GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

WHITE PAPER

THE DIGITAL IDENTITY PROBLEM
SOLVING THE ISSUE OF TRUST

June 2019

This white paper from Goode Intelligence investigates the question of how we effectively and securely identify people online and enable them to perform digital tasks in a safe and secure manner. We believe that this is one of the fundamental questions of our time.

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

WHITE PAPER

THE DIGITAL IDENTITY PROBLEM SOLVING THE ISSUE OF TRUST

June 2019

The question of how we effectively and securely identify people online and enable them to perform digital tasks in a safe and secure manner is one of the fundamental ones of our time.

The first challenge to overcome is that there are multiple definitions of what digital identity is. The market is complex and fragmented with many competing technologies being used to solve some of the issues facing our digital lives. Even NIST in its *Digital Identity Guidelines* struggles with a definition stating that “without context, it is difficult to land on a single definition that satisfies all”.

With no simple or single solution to this problem there is significant opportunity for technology companies to develop targeted solutions to solve specific problems. Is digital identity something to simply support digital onboarding and being compliant with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations or something bigger – a digital equivalent of a passport or national identity scheme and are we entering an era of person-centric digital identity or self-sovereign identity?

Digital (Electronic) Identity and document verification services (eIDV) solve an immediate problem in how to prove a person’s identity for access to online (remote) services.

In the absence of universal digital identities that can be used across services and cross-border digital identity, document verification services remedy the issue of trust between service providers and their users.

WHITE PAPER

THE DIGITAL IDENTITY PROBLEM SOLVING THE ISSUE OF TRUST

June 2019

According to David Britton, VP Industry Solutions of Experian, interviewed for the Goode Intelligence analyst report ***Digital Identity & Document Verification Market & Technology Analysis Adoption Strategies & Forecasts 2019-2024***, right now "we are in a state of transition where we will have a combination of old and new identity – physical ID documents and digital identity. This is where eIDV is solving an immediate problem."

The ability to onboard new customers to services through remote digital channels, web and mobile, is a pressing need for many organisations looking to reduce their physical footprint and support digital transformation projects while reducing the risk of fraud

