thalesgroup.com

THALES
Building a future we can all trust

Thales Gemalto IdCloud - Risk management

Enhanced security and user experience for digital banking services

Thales Gemalto IdCloud – Risk management

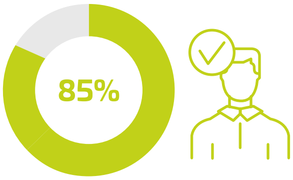
Cloud based risk management technologies to enhance security and user experience for digital banking services

Banking & Payment Services

Why is risk management key to digital banking?

With a multiplication of digital channels and massive adoption of mobile banking, financial institutions (FIs) are facing a dramatic increase of cyber-attacks. Phishing, account takeover and social engineering are just a few examples on how fraudsters constantly challenge security measures put in place. It is hard to stay ahead while maintaining a smooth user experience. Yet, that is necessary, convenience is key. FIs must reduce friction for their customers and offer a **convenient and secure digital banking experience,** while making sure they **comply with the latest security regulations,** such as PSD2 in EU.

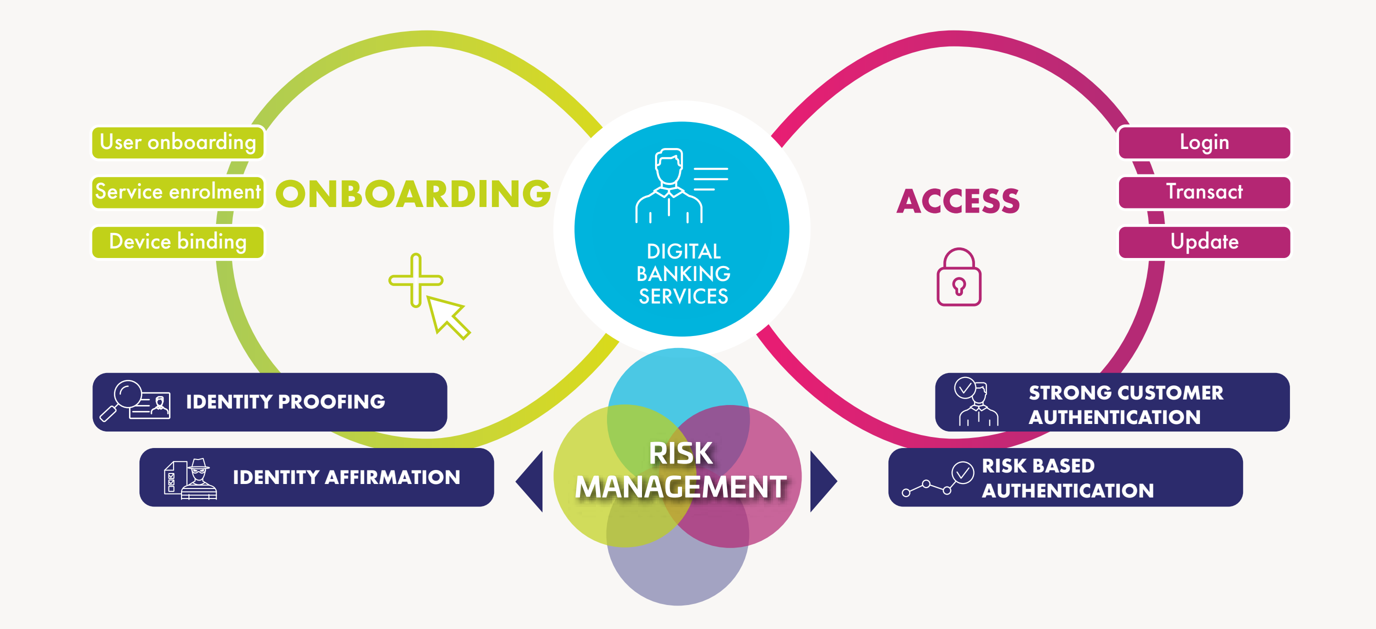
Risk management services should be at the heart of all digital banking services to **add an extra layer of security** and **improve the user experience** through the full customer journey. They protect several user endpoints by detecting abnormal behaviours, whether at onboarding, login, account sign up, or during a transaction. By monitoring the user behaviour throughout their entire online interaction, our risk management creates accurate behavioural profiles in real time to protect users from attacks, such as account hijacking or account takeover. This continuous monitoring allows companies to **recognise their good users and remove friction for a better experience.** This is especially important given that 85% of all online traffic for FIs comes from good users*, let us treat them with the trust they deserve.



