CREATING A NATIONWIDE INFRASTRUCTURE FOR AUTHENTICATION & DELEGATION OF AUTHORITY

KATSO PLATFORM FOR FINLAND – CASE STUDY

WHITE PAPER

UBISECURE™

Connecting Identity.

Transforming Digital Business.

CONTENTS

INTRODUCTION

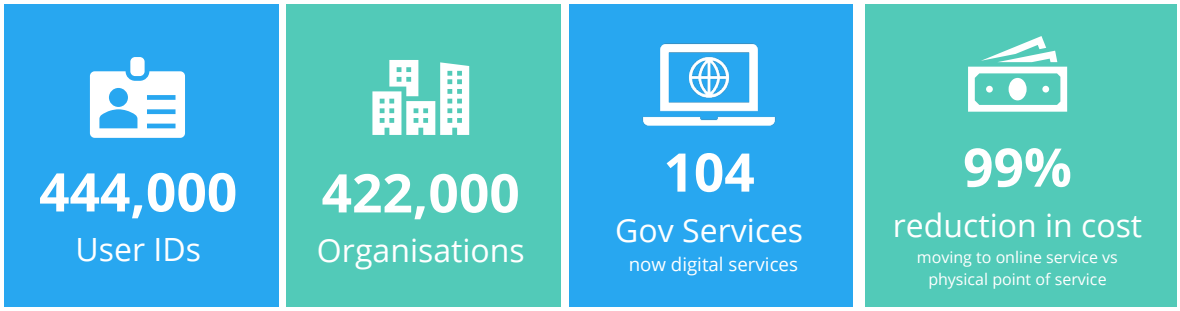
The Finnish Government is deeply committed to developing an advanced Information Society. The aim is to increase competitiveness and productivity, promote social and regional equality, and to improve citizens' well-being and quality of life through effective use of information and communications technologies.

Part of this national initiative was to implement a standards-based identity management system to enable the strong identification of organisations for online Government services such as tax and pension administration, municipal transactions and customs and excise. Unlike similar initiatives around the world, this project required the system to support "authorising someone to act on your behalf". Such delegation of authority, or online power of attorney, needed to support both agents representing organisations (such as accountants), and agents representing estates (such as individuals representing deceased parties).

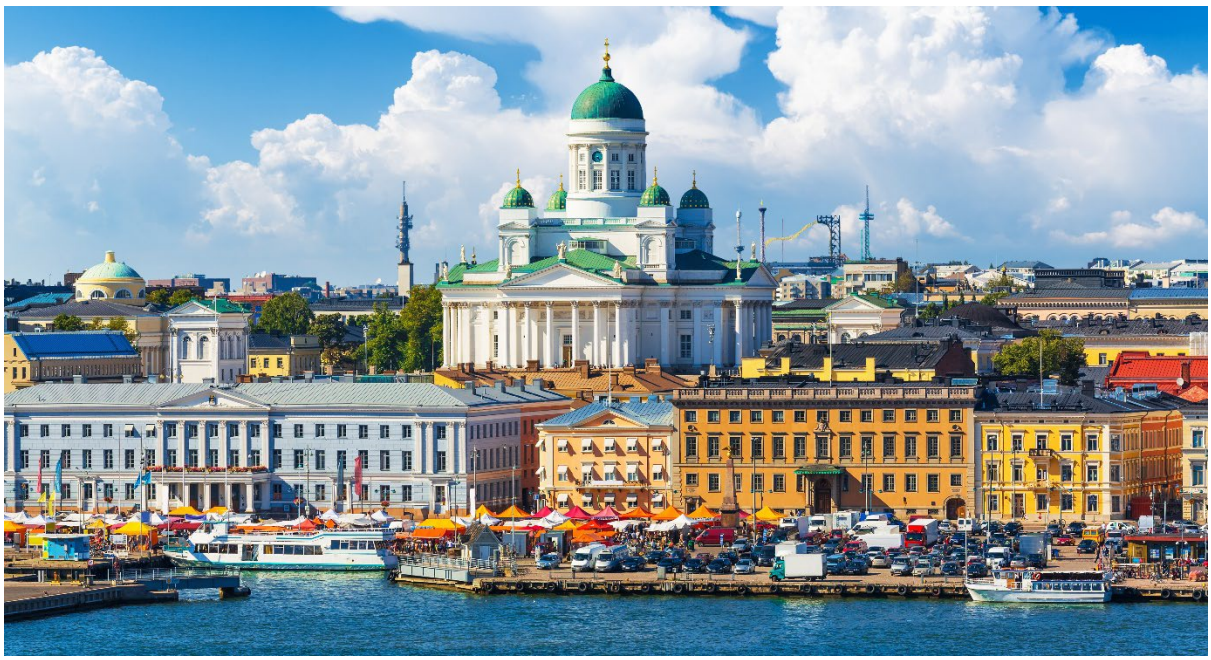
The deployed identity management solution, named the *Katso* system, is built on the Ubisecure Identity Platform and is managed by the Population Register Centre.