WHITE PAPER

THE DIGITAL IDENTITY PROBLEM SOLVING THE ISSUE OF TRUST

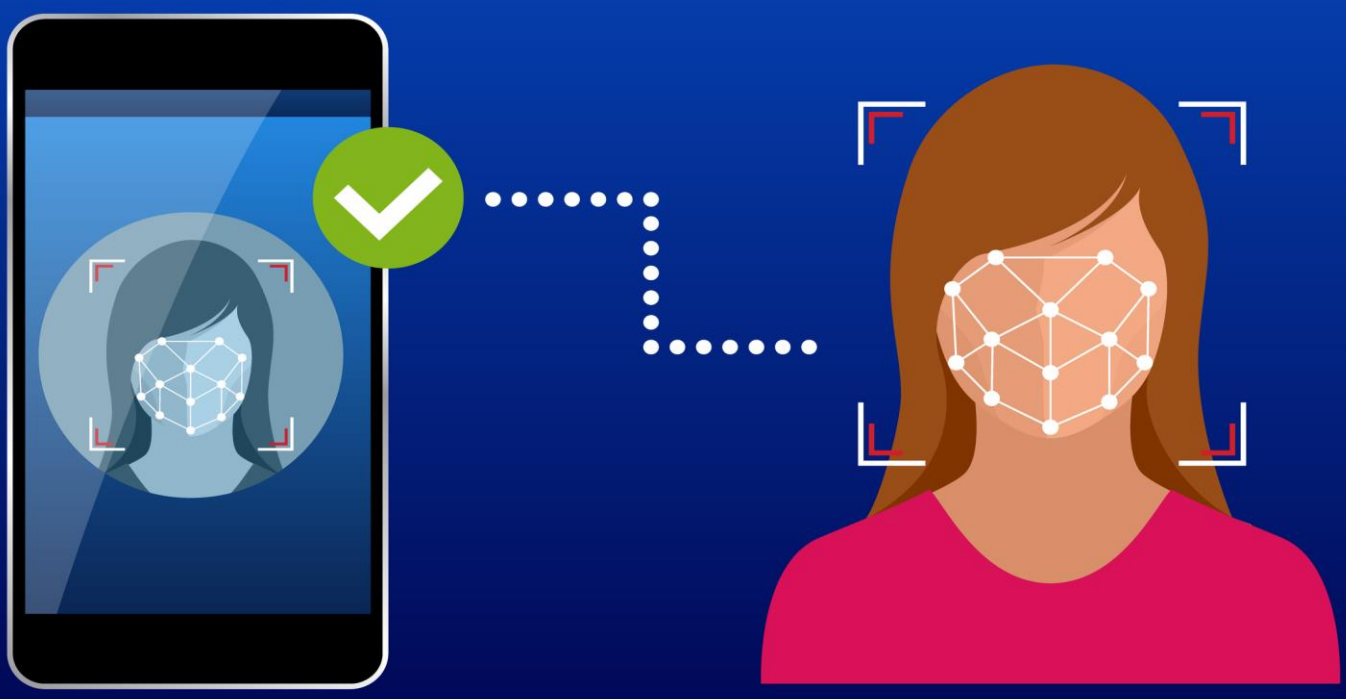
June 2019

Digital Onboarding

Digital identity and document verification services support digital onboarding and meet the latest AML, KYC and Customer Due Diligence (CDD) regulation.

These solve an immediate problem in proving an individual's identity. Specifically, digital identity and document verification answer these questions:

- Is it a real user?
- Is the user authorised to use the data it presented?
- Can the service provider conduct business with the user?
- What is the risk of doing business with the user?



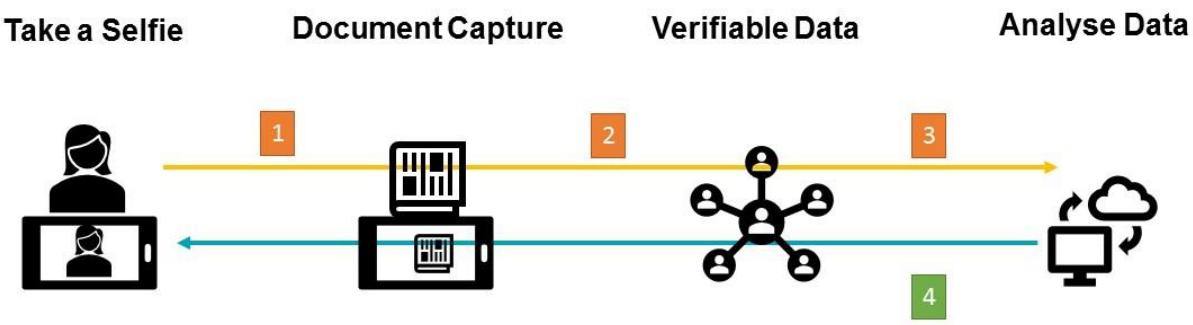
A combination of ever-more accurate facial recognition, document verification and a wider variety of verifiable identity sources (data and signals) increasingly powered by machine learning (ML) and artificial intelligence (AI) are enabling service providers to adopt digital identity and document verification services in ever-increasing numbers.

Goode Intelligence has determined that there are four main parts for digital identity and document verification linked to the four questions outlined above:

- **Genuine Presence Assurance:** That the entity is a genuine person and not synthetic: This is usually managed by using a camera; either smartphone or webcam, to capture the entity's face and then using a number of technologies to ensure that it is a live face.
- **Document Capture:** Secure capture of the trusted document that is being presented to a service provider and verification that this document is not a fake and has not been tampered with.
- **Corroboration & Risk Mitigation:** Validation of captured images, face and document. Dependent on the risk appetite, a range of other techniques, including collecting signals (device and network), and data will be used to feed into the risk engine to verify the entity's identity and validity to perform a certain task, e.g. open up an account.
- **Orchestration:** The workflow that manages the processes and ties all of the disparate technologies and data sources together.