of all online traffic for FIs comes from **trusted users***

Protecting the full digital banking customer journey

Using the same platform to secure initial customer onboarding as well as daily access brings many benefits for FIs. The same risk management technologies are used to perform background checks in both scenarios to enhance security and user experience. For digital onboarding this means you get **identity affirmation,** which brings supporting evidence for an identity claim, to increase the level of confidence and fight application fraud. For daily access you get **risk based authentication (RBA)** which let you adapt your authentication strategy to the level of risk in order to reduce recurring customer friction and prevent account takeover attacks. **All running silently in the background to provide the best end user experience.**



Four layers of risk management technologies working together

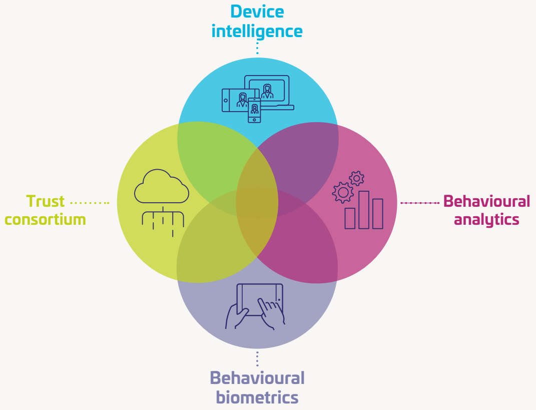
Our risk management technologies harness the power of four layers of intelligence working together. Each layer analyses anomalous activities from different perspectives to identify those that are high risk before any damage occurs.

Device intelligence

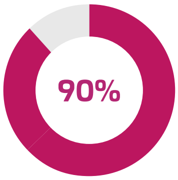
Device intelligence **gather information about the client** (laptop and mobile) **and the network environment.** The purpose is to **detect anomalies** like inconsistencies between location, time zone, language, OS, browser versions and more, as well as connections established from suspicious networks. It can accurately recognise returning devices and elevate the level of risk when a new device is used.

Our solution use a persistent device ID (PDID) that creates a unique device identifier by combining device ID, device fingerprint and the device history. This identifier is resilient to software updates, cookie wipes and other major changes within the device.

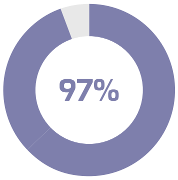
The four layers of risk management



Powered by: NuData Security mastercard



of trusted interactions come from a known device*



of fraud comes from an anomalous device or network*

Behavioural biometrics

Human behaviour makes us unique. Our risk management **recognise your legitimate end users** by analysing how they behave. This layer builds an inimitable profile of each end user by looking at how the user types, moves the mouse or holds the device, among others. Behavioural biometrics relies on these key metrics to build profiles for individuals, global populations and bots (automated attacks).

Individual profile

A behavioural biometrics profile on an individual level can detect:

Account takeover: A fraudster is trying to enter credentials that were previously phished with a fake web site or illegally acquired from stolen databases. A fraudster using stolen credentials can be detected by comparing the behaviour to the legitimate user's typical behaviour.

Social engineering attack: When fraudsters are driving legitimate users to perform actions on their behalf, sometimes in real time. Unfamiliarity with data typically means slower than normal typing, higher number of corrections and higher typing deviations. A user will for example not type the same way when copying information from a document and when instructed over the phone.

Global population profile

The statistics used to build an individual profile can be extended to build an entire population profile, which is useful in customer onboarding where the user is unknown by definition. For a group of users, behavioural biometrics aggregate individual interactions to create an overall 'good user' and 'fraudulent user' profile.

As an example, legitimate users have an average number of mouse click or touch event on a specific service, which differs from fraudsters. Legitimate users have good knowledge of their personal information but are usually unfamiliar with the web pages or application, while for fraudsters it is the opposite.

Automated attacks detection

A basic automated attack lets a bad actor test a large number of credentials very quickly but often shows tell-tale bot behaviour such as repeated use of the same IP address or same device. As a result, it is easier for security tools to detect.

