for business banking because of customer complexity. Customers will have multiple accounts that are accessed by multiple staff members – sometimes in different locations – and these will have a hierarchy of authorization level. Typically, there will be a group of staffers in the client operation creating payment instructions, with rules on how much each can authorize and an escalation process. Managing these mandates and control levels creates a complex process, raising a number of questions: Where does the security fit in? At the bank or the customer? Both?

One obvious problem when dealing with teams of people involved in a process is the tendency towards password sharing and the risks this practice poses for security, with the potential for passwords to fall into the wrong hands increasing exponentially. Biometric authentication, as well as continuous authentication using biometrics, is a means of overcoming such risks, as the need for passwords can be obviated altogether by introducing such next-generation approaches.

Any viable identity verification approach must take that into account. Moreover, it must be flexible enough to allow changes to the authorized persons list in the event of staff changes, holidays, and illness.

The exceptional value of biometrics is that the technology can add a significant extra layer of protection while at the same time helping to improve the user experience.

Onboarding can be made easier with video and chat

Another area that can be simplified with the right technology is customer onboarding. Traditionally laborious, paper-based processes, often carried out at home with no one to consult when working through a form, can be made easier and more pleasant with technologies such as secure video and chat, enabling bank officers or contact center agents to help the customer through the enrollment process. It is worth noting, however, that customer habits and preferences will vary, and some customers may not want to engage via video. Some customers would prefer self-enrollment solutions, so technology adopted in support of any initiative should offer a range of different capabilities. This help may be for completing the form, or even filling in the form on the customer's behalf, with a signature being supplied digitally (if legislation permits in a given country) or at the branch once the form itself is completed.

What does Samsung have to offer?

Samsung SDS

Samsung SDS is the enterprise IT solutions and services arm for the Samsung Group that has, for over 30 years, provided IT consulting and services to its partners and customers. Samsung SDS comes from a systems integrator (SI) background and, leveraging the SI experience, the organization has built an enterprise software and service portfolio. The company offers a range of capabilities that can help organizations to both manage digital identities and secure and manage the ever-increasing estate of mobile devices and apps being utilized in the workplace.

Samsung SDS Nexsign

Samsung SDS Nexsign is a biometric authentication platform that can help make the authentication experience easier and more seamless for users while also strengthening security around it, especially when utilized as part of multifactor authentication. It enables users to authenticate using their biometric data, such as fingerprint, face, voice, or iris. Other functions offered that help enforce security include liveness checking, secure screen blurring, and voice authentication for wearables. Samsung SDS Nexsign also offers multitenancy support and has secured Common Criteria Certification (EAL2) for its FIDO UAF Server (V1.1). Samsung advises that more than 3 million people use Samsung Pay on Samsung Galaxy phones, and Nexsign provides approximately 10 million authentications a day to Samsung Pay and Samsung Pass. This demonstrates how enabling the solution is, even at great scale.

Figure 3: Samsung SDS Nexsign

Source: Samsung SDS, 2017

FIDO certification

Samsung SDS Nexsign is certified by the Fast IDentity Online (FIDO) Alliance – an industry consortium that since 2012 has promoted interoperability between strong authentication systems via security specifications and open standards. FIDO is based on public key cryptography, which stores biometric data only on the device and not on a server, meaning user biometric profiles do not travel over a network – something that could potentially make them vulnerable to a man-in-the-middle attack. Financial services firms are increasingly leveraging this type of biometric authentication capability to protect sensitive data and

information while also delivering a more user-friendly way of authenticating around activities such as payments, logins, and money transfers via mobile banking.

Samsung SDS partners with BioCatch for enhanced biometric authentication and continuous monitoring capabilities

With a view to expanding the capabilities of its authentication platform, Samsung SDS recently announced a partnership with specialist behavioral biometric solution provider BioCatch.

The partnership will see Samsung SDS and BioCatch offer a solution that continuously monitors users' behavior patterns post login and then generates a score reflecting the perceived trustworthiness of a user session. As different people interact with technology in different ways, the solution can use invisible challenges to determine, via behavioral analysis, whether the user is genuine or potentially a bot or imposter. For example, the solutions will come to understand how a user types on a mobile device, and should deviation from the usual behavior occur, a challenge or security alert can be issued. The behavioral biometrics run in the background and biometric characteristics can also be combined to provide more comprehensive levels of security.

Technology such as this plays a key role in improving fraud and malware detection in the financial world, but it also has value to organizations in other verticals that require an equally high level of security. Regardless of the industry a company operates in, adopting technology that can help achieve an optimal balance between security and enhancing the user experience is important.

