UBISECURE®

Connecting Identity.
Transforming Digital Business.

CIAM for Europe's Utilities Sector

How utilities organisations use Customer Identity and Access Management to create secure, seamless, and trusted digital experiences.

Contents

Europe's utilities sector

Utilities organisations face mounting pressure from several angles. Not least, the sheer amount of data that utilities must collect, store and keep safe. From smart meters to smart grid, B2C and B2B data must be stored securely and compliantly - or risk a data breach, non-compliance fines and even service outages while issues are resolved. At the same time, security and compliance workflows must not prohibit operational efficiency or the all-important user experience.

Utilities face an extra layer of complexity when it comes to the types of users accessing their services. Many service providers must manage user identities across customers, in-house staff, remote workers, third-party contractors and business partners - all requiring secure access to company systems and often across joint ventures or business groups. It is critical to manage this risk and maintain granular visibility over who has access to what resources, again without impeding efficiency. Many utilities providers find themselves bogged down in time and cost-intensive manual processes, managing identities across organisational silos.

> These challenges create significant opportunities with digital transformation.

These challenges create significant opportunities with digital transformation. As the utilities sector has not yet seen the rapid rate of digital innovation experienced by other sectors, such as financial services, digital-first utilities services represent real competitive advantage for consumers.

Evolving social habits and IT advancements can be incorporated into the way utilities do business, driving digital transformation with effective use of Customer Identity and Access Management (CIAM).

CIAM capabilities

Embed proven capabilities to create secure, seamless, & trusted digital experiences for your users. Choose the capabilities you need from a single technology stack – Ubisecure's award-winning Identity Platform. From fast-to-market Identity-as-a-Service (IDaaS, cloud CIAM) to the most advanced on-premises use cases, Ubisecure Identity Platform is built to grow with your business.

> 45% of users give up if the registration process is too hard

— CIAM CAPABILITIES INCLUDE

- Registration & login
- Authentication & authorisation
- Single Sign-On (SSO)
- Identity Management
- Delegated Authority
- API Protection

View detailed feature list

> 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

REGISTRATION AND LOGIN

Creating a new identity, or asserting an existing identity, is key to the registration process. 45% of users give up if the registration process is too hard, so it's essential to minimise friction during this initial touchpoint. Logins should also be seamless to encourage loyalty to your services. CIAM can enable frictionless registration and login workflows across any device, helping you to convert and retain more customers.

AUTHENTICATION AND AUTHORISATION

Support for numerous identity providers to authenticate a user (social, professional, verified and government) at the right time in the user journey, authorising access to only the right resources. Tailor identity verification/ authentication to your target user groups, with options to avoid a one-size-fits-all approach. Strong authentication and multi-factor authentication (MFA) increase security and meet privacy regulation and expectations.

SINGLE SIGN-ON (SSO)

Offer users one identity for simplified login to all target digital services and applications. As access to all services is tied to one identity's permission settings, security is increased through easy revocation of access rights. **Federation** – building links between your service and third-party services - enables SSO to external services.

IDENTITY MANAGEMENT

Allow users to manage their own accounts in a self-service portal. Simplify migration, creation, storage, and management of users and identity data at scale. Avoid time wasted on data silos and let IT departments get back to doing what they do best.

DELEGATED AUTHORITY

Multi-tier delegated administration and delegation of authority, improving efficiency, reducing costs and enhancing security.

— WATCH THIS SHORT EXPLAINER VIDEO ON DELEGATED AUTHORITY.

API PROTECTION

Enable secure access control of APIs both within an organisation and to third-parties, such as customers and partners. Ubisecure's standards-based token server uses OAuth 2 and OpenID Connect protocols, making your APIs easy for internal developers to manage and customer and partner developers to integrate with.

Use cases

Example use cases of CIAM capabilities being leveraged by utilities.

— USE CASE: CUSTOMER FAMILY

The Smith family have shared finances. Either adult in the family wants to be able to pay bills, compare packages and make service requests. Even though the water supply contract is signed by just one adult, they can invite the other adult to have visibility of the accounts. The Smith family also have a holiday cottage, and can check the water consumption and billing information for this other property in the same view.

— USE CASE: HELPING EXTENDED FAMILY

Grandma and grandpa are getting older, and the time has come to keep a closer eye on their accounts. They have asked for help from their children. Instead of insecurely sharing login credentials for their gas provider with their children, they can digitally authorise their children to perform certain tasks and assist them when needed, without needing to contact IT Support.

— USE CASE: SMALL BUSINESSES OWNER

Sarah runs a few small businesses. She has a personal account for her home electricity consumption, and electricity contracts for every business that she runs. She can log in once and see all her accounts from the same dashboard - both personal and business.

— USE CASE: MULTI-LOCATION BUSINESS

A popular restaurant chain needs to allow their restaurant management personnel permission to view energy consumption information, but not to terminate contracts. An admin at the restaurant chain can invite each restaurant manager to their account with the energy provider, and give them access to information for only the location(s) that they manage. The restaurant manager can then invite an assistant manager or other location-specific staff member to view certain information. Head office can log in once and see all accounts from the same dashboard.

