thalesgroup.com

THALES
Building a future we can all trust

Thales Gemalto IdCloud for Onboarding

Cloud based solution to secure onboarding to digital banking services

Thales Gemalto IdCloud for Onboarding

Cloud-based solution for secure onboarding to digital banking services

Banking and Payment Services

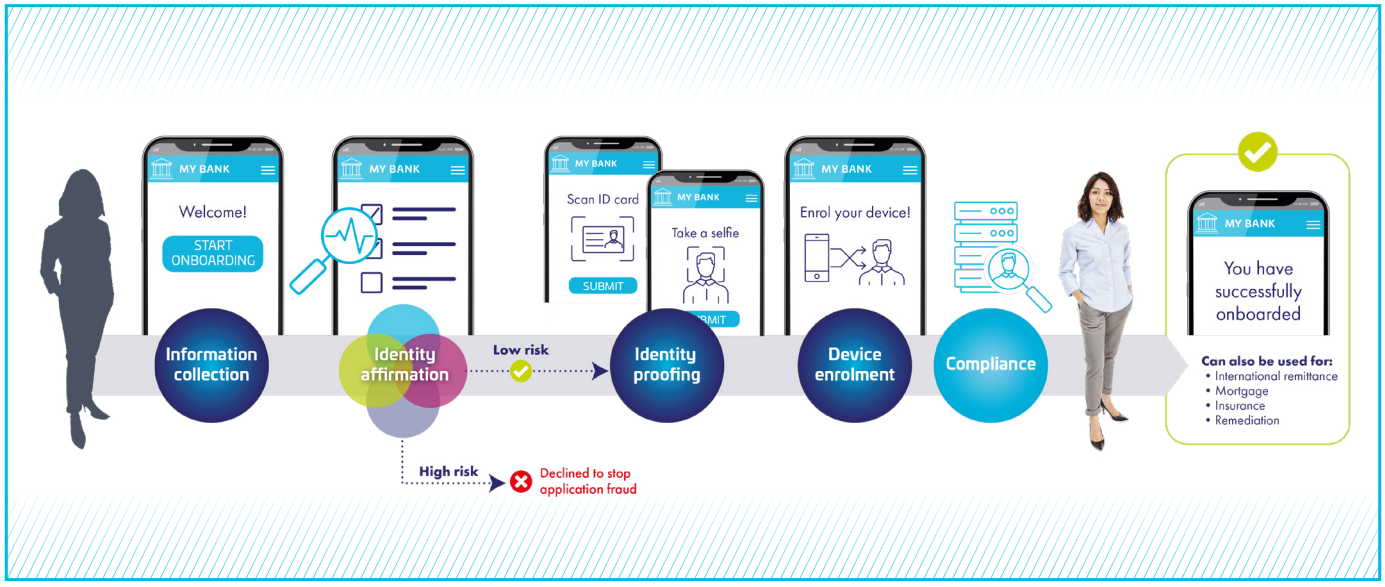
Swift and secure customer onboarding

Customers today expect to be able to open a new account online from their laptop or mobile. This means that financial institutions (FIs) need to offer a **fully digital onboarding experience** to avoid abandonment during the enrolment phase, while also adhering to stringent **know-your-customer (KYC)** regulations.

To be able to offer this you need **identity proofing services** such as document verification, face recognition and anti-money laundering checks (AML). There are many document verification solutions suppliers, but what sets our Gemalto IdCloud platform apart is that you also get access to **risk management services** which are essential in the onboarding process to **reduce application fraud.**

The Gemalto IdCloud risk engine performs additional background checks such as user attributes, device details and network information. This essential step is called **identity affirmation** and brings supporting evidence for an identity claim, to increase the level of confidence.

By adding identity affirmation you can introduce **adaptive onboarding** and start by checking for any signs of potentially fraudulent activity, before even launching the actual identity proofing process. The goal is to **prevent ID fraud** during digital onboarding, but it can also lower total cost of ownership by avoiding additional checks and abandoning high-risk enrolments at an early stage.