Providing a more secure and intuitive ATM experience

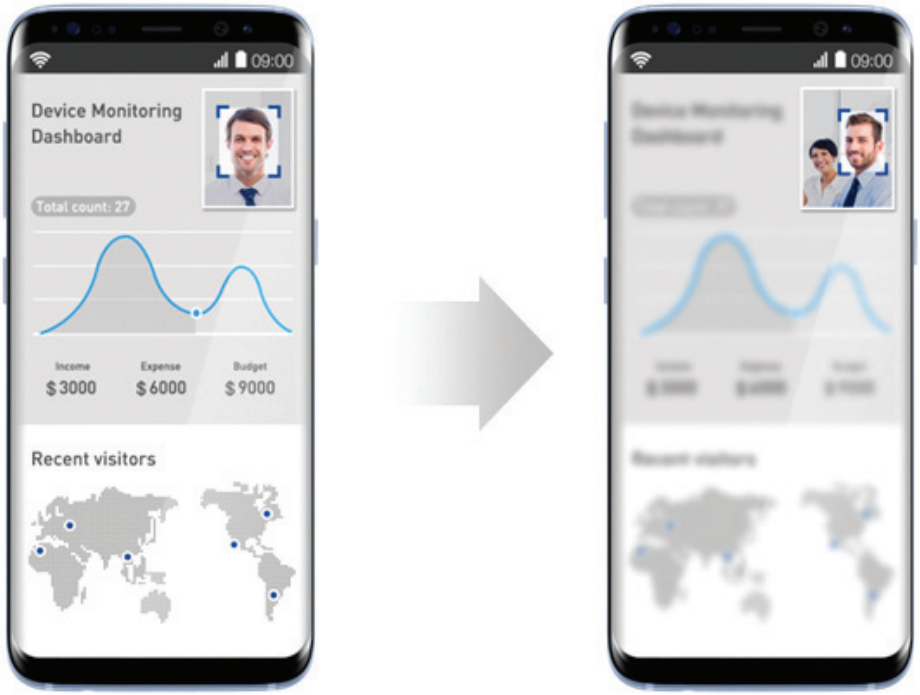
Another partnership of note forged by Samsung SDS is with Diebold Nixdorf, a company that provides financial self-service systems, such as ATMs. Together, Samsung SDS and Diebold Nixdorf have developed a mobile-based biometric authentication solution that can enhance ATM transaction security and enable cardless and pinless transactions leveraging Nexsign capabilities. The combination of Samsung SDS's Nexsign and Diebold Nixdorf's Fusion technologies enables mobile banking customers to pre-stage ATM transactions via their mobile banking application and then, using near-field communication technology or QR codes incorporated on an ATM, withdraw money post a biometric authentication process, such as via facial recognition. Using biometrics in this fashion is appealing as it is convenient and quick for users, while also being secure in bypassing the need for a PIN or a card.

Protecting sensitive business information with biometrics

Apps are a fundamental element of any mobility strategy, and mobile apps are presenting users with new ways to interact with important business systems, delivering new opportunities for innovation and business process optimization. Users are increasingly demanding more mobile-optimized experiences, and apps are essential to delivering against this mandate, but mobilizing legacy systems and applications can be challenging.

- **CA Technologies**. A recent partnership forged between CA Technologies and Samsung SDS will see CA integrate Nexsign biometric capabilities with the CA Mobile API gateway – a solution that secures and manages enterprise-level mobile APIs – to improve the user experience and add another layer of security.
- **Thomson Reuters**. Another interesting use case is how Nexsign can be used to protect individual documents, such as email attachments. Should an attachment contain sensitive information, Nexsign can be used to provide an additional level of security, meaning access to an attachment can only be granted post biometric authentication – via a facial scan, for example. Thomson Reuters has also leveraged Nexsign to protect work screens, meaning that if authentication failed based on biometric modalities, a display screen would be blurred, thus preventing unauthorized parties from viewing sensitive information. An example of this capability can be seen in Figure 4.

Figure 4: Samsung SDS screen blur capability



Source: Samsung SDS, 2017

- **Moxtra**. Samsung SDS has demoed what it calls the "bank branch of the future" in partnership with Moxtra at Money 20/20 in 2017. As part of this collaboration, Samsung tablets are equipped with Moxtra's secure collaboration tools (e.g. secure video, e-form, e-signature) and are coupled with Samsung SDS's Nexsign biometric authentication technology to provide banks with a secure way to onboard customers and maintain ongoing engagement.

Samsung Secure Mobility Suite

In addition to the digital identity partnerships mentioned, Samsung also offers enterprises an enterprise mobility solution in the form of the Samsung Secure Mobility Suite. The Secure Mobility suite is comprised of Samsung mobile and wearable devices, secured with EMM and Nexsign authentication, services, and support. Nexsign also supports voice authentication on Tizen wearables. This suite can help financial institutions implement "tablet branches" and bring in-person services to their customers anytime, anywhere – all while fully securing sensitive enterprise data.