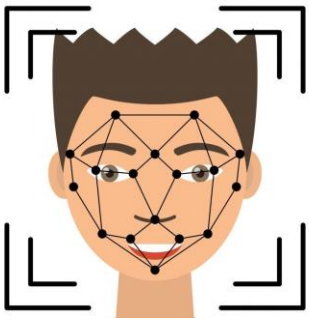
The following figure is based on the four main components, visualising an end-to-end process and outlining the main technology methods commonly used.

Figure 1: End-to-End Digital Identity Verification Process



1. User takes a selfie using facial recognition software
2. User scans a Government-issued ID document
3. Verifiable data is collected to corroborate ID & biometric data already captured
4. System validates data and creates identity verification score

Genuine Presence Assurance Using Biometrics



According to Clive Bourke, President EMEA & APAC at Daon, “methods to prevent impersonation which ensure it is a real person are vital. Liveness detection algorithms that combine both passive and active assessments provide the best protection against fraud”.

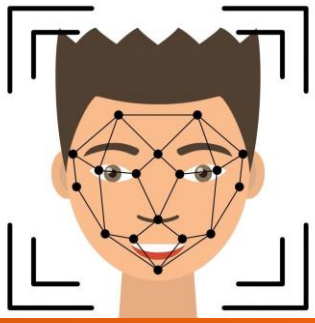
Why is this important? In remote identity verification scenarios, it is essential to know that it is a living person and not a ‘fake’ person that is trying to spoof the system into thinking that it is genuine.

Biometrics is a vital technology for enabling digital identity verification services. It replaces the human when verifying the identity of a person in remote, unattended, scenarios. Instead of a bank or telecommunication company employee verifying the image on a government-issued document against the face of the customer in-branch or in-store, facial recognition software captures a facial image and then verifies it against the image extracted from the government-issued document.

An essential part of Genuine Presence Assurance is liveness and spoof detection, commonly called Presentation Attack Detection (PAD).

A robust facial recognition system that is used for digital identity verification services must be able to deter common spoof attacks and must be able to determine whether a person is real and present during the identity verification process.

Improvements in Facial Recognition

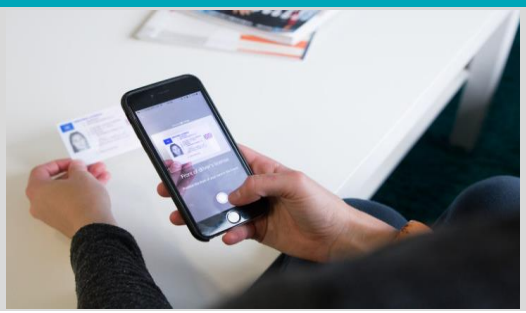


Modern facial recognition algorithms offer multiple benefits:

- Quality assurance of the live image captured and the scanned image to make sure they are suitable for facial recognition
- Liveness techniques including eye blink, head movement, texture, light reflection, sharp lines, perspective changes and behaviour
- Facial watchlist searching of previous fraudulent applications
- Facial search of previous applicants in a specific period or high risk cohort of applicants or all applicants to look for applications with different claimed identity data but same persons face

The level of accuracy improvement in facial algorithms has been significant due to the availability of Machine Learning (ML) and Deep Neural Network (DNN) capabilities combined with much larger and more diverse data sources and the ability to continuously train algorithms on real data.

Document Capture and Verification



It is important that a document that is being presented to a service provider is not a fake and has not been tampered with.

Types of document that are used include:

1. Passport (Biometric and non-biometric)
2. Driver's Licence
3. National Identity Card

Depending on the workflow, this is generally either the first or second process that will be followed as part of the end-to-end digital identity verification service.

