

IDENTITY CONFIRMED

Jérôme Frou explores the role of identity documents and finds out what can be done to protect them

Every year, millions of people are denied basic rights simply because their identity is not recognised. An identity document is far more than just an administrative formality. It is the key that allows an individual to exist legally, to travel, work, vote and access healthcare or education. Without it a person has no official recognition and is deprived of fundamental rights, which is still too often the case today, as the United Nations regularly reminds us. On the other hand, individuals should benefit from security, dignity and protection.

This is the promise of every identity document: to give each person a legal existence and to protect that existence against exclusion or fraud. But today, this promise is increasingly under threat. Counterfeiting, identity theft and the misuse of documents by third parties undermine trust and turn what should be a safeguard into an additional vulnerability, both for the rightful owner of the identity and for the internal security of states, especially in today's unstable geopolitical context.

In recent years, identity document fraud has become more sophisticated. Organised criminal networks are no longer merely forging documents; they are exploiting the very technologies designed to ensure security. While documents have evolved significantly using polycarbonate materials, electronic chips and biometric identifiers, attackers have kept pace, developing new methods to circumvent these protections.

WORLD IDENTITY DAY (16 SEPTEMBER) REMINDS US HOW WE CAN BETTER PROTECT DOCUMENTS

One alarming tactic is the discreet deactivation of the chip embedded in a passport or identity card. In some cases, the document remains visually intact and appears legitimate. Legal constraints often prevent authorities from refusing entry to individuals carrying such documents, especially if the chip's intentional failure is not immediately detectable. As a result, some fraudulent entries are only discovered afterward, by which point it is too late to act preventively.

This challenge exposes structural vulnerability in current identity verification processes. Although technical systems support frontline officers, a significant part of detection still relies on human judgment. In an environment where fraud techniques evolve rapidly, this reliance places a heavy burden on border and customs personnel.

Adding to the challenge is the emergence of artificial intelligence, which can generate hyper-realistic



forgeries of facial images. As traditional checks become less effective, more advanced and integrated solutions are required.

NEAR-FIELD COMMUNICATION

Another key area of innovation is the use of NFC technology. Because NFC allows secure, encrypted and contactless data exchange, it strengthens the authentication process and reduces reliance on visually inspected elements. It is increasingly seen as a trusted tool in the fight against both physical and digital fraud.

Yet in the midst of these digital innovations, the physical identity document remains irreplaceable. It provides a tangible, sovereign and verifiable link between an individual and the state. Unlike digital systems, it is not connected to any network and cannot be hacked remotely. This physical nature offers a layer of protection that is inherently resistant to cyber attacks and reinforces its credibility in high-security environments.

An identity document is not simply a form of protection. Its strength comes from the combination of technical robustness, legal frameworks and institutional transparency. If even one of these elements is lacking, the document ceases to be a tool of trust and can turn against the very person it is meant to protect. World Identity Day (16 September) reminded us to ask how we can better protect identity documents. How can we support law enforcement and customs in detecting fraudulent uses more effectively? The answer lies in collective vigilance and adaptability to keep pace with evolving threats. Protecting identity isn't just about technology. It's about ensuring that the documents entrusted to us truly safeguard every person's legal existence and security ●

Unlike digital systems, physical ID documents are not connected to any network and cannot be hacked remotely

Jérôme Frou is Linxens Government Business Unit Vice-President.