ReadID Paper

Mobile Service in the Context of the Entry-Exit System

Exploiting NFC and biometrics to optimise logistics

Challenges in smart borders

Europe has set up the smart borders programme to modernise the management of external borders. Member states are confronted with ever-growing numbers of third-country nationals that travel to Europe.

This is both a joint European challenge as well as an individual responsibility of the member states. Under the central infrastructure as set-up by EU-Lisa every state must work on improving the quality as well as the efficiency of external boarders at every point of entry, be it road, port of airport.

Despite national responsibilities the European Commission stimulates the use of industry best practices to help to reduce the logistic issues every country faces: how to reduce the time needed at border-crossing points, especially for first time arrivals, without compromising security?

Traditionally, border control is done at border control points, possibly with e-gates, or through mobile border agents. Many border-crossing points do not have the resources, both space and people, to handle large streams of third-country nationals to register them, obtain biometric data including fingerprint and evaluate risks involved.

Self-service kiosks can alleviate this somewhat, but it can still take several minutes of processing leading to long queues, frustration and possibly aggression at border control points.

Fortunately, other use case show how self-service can be done securely and reliably with self-service kiosks, using mobile technology.

The functionality needed to read and verify passports as well do holder verification is part of any modern smartphone.

This opens the possibility to move a substantial part of the process from the point of entry to an earlier stage, even from home.

In the EES and ETIAS regulations self-service systems are explicitly mentioned and advocated. This mobile technology can be seen as a form of self-service technology, as are kiosks. From a legal perspective there are, to the best of our knowledge, no obstacles to use mobile technology.

In this whitepaper we explain how the technology works in general and how it can be applied in the context of smart borders. We illustrate this with proven use cases.

Mobile identity verification: NFC + biometrics

Modern passports are equipped with a chip following the ICAO 9303 standard. This means that all information is digitally signed and encrypted and cannot be manipulated. Also, the face image is available at a high resolution, without any additional watermarks. Therefore, they are much more suitable for face matching than the printed face image. Finally, a copied chip can be easily detected.

The big breakthrough in this technology came with the availability of smartphones with NFC. Which is now available on all modern smartphones are equipped with NFC, and often used for mobile payments.

A smartphone can be used to read and verify the chips in identity documents, without the need for expensive kiosk hardware.

Our software product ReadID works on both Android as well as iPhone. ReadID is used to read the chip, and our software at the server is used verify the data and send the validated information to the entry-exit system.

iproov

READID

ReadID Paper

Identity Verification in 2 simple steps

1. SCAN

Scan MRZ and Capture Visual Inspection Zone

2. READ

Read the NFC chip (or pass to optical solution if no chip is available)

We regard smartphones data-storage as unsafe, as a matter of principle. The validation and processing must be done in the cloud, and not on the smartphone, as smartphones can easily be manipulated, lost or stolen.

Only on trusted devices, under strong control of the organisation such as a police force or border control agency, the software can be used client-only.

Reading the chip digitally allows to verify the validity of the identity document and read the customer information without the risk of any OCR or typing mistake. In an identity proofing or preregistration process we can also verify via face matching, that the person owning the passport is currently holding the passport (holder verification).

iProov does both face matching – linked the holder to the image in the chip – as well as advanced liveness detection (called Genuine Presence Assurance), which prevents spoofing /impersonation attacks and even complex AI based attacks including deepfakes.

A complex process where the software should be strict enough to have almost no false positives (incorrectly accepted persons, for example look-a-likes or masks), but liberal enough to deal with beards, ageing and different lighting conditions.

The combination of ReadID and iProov has shown to be successful in many mobile onboarding cases. After Brexit, the UK Home Office incorporated our technology in their app for the EU Settlement scheme, allowing EU nationals to apply online for residence status. More than 6.3 million EU nationals successfully went through this process. The same combination of technologies is used for Eurostar self-service.

Eurostar used our combined technologies successfully for touchless, ticketless, secure travel. Prior to travelling the individual simply enrols via their own device to the Eurostar SmartCheck app. This gives access to an accelerated pre-boarding option, allowing the traveller to add and verify their passport and tickets. This approach removes the need for the traveller to present tickets or a passport at checkpoints as they depart. Ultimately providing a secure and effortless travel experience with a quicker through-concourse journey on the day of travel. 84% of SmartCheck users would use the remote pre-boarding options in the future.

These cases have shown that remote identity proofing is possible with the highest security level, and all fully automated. The data gathered can be used by border forces to streamline processes at the border-crossing points, to enable early screening with respects to watch lists, and allows a faster simpler traveller experience ahead of border arrival. With mobile pre-registration we can reduce border congestion.

