improve
the user experience
with a trusted authentication

Worldline

Improve the user experience with a trusted authentication

The Internet and mobile terminals are powerful tools for driving global commerce

Online banking, electronic and mobile commerce, and the use thereof on mobile endpoint devices have grown substantially over the past years. Consequently, authentication services are becoming an important security differentiator on the market: trust is hard to gain but easy to lose.

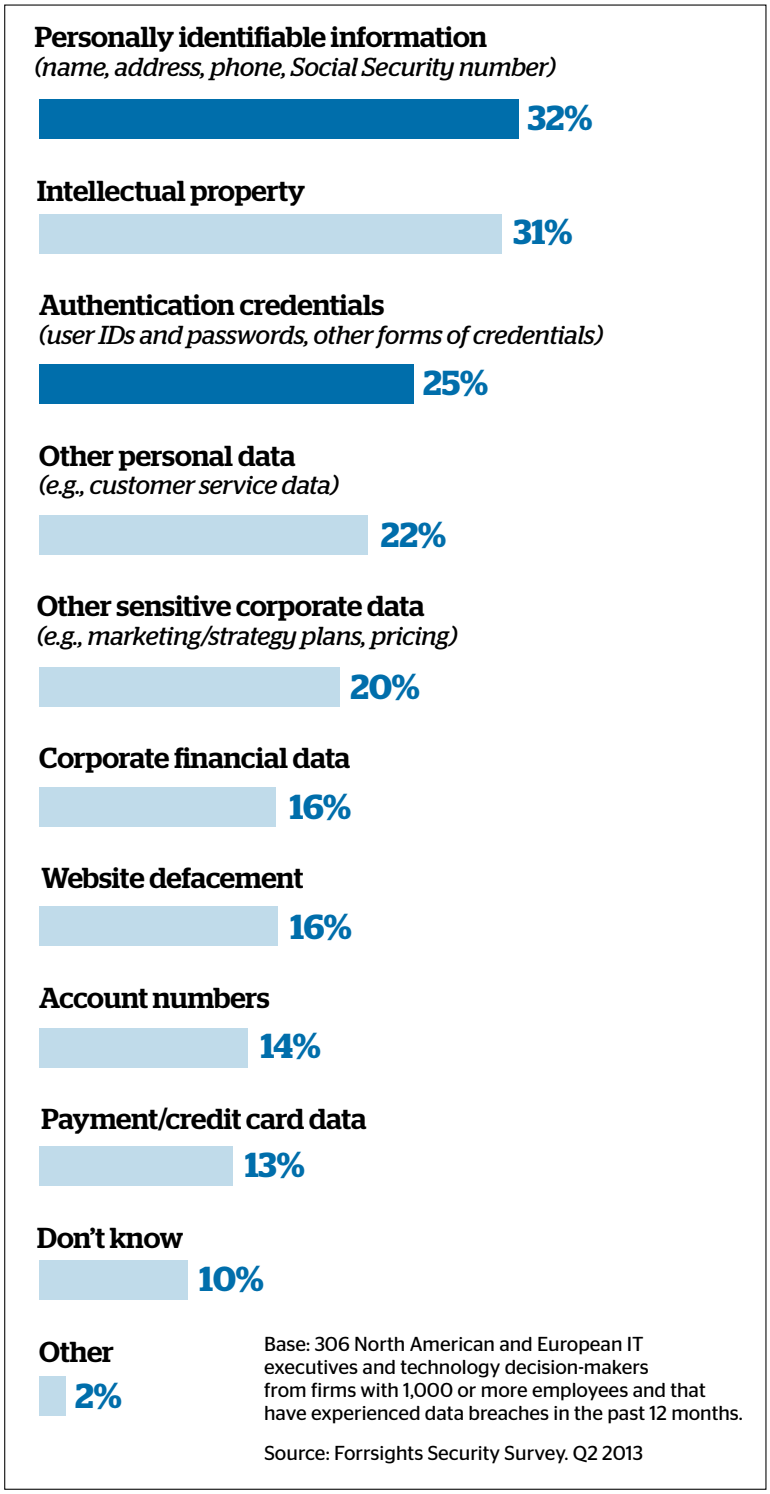
This position paper examines the key challenges on the user authentication market (B2C and B2B) – whether the service is used to provide payment wallets (online and face-to-face), home banking access, digital signatures or validation of users' sensitive operations.

