thalesgroup.com

THALES
Building a future we can all trust

Key best practices for **digital onboarding**

for a seamless Know Your Customer (KYC) onboarding process

This white paper highlights the key best practices we have identified during deployments of KYC projects using our solution in the private banking sector, and the key technologies to use to enable smooth onboarding and reduce identity fraud.

Key best practices for digital onboarding

A user-centric approach

Today, new customers increasingly expect to be able to open a new account online using their laptop or mobile. It means that financial institutions (FIs) need to offer digital onboarding via online and mobile channels. However, there are still many that are unable to provide this service. Some may have elements of their onboarding process online but customers still need to sign a final document in-branch. This can be a big obstacle for new customers and result in increased rates of abandonment. Others may offer a fully online experience but the onboarding process is too complex and customer unfriendly, which also leads to abandonment.

The customer experience is critical for a successful KYC onboarding process. Competition for customers is fierce and there is a huge number of offers in the market. The challenge is to pair the best digital identity verification and risk management mechanisms to streamline your onboarding process. Both are essential and one should not prevail over the other.

It is important for FIs to make processes as simple and convenient as possible for their customers. A mobile onboarding solution must be user friendly right from the start. By successfully digitalising their customer onboarding process, FIs can avoid a high rate of abandonment, ensure secure and convenient onboarding, and better serve their end customers.

To provide a frictionless user experience while avoiding identity fraud, FIs need to focus on the following key areas in their digital services:

- Provision of strong identity verification technologies and mechanisms
- Provision of robust biometric verification
- Provision of additional verification services for scoring, reputation and risk management
- Setting up business rules associated with the onboarding process (acceptance, rejection, step-up verifications, AML sanctions lists and so on)
- Provision of a frictionless digital user experience for apps and services
- Ensure that state-of-the-art security checks are performed in accordance with regulations.

Strong identity verification technologies

The challenge starts with the document authentication done by the customer in the initial phase of the digital onboarding process. FIs need a reliable, automated, digital authentication system to handle the processing of those documents which can include passports, IDs and driver's licenses. The authentication needs to include mechanisms to isolate and distinguish most of the security elements embedded in a document and also be able to extract the information needed and confirm authenticity. International FIs providing services across countries need to consider this factor on a worldwide scale.

The digital authentication process removes the need for costly and time-consuming manual verification processes. Manual verification is used only when extra verification is required by government regulation or business rule sets.

A wide spectrum of documents – with all their (visible) security features – needs to be covered, to enable the full authentication of the documents during digital onboarding. This replaces cumbersome processes such as knowledge-based authentication (KBA) or manual verification, which are costly, inconvenient and not sufficiently secure.

As documents and security features evolve, FIs need to be able to rely on a trusted verification partner which can make sure any changes are taken into account as they happen. A partner in the document manufacturing business can guarantee that all the latest document security updates are supported by the identity verification service.

Document verification is a digital verification process used to verify the authenticity of a user's ID document. The customer uses their own mobile device to capture the document during the onboarding process. Document verification is processed by a server to screen for all the security elements that prove authenticity. Each document is given a verification score and the FI is told whether a customer's document is fake or genuine.

Advanced document verification includes:

- Data integrity checks
- Data format checks
- Visible security feature or pattern checks: watermarks, stamps, line patterns
- Machine Readable Zone (MRZ) inspection and cross-verification with visual information
- Expiry date check
- Data extraction, such as the name and date of birth to be used in the banking systems

Benefits for the end user:

- Fast and easy onboarding in less than a minute
- Full digital user experience via mobile or web channel

Benefits for the FI:

- Automated ID verification process: no further manual checks required
- No additional staff needed to assist with onboarding and training
- Consistent results and verifications
- Regulatory compliance, including anti-money laundering (AML) and customer due diligence
- Reduce risk of fraud

Best-of-class facial match

To complete the remote onboarding process, customers must be able to prove they are who they say they are and physically present at the time. This step is essential to associate the physical user with the use of their document. However, this step must be treated with care as it is open to fraud as well.