Adaptive onboarding

Document verification

Document verification is a digital verification process used to **verify whether a user's ID document is authentic.** The customer uses their own mobile device to capture the ID document and sends the photo to the Gemalto IdCloud server for the verification process, which screens for all security elements to prove authenticity. A score is produced for every verification screening and the FI will be informed whether a customer's document is fake or genuine.

Advanced document verification includes checking:

- Data integrity
- Data format
- Visible security features or patterns – water marks, stamps, line patterns etc
- Machine Readable Zone (MRZ) and cross-verification with visual information
- Expiry date
- Data extraction, such as name and date of birth to be used in the FI's CRM system

Our solution also supports **NFC to read electronic ID documents** giving a foolproof way to extract data stored on the ID chip and obtain the customer's information, including a high-quality digital copy of their image.

Facial recognition

To complete the remote onboarding process, customers must be able to prove they are a real person and physically present during the onboarding process. This step is essential to associate the physical user with their ID document.

The facial match service asks the user to take a selfie which it then compares with the image extracted from the ID document, which has already been verified as genuine. Again, customers can use their mobile to do this, so streamlining the remote process.

Thales' facial recognition technology is one of the best in the world. Our service also includes **passive liveness detection** of which the end user will be unaware to guarantee a live person is performing the request.

The onboarding experience from an end user perspective

Risk management for identity affirmation

Identity affirmation technology harnesses the power of four layers of intelligence. Each layer transparently analyses user and environment activities from different perspectives to **identify high risk** before any harm is done.

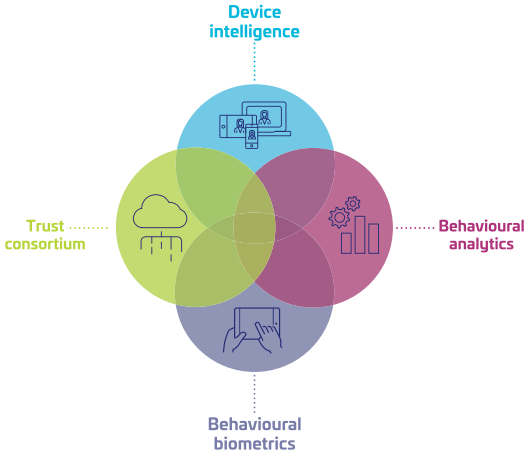
Together, they create a dynamic profile of each event, giving you the confidence that you are identifying 'good' consumers based on their online interactions.

Device intelligence allows you to accurately identify recurring devices, detect high-risk networks and locations and spot device anomalies which can indicate fraudulent activity.

Behavioural biometrics looks at inherent user behaviour and analyses how someone types, moves the mouse or holds the device. At the onboarding stage this can be used to compare each individual with a population profile to detect potentially fraudulent users or distinguish between humans and bots.

Behavioural analytics analyse user habits at the service level to create a 'good user' and 'fraudulent user' profile for a specific application form.

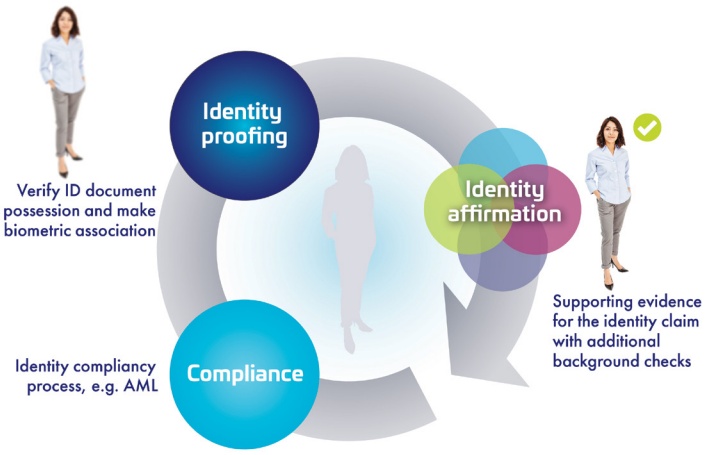
Trust consortium evaluates billions of events to help you know who to trust, even if they are new to you, by gathering anonymised and encrypted insights from online events across our clients. If an IP address, email domain or device ID is linked to past fraud in another environment a warning will be issued.