Connected devices, cloud services and big data are driving the transformational process of the commerce world, generating opportunities and concerns for all the participants in the ecosystem.

Consumers demand increased mobility and connectivity while worrying about the safety of their transactions and the privacy of their personal data. Issuers and merchants are concerned by the risk of fraud and the additional costs incurred because of security requirements and compliance.

For a long time, security was not publicly discussed. It has been brought into the limelight in recent years, when major data breaches showed that the current data protection and authentication methods had gradually become outdated in a world that changes visibly every day. New trusted authentication methods are needed quickly in order to limit vulnerabilities.

Type of data potentially compromised in the past years



Base: 306 North American and European IT executives and technology decision-makers from firms with 1,000 or more employees and that have experienced data breaches in the past 12 months.

Source: Forrsights Security Survey. Q2 2013

Advanced authentication methods balance security and usability

- User authentication has been present since the early days of the digital world. Initially, it was seen as a "one-time operation" that was necessary to log in to a specific system or device. The methods typically focused on security, beginning with simple passwords and evolving towards hardware tokens (RSA SecurID OTP) or PKI smartcards.

- Later, the devices that end-users adopted became more diversified, including, among others, mobile phones.
  New authentication methods became possible. The most common ones included SMS OTPs, mobile apps with software-based OTP tokens or multifactor authentication using OOBA (Out of Band) methods. Although these methods have improved the user experience, the latter needs to become better and better as new technologies are becoming available.

- The latest trends in authentication methods focus on the smartphone, which is seen as a box full of sensors. Within the next years, biometric, contextual or inferential authentication methods will appear on the market.

- These new challenges force all players to invest in cutting-edge trusted authentication methods that ensure the openness, scalability and interoperability of the system to achieve perfect balance between strong security demands, user convenience and mass distribution.

Challenge 1: Maintain a high level of security in complex and often non-secure environments

Securing interactions with end users on multiple devices

Nowadays, securing interactions with end users is a real challenge, but it is crucial to deliver trustworthy services to the market. Pure hardware solutions are not suitable for customers' mobility requirements. Solutions based on mobile network authentication are often unavailable outside the Telco domain or are limiting the scope of the deployed solutions. Additionally, device manufacturers have failed to reach a critical mass in the deployment of devices accepted as trusted environments. Consequently, in most cases, credentials cannot be stored securely on these devices. Service providers have to rely on software solutions, but the actual Operating Systems were not designed for payments, and unsafe user behavior makes things even more complex. Since the security best practices defined by regulatory bodies often lack precision, the responsibility for ensuring the security of mobile applications is too often left to banks themselves.

What is our recommendation concerning this challenge?

- State-of-the-art solutions rely on high-technology software that is deployed on the device and constantly communicates with a server in real time. The proof of device ownership is based on a PIN and "device fingerprinting" techniques.
  Protection is provided by "tamper-resistant" techniques. The solution should cover all OSs and has to be designed for multiple devices. Moreover, connectivity between multiple devices should be used to reinforce security.
  The entire range of security attacks related to Internet and mobile terminals has to be taken into account: MITD (Man in the Device), MITM (Man in the Middle), MITB (Man in the browser), DOS (Denial of service), phishing, etc...

- Privacy data have to be kept anonymous and protected inside the digital device and avoid to be frequently transferred and stored in unsecure places.
  The key element to achieving this is the use of state-of-the-art cryptography techniques, dynamic virtual keyboards for PIN operations or PCI-DSS-compliant platforms.

Operation and interconnection with untrusted parties' environments

In the new competitive environment, the risk for issuers is to be reduced to back-office utilities by the new entrants on the financial market, while the latter become the new faces of their customers' financial lives.