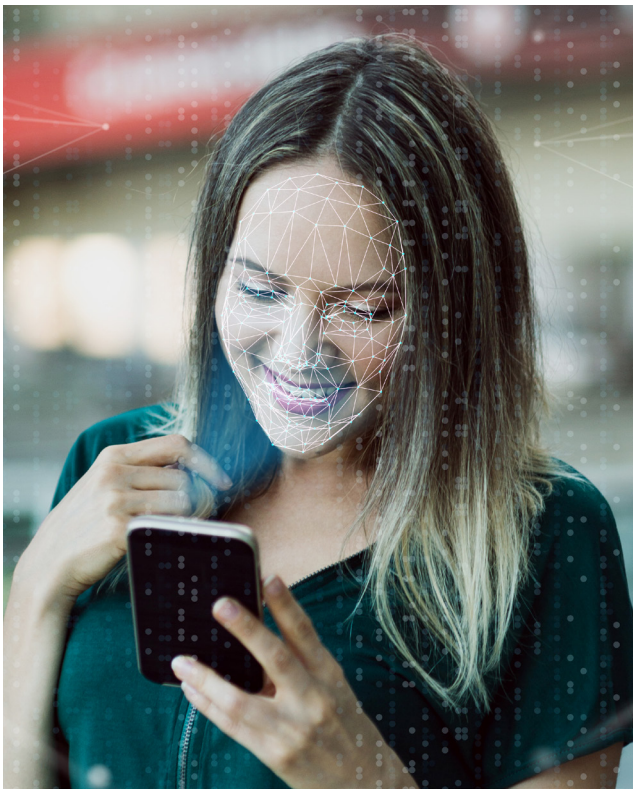
In some countries, video verification is required. But this does not provide fully automated onboarding and adds a constraint for both the end user and the FI: they need to connect which each other to complete the verification. This means that FIs need to maintain a customer service interface to enable consumers to connect with them, which is complex and costly for FIs.

The principle of a facial match service is to compare a simple selfie of the user with the picture extracted from their ID document, which has already been proved genuine. Again, the customer can use their mobile device to do this and so streamline the remote process.

Facial match services use advanced algorithms to compare facial biometric parameters: the shape of eyes, nose, ears, hair and lips; their colours, and the size and distance between them. The comparison results give a matching score, resulting in a conclusion that, potentially, this is the same person. FIs need to use the most advanced algorithms to avoid false positive rejections or false acceptances. They want to avoid repeating the process because it could cause the user to abandon the onboarding process.

Before selecting the appropriate technology we recommend that FIs consult organisations such as the National Institute of Standards and Technology (NIST), a US public body, which classifies the performance of biometric suppliers, or a similar organisation in the region in which the FI is active.

It is important to note that, to avoid fraud using a static image, the technology needs to employ liveness detection during the selfie stage. Liveness detection is used to prove that the selfie is from a live person. It can include active methods, such as requesting the customer blinks their eyes or makes random head movements, or more advanced passive methods. FIs potentially need to consider the best mix of frictionless methods and best-performing scoring methods for their needs. Liveness detection technology must guard against the use of masking technologies, pre-recorded video or high resolution images.



Regulatory compliance

Anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations are being imposed and reinforced all over the world for onboarding new customers and to fight identity fraud. FIs need to strengthen customer identification using reliable and independently sourced documents or data. Additionally, they must store all customer ID records, including copies of ID documents, and they must check information veracity and prove the means and processes that they have implemented to counter identity fraud. The latest AML v5 and v6 regulations require PEP and sanction checks for all new customer registrations and for the implementation of proper risk assessment policies. As well as risking their reputation, FIs are exposed to a heavy financial risk and fines if they fail to comply. They need to ensure that during the customer due-diligence and onboarding process, all mechanisms and proofs are stored digitally to ensure full compliance. They need to check IDs against formal sanctions lists provided by national organisations and public regulators.

It is vital to anticipate new regulations and to extend the KYC verification processes to all use cases, including onboarding, account opening, credit and lending, credit/debit card issuance, and other bank-specific value-added services.

ID verification can be completed only once these additional AML sanction lists are checked for each end customer wishing to open an account.

FIs need to be able to reassess the account holder during the whole customer life cycle. Continual reviews need to be carried out.

Enhanced onboarding with risk assessment

The point at which an account is opened is when it's essential for FIs to protect against fraud. They need to use everything in their armoury to reduce the fraud risk to zero.

Verification by existing credit bureaus is limited because their approach is based on fixed personal information, which makes them less likely to detect fraud. Add to this the volume of stolen personal information being used to open accounts, which has caused fraud rates to increase rapidly over the past few years.