Using a government-issued document with an image for identity verification meets AML/KYC regulation and has traditionally been carried out in a physical office or retail store under the supervision of a trained person, for instance in a bank branch when opening up an account.

With the growth of digital services and a move away from having physical bank branches and retail stores, document capture and verification is moving to digital.

Document Capture and Verification

Identity information is captured from the document either using a camera, either a smartphone or personal computer (webcam), or via NFC when an identity chip exists, e.g. biometric passports.

The introduction of machine learning and artificial intelligence (AI) technology to this area is having a positive effect on accuracy rates and reliability. However, it is important not to oversell the capabilities of AI especially when applied to document verification and authentication. Even with the help of AI accuracy rates for document verification are generally in the 80 percent bracket and human analysis is often required to increase accuracy.

What is MRZ or MRTD

MRZ is an abbreviation for Machine Readable Zone, whereas MRTD refers to Machine Readable Travel Document. MRZ is a format found on most passports and identity documents worldwide. It contains the document holder's data in a form which is both visually readable and encoded with optical character recognition.

Accuracy Rates with Document Capture and Verification

Document capture and verification accuracy is an important metric for assessment as a solution has to be able to capture fake identity documents to ensure AML/KYC compliance and to ensure fraud rates are manageable. Document verification has varying levels of accuracy and Goode Intelligence's research shows that accuracy rates, where auto verification is successful, are currently in the 80 percent bracket. 15 percent are generally viewed as being suspicious and require additional verification – usually by human analysts – and five percent fail and are viewed as fraudulent.

According to Clive Bourke, President EMEA & APAC at Daon "document accuracy is not where it should be. The combination of machine learning and human review may add grit into the process and introduce cost but serves to provide a positive outcome for customers."

Accuracy rates can be higher with biometric passports where information, including biometric data, is read from a chip using NFC and are then verified. Not all passports are biometric and it is still only available on certain Android devices, although a recent announcement by Apple points to iPhone's supporting this feature in the next version of iOS (13), for iPhone 7 handsets and above, available later in 2019. Leveraging NFC for biometric chip reading improves the quality of the images used by extracting directly from a chip rather then using a scanned image.

Corroboration, Risk Management & Orchestration

The final components of digital identity and document verification are corroboration, risk management and orchestration.

Corroboration uses signal and data collection to improve accuracy rates for identity verification. Orchestration, or workflow, services are an imperative for service providers aiming to offer comprehensive end-to-end identity and document verification services. The section also investigates the use of behavioral biometrics to prevent fraudsters getting as far as the front door.

The decision making or risk management aspects of identity and document verification are increasingly important as they ultimately decide, based on the data passed to them, whether a person's identity can a. be trusted, b. is not illegal and c. is tied to a person that is authorised to perform a certain action, e.g. open up a bank account or reserve a shared room.

GI DEFINITIONS

False Positive & Negative: A False Positive is when a genuine document is flagged as being fake or suspicious.

A False Negative is when a fake document is flagged as being genuine and accepted by the system.

Corroboration, Risk Management & Orchestration

Identity Signals & Data

Identity signals and data can be a significant method of improving the accuracy of identity verification supplementing other components – document verification and facial recognition.

These data sources range from the traditional, name, social security number and mobile number, to what David Britton, VP Industry Solutions of Experian calls "digital exhaust consumers are emitting" including data derived from social networks.

- **MNO:** Active data from MNOs & the mobile device itself
- **Citizen:** Data sourced from a utility or government database
- **Consumer:** Data sourced from direct marketing campaigns
- **Credit:** Data derived from a registered credit agency, or bureau, which manages consumer credit information on individuals
- **Electoral Roll:** Government collated & issued data for citizens enrolled to vote
- **Government Issued:** Government collated & issued databases includes national insurance, driver's licences & passports
- **Property Files:** Data issued by the government detailing property ownership
- **Utility:** Data issued for a national utility provider. Telephone, gas, electricity & water
- **Watchlists:** Country screening programme list. OFAC & DFAT

Market Drivers & Adoption

There are a number of key market drivers for digital identity and document verification services that include supporting **Digital Onboarding, Age Verification**, meeting **AML** and **KYC** legislation and being a foundation for **Trust in the Sharing Economy**.

