A post-pandemic year shaped by security, interoperability, and mobility solutions

A dive into how the identity industry addresses some of the trends and challenges that have shaped 2022 and will likely be with us in the coming months, if not years.

IDENTITY
TRAVEL
JUSTICE & PUBLIC SAFETY

POSTED ON 10.28.22

Today's global society exists due to the ease of communicating, interacting, and doing business with one another beyond national borders. A digital society based on remote working and remote identity verification can only be successful in the long run if the same global – or at least regional – standards are applied. However, the pandemic emphasized several challenges that still need to be addressed so that people can access their rights by proving their identity remotely, or fulfill their missions in a more flexible way:

- **Security** remains a key concern while an increasing number of people interact remotely and require technologies that enable remote access to data.
- As the pandemic struck all countries, irrespective of borders, it revealed an important additional element to the equation: **interoperability**.
- **Mobility** and flexibility are key words that have very much influenced our way of working over the last two years. With many people returning to their offices at least a couple of times a week, the focus on flexible—and often time-saving—work arrangement remains. The law enforcement community is no exception, which is why over the last few months we have seen an increasing demand for more mobile solutions to be made available.

Let us dive further into these trends that have shaped 2022 and will likely be with us in the coming months, if not years.

Security

Biometric technologies facilitate people's lives, making the world a safer and securer place to live in. The sensitivity of biometric data cannot be stressed often enough, and in previous articles we presented several solutions to safely use them. But this time, we are going beyond securing data and the challenges of the present.

One step before: secure manufacturing

Due to the ease of use, convenience and security, there has been a significant increase in the implementation of connected devices such as biometric access control terminals. However, the drawback of using successful technology is that it often becomes a preferred target. Security is only as strong as the weakest link, which is why technology

providers have had to reevaluate the full product lifecycle, especially the first step—manufacturing—to **ensure the highest level of security**.

Without appropriate security measures in place, **a product is particularly exposed during the manufacturing process**. For example, the firmware could be duplicated or modified in order to introduce security breaches that could later be exploited once the product is operational. Product counterfeiting, product duplication and theft of secure information such as keys are real risks when a device is being manufactured.

Although **secure manufacturing has been in existence for many years** for microprocessor chips used in bank cards and SIM technologies for instance, it has only just been introduced to connected device manufacturing.

There are three main pillars of secure manufacturing:

- **Establishing a 'root of trust' using secure hardware, firmware and cryptographic keys**
  The root of trust is made up at least of three elements; a secure microprocessor or another secure element that is able to create a 'security safe' in the device, signed and encrypted software associated to a secure boot functionality, and a Hardware Security Module (HSM). The objective of the HSM is to protect the main secrets and the communication link with the device during the manufacturing process.
- **Auditing and certifying the manufacturer's provisioning process**
  The audit ensures that the manufacturing process is in compliance with the defined security rules, and that only certified security components are used.
- **Traceability of manufactured devices**
  Traceability necessitates tracking and logging all stages of the device's lifecycle, from the first step of the supply chain to when the device is delivered to the customer.

Secure manufacturing enables companies to work with subcontractors without fear of the device being modified or hijacked with an alien element. It is also the foundation to guarantee that the device is well prepared to resist in the future.

Instead of creating a product and then trying to protect it, secure manufacturing focuses on eliminating vulnerabilities from the get-go.

One step ahead: Post-Quantum Cryptography

Since the beginning of the 1990s, major advances have been made to exhibit how a computer based on quantum mechanics could **speed-up the resolution of intractable numerical problems**. Currently, there is a worldwide effort to build quantum information processors. While the path to a general-purpose quantum computer is still long and uncertain, powerful special-purpose machines could arise in the coming years. One of the fields that will be impacted by the advances is cryptography—the technology used to **secure our digital life through encryption, authentication and digital signatures**.

Researchers have already designed quantum algorithms that could be used to speed-up attacks on the cryptographic technologies currently being used. For some algorithms, the speed-up is limited, and enlarging the cryptographic key is sufficient to thwart the threat. However, for other algorithms, which constitute the core of any modern security protocol, this means that, at the instant when a sufficiently powerful quantum computer will be available, it will be very difficult to ensure confidentiality. If security solutions should resist quantum computers, they need to be updated with **new cryptographic techniques called Post-Quantum Cryptography (PQC)** that remain resistant against such a threat.