Issuers cannot respond to these threats simply by "increasing digitization," (e.g. providing online banking services or digital payments). They will need to be part of consumers' commercial lives by enriching their offerings with Value-Added Services.

Such changes result in greater interconnectivity with third-party systems, dealing with external application users, hosting of multiple applications, and an increased number of untrusted channels and devices used to access these applications.

What is our recommendation concerning this challenge?

- The risk can be reduced by implementing "holistic" multilayered authentication. The regular authentication methods should be enriched with tokenization for certain situations (e.g. payment wallets), and with effective fraud tools. These tools will assess the risk of misuse, thus acting as a first line of defense in order to filter out illegitimate users before focusing on the unique identification of honest customers.

- In an increasingly connected world, risks occur in real time. Authentication service providers need to adapt their processes and capabilities to provide cross-domain cyber intelligence. They need to capture huge amounts of transactional data as well as "users on the go" data coming from a variety of channels and devices.

- In the absence of global specifications or certifications for authentication services, issuers have to create their own security standards. They have to rely on flexible, compliant, auditable service providers. These providers will have to comply with the existing standardization initiatives (e.g. Fast Identity Online Alliance FIDO, Natural Security Alliance NSA and Open Authentication OATH). Domestic and European regulation bodies have already been issuing recommendations for the use of strong authentication services for high-risk user operations (e.g. the SecurePay forum recommends the deployment of cardholder authentication for Internet payments by 1/2/2015).

Challenge 2: Foster adoption and usage by gaining users' trust

Strategize to gain trust

Associating authentication with security is common, but trust, which is the equivalent of security from an end-user's perspective, is much less talked about. Although they are two sides of the same coin, both concepts are not always linked: users can trust a solution even if it is not secure while they do not always trust a secure solution.

Trust and convenience are the two pillars that influence users' habits and incite them to adopt new products.

1 A three-step approach to gaining trust

What is our recommendation concerning this challenge?

- **Design:** products have to be perceived as easy-to-use during the entire customer journey: from user onboarding, login, multi-account management and validation of sensitive operations. During every user interaction, issuers have to reassure the users about the safety of their solutions (e.g. context reminder display, sound alerts when a payment transaction is approved, dynamic virtual keyboard, and real-time multi-device authentication).

- **Educate:** after designing trustworthy solutions, issuers have to communicate and educate users on how to use their products securely. End users have to be provided with all the necessary information on how to protect their passwords or manage their devices properly (e.g. downloading and keeping security packages up-to-date).
  Clear instructions have to be provided about how to act in case of suspicious activities, lost/stolen mobile phones or unusual activity on computers or tablets.

- **Respect privacy:** as we are moving more and more towards seamless, more privacy-invasive authentication methods, where the user is authenticated through deduction and not on what they know or have, a proper level of transparency has to be maintained with regard to the use of private data.

- Issuers have to choose service providers who are constantly developing solutions with this goal in mind (e.g. use of adaptive authentication i.e. involving the use of a limited subset of relevant contextual data instead of full contextual data).

2 Convenience through improved consumer experience

With e-commerce becoming m-commerce, smartphone-as-a token is now a well-established authentication method.
Today, we cannot expect all population segments to be ready to use them on daily basis, but when this is the case, smartphones can provide considerable advantages by improving the user experience.

Some of the previous concerns (like the mobile terminal not being in a legitimate user's possession or the guarantee that the device is kept locked all the time) can now be mitigated through biometric features [e.g. face and voice recognition, interface interactivity (e.g. typing rhythm), fingerprint, passive biometrics (face topography & iris structure), blood vein authentication].

What is our recommendation concerning this challenge?

- Biometrics can create a better user experience, despite the fact that not all the solutions available on the market are 100% foolproof. Methods based on fingerprint and voice recognition seem to be gaining popularity.
  Evolutions of the biometrics market also depend on mobile device manufacturers and their mass deployment capabilities.