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

The Katso system has an enormous user base, as all Finnish companies need to have a Katso ID in order to use the online services provided by the Finnish government. The initial version was deployed in 2005, and since then Katso has become one of the largest deployments of digital identity management, authentication and attribute distribution solutions in the world. **Katso has become the de-facto identity management solution used by all Finnish organisations to use Finnish online government services.**



To understand the scale of the system, the population of Finland is 5.5 million (Nov 2018) and has 275,006 registered limited companies and 209,954 registered sole traders (July 2018).[1]



Some of the online Government services using the Katso service include:

- ☑ **Tax Administration**
- ☑ **Kela (Social Insurance / Benefits Institution)**
- ☑ **The Finnish Centre for Pensions**
- ☑ **Keva (Pension agency)**
- ☑ **Customs**
- ☑ **Ministry for foreign affairs of Finland**
- ☑ **City of Helsinki**
- ☑ **Police**
- ☑ **The Unemployment Insurance Fund**
- ☑ **Finnish Forestcentrum**
- ☑ **The Association of Finnish Local and Regional Authorities**
- ☑ **State Treasury**
- ☑ **Ministry of Defence**

This white paper introduces readers to the development process of the Katso system, deployment and use cases of the system.

[1] Source: Finnish Patent and Registration Office https://www.prh.fi/fi/kaupparekisteri/yritystenlkm/lkm.html

KATSO – INITIAL REQUIREMENTS

Katso was designed to replace an authentication system called TYVI. For the customer (initially the Board of Taxes and Social Insurance Institution) there were several driving factors behind the Katso project.

COST SAVINGS

The primary transformational driver for Katso is the reduction of visits people made to the Government operated physical point of service by moving the services online. It was estimated by the Board of Taxes that each point of service visit costs between 20 – 50 Euros. Online service transaction cost was estimated to be 10 – 50 Cents, or 1% of the point of service cost, meaning 99% reduction in cost equating to hundreds of millions of euros potential savings. Katso is the enabling platform for the online services. Katso ensures strong authentication of organisations and their representatives. Without proper authentication, the services cannot be made available online.

By digitalising government services:

- ☑ **The number of physical service points has decreased from over time to only 50 in 2018[2]**
- ☑ **The number of persons employed by the tax administration reduced 20% year on year since launch of the initial Katso system[3]**
- ☑ **Visits to tax.fi service in 2016 increased by 7m over 2014[4]**

Another transformational goal was that management of identities and authorisation relationships needed to be outsourced from the government itself. Government organisations do not have the resources or mandate to maintain corporate identities or create and manage authorisation relationships between different organisations, such as a corporation and its tax administrator. The system therefore needed an outsourcing framework for ID management and authorisation. However it was not possible to outsource the ID management to an external service provider as the volume and dynamics of the information stored in the system was too high scale. The ID management needed to be handled by the very companies that utilise the system.

AUTHENTICATION

Online government services require a level of trust and some services require strong authentication of users. There were several proprietary authentication methods available for government online services and one of the Katso requirements was to deprecate legacy authentication options and harmonise the authentication infrastructure.

[2]List available at Finnish Tax office site: https://www.vero.fi/tietoa-verohallinnosta/yhteystiedot-ja-asiointi/verotoimistot/?showAll

[3] Chart available at https://annualreport2017.vero.fi/figures/staff-economy-and-customer-survey/