A sophisticated automated attack imitates real human interaction by running scripts that tries to mimic human behaviour. Sophisticated attacks are still lower in volume, but constantly increasing. These are much harder for common security tools to detect, but our behavioural biometrics layer also detects sophisticated attacks.

Behavioural analytics

Behavioural analytics

The behavioural analytics layer analyse user habits at individual and population level to **detect anomalous situations.**

At individual level, the engine looks at the typical device, location and spending patterns, among other things, for a specific user. While at a population level, the system creates patterns that are typical for the service as a whole. If a specific user or service is having too many signals deviating from the average legitimate usage, it is a good sign that it is a fraudster interacting with the service.

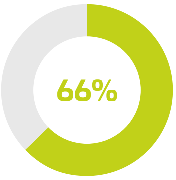
Trust consortium

Trust consortium

This layer aggregates selected data points across the client base to build **reputation analysis.** It builds fraud and reputation scores based on previous scores where the data points were seen. Data comes from a global consortium database populated by other entities using the same solution.

Trust consortium input:

- IP address
- Device endpoint
- Email domain



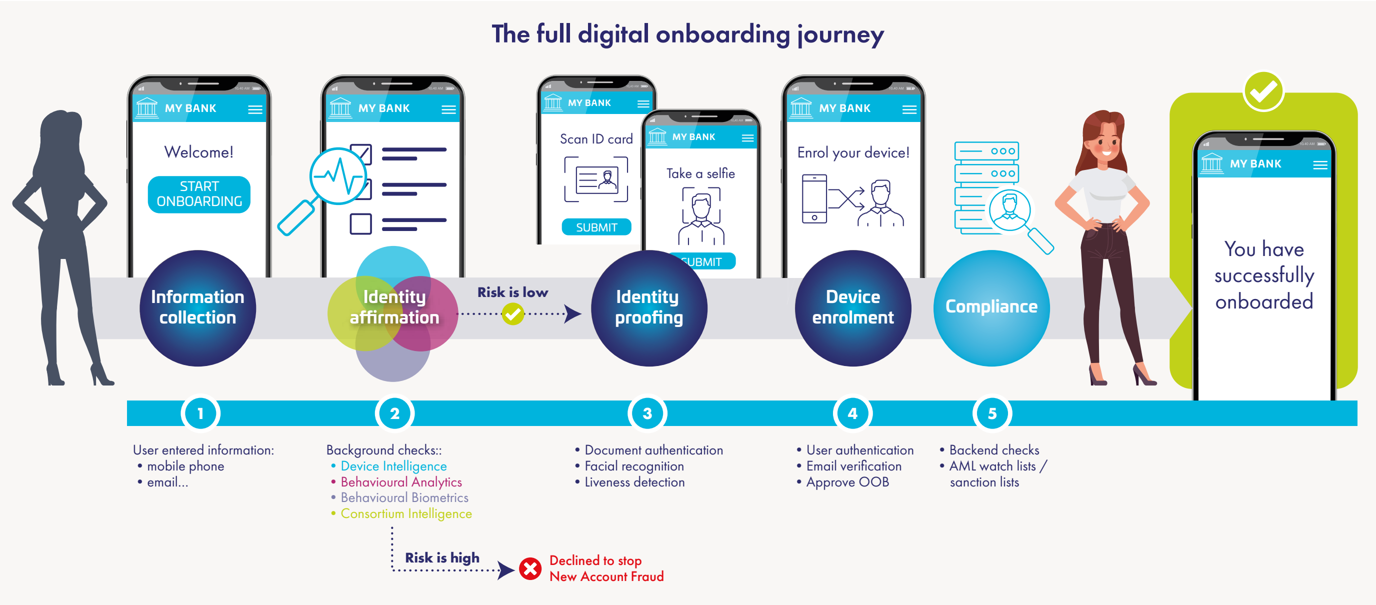
of attacks in 2020 had bad-reputation IPs, flagged by the consortium, proving its benefits*

Risk management in action

One of the strengths with Gemalto IdCloud is that the same platform is used to secure and enhance the full customer journey, from initial onboarding to daily access. Below you can see two examples of how risk management is active in both these use cases.

