Connecting Identity.
Transforming Digital Business.

Case Study:
Government Funding Service

Customer IAM solution for managing individual and organisation identities

Background

This government organisation offers and co-ordinates funding for research, product development, and many other kinds of business development needs. Applicants for funding can be individuals, teams, companies or groups of companies.

It set out to revamp its online services to provide seamless experiences for its employees and external users, solving key identity management challenges (see below).

Challenges

MULTIPLE ROLES AND COMPLEX IDENTITY RELATIONSHIPS

Individuals must be able to represent their team or organisation when carrying out funding applications. This must be done digitally, and needs to be a trusted assertion of their identity and their rights, as well as the organisation's.

Multiple individuals should be able to access the application online, at varying levels of authorisation (at times with different roles in different projects), in order to contribute and monitor progress.

Further, some applications may require users from third party organisations to have secure access to the application, requiring B2B identity relationship management capabilities.

SENSITIVE INFORMATION TO PROTECT

This organisation handles confidential information related to funding applications. The applications include highly sensitive information about future projects, product concepts, solution descriptions etc., and therefore require robust authentication and authorisation policies to avoid it ending up in the wrong hands.

USER EXPERIENCE

This organisation serves thousands of customers and has hundreds of technology programmes running annually. Whilst the technical requirements of the solution are advanced, the front-end service to customers must be easy to use and cater to a wide variety of users (with varying technical ability) – to relieve internal manual support burden.

Solution

Ubisecure's Identity Platform enabled the following identity and access management capabilities.

STRONG AUTHENTICATION

This organisation implemented Ubisecure APIs for strong authentication of internal and external users. External users are prompted to verify their identity using their bank or mobile ID, through a common identification service for public administration transaction services - which includes a number of identity provider options.

— KEY BENEFITS:

- As these identity providers (banks and telcos) have already conducted a high level of KYC (Know Your Customer), there is a very high level of assurance that these identities are linked to real-world identities.
- Multiple identity provider options means that customers can choose which identity they already own, without having to create a new set of credentials. This is a customer experience win, and removes the need for insecure passwords.

IDENTITY RELATIONSHIP MANAGEMENT (INCLUDING B2B)

With Ubisecure's advanced identity relationship management capabilities, company administrators (e.g. contact person/project lead) can invite colleagues and other necessary users to be part of the application. Uniquely, a delegation of access rights can be given to another company (B2B delegated authority), who then control their own users' access to the project.

— KEY BENEFITS:

- It is more secure for each user to have their own account with its own authorisation of access. Otherwise, users may end up sharing one account – which risks unauthorised access and poor user experience when it comes to authentication.
- B2B delegated authority saves time for the main administrator (or the

government organisation’s support staff), who would otherwise have to manually invite each project member from the partner company. It’s much quicker, easier and more secure for the partner company, who knows their own employees better, to control this access themselves within defined parameters.

ROLE-BASED ACCESS CONTROL (RBAC)

When inviting other users to join projects, users may be assigned specific roles. These roles govern what level of access a user is entitled to, and what permissions they have – e.g. authority to invite further users. Further, users may have multiple different roles assigned to their identity for multiple different projects, ensuring that control over access for individual projects remains granular.

— KEY BENEFITS:

- RBAC ensures users only have the minimum access necessary to complete their part in the project, enhancing security with the principle of least privilege.
- As authorisation is grouped by role, an administrator may invite a user much more quickly - without having to repeat permissions settings on an individual basis.

SINGLE SIGN-ON (SSO)

Following authentication, users are granted access to every part of the service that they are authorised to – e.g. applicant information, project implementation and funding status. Single sign-on (SSO) allows this seamless access without requiring repeat logins for each part of the service.

— KEY BENEFITS:

- The user experience with SSO is much more frictionless than requiring multiple logins.
- SSO also means single sign-out and just one set of credentials to revoke access (for example when an employee leaves the company), meaning far fewer unauthorised access incidents and forgotten-about accounts with privileged access.

Summary

This organisation solved its identity management challenges with Ubisecure's Identity Platform. It chose Ubisecure because of the flexibility of the solution (with further capabilities being added as required), support for several different authentication methods and extensive authorisation features.

Get in touch to find out how Ubisecure can enable your digital services.

Get in touch

ubisecure.com/contact

sales@ubisecure.com

About Ubisecure

Ubisecure is a Europe-based Identity & Access Management (IAM) specialist and offers a comprehensive identity management platform deployed as IDaaS (Identity-as-a-Service) or on-premises software. The company is also GLEIF-accredited to issue Legal Entity Identifiers (LEI) via its RapidLEI service and has quickly become the global #1 LEI Issuer both in terms of volume and data quality.

As well as managing risk against data breaches, Ubisecure enables Zero Trust to greatly improve the security and experience of how users authenticate, register, access, engage and use the organisation's application, whether it's a web, mobile or a legacy service.

Enterprises use the Identity Platform to quickly implement use cases like single sign-on (SSO), multi-factor authentication (MFA), access management, authorisation and consent policies, advanced identity relationship management, login-as-a-service, and KYC/onboarding.

The platform has native support for a wide range of digital identities to enable real time identity verification and proofing, including Bank IDs, EU eIDs, mobile IDs, enterprise and social identities. Additionally, the RapidLEI service helps banks and FIs to manage and issue large volumes of LEIs to improve organisation-based authentication, meet compliance regulations, and provide better KYC/onboarding experiences for clients.

UBISECURE®

www.ubisecure.com
sales@ubisecure.com