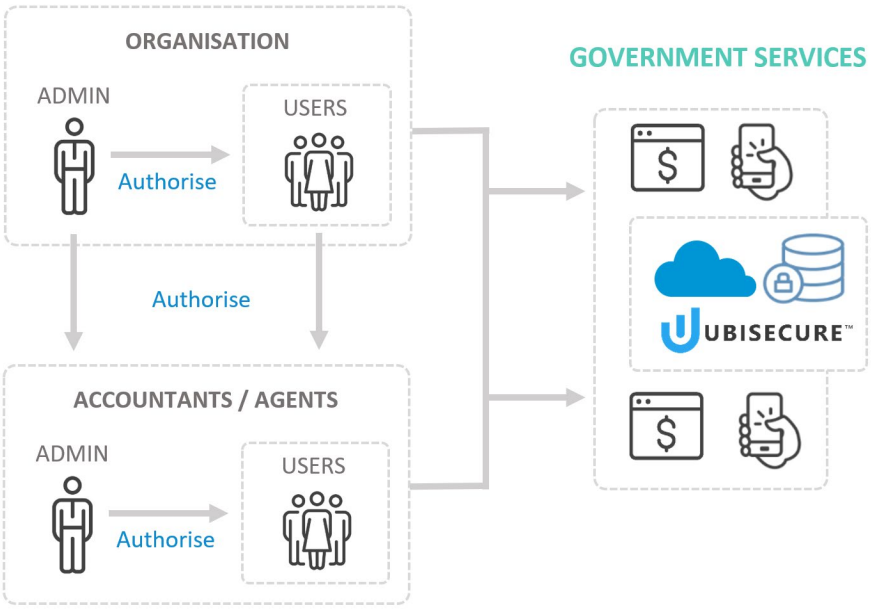
[4] Data available at http://finnish-tax-administration-annual-report-2016.tax.fi/

The initial requirements for the Katso system were designed in 2005 and stated that there should be two authentication methods available, Katso Password (Katso PWD) and Katso One Time Password (Katso OTP). These authentication methods would be used to authenticate the users of the online government services. Through the Ubisecure Identity Platform's Authentication Adapter, other authentication methods can be used, so that in the future new authentication methods can be deployed to the services within seconds.

Banks have a one-time-password (OTP) authentication scheme that is well established in Finland and almost everyone uses the bank authentication method. Banks charge a small fee for each authentication event, providing a greater ROI on the Know Your Customer investments they make regardless of the Katso system.

AUTHORISATION – ALLOWING OTHER ORGANIZATIONS TO WORK ON YOUR BEHALF

One of the most innovative aspects of Katso is the ability to authorise other organisations to act on your behalf. The Board of Taxes and Social Insurance Institute needed a system where organisations can authorise other organisations to act on their behalf and maintain these authorisations themselves. The requirement was that authorisation should be flexible, and at the same time maintain security and privacy. This concept is referred to within the ecosystem as delegation of authority.



IDENTITY MANAGEMENT

The Katso system now has over 422,000 companies registered nationwide. The number of users within these companies increases to 444,000. The scale of users required a system design that allowed the user lifecycle management to be managed by the organisations themselves.

ROLE BASED IDENTITY

The Finnish Government operates many online services with varying levels of information sharing needed between the company, individual and the service. Confidentiality levels vary between services and functionalities within a service. To support this model, Katso users are authorised based on roles. A given role defines a user's access to services. Katso role definitions and descriptions are well defined across all services[5]

INTEGRATION TO THE EXISTING AUTHENTICATION SERVICE

One of the requirements of Katso was the ability to integrate to the existing authentication service operated by the government. The legacy authentication service was designed to authenticate only citizens to the online government services, not organisations. Through integration to the existing authentication service, using the Ubisecure Identity Platform, this organisation authentication, identity management and authorisation system needed to be integrated to a single authentication service.

PRIVACY

One of the concerns highlighted during the specification phase was privacy. In a distributed environment where authentication is outsourced, a user can access the services using any computer available. Although information that flows through the browser or the client application is encrypted it was obvious that the amount of information should be limited and even masked.

SUPPORT FOR STANDARDS

The authentication service and identity management service offer services to wide variety of service providers (SPs). These services are not just government services as there are also operators and other service providers that rely on the Katso authentication and identity information. This means that Katso was required to support open standards in user authentication for Web applications, legacy client applications and identity attribute queries. Identity standards were chosen and specifically SAML 2.0 (http://www.oasis-open.org) and Liberty ID-WSF 2.0 (http://www.projectliberty.org/resources/specifications.php).

[5] Katso role definitions - https://www.vero.fi/globalassets/tietoa-verohallinnosta/sahkoinen-asiointi/katso-tunnistus/katso-role-naming-convention-current-list-of-roles.pdf

KATSO PROJECT

USABILITY REFINEMENT

Digital identities are our passports in the network, and therefore privacy by design should be a major consideration. Personally Identifiable Information (PII) should never be made available, intentionally or unintentionally, outside of the system. In Katso it was decided that only a minimum set of information should be delivered to the application when authenticating the user. If the application required more information about the user, it could use SAML AttributeQuery and get the required information in the backend from the Ubisecure Identity Platform. The received information could then be used to authorise the user to perform different type of actions.