Today, all encrypted data exchanged can potentially be recorded and stored until a machine powerful enough to threaten current cryptography is available, allowing anyone to reveal the plain data. For some applications, data has to remain secure for several decades, not forgetting that migration to new systems could take years. The National Institute of Standards and Technology (NIST) has initiated a **standardization process** for PQC. It started late 2017, as an open and transparent 'competition' in which 69 candidates participated, and by 2024, a handful of them will be standardized.

However, moving to this new cryptography will not be an easy journey. First, a significant **increase in computational complexity and the size of data**

(keys and ciphertexts) will have to be compensated by **new hardware and the optimization of software**. Moreover, the brand-new algorithms will necessitate years of scrutiny in order to reach the high level of confidence in the current cryptography, to which society has committed decades of research. To cope with this, government agencies and leading industry players will work hand in hand, at the beginning, to deploy hybrid protocols that carefully mix today's cryptography and PQC in order to **avoid regression** and to **implement crypto-agility**—mechanisms that enable the update of protocols for products already in the field. IDEMIA and other leading industry players are well aware of their responsibility toward society. They understand that in order to mitigate the risks of tomorrow, they have to start investing today.

Interoperability

Digital wallets are far from new. However, until now the emphasis has been on payment methods—the digital wallet replacing the physical wallet, and the need to withdraw cash. Users are already familiar with storing a digital boarding pass in a digital wallet on a smartphone or having a digital version of their loyalty cards. What is new is the creation of a digital wallet built for our diverse credentials including the invaluable identity documents. In 2022, Apple and Samsung, two giant tech providers added digital ID offerings to their digital wallet solutions. Another novelty is the aim to build an international solution that goes beyond a national system. Let us look at the EU digital wallet as a hot topic of 2022.

The EU digital identity wallet: secure, interoperable and convenient

Today, only about 60% of the EU population in 14 Member States are able to use their national eID cross-border.[1] Announced in June 2021, the EU digital identity wallet will be **available to EU citizens and residents** who want to identify themselves or provide confirmation of certain personal information. Used for both online and offline public and private sector services in the EU, this secure digital wallet could contain an individual's credentials such as their ID card, driver's license, diplomas, payment methods, vaccination records, and many more.

Once in place, the EU digital wallet will be accessible via an app on the user's smartphone, which allows them to **maintain control over their credentials at all times**. They will be able to decide which specific elements they would like to share. For example, if a user needs to prove that they are over 18, they can prove just that, without divulging their exact date of birth, age, name, address and other personal details.

The EU digital wallet would also allow entities with whom individuals are sharing their credentials, to be sure that they are genuine and do indeed belong to the holder. The EU digital wallet is meant to become a secure, simple and safe way for people to share information with service providers.

And most importantly: independent from the exact approved digital wallet solution that each EU Member State will go for, **interoperability with other Member States** will be guaranteed.

Mobility

Pre-pandemic, many companies did not encourage working from home. Accessing the company's secure network via VPN was acceptable for a select few employees or for organizations where the majority of the team was regularly traveling. The same security concerns remained for law enforcement agents, notably field officers who had no choice but to conduct everyday tasks at the station, losing out on valuable time that could be spent keeping citizens safe in the street.

Remote working for law enforcement officers

Thanks to securer technologies, the trust in mobile solutions is steadily increasing so that officers can **perform tasks such as ID verification remotely**. By using an app on their smartphone that is linked to the national AFIS/MBIS (via a dedicated cloud-based platform), officers can now conduct on-the-spot face and fingerprint biometric checks to verify or establish the identity of an individual instantly **as they would do at the police station**. The back camera of a smartphone is capable of capturing detailed photos of a person's fingerprints, enabling a 1:N match.

Cloud-based law enforcement solutions benefit from efficiency, scalability and elasticity, which translates to a **rapid response time for officers in the field**, and various overall advantages for the entire organization. For example, the cloud-based platform could be used by many concurrent users such as field officers, without necessitating an investment in very large computing capabilities. Additionally, the platform could be started up or shut down in a matter of minutes, providing the law enforcement agency with maximum flexibility. Furthermore, specialized platforms could be created to **specifically manage particular events**; large public gatherings such as the Olympic Games, or major public security incidents, etc. With the technologies developed over the last few years and the increased security that comes with them, law enforcement agents should now access and benefit from the same flexible way of working that the pandemic has introduced for many other sectors.

---

[1] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

---