UBISECURE®

Connecting Identity.
Transforming Digital Business.

Onboarding and KYC

How Ubisecure optimises customer onboarding for seamless, secure and compliant Know Your Customer (KYC) workflows

Onboarding and KYC

Onboarding is a critical part of any digital service that requires knowledge of a user's identity. Whether the onboarding user is an individual or organisation, onboarding plays a key role in the service's success.

User experience is widely accepted as a competitive differentiator in digital business. As onboarding is often the first interaction with your service, a good user experience in this step is paramount. In fact, **45%** of users will give up if the registration process is too manual, complex or time consuming. If you find that prospective users are dropping off in this phase, improving your onboarding workflows can have a big impact on your completion rates.

> **Whether the onboarding user is an individual or organisation, onboarding plays a key role in your service's success.**

Security and fraud prevention are further key focus areas for onboarding. The level of identity assurance needed will depend on your type of service and regulatory context, but trust in who users are and the accuracy of user data captured are generally high priority. However, while security is clearly a crucial factor in onboarding, an incorrect balance of security measures with user experience will put off your intended users.

You will also need to consider compliance to applicable regulations in any onboarding workflows. Take banks for example, which are often mandated to conduct a level of Know Your Customer (KYC) in the onboarding phase. How this is achieved will vary between services, but as with security, a digital-first, user-friendly approach is imperative to success.

— KEY ONBOARDING OPPORTUNITIES:

- UX
- Security
- Compliance
- Efficiency

Onboarding is also an opportunity to improve operational efficiency. This is a chance to take manual workflows and automate them, saving costs and maintaining efficiency at scale. In other words, you need a digital onboarding solution that grows with your business, not one that holds back growth. This is particularly important as organisations around the world reduce face-to-face interactions with the lingering threat from COVID-19.

Ubisecure's expertise lies in helping you achieve the correct balance of user experience, security, compliance and operational efficiency in your digital services. Ubisecure is a leader in digital identity solutions for individual and

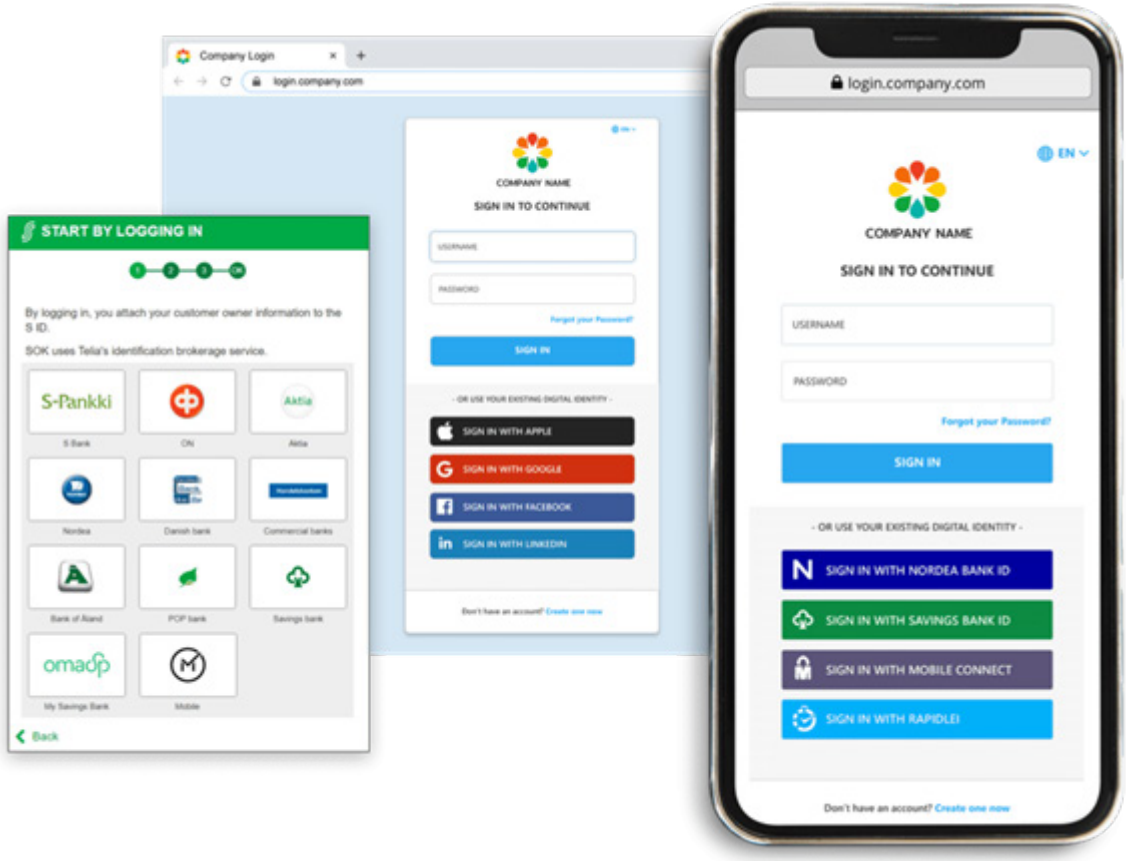
organisation users, with its award-winning Identity Platform (Customer Identity and Access Management/CIAM) and GLEIF-accredited status as a Legal Entity Identifier (LEI) issuer.