Biometric authentication and blockchain

Samsung SDS has also combined both Nexsign biometric authentication and its Nexledger blockchain solution to deliver mobile customer authentication between Samsung Card (a major Korean credit card company) and their registered partner affiliates. Samsung SDS advises that Nexledger's time-stamping solutions helped eliminate the third-party data leakage risk while reducing the cost of customer acquisition by 35%.

The combined application of Nexsign and Nexledger offers three advantages: transaction transparency, storage security, and scalability through leveraging mobile devices. The combination can help enable financial institutions to access customer data without additional infrastructure while also addressing some roadblocks of blockchain adoption. It eliminates identity processing capacity issues, improves operational management monitoring, and reduces issues with time latency. For example, conventional Bitcoin block generation takes 10 minutes, while Samsung SDS Nexledger can complete block generation in one second.

Conventional Bitcoin transaction confirmation usually takes 60 minutes, but Samsung SDS Nexledger executes this confirmation in real time.

Blockchain-based PKI authentication allows customers to configure and store biometric data securely on mobile devices, while registration data, public keys, and authentication history are securely stored on blockchain networks. In addition, customers can configure their own privacy controls, allowing them to authorize and select how they share identity information. Usability and convenience can also be optimized as customer identification data is seamlessly shared with affiliates. The customer is no longer burdened with having to install additional apps from different service providers. From the perspective of the financial institution/affiliate, this can also help reduce abandonment rates and preserve affiliate relationships.

Samsung SDS Nexledger and Nexsign were also deployed by the Korea Federation of Banks (KFB), consisting of 16 major banks representing 90% of the Korean banking market (in a joint authentication system).

Adopting a more advanced authentication approach is becoming increasingly important for organizations across industries

With ever more customer interactions with financial institutions moving online and the customers themselves now rarely if ever going into bank branches, the need to authenticate them reliably becomes increasingly critical. Meanwhile hackers and other threat actors have grown more sophisticated in their modus operandi, a scenario that calls for more advanced forms of authentication.

Additional factors beyond user name and password are now required to help verify identities, and while one-time passwords have been championed in that role for a number of years, biometric technology now provides a more guaranteed, tamper-proof alternative. Indeed, its ability to underscore behavioral biometric monitoring makes it the basis for the continuous authentication approach that is gaining currency as the future of authentication.

Appendix

Authors

Rik Turner, Principal Analyst, Infrastructure Solutions
rik.turner@ovum.com

David Bannister, Principal Analyst, Ovum Financial Services Technology
david.bannister@ovum.com

Adam Holtby, Senior Analyst, Workspace Services
adam.holtby@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

ABOUT OVUM

Ovum is a leading global technology research and advisory firm. Through its 180 analysts worldwide it offers expert analysis and strategic insight across the IT, telecoms, and media industries. Founded in 1985, Ovum has one of the most experienced analyst teams in the industry and is a respected source of guidance for technology business leaders, CIOs, vendors, service providers, and regulators looking for comprehensive, accurate and insightful market data, research and consulting. With 23 offices across six continents, Ovum offers a truly global perspective on technology and media markets and provides thousands of clients with insight including workflow tools, forecasts, surveys, market assessments, technology audits and opinion.
In 2012, Ovum was jointly named Global Analyst Firm of the Year by the IIAR.

For more details on Ovum and how we can help your company identify future trends and opportunities, please contact us at marketingdepartment@ovum.com or visit www.ovum.informa.com. To hear more from our analyst team join our Analyst Community group on LinkedIn www.linkedin.com/company/ovum and follow us on Twitter www.twitter.com/Ovum.

SAMSUNG SDS

ABOUT SAMSUNG SDS

Founded in 1985, Samsung SDS began as the ICT arm of the Samsung Group, and is now a global IT solutions and services provider with presence in 30 countries. Its business areas span IT and cloud services as well as enterprise solutions. Using advanced analytics platforms, AI, and blockchain technologies, its solutions serve a diverse range of industries, including financial services, smart manufacturing, global logistics, and retail. The vision of Samsung SDS is driven by a desire to get to the core of problems, leveraging the most advanced ICT technologies and solutions to discover actionable insights.

For more details on Samsung SDS, please visit www.samsungsds.com. To learn more about our solutions, visit our YouTube channel www.youtube.com/samsungsds. Also, join us on LinkedIn www.linkedin.com/company/samsung-sds and follow us on Facebook www.facebook.com/samsungsdsglobal.