How to build trust in online services

Interview with Guillaume Yribarren, Vice President Marketing Digital Security and Authentication at Safran Identity & Security

PAYMENT

POSTED ON 12.13.16

For banks, retailers, social networks and online services the digital transformation is picking up momentum and opening up opportunities in terms of more efficient processes and new added-value services for citizens and consumers. Yet the success this transformation, regardless of the size of the business, will depend on customer acceptance, and ultimately user trust.

Does the end user already trust online services and digital transactions?

GY: Going digital offers incredible prospects for creating new services based on convenience. However, end users must trust these systems in order to adopt them wholeheartedly. Clearly they are confident about online transactions: worldwide retail ecommerce sales will reach $1.915 trillion this year, with double-digit growth that will continue through 2020, when sales will top $4 trillion (eMarketer). And end users are ready to take calculated risks when they believe the benefits – time and money saved and greater convenience – outweighs the probability of fraud. That's why they usually prefer to deal with major brands they trust.

Nevertheless, large-scale security breaches that affect even big players such as Yahoo and Twitter may affect user confidence and hamper the development of online services and transactions. Furthermore, the development of mobile usage (now representing 65% of digital media time, according to comScore) poses a tremendous challenge to security, since mobile devices are open environments supporting different applications that are difficult to secure and inherently vulnerable owing to this versatility.

To support online service providers from all sectors in offering solutions users can trust, Safran has developed a Digital ID & Transaction Platform. Which functions does it have? And what are typical use cases for it?

GY: The Digital ID & Transaction Platform has all the functions necessary for a secure, end-to-end digital journey:

- Identity proofing and verification
- Adaptive authentication (biometrics, mobile, etc.)
- Transaction security guaranteed by a digital signature
- Mobile payment
- Legally binding archiving

For example, "not-yet-customers" are able to register for an account by using nothing more than their smartphones. They use their phones to register their personal and biometrics data, then prove their identities by taking a selfie and a

picture of their passport data pages or ID cards and supporting documents.

All the other steps required to create a customer account are handled by the Digital ID & Transaction Platform. Data is acquired and a background check is completed to verify the identity's uniqueness and the user's eligibility.

In another example, banks can suggest that customers sign for contracts (loan and savings contracts or life insurance) using tablets. The bank can also offer its customers a mobile wallet, enabling them to pay securely with their mobile phones both in stores and online.

You mentioned "adaptive authentication" as one of the Digital ID & Transaction Platform's functions. What different ways to authenticate end users will the platform offer?

GY: Our platform provides "intelligent" authentication, meaning that it combines versatile authentication with risk-based authentication. End-users can authenticate themselves among a wide range of possibilities (mobile, biometrics, SMS OTP, certificates, etc.) depending on the context and the risk of each transaction, according to the risk policy defined by the service provider.

For example, if a grandparent is accustomed to transferring money to his or her grandchild every month, an authentication with a low level of security such as login/password (defined by the risk policy established by the bank) is sufficient, and no further action is required. However, if the same grandparent, who rarely travels, suddenly logs in from a new country Russia and wants to transfer money to a new beneficiary, then we are probably dealing with a fraudster. The user is then prompted to perform a higher level of authentication, such as our Cloudcard+ solution, a two-factor authentication method based on a mobile phone ("what I have") and facial recognition ("what I am").

This risk-based approach lowers the burden on legitimate users while keeping fraudsters at bay, and strikes the best balance between security and convenience.

Where is the platform in use?

GY: Our Digital ID & Transaction Platform has proven its worth in a variety of contexts, in both public and private sectors (banks, retailers, industry) for more than 15 years to ensure the security and trust of their digital transformations.

Today we are offering new approaches to delivering trust functions through self-service API (application programming interface) in order to make deployment simpler and easier and accelerate go-to-market. We are also working on a mobile-first approach, before designing it for the desktop or any other device, now that mobile usage exceeds PC usage.