With the rise of FinTech suppliers and challenger banks, the need to have a robust digital onboarding solution that meets AML and KYC legislation is an imperative and this is why we see challenger banks such as Monzo, Revolut and Starling Bank leading the way in supporting digital identity and document verification services. This is an extremely buoyant market and industries leading the push for adoption include:

1. **Financial Services including insurance (BFSI)**
2. **eCommerce including the sharing economy and adult markets**
3. **Telecommunications both mobile and fixed**
4. **Gaming including gambling and video gaming**
5. **Physical Retail**

Adoption of electronic identity and document verification services for the financial services has been strongly driven by a combination of AML/KYC compliance, fraud reduction and digital transformation programmes within the financial service providers.

Market Drivers & Adoption

The ability to quickly and securely onboard new customers to a financial service using smartphones has many benefits to financial service providers and fits in with the strategy of challenger banks and FinTech providers who only have a digital presence.

According to Clive Bourke, President EMEA & APAC of Daon in an exclusive interview with Goode Intelligence in February 2019 “Across banks there is a growing interest in eIDV and every second bank that Daon engages with in terms of sales engagement is interested in this area”.

There is significant activity from the ‘Challenger’ bank community which pride itself on being ‘digital only’ and ‘mobile first’. For these banks the ability to run financial services without a physical presence (branch) is a prime consideration, so the ability to onboard new customers and allow them to open accounts by proving their identity on a smartphone or via a web session is essential.

Another sector seeing strong adoption growth is **telecommunications** where there are two main scenarios where the telecom operator is a:

1. **Service provider of eIDV**
2. **Buyer of eIDV services for its own customers**

There is significant opportunity for telecom providers to play a pivotal role in the identity verification market as MNOs hold valuable information about mobile subscribers including name, mobile number and geolocation information. Vendors such as Gemalto, a Thales company, are strong in this sector.

Market Drivers & Adoption

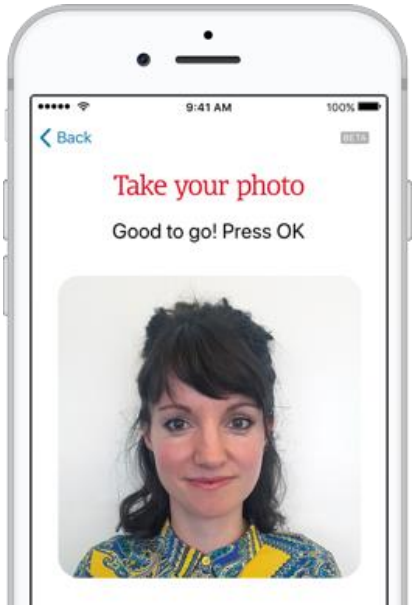
The Experian 2018 UK&I Fraud Report points to a **32%** rise in personal loan fraud, whilst current account fraud still accounts for **60%** of all fraud. In the insurance sector, identity fraud skyrocketed **10250%** between January and June 2017 compared to the same period in 2016.

Case Study - Daon New Zealand Department of Internal Affairs

Organisation: Department of Internal Affairs (DIA), Government of New Zealand

Business Objective: Increase uptake of the **RealMe** verified identity, a government-issued digital identity that New Zealanders use to prove who they are online. Includes opening up a bank account to applying for student loans.

Solution: A national digital identity establishment capability, via a web photo capture or mobile app, secured by Daon biometrics, incorporating client and server-side liveness challenges.