This resource shows how capabilities from Ubisecure's technology stack enable you to enhance your onboarding and KYC workflows for both B2C and B2B scenarios, by putting best-practice individual and organisation identity at the core.

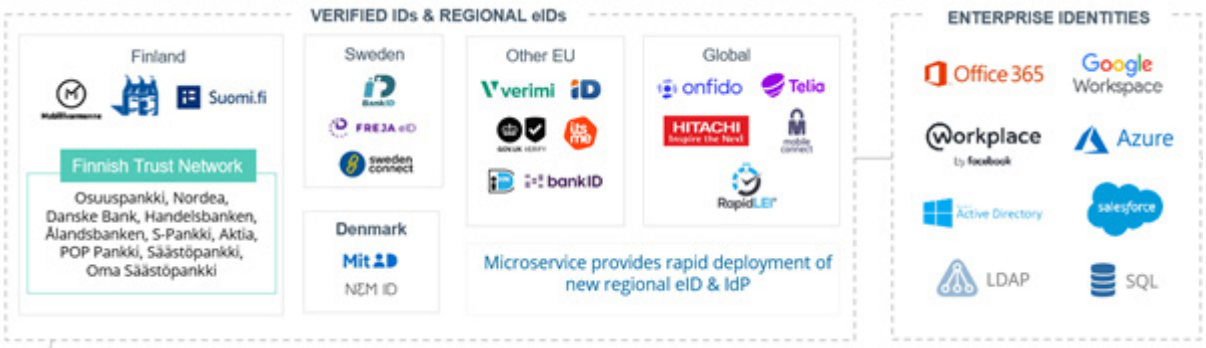
Ubisecure for onboarding

IDENTITY VERIFICATION USING 3RD PARTY DIGITAL IDENTITIES

Organisations often want, or need, to verify the identities of users onboarding to their services – whether for enhanced security and/or KYC/AML requirements. There are many possible identity verification methods that allow you to balance this need with frictionless user experience. The method(s) that you offer will need to be appropriate to your specific organisation and its user base – preferably with multiple options to suit your range of users (including geographical location, demographic preferences, and accessibility needs).



Ubisecure connects the Identity Providers (IdPs) and e-IDs to your services that you need to achieve seamless, secure, compliant and efficient identity verification. It supports dozens of external IdPs, e-IDs, and regional identity schemes, and powers the world's most extensive identity brokering platforms, enabling you to provide identity verification methods that are best suited to your organisation's users and regulatory context.



IDENTITY VERIFICATION USING DOCUMENT VERIFICATION OR PHYSICAL BIOMETRICS

Ubisecure enables real-time identity verification using government-issued identity documents and facial biometrics, in close **partnership with Onfido**.

The combined solution from Onfido and Ubisecure offers Identity-as-a-Service capabilities and scans physical ID documents from over 4,500 document types from 195 countries, and can use biometric technology to verify that the document truly belongs to the person being onboarded. This is particularly useful for service providers needing/wanting to carry out digital-first identity verification, but that operate in countries that do not yet offer standardised verified digital identities.