Service enrolment

We start monitoring user activity with background checks as soon as they start filling in personal information, which can very quickly alert about the risk of fraud. In this case, we can avoid the cost of a complete ID and facial recognition service when there is already a high suspicion that it is a fraudster who initiated the process.



The full digital onboarding journey

User entered information:
- mobile phone
- email...

Background checks::
- Device Intelligence
- Behavioural Analytics
- Behavioural Biometrics
- Consortium Intelligence

- Document authentication
- Facial recognition
- Liveness detection

- User authentication
- Email verification
- Approve OOB

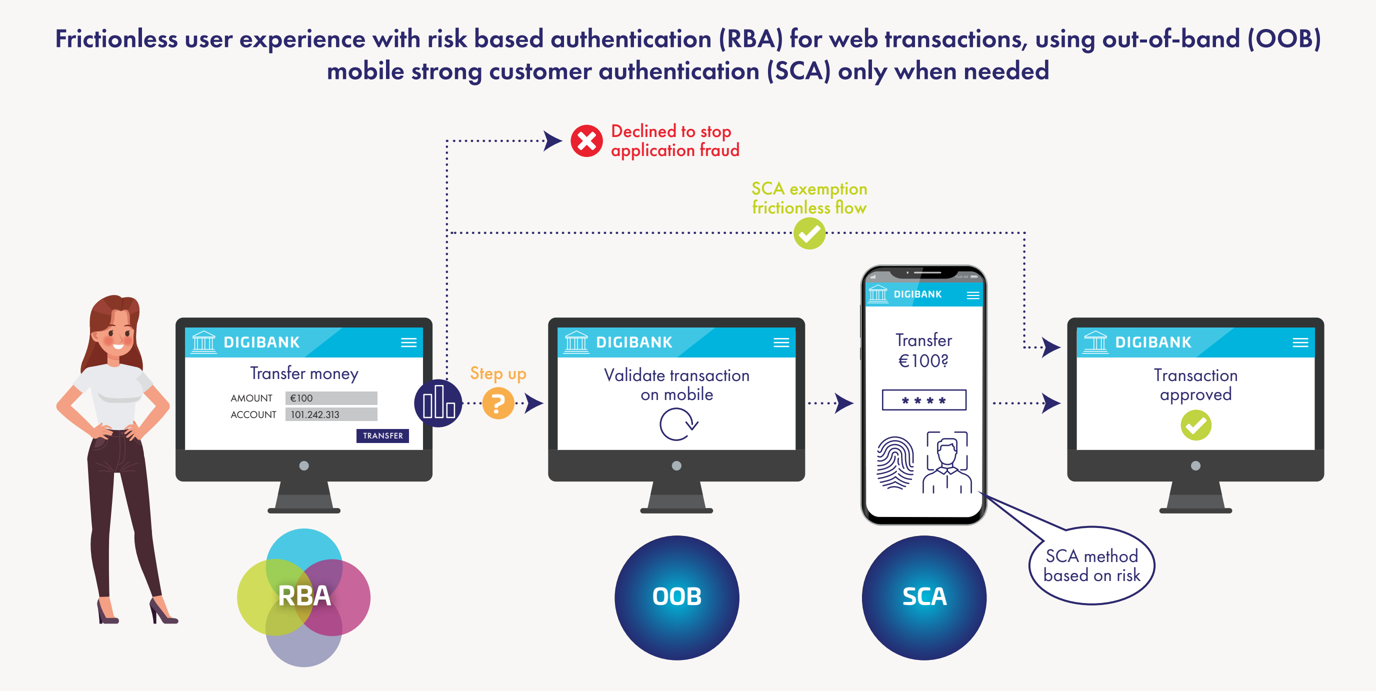
- Backend checks
- AML watch lists / sanction lists

Risk is high

Declined to stop New Account Fraud

Making a transaction

By combining risk based authentication (RBA) and strong customer authentication (SCA) you can simultaneously improve the user experience and security of your services. Here is an example of a typical access flow from a laptop, using RBA to deliver frictionless access for most authentication attempts and relying on out-of-band SCA to prevent unauthorised access only when judged necessary according to risk engine´s assessment.