Daon &
Te Tari Taiwhenua
Internal Affairs
RealMe®

Case Study - Daon New Zealand Department of Internal Affairs

The Challenge: The RealMe verified identity is a government-issued digital identity that New Zealanders can use to prove who they are online for a range of purposes, from opening a bank account to applying for student loans. A RealMe verified identity, along with a user's proof of address, is convenient both for the individual and online service providers such as banks, who need to satisfy Know Your Customer and Anti-Money Laundering regulations. But many people who applied for RealMe verified identities stopped short when they got to the final step requiring them to visit a New Zealand PostShop for an in-person face image capture using Daon's retail outlet desktop software. About 43% of people applying for a RealMe verified identity dropped off at this verification stage due to the requirement to go to a PostShop. The DIA needed a way to improve convenience by letting applicants take a selfie on a mobile app, or through a mobile or desktop web browser, and send it digitally to the DIA.

The Solution: The Department of Internal Affairs and its partner in the project, Kiwibank, collaborated with Daon on what would be a long-term project of designing, deploying, testing and securing the innovative service. In particular, Daon provided a combination of multiple client-side and server-side liveness capabilities—a unique proposition that other vendors could not match. This would allow any New Zealand passport holders to not only take a selfie and transmit it via the RealMe Now app, or a mobile or desktop web browser, but it would also allow Daon's IdentityX Server Platform to issue liveness challenges via the app or browser. (These liveness techniques include both passive and active; active, for example, includes asking an applicant to nod, shake and blink.) The resulting liveness challenge response videos would then be checked in real time by the server platform, countering potential attacks and helping ensure that the applicant truly was the individual contained in the selfie.

The Results: Working with the DIA and its technology partners, Daon developed the biometric capability at the heart of the RealMe Now app, which has been enthusiastically welcomed by the public. In just a few months, some 10,000 New Zealand passport holders have used the RealMe Now app to successfully apply for a RealMe verified identity. The addition of the secure web channel has also extended RealMe facial capture to web browsers and other devices, giving more New Zealanders the option to take their own photo.

WHITE PAPER

THE DIGITAL IDENTITY PROBLEM
SOLVING THE ISSUE OF TRUST

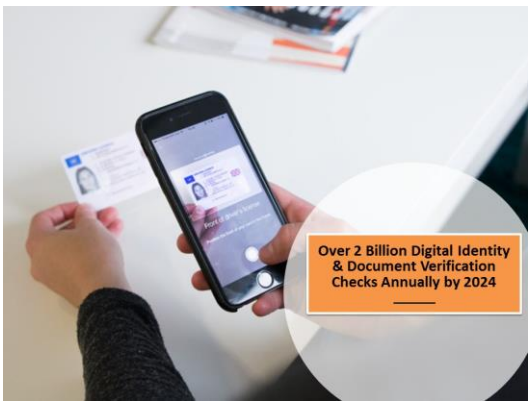
June 2019

Digital Identity & Document Verification: Market & Technology Analysis, Adoption Strategies & Forecasts 2019-2024

The first edition of **Digital Identity & Document Verification; Market & Technology Analysis, Adoption Strategies & Forecasts 2019-2024** is a 172-page analyst report that provides detailed analysis of the market and adoption digital identity and document verification services.

The report includes:

1. Review of current global adoption
2. Market analysis, including key drivers and barriers for adoption
3. Adoption Strategies and examples segmented by region and industry
4. Technology analysis
5. Analysis of important technology vendors and services providers operating in this sector
6. Forecasts for identity & document verification checks and revenue by segment and biometric technology within the six-year period 2019 to 2024



WHITE PAPER

THE DIGITAL IDENTITY PROBLEM
SOLVING THE ISSUE OF TRUST

June 2019

About Goode Intelligence

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Goode Intelligence is a leading identity and biometrics research, consulting and events organisation founded in 2007, headquartered in London.

For more information on this or any other research please visit www.goodeintelligence.com.

Follow us on Twitter.

Further information about the Digital Identity & Document Verification Market & Technology Analysis & Forecasts 2019-2024 report can be found at https://www.goodeintelligence.com/report/digital-identity-document-verification-market-technology-analysis-adoption-strategies-forecasts-2019-2024/

With thanks to Daon for permission to use the case study.

Daon