So it is essential for FIs to combine a risk management engine with identity verification, a solution that can greatly reduce the risk of fraud. Our focus is on new account origination risk management. At this stage, risk parameters such as the device, email and IP address can be analysed and allow the FI to score the individual more accurately. A risk-based analytics approach can flag suspicious activity or fraudulent behaviour and allow FIs to abort final account opening process verification, so minimising the overall verification cost. During user onboarding, the risk engine records the IP address, geolocation data, the device used, mobile operator data and information from any other third party that's required for additional checks, such as national registers to check against stolen IDs or deaths.

FIs can determine in their business rules what elements trigger the step-up to the next stage of verification depending on their scoring. They define business rules via policy management.

Policy management allows FIs to perform additional checks related to the information that has been collected and to work out whether to accept or reject an end user's application. The main objective is to reduce ID fraud using additional parameters to pinpoint fraudulent behaviour.

With this additional, risk-based approach combined with an identity verification solution, FIs can drastically reduce ID fraud at the account opening stage.

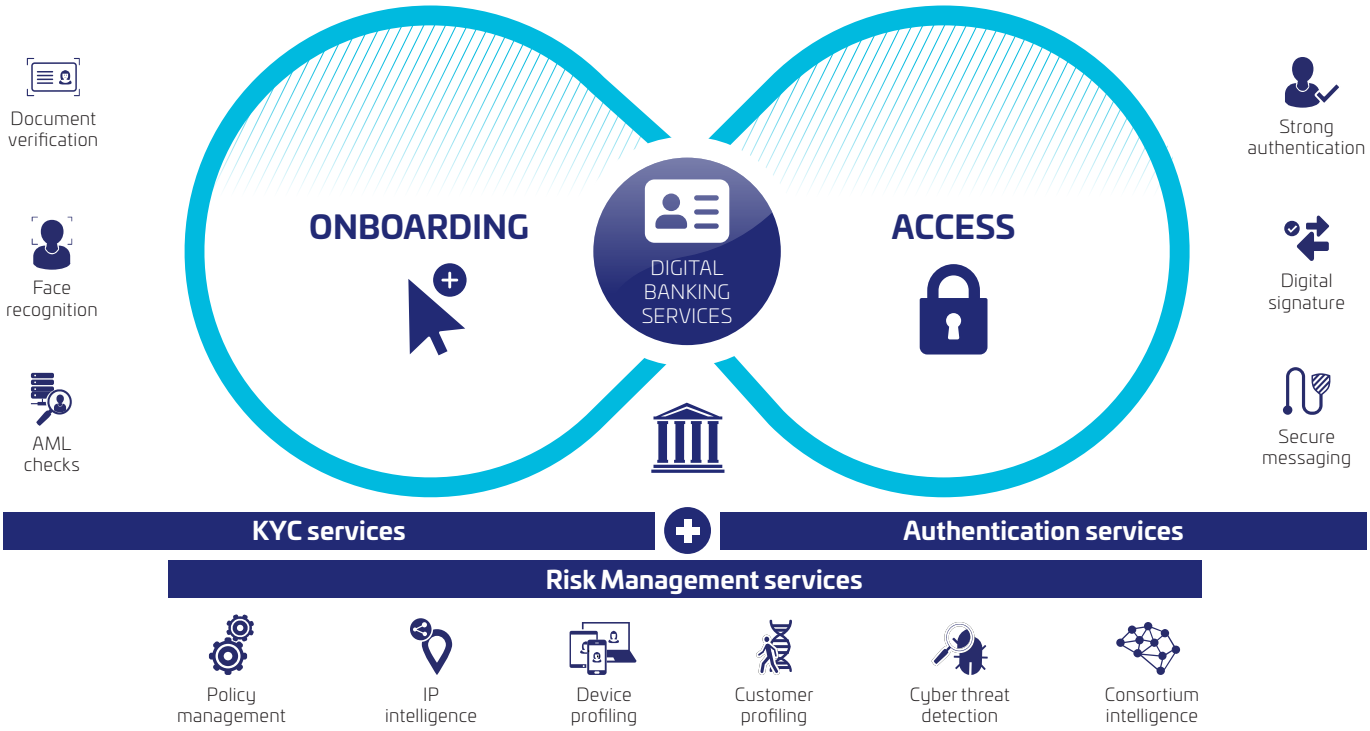
Multi-layer identity verification service approach

FIs need several layers of verification during the onboarding process and to ensure that these are deployed with a minimum of impact on their existing infrastructure. Today, cloud services can offer an optimal approach to providing these verification services without FIs having to completely reorganise their business. Cloud suppliers should provide security mechanisms to enable efficient GDPR-compliant services plus a business continuity plan and a service level agreement. A cloud approach can provide immediate benefits, enhancing the customer onboarding experience while guaranteeing best-in-class risk assessment.