- Like contextual or inferential authentication methods, biometrical methods can be rejected by certain users who fear profiling, tracking and privacy intrusion. Careful segmentation of use cases and scope limitations (device or application unlocking), and use of trust elevation can offer viable options without damaging the overall user experience.
  The solutions have to guarantee adaptability and make sure that they take advantage of the rapid evolution of device capabilities, e.g. Trusted Execution Environment. The universality of the solution becomes a major criterion not only for including all devices and OSs, but also all browsers and in-app uses.

Challenge 3: Choose a trusted partner with a proven track record

A recent analysis by Gartner found that over 200 providers provide some kind of user authentication services worldwide, but fewer than 50 of them offer credible solutions.

Pay less for the same security and user experience

What is our recommendation concerning this challenge?

- Consumer authentication is a pivotal service for a varied range of products used in the retail and banking worlds. Issuers are challenged to be innovative in creating business-enabling security solutions with positive impact on revenues.

- Software Secure Element (SSE) solutions offer more sustainable business cases as they are eliminating the deployment and maintenance costs incurred with traditional hardware solutions. They also respond better to today's deployment trends such as embedding applications in the mobile through SDKs (Software Development Kits), APIs (Application Programing Interface) or SaaS (Software-as-a-Service) solutions.

- Providers have to be able to deliver industrialized solutions (strong SLAs commitments, scalability, flexible releases and regular audits) while maintaining the highest level of security (multisite instances, disaster recovery plans and proper procedures for operation traceability, ongoing risk mitigation).

- The authentication service provider has to be capable of offering packaged solutions for all use cases that will guarantee better time-to-market and lower integration costs, either through continuous R&D projects and innovative roadmaps, or partnerships.

- Paying attention to privacy and data protection laws is critical as commerce becomes more and more international. Handling data from many countries and regions can become complex for service providers who are only used to deal with domestic deployments.

Security and Trust Services for the businesses

- **Distribution to banks' corporate clients:** the access control and validation of the sensitive operations on distributed PC and connected devices (mobile phones, tablets, etc.) have to take into account the entire range of constraints of the deployed proxy solutions available on the market. It has to enable the company's network administrators to validate and authorize the enrollment, and to manage the user hierarchy and life cycle properly.

- **Distribution to bank's employee:** the solution has to enable to all of a business's branches to improve local services, particularly on their premises. The solution should be compatible with all VPN solutions existing on the market and with protocol standards such as SAML, OATH, and FIDO. It has to provide efficient multi-user management for employees equipped with smartphones, tablets and other devices.

With these recommendations, you will be able to choose the right partner for authentication in paying attention on a numerous of aspects:

Security and fraud risk management
User adoption thanks to trust and convenience
Reliability and sustainability of the target solution

With more than 10 years' experience and expertise in the authentication field, Worldline is positioned as your competent business partner to discuss the challenges, and propose you the adapted authentication method according to your services.
Worldline has developed Trusted Authentication solution to meet today's and tomorrow's needs.
It is a scalable software-type strong authentication solution intended for banks and any type of organization that needs to make remote access secure for its users. For more info, **worldline.com**.

About Worldline

Worldline [Euronext: WLN] is the European leader in the payment and transactional services industry. With innovation at the core of its DNA, Worldline's core offerings include pan-European and domestic Commercial Acquiring for physical or online businesses, secured payment transaction processing for banks and financial institutions, as well as transactional services in e-Ticketing and for local and central public agencies. Thanks to a presence in 30+ countries, Worldline is the payment partner of choice for merchants, banks, public transport operators, government agencies and industrial companies, delivering cutting-edge digital services. Worldline's activities are organized around three axes: Merchant Services, Financial Services including equensWorldline and Mobility & e-Transactional Services. Worldline employs circa 11,000 people worldwide, with estimated pro forma revenue of circa 2.3 billion euros on a yearly basis.

Financial Processing & Software Licensing

Financial processing provides banks and other financial institutions with a comprehensive set of services to help them and their customers manage their cashless payments. Our services and innovative software solutions support the full range of card and non-card payments for acquirers and issuers. By combining our core services with a growing list of value-added services and full integration with in-house systems, we help our clients offer their customers a customised, profitable, secure, extensive and innovative product portfolio.

For further information
infoWL@worldline.com