ATTRIBUTE COLLECTION & AGGREGATION

Effective onboarding requires the organisation to simplify identity management by consolidating, and therefore centralising, the onboarding data set. Ubisecure's CIAM solution supports the collection, aggregation and exchange of user attributes to offer Zero Trust networking while respecting user privacy. The core functioning includes:

Offer Zero Trust networking while respecting user privacy

- Normalising data from different providers to simplify application integration
- Masking user data according to minimum information disclosure principles
- External service queries - resolving a common attribute through a commercial or in-house web service. E.g., citizen uses eID card to log in, we query a government service to resolve the national ID number and use that to find the internal customer number and all available services, like connected contracts or available applications for their use.

Efficiently integrate data sources

Ubisecure CIAM is used to efficiently integrate data sources so the user's identity-related data can be retrieved and utilised on a per-session basis. The result is an individual identity profile, specific to each connected application or outbound federation link. The identity attributes of the user are collected and modified so that they will match the access and authorisation requirements of the application that the user is trying to access. Only those attributes needed for functioning, and authorised by the user, are shared.

DELEGATED AUTHORITY

In more complex onboarding scenarios, for example invitation-based or organisation-based onboarding, Ubisecure offers an advanced delegation solution. **Delegated Authority** enables multi-tier delegated administration and delegation of authority, improving efficiency, reducing costs and enhancing security.

Watch this short explainer video on Delegated Authority.

kuppingercole ANALYSTS

"UBISECURE HAS DEMONSTRATED ITS VALUE SPECIFICALLY IN SCENARIOS WITH COMPLEX B2B2C RELATIONSHIPS, WHERE ITS STRENGTH IN DELEGATING ACCESS IS A DIFFERENTIATOR TO OTHER PROVIDERS IN THE MARKET.

Martin Kuppinger, KuppingerCole

Delegated Authority allows the principle of "verify, delegate, assert" to be implemented on a large scale, within both closed and open ecosystems.

- **B2C/G2C example** – one admin user from a customer group plan (e.g. parent within family) carries out the onboarding process, then sends invitations to others in the group with role-based access.
- **B2B/G2B example** – one admin user from your partner organisation takes responsibility for their colleagues' access to your digital service, within your defined parameters. The partner admin delegates access/authority to users within their own organisation.

> **Both scenarios remove manual work from your own IT/ Support team and eliminate the need for shared access credentials which present a security risk.**

LEGAL ENTITY IDENTIFIERS – VERIFIED ORGANISATION IDENTITIES

A Legal Entity Identifier (LEI) is a 20-character global identifier that identifies distinct legal entities that engage in financial transactions. It is defined by the ISO 17442 standard, endorsed by the G20 & FSB and is intended to be "the one identity behind every business". The LEI is a global identifier to not only provide access to verified organisation reference data, but also to connect the numerous different regional and private organisation identifiers used in KYC/AML.

RapidLEI is the organisation identity service from Ubisecure, a Local Operating Unit (LOU) of the Global Legal Entity Identifier Foundation (GLEIF) and accredited issuer of LEIs. RapidLEI is the number one issuer of new LEIs worldwide and offers both SaaS and API-based solutions for LEI issuance and management.

> TODAY, THE GLOBAL BANKING SECTOR SPENDS AROUND U.S.$40 BILLION ON CLIENT ONBOARDING ANNUALLY. THAT'S AN ESTIMATED U.S.$54M PER BANK, U.S.$31M OF WHICH IS 'PEOPLE' COST. PRODUCTIVITY IMPROVEMENTS GAINED THROUGH LEI USAGE COULD GENERATE CROSS-SECTOR COST REDUCTIONS OF BETWEEN 5-10% ANNUALLY.
>
> Global LEI Foundation

The use of LEIs in B2B KYC/AML and onboarding has the potential to be a significant cost saving tool in financial services and beyond, as well as having a measurable impact to people and staff productivity, streamlining processes, and improving transparency into available entity data. Service providers can view live, verifiable data about clients to ensure higher levels of trust for Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).

Entity verification processes do not stop with the conclusion of the onboarding process. The client data must be kept up to date throughout the business relationship, which includes regularly verifying business card information and changes to the ownership structure. The use of LEIs in KYC/AML makes this possible.