One the most complex refinements during the Katso project was to determine the relationships where different authorisations could take place. A fundamental requirement for the Katso was the ability to authorise other entities in the Katso systems. This authorisation created a web of different relationships between users, private sector organisations and government organisations. The challenge is to use a data model that supports the complex requirements of every use case. The Ubisecure Identity Platform data model is highly flexible and therefore able to support this use case.

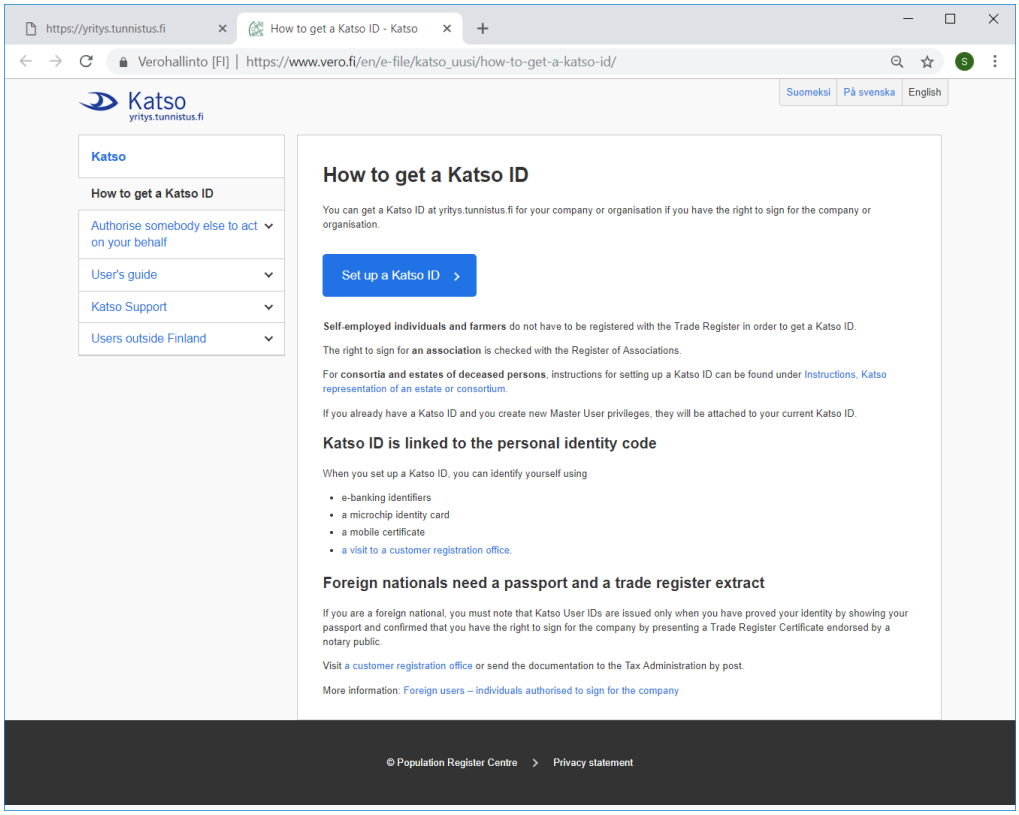
KATSO USE CASES FOR ORGANISATIONS

ACQUIRING A KATSO ADMIN ACCOUNT

The organisation administrator is responsible for creating new Katso Identities. The admin is also responsible for i) authorising other organisations and Katso Identities, ii) accepting new authorisations from other organisations, and iii) delegating the received authorisations to Katso Identities within the organisation.

The requirements for admin account is that the individual is a registered signatory for the company and is authenticated properly preferably using strong online authentication or, as a fall back, through face-to-face authentication at a service point.

Account creation requires identity authentication using a national eID card, mobile operator issued sim identity or a Bank ID. These strong authentication methods are regulated by law, subject to strict audit requirements and can be used to reliably verify the identity of the applicant without a service point visit.



CREATING KATSO SUB ACCOUNTS

Katso sub accounts can be created within the organisation. The Katso sub account is a quick way to delegate day-to-day tasks for the personnel of the company.

UPGRADING THE SUB ACCOUNT TO A KATSO ACCOUNT

Sub accounts can be upgraded to Katso accounts. Katso accounts use strong authentication methods and have extended privileges. This enables admins to assign more roles to the Katso accounts that are not available for the Katso sub accounts.