It can also be scaled up over time as regulatory requirements or industry standards for verification evolve while at the same time minimising the threat of identity theft fraud.

A cloud solution should enable FIs to configure the necessary verification flows depending on the results, scores or business rules that apply for the service.

A strong multi-layer identity verification service approach combined with the best user experience will definitely support consumer acquisition growth.



Customer retention strategies

A KYC identity verification solution can help FIs to develop an effective customer retention strategy, leveraging best-in-class document authentication, biometric verification and additional risk management service checks.

Biometric data such as face or fingerprint can be used for further customer authentication in other value-added services that the financial institution may want to offer during the full account lifecycle (mortgages, loans, insurance, credit cards, debit cards, international remittances).

On the commercial side, as online and mobile transactions grow, new forms of multi-factor authentication and identification are needed. Combining best-in-class technologies, financial institutions have access to available trusted identities and strong biometric authentication to develop through the digital economy.

Once an account has been authorised, FIs need to ensure that customer account access and information is secure. Each access requires advanced authentication. Some service requests may require remediation or additional verification to be performed.

Access, authentication and service acceptance also need an optimised user experience to guarantee customer retention.

To provide the highest level of security, FIs need to ensure that adaptive authentication methods are in place, using new technologies such as behaviour analytics, and location and device integrity checks.

The digital user journey must be adapted according to the risk associated with the service and the authentication step-up required.

Digital audit trails

Following the latest AML regulations and directives, FIs need to prove account opening verification. For this reason, they must keep records of the verification performed at account opening or transaction level. Audit trails have to be retained. The solution must be able to store all details at the point of verification, including image evidence (document, face) and the scoring associated with it, so this can be retrieved at a later stage if needed. This enables FIs to protect themselves against legal claims and disputes related to any fraud attempts committed by end customers.

Thales Gemalto IdCloud **is a business priority**

Customers today expect opening an account to be fully digital. Banks, neobanks, fintechs and other FIs need to provide mobile and web account opening services which deliver a customer-centric experience to streamline onboarding and service adoption.

Remote account opening is crucial to FI growth, and customer identity verification remains a key initial step in enrolment and fraud prevention. The challenge is to provide a frictionless process that enables smooth onboarding. Fraud and identity theft is a growing risk for FIs and a key element to consider in the onboarding process. Regulations and compliance are reinforcing customer due diligence procedures and directives.

At Thales, we have an R&D engineering team with a total of more than 40 years of experience in the fields of authentication, ID verification and fraud prevention. Every member of the team is dedicated to sustaining and developing our Gemalto IdCloud services for onboarding and access.

Thales Digital Identity and **Security**

Businesses and governments rely on Thales to bring trust to the billions of digital interactions they have with people.

Our identity management and data protection technologies help banks to exchange funds, people to cross borders, energy to become smarter and much more.

More than 30,000 organisations already rely on Thales solutions to verify the identities of people and things, grant access to digital services, analyse vast quantities of information and encrypt data.

In early 2019, we acquired the international security company Gemalto and have combined it with our existing digital assets to create a new leader in digital security. Every organisation around the world is in the midst of a digital transformation and stands to benefit from our joint innovations.

As the world becomes more connected, Thales makes it more secure.

Key figures for Thales Digital Identity and Security

16,000 employees
delivering digital identity & security solutions to
30,000+ businesses & governments

3,000+ financial institutions
rely on us to protect their
payment and banking services

200+ government programs
deployed for civil identity, biometrics
and law enforcement

US $1 trillion interbank fund transfers
per day protected with our data encryption platforms.

Managing identities
and protecting data for **billions**
of people and things every day

THALES

Building a future we can all trust

> Thalesgroup.com <