By streamlining low-risk passenger flow, border control agents can focus on persons-of-interest.

iproov

www.inverid.com

READID

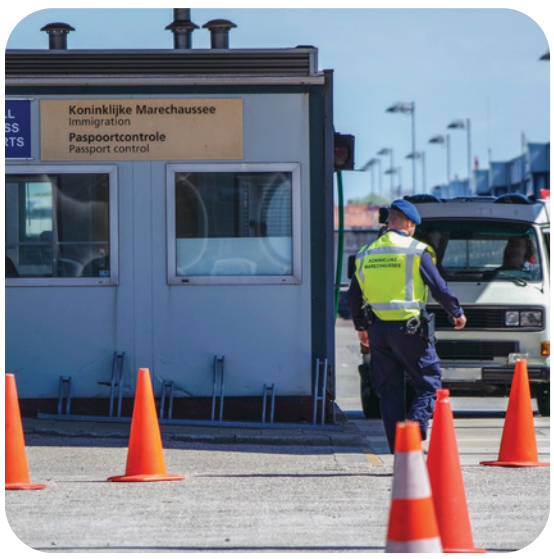
A customer journey that starts at home

How could this be applied in the context of smart borders? Pre-travel third country nationals (TCN) can notify their plan at the EU site for pre-registration. They are invited to download a verification app on a smartphone. The smartphone is used as passport reader and photo camera only.

After downloading the app the TCN performs the identity proofing, allowing to create a profile in the EES/ETIAS systems. This profile contains all data from the passport as well as a recent picture taken for the face verification process. This step does not allow to obtain fingerprints that are needed in the profile as well. Fingerprints can be captures when the TCN attends the border point for the first time.

On the basis of this profile the member state can assess type of visit: what risk category is the TCN in? Should additional measures be taken?

When travelling, the TCN can notify border control forces of the ETA. This allows to plan resources better and could, for example, generate a QR code for the TCN that can be used for fast lane access if appropriate.



If the TCN is a returning visitor no finger prints need to be re-taken and border control can allow for fully automated border passing.

At the point of entry, a picture can be taken under controlled circumstances. Finger prints can be obtained in a supervised manner. For high-risk profile individuals, additional checks can be performed by border agents. In this customer journey supervision by border control agents is still an important step. Self-serving data acquisition and identity proofing can optimize the border activities as well as reduce stress for travellers at border crossing points.

Much of the data capture can be done from a location suitable for the traveller, often in the relative quite context of their home, with little or no time pressure. At the point of entry only the supervised steps need to be carried out, and for returning visitors a completely automated process might be considered.

To support the United Kingdom's exit from the European Union, the EU Settlement Scheme was established by the Home Office to allow EEA nationals living in the UK to apply for a UK immigration status. WorldReach Software was selected by Home Office for the operation and management of the digital verification capability supporting EU Settlement Scheme (EUSS). Together with ReadID and iProov, the consortim managed to create the world's largest, most successful digital on-boarding immigration programme using remote identity verification.

Applicants need only to complete three steps:

1.Prove their identity
2.Show that they live in the UK
3.Declare any criminal convictions

As UK Home Office wanted to make the application process as easy as possible for the estimated four million EEA nationals who would need to apply, they sought out new innovative and effective capabilities to include in an optional end-to-end digital application channel. NFC and biometrics were the preferred technologies.

The EUSS is a very successful, scalable proof-point of what's possible and achievable with the right end-to-end processes, technology and collaborative team. It handled more than 6.595.200 applications as of 30 April 2022. A high percentage completed their application in under 10 minutes, with a high level of identity assurance.

ReadID Paper

NFC and biometrics to optimise logistics

In this whitepaper we explained how mobile remote identity verification works and how it has had a transformational role in different industries.

The technology is mature, scalable, secure, and user friendly. We argued that the same technology can be used in the context of smart borders to complement activities at border crossing points, not to replace them.

From a security perspective, NFC based remote identity verification is a mature, proven technology. The authenticity of passports can be established with 100% certainty, based on country certificates. This covers both the data inside the chip as well as the fact that it is an original passport. None of our customers ever reported a false positive in millions of identity verifications, whereas optical verification can easily be fooled. Entrust, Inverid (formerly known as InnoValor) and iProov have collaborated on many use cases in different industries. We are more than willing to assist in setting up a proof-of-context to develop a joint understanding of how our technology can help to keep Europe safe and hospitable to those who are welcome.

Further information

Information on NFC-First identity verification technology and on biometric authentication. Deep dive into use cases such as Eurostar and the EU Settlement Scheme.

inverid
Creators of ReadID

Jim Slevin
Regional Director UK and Ireland

jim.slevin@inverid.com

+44 7771 976003
www.inverid.com

iproov

Mike Summers
Sales Director EMEA

mike.summers@iproov.com

+44 7585 800950
www.iproov.com

READID