SUB ORGANISATION MANAGEMENT

Katso supports sub-organisations. The admin is responsible for creating the sub organisations. Only address information and the identifier (extended VAT number) are required. It is possible to request an admin account for the sub organisation. The process follows the admin account creation process.

AUTHORISING – DELEGATING ACCESS TO OTHERS

Authorisation is a process where the authorising party assigns a role, or a role set to an entity in the Katso system. The roles are specific to a government organisation and optionally specific to a certain online service. Entities are organisations, Katso IDs or Katso sub IDs.

In Katso a company can authorise other companies to act on their behalf in certain tasks. For example, corporations can authorise an accountant company to manage their taxes. The Katso admin creates an authorisation in the Katso system and assigns the required roles to the authorisation. This authorisation is assigned to a specific entity in the Katso system, i.e. another company within the system (accountant firm). Once the assignment is done and the correct roles are tied to the authorisation, it is forwarded to the receiving company, namely to the Katso admin of the receiving party.

The authorisation can be temporary or effective for a determined period.

Authorising Katso accounts

Authorisations must be assigned to a Katso ID or a Katso sub ID. Katso admins can authorise (grant roles) to Katso IDs within their organisation or to a Katso ID located in another organisation.

Authorisations within the organisation can be either internal or assignments of received authorisations from another organisation. In either case the Katso admin is responsible for delegating the received authorisation or creating a new authorisation that is assigned to a Katso ID within the organisation.

PUBLIC AUTHORITY AUTHORISATION FOR KATSO ORGANISATIONS OR KATSO ACCOUNTS

Occasionally there is a need to create authorisations by the public authorities. This could happen is someone is declared incapable, a corporation goes to bankruptcy, or a company is assigned to care of the assets of an estate of a deceased person.

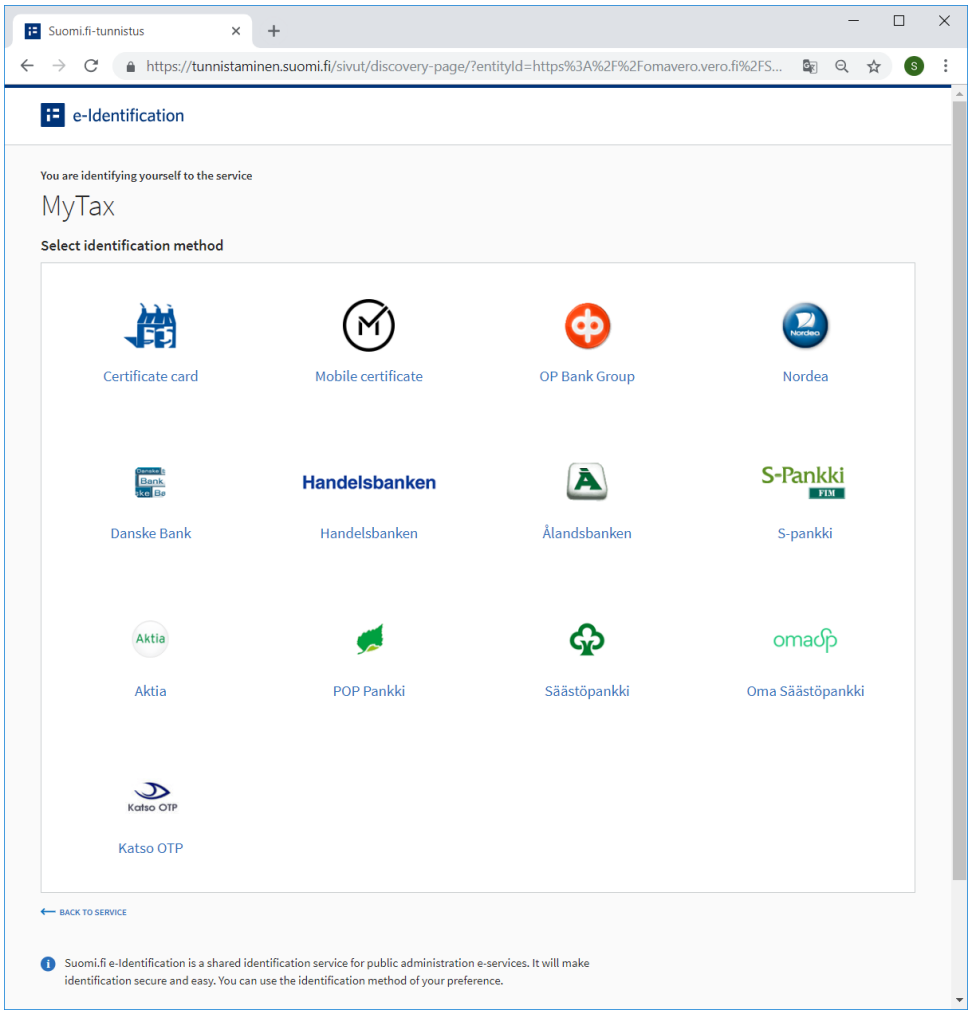
The public authority authorisation characteristic is that there is no authorisation party, but the authorisation is created by a third party. For the receiving Katso admin this authorisation is just like any other received authorisation. But most of the times public authorities will assign authorisation to Katso IDs directly.

