**Q&A: What consumers really think about Trusted Digital IDs**

*Last updated: 12 March 2020*

Digital identities are an intrinsic part of the online user experience. Today, most consumers own many digital IDs that consist of different username and password combinations to access all kinds of online services, from email, shopping or streaming accounts to online banking, social media or eGovernment services. These IDs are usually a disparate collection of different components – for example, some will use full names, some will use email addresses, and some might only be based on a nickname or pseudonym.

These digital IDs, at present, will also have their own ways to verify that the user is who they say they are during the digital enrolment and the authentication phases. When dealing with online services, particularly highly sensitive ones like online banking or eGovernment services, having a [Trusted Digital ID](https://www.gemalto.com/mobile/id-security) –- enhances trust, improves the customer experience and reduces fraud. A Trusted Digital ID is created when the information provided has been verified, or checked for authenticity.

We polled more than 800 consumers from eight countries around the world to find out what their attitudes and expectations towards Trusted Digital ID, enrolment, security, authentication and customer experience are.

In this blog, I am joined by my colleague Pauline Pinzuti, Marketing Manager, as we discuss some of the key findings from the survey.

**How often do consumers use digital IDs and have they had their credentials and personal information compromised?**

**PP:**Our study showed that more than half of global respondents who log into online services by typing in their credentials every time they open the app/ website do it at least five times a day. And still, nearly half of them have declared they had experienced some security and privacy issues such as having their personal data (name, date of birth, etc.) stolen, their credit card information compromised, or their social media account broken into.

**DB:**These results show us that convenience and security are the key considerations among consumers that regularly log into online services, meaning that there is an appetite for a universal convenient and secure solution that provides quick and easy access to mobile apps and websites – Trusted Digital ID.

**Was there discrepancy between consumers’ definition of the term ‘digital ID’ and how it is defined among experts?**

**DB:**We were pleased to find out that nearly a third of global consumers have a clear understating of what a digital ID is; however, in order to make the case for the importance of the adoption of Trusted Digital ID on a global scale, consumers must be able to clearly define the concept. And we believe that [MNOs and OEMs](https://www.gemalto.com/brochures-site/download-site/Documents/tel-trusted-Digital-ID-Technology-for-MNOs.pdf) have a special role to play as they not only have a close relationship with their customers, but also have access to large amounts of customer data that can be used for personalized services. For instance, they know the types of accounts consumers have (prepaid or postpaid), their mobile devices, including their usage record, location information etc. Obviously, this information should be used whilst meeting privacy and data protection regulations.

**What type of organizations do consumers trust the most in order to have their Trusted Digital ID created?**

**PP:** The creation of a secure digital ID needs to be done by an organization that is trusted by consumers, as reflected in our survey. Overall, respondents have declared four organizations as the most trust-worthy: starting first with banks (more than half), followed by the government , consumer tech companies such as Samsung and Apple, and MNOs; meaning that they’re in a good position to become the trusted providers of digital IDs for their customers and help for the global adoption of this service. By extension, a mobile network operator working with a third party that delivers secure services to banks and governments, can be trusted to become the main provider of Trusted Digital IDs.

**What type of data are consumers willing to share in order to have their trusted digital ID created?**

**DB:**To be able to create secure digital IDs, banks and MNOs alike need data. But to be willing to share their data, consumers need to know what information of theirs is stored, and how it is protected and used. They also need to have control of their data by being able to give consent for its use and manage its privacy options.

Nearly half of global consumers are open to sharing their biometric data in order to have their Trusted Digital ID created. This acceptance of biometric attributes by end-users, which are used as the foundation for Trusted Digital ID, is seen as a global trend. Nevertheless, each country has its specificity and regulations which would impact how biometrics is handled when not in possession by the end-user.



Representation of Trusted Digital ID services platform

**Did you come across any specific consumer perceptions about digital ID authentication and security? What are the benefits that consumers recognize from having this service?**

**PP:**Our survey found that globally consumers have three main security concerns with regards to digital IDs: having their personal data stolen (67%), sharing personal details such as date and place of birth with third parties (36%) and not having control over who has access to their digital ID (35%).

This is certainly one of the reasons why when asked if they would be ready to pay for more security, half of respondents globally have said that they’re willing to pay a premium for a service that guaranteed secure access to online services with the use of their Trusted Digital ID. This score reached peaks in regions where consumers experience fraud the most. Security is selected as the biggest benefit of [**Trusted Digital IDs**](https://www.gemalto.com/mobile/id-security) by nearly half of global respondents.

**DB:**Security must be at the center of any digital identity system. Consumers using online services need to be guaranteed security as they share personal information such as names, address and payment information. Robust security measures will be the obvious response to consumer and regulatory demands for trust in all exchanges between users and private organizations such as MNOs and OEMs.

[Biometrics](https://www.gemalto.com/biometrics) is one of the verifiable security attributes used in the creation of trusted digital IDs, enabling seamless user experience while also deterring fraud. Globally, consumers are open to using a form of biometrics for authentication with fingerprint (more than half) being the most popular factor, followed by [face](https://www.gemalto.com/review/facialrecognition/index.aspx), iris and voice. This is not surprising as these first two types of authentication have already been made mainstream by their use within smartphones.

**Looking into the near future, how comfortable do consumers feel with having their identity stored on their mobile, and how do they feel about being authenticated based on behavioral biometric factors such as the way they walk or type on their keyboard?**

**DB:**Nearly sixty percent of global consumers think that having their passport, national ID card or driving license stored securely on their [mobile](https://www.gemalto.com/mobile/id-security/mobile-id) is a good idea, which is a very promising response. But in order to make consumers feel comfortable with having their IDs saved down on their mobile, organizations such as MNOs and banks need to ensure that sensitive data is secured through various means such as a tamper proof hardware.

**PP:** Recently, we’ve seen an explosion in new technologies built on passive behavioral authentication, meaning that this type of authentication will soon become quite normal. When we asked global consumers how they would feel about being authenticated by a combination of factors including the way they walk, the tone of their voice, the way they use their keyboard or mouse, more than a third declared that they’d be happy with this at it would remove the stress of having to remember multiple username and password combinations.