LEGAL ENTITY IDENTIFIERS – VALIDATION AGENTS

> BY SIMPLIFYING AND ACCELERATING THE LEI ISSUANCE PROCESS, THE NEW FRAMEWORK ALSO PAVES THE WAY FOR FIS TO EXPAND THEIR USAGE OF THE LEI BEYOND CAPITAL MARKETS TO ENCOMPASS ALL BANKING BUSINESS LINES, AN OPPORTUNITY ANTICIPATED TO SAVE THE INDUSTRY U.S.$2-4 BILLION ANNUALLY IN CLIENT ONBOARDING COSTS ALONE.
>
> Global LEI Foundation

Further, KYC service providers, banks, FinTechs, & Trust Service Providers can leverage the **GLEIF Validation Agent (VA)** solution with RapidLEI. Organisations using the VA solution can leverage existing KYC, AML and Compliance-as-a-Service workflows to obtain LEIs for clients when verifying a client's identity during initial onboarding or during a client refresh update. Both the validation of legal entity identity data and the subsequent registration (and renewal) of the LEI can be automated to occur in parallel with existing workflows, all in real-time, and without the usual duplicative processes.

ULTIMATE BENEFICIAL OWNERSHIP (UBO)

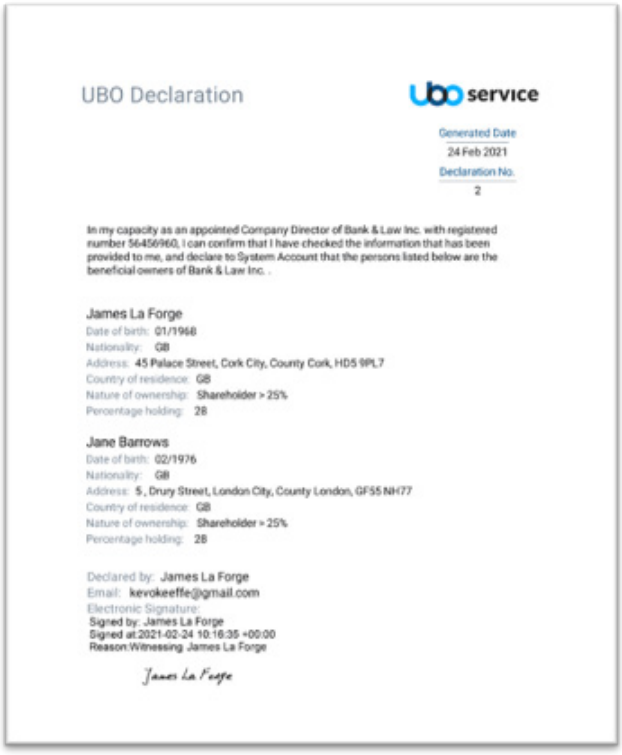
According to the Financial Action Task Force (FATF), the "beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement."

The European 4th AML Directive (2017) and the US FinCEN CDD Final Rule (2018) both contain provisions for capturing beneficial ownership (UBO). Penalties for non-compliance are significant, so maintaining proper UBO information is critical.

KYC/AML procedures and processes must collect information about the beneficial owner, including the identity of all individuals who have a significant ownership or control position. The beneficial ownership information includes:

- The natural person opening the account: name and title
- The legal entity customer: name and address
- The beneficial owners:
  - Name (and title for the controlling individual(s))
  - Date of birth
  - Address
  - Social security number, or passport number and country of issuance or similar ID number

— THROUGH A STRATEGIC PARTNERSHIP WITH UBO SERVICE, UBISECURE MAKES CAPTURING UBO EASY. YOU CAN FIND MORE INFORMATION ABOUT RAPIDLEI'S UBO SERVICES AT RAPIDLEI.COM/ULTIMATE-BENEFICIAL-OWNERSHIP


UBO Declaration

ubo service

Generated Date
24 Feb 2021
Declaration No.
2

In my capacity as an appointed Company Director of Bank & Law Inc. with registered number 56456960, I can confirm that I have checked the information that has been provided to me, and declare to System Account that the persons listed below are the beneficial owners of Bank & Law Inc. .

