Unsplash © Ari He

Digital identity is one of the 21st century’s biggest challenges

As the classic New Yorker cartoon says, ‘on the internet, nobody knows you’re a dog’. This image from as far back as 1993 outlines a key feature of (and some would say a major problem with) the internet: there is often no way to tell whether any digital identity is authentic.

This is valuable in some places: political dissidents, whistleblowers or just those who would like to remain outside of the public eye can all – to some extent – hide their identities online, but there are other instances where being anonymous harms instead of helps.

In ecommerce and digital finance, particularly when it comes to things like taking out loans or transferring money, it is vital that the person logging into an account is the person associated with it and not a fraudster. *Fraud* does happen in physical spaces, but it is much rarer because a person trying to pay on a card can simply be asked for an identity document like a driver’s license to prove their identity, and even if they have forged a driver’s licence, they will be visible on security cameras. Digital spaces don’t have anywhere near that level of deterrent.

The idea that there should be ways of proving one’s identity digitally that are as secure as those in the real world is not new. The UK government has already

created a framework that would *allow private companies to create digital identity systems* called *Verify*.

Analogue identity checks are based on a document with a high level of protection against forgery that is issued by a trustworthy authority, such as a passport or driver's license. How can we create something just as trustworthy and secure in the digital space?

How are digital identities created?

Currently, many websites offer customers the option of logging in via existing Google and Facebook accounts, often with two-factor authentication or app-based verification. These are, by definition, digital identities, but they are flawed in that anyone can create a new Google or Facebook account and there is no need to use something like a passport to verify your identity when setting one up.

There is no equivalent of what the UK government wants to create – a single digital 'document', perhaps based in an app with biometric features, that allows anyone to prove that they are who they say they are. It would have to involve submitting analogue forms of identification like passports, which would then have to be verified as authentic either digitally or by humans, both of which have their problems.

The transfer of an analogue proof of identity into the digital space is only one of the challenges with electronic identities. The other is to protect eIDs against misuse and data leaks. This means that there must be a simple way for a verifying authority to determine whether an eID presented to it is genuine. Under the new UK digital identity plans linked to above, the authority that issues and manages the digital identity plays a major role here: your integrity is guaranteed either by the fact that it is issued by a government institution or through certification and audit procedures if it is a private company.

The checking authority knows which issuers of certificates that confirm the digital identity are considered trustworthy and will generally only accept such certificates: in the UK they will have to follow a *trust framework*. However, it still remains to be clarified whether the certificate is genuine. This requires a process that guarantees a very high level of protection against forgery as well as easy verifiability and can be automated.

This is where asymmetric cryptography comes into play: the method is based on a private and a public key connected to each other using mathematical operations that are difficult to reverse, such as the multiplication of large prime numbers. Generating the public key from the private key is therefore trivial, but getting to the private key from the public key is extremely difficult. The

public key can be made available to everyone. If this matches a certificate that was created with the corresponding private key, the certificate is considered authentic.

Any framework will have to be based on a public-private key architecture. Asymmetric cryptography – where freely available public keys can be used to verify a private key held by one person – is a highly scalable, robust method for keeping digital IDs secure, and is already used in thousands of applications in the public and private sector.

Promising approaches

But there is also an Achilles' heel to this procedure: the private keys must absolutely remain secret. Regardless of whether they are private trust service providers or state institutions, anyone who offers identity services based on asymmetric cryptography must ensure that the private keys are optimally protected.

Hardware security modules (HSMs) are the ideal choice for generating and securely storing strong private keys. Compared to software solutions, they have the advantage that the keys themselves are not read into the main memory of a computer, which means that they cannot be compromised remotely. The HSMs from Utimaco also have a real random number generator, which is important for generating top-quality keys.

Digital identity documents are likely to become more common – despite the pushback they get when they are proposed – because they solve one of the key issues in the digital world: being able to tell that somebody is who they say they are. For this reason, they need to be secured to the very highest standards, and the level of security that is possible with modern hardware security modules will be a key way in achieving this.

Malte Pollmann is CSO at *Utimaco*.

Article by MALTE POLLMANN