

ReadID

NFC First Approach to Instant Mobile Onboarding



About Maarten Wegdam: Maarten Wegdam, PhD, is CEO and co-founder of InnoValor/ReadID. Maarten is an expert in the area of digital identity and online identity verification.

Maarten Wegdam ■ CEO and co-founder ■ InnoValor/ReadID



About Wil Janssen: Wil Janssen, PhD, is CMO and co-founder of InnoValor/ReadID. His focus is on impact of digital technologies on organisations.

Wil Janssen ■ CMO and co-founder ■ InnoValor/ReadID

The pressure on banks to make their KYC processes more secure is strong. At the same time, KYC should be as smooth as possible to create a good customer experience. NFC-based mobile onboarding makes it possible to bridge this dilemma. We describe how NFC can lead to an optimal mobile KYC process and what this means for Open Banking.

The trust dilemma

Customers are more demanding than ever. They accept no less than real-time digital services, around the clock. If a bank cannot deliver fast enough or creates, in the eye of the customer, unnecessary hurdles in the process of becoming a customer, a digital competitor is virtually around every corner. At the same time, regulatory pressure increases: anti-money laundering legislation has led to substantial fines already in the industry. The importance of high-quality KYC processes is higher than ever. Traditionally, KYC comes with visits to branch offices. Time consuming, costly and limited to office hours. Digital solutions for KYC have been in the market but have their disadvantages. Optical solutions using photos of identity documents are not secure, video sessions for matching customers to IDs are invasive and costly. Both have a poor conversion and take too long.

This is the trust dilemma banks face in onboarding new customers, as well as for re-verification, app activation, password reset, and other use cases in which the identity of an existing customer has

to be re-verified. And not only banks: pension funds need attestae de vitae for their customers and border control moves from the big hubs to mobile control. The need for effective mobile identity verification is growing fast.

Fortunately, NFC is increasingly helping banks to overcome this dilemma. The same NFC chip in mobile phones that enables payment, also enables mobile identity verification. NFC can be used to create of smooth customer experience with a high level of trust at a lower cost.

How does NFC work in identity document verification?

Modern passports are great – they are equipped with a chip following the ICAO 9303 standard. This chip contains similar information as is printed on the passport, but with a number of crucial differences. First and foremost: 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, it is much more suitable for face matching than the printed face image. Finally, a copied chip can be easily detected. Moreover, most modern ID cards have the same chip, the EU even has a regulation mandating this for new ID cards.

→



The big breakthrough in this technology came with the availability of smartphones with NFC. Basically, all modern smartphones are equipped with NFC, often used for mobile payments. A smartphone can be used to read and verify the chips in identity documents, without the need for expensive additional hardware. This is a great opportunity: by leveraging two things everybody has – a passport and smartphone – identity verification can move to a next level.

Our software product ReadID works on both Android as well as iPhone. The app is used to read the chip, and our software at the server is used to do all kinds of verifications and send the validated information to the bank. These calculations should be done in a safe environment, and not on the smartphone, as smartphones can easily be manipulated. We regard smartphones as unsafe, as a matter of principle. Only if the smartphone is under strong control of a company, ReadID is allowed to work client-only. The Dutch police, for example, has taken this approach.

An optimal KYC process

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 – an important first step and sufficient for many processes. In a KYC process more is needed. We need to verify that the person owning the passport is currently holding the passport (holder verification). This implies that as a second step face matching is needed.

We work with partners such as the UK-based company iProov that do both facial matching – linked the holder to the image in the chip – as well as liveness detection. Quite a difficult process: the software should be strict enough to have almost no false positives (accepted persons, for example look-a-likes or masks), but liberal enough to deal with beards, aging, and different lighting conditions.

The combination of ReadID and iProov has shown to be successful in many mobile onboarding cases. Large banks such as ING, Rabobank, and DNB Norway use our solution. The UK home office has incorporated our technology in their app for the EU Settlement scheme, allowing EU nationals that, as a consequence of Brexit, need a residence status to apply for this online. More than 2.5 million EU nationals already successfully went through this process.

These use cases show that the trust dilemma can be overcome. NFC-based identity document verification creates a smooth customer experience, combined with the necessary level of trustworthiness at affordable cost. NFC first is the way forward in KYC processes.

About ReadID: ReadID is the leading NFC based mobile identity verification provider. ReadID originated from research at the Dutch fintech company InnoValor and is now a solution for mobile identity verification using NFC and smartphones that is adopted quickly in different sectors and application areas where fraud prevention is key, such as banking, border control, and digital signing.

www.readid.com