Anti-money laundering checks

Anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations are being imposed worldwide when onboarding new customers. These regulations are also being used to fight identity fraud, so FIs need to strengthen their customer ID checks using reliable and independently sourced documents or information.

With the latest AML v5 and v6 regulations, new customer registration requires **PEPs and sanction lists verification** and proper **risk assessment policies** to be set in place. Identity verification can be completed only once these additional AML sanction lists are checked for each customer seeking to onboard.



A full digital onboarding process need multiple verification layers

Benefits for financial institutions

OPTIMISE USER EXPERIENCE
- Frictionless capture /enrolment experience
- Reduce abandonment rate
- Automated data extraction

REDUCE APPLICATION FRAUD
- Prevent mule account creation
- Bundled and tested rule templates
- Real time fraud strategies optimisation

REDUCE OPERATING COSTS
- One integration to access multiple technologies
- Optimise usage of service verification to apply only if initial checks are passed
- Cloud reducing integration time and lead costs

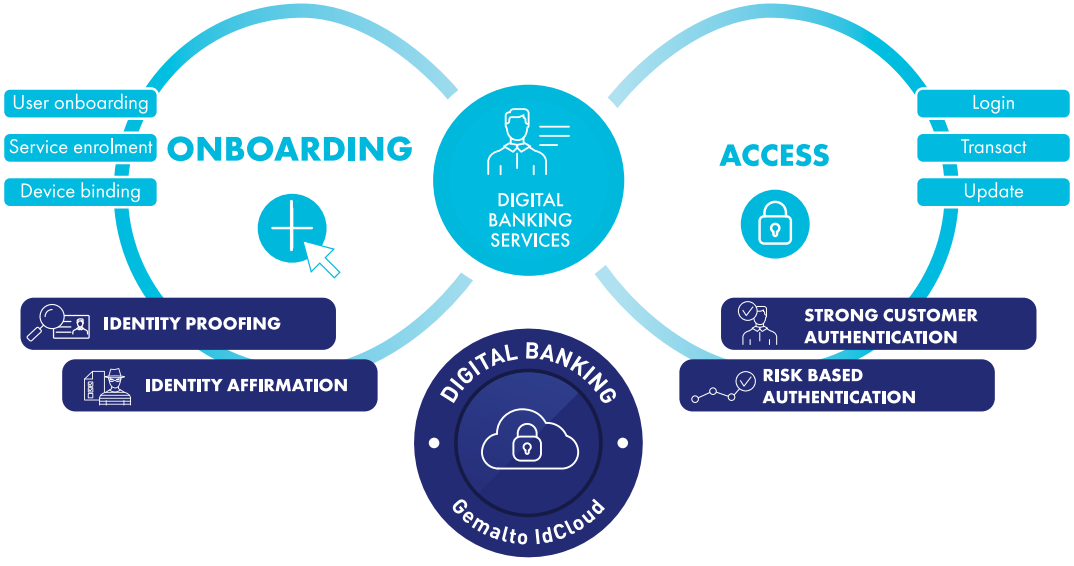
MOBILE & WEB
- Optimise conversion rate
- Mobile NFC option
- Adapted to bank use cases

TECHNICAL BENEFITS
- Scalable
- UV/IR option
- Bank grade security

COMPLIANCE
- GDPR/CCPA compliancy on data privacy
- AMLD5 compliant

Thales Gemalto IdCloud - a cloud platform for secure onboarding and access to digital banking

Our cloud-based managed services enable FIs to combine identity proofing and strong customer authentication to provide secure onboarding and access to digital banking. By adding risk management you can further increase security and enhance the customer experience with identity affirmation and risk-based authentication. With one single platform.



> Thalesgroup.com <