Biometric On-device*: the Key to Secure and Privacy-Respectful Authentication

Security and protection of personal data are paramount concerns for citizens, governments and the companies that use them.

The expansion of digital practices, the widespread adoption of mobile applications, and online services simplify daily life for everyone. As these services become more personalized and offer greater added value, it becomes essential to strengthen authentication methods.

Thus, service personalization requires the processing of sensitive data pertaining to user identity and profile. This evolution makes the verification of each user's identity even more crucial: it is vital to ensure that users are indeed who they claim to be.

The use of biometrics has emerged as a reliable authentication factor, particularly for mobile devices such as smartphones and tablets. By extension, it is also employed online for financial transactions and in the healthcare sector, as well as in face-to-face scenarios for access control in businesses and the transportation sector.

In this context, IN Groupe guarantees trusted authentication based on biometric on-device authentication, entirely under the control of individuals. This solution seamlessly integrates within the regulatory framework, notably eIDAS 2.0, ensuring enhanced security and interoperability.

Biometrics and its everyday uses

With the acceleration of digitalization across numerous services, biometrics has become an easily accessible technology for ensuring reliable verification. Its adoption is driven by several factors:

- Reliable and simplified authentication: Facial recognition and fingerprints provide a fast, secure access. Their use is part of the digital transformation of our daily lives.
- Reduced Password Reliance: The simplification of authentication journeys makes the user experience simpler and more fluid.

The digital era is transforming our interactions with public and private services, altering the way we authenticate:

- Access control: Automated access control is used on a regular basis in businesses, secure buildings and critical infrastructures.
- Secure payments: Banking institutions and payment platforms are adopting biometrically authenticated payments to mitigate fraud risks.
- Healthcare: Biometrics provide secure access to medical records, avoiding the risk of information theft or mistaken identity, especially for prescriptions.
- Transportation: Facial recognition has become an increasingly widespread method of controlling boarding at airports, stations and ports.

However, some service providers, because of a lack of awareness and a lack of alternatives, carry out biometric checks using databases. For instance, in face-to-face verification, a user's face, presented in front of a camera, will be compared with images of eligible users stored in a centralised database. These databases are located on private servers or in the cloud, exposing users to risks of potentially massive cyber threats. These databases represent genuine "honey pots" for cybercriminals. This is where biometrics on-device provides an appropriate, secure alternative that guarantees the protection of personal data.

Biometric on-device authentication: definition and Functionality

Biometric on-device authentication operates on local authentication and ‘one-to-one’ comparison. Biometric data, such as fingerprints or facial images, are stored directly on the user’s personal device and remain under his/her sole control. This device may be a biometric smart card, a cryptographic module integrated into the user's telephone, computer or tablet (Trusted Platform Module - TPM), or a biometric identity document whose security is guaranteed by the State in terms of the level of security of the chip containing the data (identity card or passport). These media are certified by a reputable company or provider.

This method avoids the transmission of sensitive data, thereby reducing network vulnerability. Furthermore, it prevents the storage of biometric data on remote servers or in the cloud, where the security level can vary and be difficult to verify.

Biometric on-device authentication avoids centralised data storage, reducing the level of risk associated with cyber-attacks (data compromission, identity theft). The data remains under the exclusive control of the user. When an individual wish to authenticate, their biometric data is compared locally: the information captured by the authentication device (e.g. a camera or fingerprint reader) is compared with that recorded on the medium under their control (one-to-one comparison). If they match, access is granted. There is no transfer of data to an external system, which limits the risk of biometric data being exposed outside the user's personal device.

Biometric on-device authentication adheres to the data minimization principle mandated by the General Data Protection Regulation (GDPR). due to the absence of centralized storage. No biometric data is transits over a remote network or server, reducing the risk of abusive surveillance and protecting individual privacy.

Biometric on-device authentication is accessible by all populations, including those without smartphones or living in areas with poor connectivity. In rural areas and industrial sites, this model provides secure authentication without the need for a complex network infrastructure.

Finally, the ease of use and speed of authentication make biometric on-device authentication an ideal solution for all areas of daily life, whether public or private.

A solution that complies with standards and regulations

Biometric on-device authentication is based on several international standards guaranteeing a high level of security and interoperability:

- ISO/IEC 19794: Standard for the representation and interoperability of biometric data
- ISO/IEC 30107: Standard on the detection of presentation attacks (PAD) to prevent biometric fraud
- eIDAS 2.0 regulation: European regulation defining electronic authentication and digital identity standards
- ICAO 9303: Standard governing biometric travel documents, in particular electronic passports
- RGPD, CNIL 1: Regulatory requirements for the protection of personal data

Fly'IN: biometric on-device authentication for smoother travel

Developed by IN Groupe, Fly'IN - Fast Track is an inclusive solution that integrates biometrics into the passenger's profile.

Passengers set up their profile at home using the airline's/airport's mobile application by entering their identity data using their passport, identity card, residence permit or any other official document.

This identity information, together with the boarding card details, is then bundled into a unique QR code. This allows passengers to move quickly and freely within the airport.

Passengers are the sole owners of their personal data. Their identity and travel document can be authenticated without the need to access an external database. As the sole owner of their personal data, they can withdraw their consent at any time from their smartphone, a website or a form.

Biometric on-device authentication is currently the most effective solution for combining security, data protection and a smooth user experience. It enables:

- Increased security against fraud.
- Optimal protection of personal data to prevent identity theft.
- A universal solution, adapted to all aspects of daily life, whether in the private or public sector.

This secure, regulatory-compliant solution is essential for authentication that respects personal data. The adoption of Fly'IN represents a strategic advancement in ensuring trusted authentication, entirely under the control of individuals.

** Biometric on-device: This term refers to a specific way to implement a biometric solution, whereby the holder of the biometric data stores, controls and manages the use of these data on his/her personal device (phone, card, QR code…). Because this personal device remains under the sole control of the owner, this implementation of a*

biometric solution offers the best protection against data theft. In access control, a corporate badge containing fingerprint data of an employee can be considered as a "on device" biometric solution: the employee uses a fingerprint reader to access a building, then scan his/her badge to confirm that the live data match with the one encoded on the card. In such a model, the biometric data never leave the badge (the device) and is not transferred to any external system or database.

This model can be compared with "database-centric" ones whereby biometric data are stored on online servers. While these solutions do not require the use of devices, they are dependent on connected software and databases that are governed by external parties.

About IN Groupe

As a European specialist in identities, trusted transactions and digital services, IN Groupe is a trusted partner in the management and protection of sensitive data to governments, public and private organizations around the world.

By mastering the entire identity value chain, IN Groupe extends its expertise from citizen identity to solutions and services for professional and object identities. IN Groupe is a key player that guarantees the right to be you in both the physical and digital spheres.

With 2,000 employees across all continents, IN Groupe achieves a turnover of approximately 600 million Euros. The group is a trusted partner for governments and its private and public sector clients in over 130 countries.

For more information: **www.ingroupe.com**

Press Contact : Céline Fauvet celine.fauvet@ingroupe.com (33 6 43 85 06 43)