Typically, public authority authorisations are not permanent. In Katso, the basic use cases for authorisation use fixed roles that are created by the government organisations to the system, but public authority authorisations can be short lived.

ACCESSING ONLINE GOVERNMENT SERVICES

The Katso system provides a common platform for delegation of roles that specify which resources are available. Government services that utilise Katso can offer a wide variety of authentication options for the user. When an online service is created, confidentiality requirements are resolved, and a suitable authentication method can be chose based on the sensitivity of the information handled by the service.

During the authentication event a minimal set of PII is sent to the service.



ACQUIRING ADDITIONAL ATTRIBUTE INFORMATION ON USERS

Each service accepts certain roles. These roles are maintained by the government officials[6] and assigned to Katso IDs by Katso admins in the organisation.

[6] Katso role definitions - https://www.vero.fi/globalassets/tietoa-verohallinnosta/sahkoinen-asiointi/katso-tunnistus/katso-role-naming-convention-current-list-of-roles.pdf

Once the service receives the user's organisation and roles, the service can grant access to those portions of the service. Katso IDs with authorisations from multiple organisations generate responses combing the role information with the authorising organisations thereby allowing user to properly act on behalf of these organisations and in a correct capacity.

CONCLUSION

Katso is a standards-based identity management, authorisation and authentication solution for government organisations. Through Katso, government organisations in Finland have been able to reduce cost when conducting business with private sector organisations and individuals. Traditionally manual processes have been streamlined and brought online, eliminating significant personnel, support and branch office costs. Katso can satisfy a wide range of use cases for the organisations in the private sector.

Katso is a digitalisation success story. Using product components, the development of the whole infrastructure took only a few months from the starting date to the production date, and now over 444 000 organisations use Katso as their main identity solution when dealing with government institutions.

The Ubisecure Identity Platform can provide government organisations a tried and tested way to deploy identity management, authentication and authorisation infrastructure at the scale of a nationwide solution.

CONTACT INFORMATION

To learn more about Customer IAM and Company Identity solutions visit www.ubisecure.com or contact us at sales-team@ubisecure.com.

Ubisecure UK
The Granary, Hermitage Court
Hermitage Lane, Maidstone
Kent, ME16 9NT, UK
UK: +44 1273 957 613

Ubisecure Finland
Vaisalantie 2
FI- Espoo, 02130
Finland
FI: +358 9 251 77250

Ubisecure Sweden
Blekholmstorget 30 F
111 64 Stockholm
Sweden
SE: +46 70 603 34 83

UBISECURE™

Ubisecure is a pioneering European b2b and b2c Customer Identity & Access Management (CIAM) software provider and cloud identity services enabler dedicated to helping its customers realise the true potential of digital business.

Ubisecure provides a powerful Identity Platform to connect customer digital identities with customer-facing SaaS and enterprise applications in the cloud and on-premise. The platform consists of productised CIAM middleware and API tooling to help connect and enrich strong identity profiles; manage identity usage, authorisation and progressive authentication policies; secure and consolidate identity, privacy and consent data; and streamline identity based workflows and decision delegations. Uniquely, Ubisecure's Identity Platform connects digital services and Identity Providers, such as social networks, mobile networks, banks and governments, to allow Service Providers to use rich, verified identities to create frictionless login, registration and customer engagement while improving privacy and consent around personal data sharing to meet requirements such as GDPR and PSD2.

Ubisecure is accredited by the Global Legal Entity Identifier Foundation (GLEIF) to issue Legal Entity Identifiers (LEI) under its RapidLEI brand, a cloud-based service that automates the LEI lifecycle to deliver LEIs quickly and easily. The company has offices in London and Finland.