Article
The rise of facial recognition

International Security Journal - Issue 20 - October 2020

SPECIAL REPORT
INDUSTRY EXPERT

THE RISE OF FACIAL RECOGNITION

Vincent Dupart, CEO of STid explains why facial recognition solutions are growing in demand

Vincent Dupart, CEO of STid

Facial recognition is one of the technologies used in biometry. Biometry enables the identification and authentication of an individual based on the quantification of their physical, physiological or behavioural characteristics (fingerprints, vein pattern, iris, etc.).

Identification means the ability to pick out someone from within a group in a location, image or database; authentication means verifying whether someone is really who he claims to be. All biometric systems are subject to strict controls under the EU's General Data Protection Regulation in Europe. Having established this context, what about the access control market?

Organisations are facing an increasing number of cyberattacks. For this reason, the notion of security is a key issue. And this is precisely STid's core business, protecting people, assets and data by making identity and access secure. In the case of facial recognition, data theft is a real threat. This is because data is universal, unique, permanent, comparable over time and non-falsifiable. In a word: valuable. Yes, we encourage the use of facial recognition, but in conjunction with guarantees of faultless end-to-end security, in particular through the Secure & Smart Communication Protocol (SSCP).

Here, the distinction between identification and authentication remains essential. For STid, this does not involve the implementation of intrusive systems that aim to indicate an individual's identity, but simply to authenticate this person. But how? A verification is performed to ensure that biometric data stored in the badge, corresponds to the badge holder. The system does not store any data in a database. In France, the French Data Protection Authority (CNIL) recommends storing this biometric data on an individual medium that the user physically keeps in their possession. Solutions for storing data in a central location are prohibited. If the user loses their badge, the credential is cancelled and the data disappears.

Five key features of an effective biometric system

COVID-19 is driving organisations towards new access control solutions. They are currently questioning the use of contact -based biometric solutions such as fingerprints and gradually moving towards the use of contactless solutions.

With the increasing number of smartphones, these contactless technologies are becoming more widespread. STid has developed the STid Mobile ID app, which digitalises all access credentials into one single app. Smartphone biometry, including

Article
The rise of facial recognition

International Security Journal - Issue 20 - October 2020

facial recognition, joins virtual badges in offering an additional layer of security for identification.

It enables the simplified management of access points, both for company's employees and its visitors and provides access to related services (workstation access, etc.).

These issues highlight the key features of an effective biometric system. Five concepts are key:

1. Speed: The system must allow fluid access to ensure its adoption by users. There is no point in enhancing security if the system is perceived to be an inconvenience!
2. Compatibility with existing systems: The choice of a biometric solution should not make existing systems obsolete and should remain easy to deploy.
3. Performance: The system should target a high level of authentication quality, or risk being a source of blocking points in daily usage.
4. Compliance with the recommendations of the CNIL/ GDPR: While legislation varies from country to country, France (with the CNIL) and Europe (with the GDPR) campaign for personal data protection. The access control market is seeking solutions to protect citizens' lives.
5. Security: Solutions should guarantee data protection through proven or certified encryption and authentication mechanisms.

In summary, this is basis of STid's expertise in high-level security.

WHY CHOOSE THE SSCP PROTOCOL?

The communication protocol installed in the buildings must be resistant to potential attacks.

SPAC has built the SSCP Protocol, an architecture allowing integrity and confidentiality by the encryption of sensitive data. The Secure & Smart Communication Protocol (SSCP) protects the communications of physical and digital access control equipment. It provides a secure connection between the readers (inspection devices) and the management system (concentrator) to guarantee a level of security in line with government requirements.

The SSCP protocol provides uniform protection for all your applications by protecting interface communications (RS485, USB, TCP/IP, etc.).

It guarantees the interoperability of all equipment through compliance certification. Why? To provide businesses with genuine technological independence, giving them greater freedom!