Frictionless user experience with risk based authentication (RBA) for web transactions, using out-of-band (OOB) mobile strong customer authentication (SCA) only when needed

Regulatory compliance and security certifications

Gemalto IdCloud is the perfect answer to new security requirements raised by regulations such as PSD2 and FFIEC. It allow FIs to meet PSD2 requirements for SCA and dynamic linking and offer real-time monitoring of the authentication and transaction process risk, as required in the regulatory technical standards (RTS) of PSD2. Complex security policies can be defined, based on the level of risk, the type of transaction and the user profile as recommended by FFIEC. It contributes to meet the requirement for stronger risk management to fight against increasing attacks and fraud levels.

Data privacy regulations are becoming more stringent these days, especially with GDPR in Europe and CCPA in US. This can be a challenge to comply with if several different vendors process risk assessment data. Gemalto IdCloud is designed for GDPR and CCPA compliance.

COMPLIANT • EU GDPR • COMPLIANT •

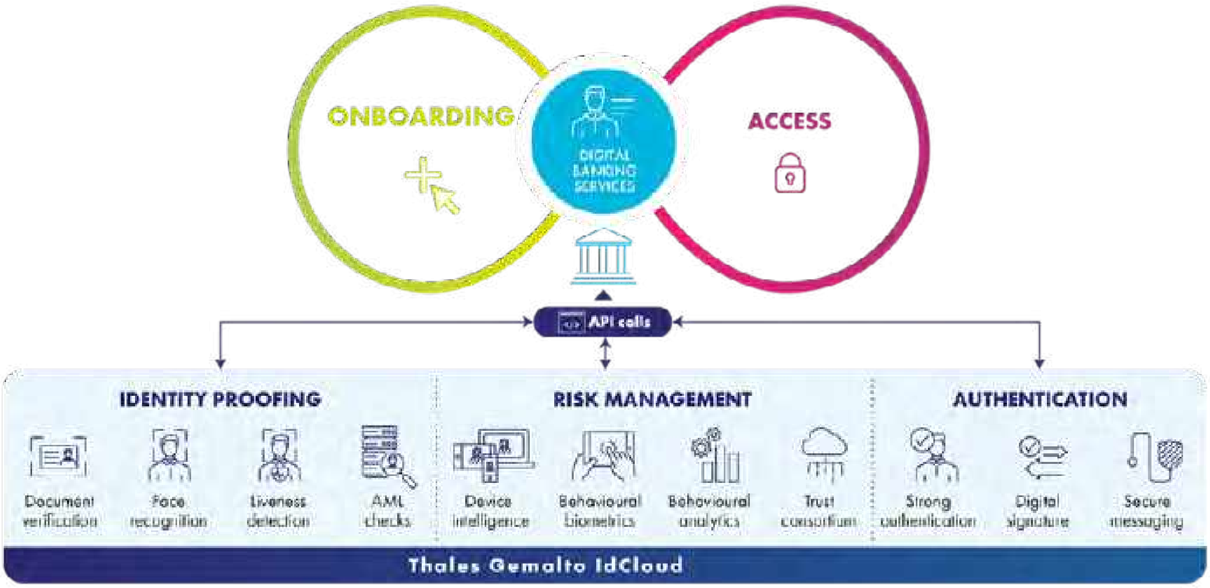
Your trusted partner

As the market leader in strong authentication and identity verification solutions, we are a trusted partner for banks and financial institutions that want to raise the security bar of their services and to achieve regulatory compliance. Our solutions already provide secure and convenient onboarding and access to digital banking services for hundreds of millions of end users worldwide. Moreover, we are committed to support our customers to ensure both data security and privacy.

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

Our cloud based managed services lets financial institutions secure onboarding and access to digital banking with identity proofing and strong customer authentication. Risk management further increase security and enhance the customer experience with identity affirmation and risk based authentication. With one single platform.

WANT MORE?
DOWNLOAD OUR SOLUTION PAPER



About Thales

Thales creates technology for a range of sectors - aerospace, digital identity and security, defence and security, ground transportation and space. With the combined expertise of 80,000 employees and operations in 68 countries, Thales is a key player in creating secure, world-class technology.

* *NuData Security*

THALES

Building a future we can all trust

> Thalesgroup.com <

© Thales 2020. Photos credit: Gettyimages - January 2020 - Design: Jubemo