James La Forge
Date of birth: 01/1968
Nationality: GB
Address: 45 Palace Street, Cork City, County Cork, HD5 9PL7
Country of residence: GB
Nature of ownership: Shareholder > 25%
Percentage holding: 28

Jane Barrows
Date of birth: 02/1976
Nationality: GB
Address: 5 , Drury Street, London City, County London, GF55 NH77
Country of residence: GB
Nature of ownership: Shareholder > 25%
Percentage holding: 28

Declared by: James La Forge
Email: kevokeeffe@gmail.com
Electronic Signature:
Signed by: James La Forge
Signed at:2021-02-24 10:16:35 +00:00
Reason:Witnessing James La Forge

James La Forge

RIGHT TO REPRESENT

Right to Represent is a Ubisecure service which allows service providers or government departments to connect to and check a company's verified identity and the rights of individuals to request on behalf of, or represent, the company. Representation attributes can include legal, financial, administrative or other authoritative powers. Traditionally, such governance has been administrative and, therefore, time consuming and costly. Right to Represent digitises that administrative governance to technically implemented governance, making way for automated workflows that can reduce the cost of manual workflows by as much as 99%.

Combining Ubisecure's Identity Platform and LEI issuance (RapidLEI) technology, Right to Represent enables "Sign in with RapidLEI" to allow LEI-based accounts to authenticate organisation affiliation and rights. This reduces fraudulent organisational representation during the onboarding of new customers.

Digitising representation workflows also enables compliance to regulations by enhancing security and increasing transparency over who has rights to do what on behalf of the organisation. Because Right to Represent provides advanced KYC and ties an individual to an organisation, it can also dramatically reduce the time to execute successful corporate KYC/AML.

Case study: Katso

FINNISH GOVERNMENT

Katso
yritys.tunnistus.fi

The Finnish Government needed an identity management system to enable the strong identification of individuals and organisations for online government services that scaled nationwide, and supported online power of attorney. Ubisecure provided the solution, now known throughout Finland as Katso.

As a representative of an organisation, users create a Katso ID online, manage organisation data, manage sub-IDs and authorisations (using Delegated Authority). Organisation representatives and their staff, or any other authorised third-party, can then log in to over 100 government applications.

Since initial deployment, Katso has become one of the largest examples of digital identity management, authentication and attribute distribution solutions in the world. It has resulted in a 99% reduction in cost by moving to online service versus a physical point of service.

Read the full case study

Summary

Ubisecure's technology enables frictionless onboarding for individual and organisation users. Many years of experience facilitating onboarding and KYC workflows for both B2C and B2B scenarios make Ubisecure an ideal partner to help you achieve high completion rates, loyalty, and regulatory compliance.

Talk to Ubisecure about your digital identity and onboarding goals.

sales@ubisecure.com
www.ubisecure.com/contact

About Ubisecure

Ubisecure provides feature rich customer identity management software and services to help companies reduce identity data breach risk, improve operational efficiencies, and improve user experience.

The company provides a powerful Identity Platform, deployed as IDaaS (public or private cloud) or on-premises software. The platform consists of productised Customer Identity & Access Management (CIAM) middleware and API tooling to enable single digital identity benefits across multiple applications. Capabilities include enabling complex authorisation and delegation workflows, single sign-on (SSO), frictionless multi-factor authentication (MFA), user identity management, and pre-established connections to dozens of third-party identity providers (social, mobile, and verified).

Ubisecure's Right to Represent is a representation governance solution offering a fast and easy way to assert and verify an individual's mandated rights to electronically represent their company, including financial, signatory, or other authority. Ubisecure's widely used Delegated Authority solution allows individuals and organisations to manage which users and organisations can act on their behalf to dramatically reduce costly, time consuming and delay-prone manual workflows.

Ubisecure is accredited by the GLEIF to issue Legal Entity Identifiers (LEI) under its RapidLEI brand. RapidLEI is a cloud-based service that automates the issuance and registration of these highly assured organisation identifiers.

UBISECURE®

www.ubisecure.com
sales@ubisecure.com

UBISECURE UK
The Granary, Hermitage Court
Hermitage Lane, Maidstone
Kent, ME16 9NT, UK

UBISECURE FINLAND
Vaisalantie 2
FI- Espoo, 02130
Finland

UBISECURE SWEDEN
Blekholmstorget 30 F
111 64 Stockholm
Sweden

UBISECURE DACH
Franz-Joseph-Str. 11
80801 Munich
Germany