— USE CASE: DELEGATION BETWEEN ORGANISATIONS

This large enterprise customer outsources refuse and recycling management services to a third-party service management company. They can choose to delegate access to the system between the organisations and allow the service management company to determine who at their company can access this client's information. The service management company users can sign in once to see all of their clients, and move seamlessly between the views without signing in repeatedly for each client. When the contract expires or the service management company changes, all access from all third-party users can be revoked in one step.

— USE CASE: FEDERATION TO COMPLEMENTARY SERVICES

An energy company has partnered with third-party services, including an electric vehicle charging network, a solar energy financing company, a mobility-as-a-service electric scooter rental provider, and a creative energy audit gamification tool for helping families reduce their carbon footprint. Customers can use these third-party services without complex registration processes and without signing in again. The energy company gets a referral fee for new members.

— USE CASE: THIRD-PARTY INSTALLERS

An energy company has partnered with third-party electricians who work on installations in customer homes, performing maintenance and installation tasks. Some of them are sole-traders, others small businesses and some nationwide service providers. The energy company uses their CIAM system to control who has access to which target services and what customer data is visible to them.

— USE CASE: THIRD-PARTY SALES AGENTS

An energy company has subcontracted a third-party to perform marketing campaigns and help customers select energy plans and commit to new contracts. To do this, the third-party company needs restricted access to customer data and access to a sales management tool. The sales agency determines who can invite their staff to the system and determine the level of access for each type of user.

Case studies

Selected examples of how Ubisecure customers in the utilities sector are leveraging the Identity Platform.

LEADING NATIONAL ENERGY COMPANY – CLOUD-BASED IDENTITY SOLUTION

This energy company is responsible for critical infrastructure, serving close to a million customers. It required a cloud CIAM solution (private cloud IDaaS) to support both end users and B2B partners. Ubisecure deployed its Identity Platform to enable the strong initial and ongoing authentication of user identities, with one identity and a seamless experience across their website and mobile app.

— VIEW FULL CASE STUDY: CLOUD-BASED IDENTITY SOLUTION

LARGE ENERGY COMPANY – SSO AND DELEGATED AUTHORITY

This energy company serves more than 450,000 customers, including corporate and private customers. With Ubisecure CIAM, the company consolidated its various services with one login for access to all authorised services (SSO). Customers with both roles – corporate and private – still use only one set of credentials to access both accounts. Authentication with BankID is enabled for identity verification, and users can self-register and manage their own accounts. Delegated Authority enables the delegation of access to, and authority within, accounts for B2B customers.

— VIEW FULL CASE STUDY: SSO AND DELEGATED AUTHORITY

Benefits

SECURITY

Robust security is important for any digital service, and especially utilities services given the amount of personal and organisational data that is collected and stored. As **80% of security breaches** are caused by weak or stolen passwords, password-only access to utilities systems is a major red flag that needs urgent resolution. CIAM capabilities like connecting identity providers and enabling MFA greatly reduce this risk, providing stronger assurance that the user logging in is who they say they are.

> 80% of security breaches are caused by weak or stolen passwords

SSO enhances security through easy revocation of access rights - as well as reducing credential fatigue, encouraging better password 'hygiene' and uptake of optional MFA. Delegated Authority stops both data and credentials being shared in other, more vulnerable ways – as well as allowing you to set granular, role-based access and maintain visibility over who exactly has access to what.

REGULATORY COMPLIANCE

Given that utilities are highly regulated, compliance is high priority for any IT strategy. CIAM enables compliance to regulations like GDPR and The Electricity Market Act, as well as directives like the NIS Directive, by enhancing data governance even across complex structures and real-time billing transparency. Where CIAM is used to integrate data siloes (such as across IAM systems within a business group or from IAM to other systems like a CRM), having one centralised identity management system suddenly makes compliance a whole lot simpler.

CIAM capabilities like strong authentication and/or MFA will not only count towards GDPR-mandated “appropriate technical and organisational measures” to protect personal information, but also help with PSD2 compliance when it comes to e-commerce.

> — 50% OF OUR SURVEY PARTICIPANTS SAID THAT ACHIEVING GDPR COMPLIANCE WITHOUT CIAM WOULD BE IMPOSSIBLE.

USER EXPERIENCE

Customer IAM systems, as opposed to staff-focused legacy IAM systems (see IAM vs CIAM), are purpose-built to facilitate gold-standard user experience (UX) across stakeholder groups. CIAM offers out-of-the-box UX workflows that have been tried and tested to get the best results in similar use cases.

Self-service functions make life much easier for your users by giving them control over their own account settings, without having to wait for your IT Support desk. SSO also reduces friction when users are moving between areas of your service. CIAM will help you implement a multi-channel identity solution, so that capabilities work across user devices.

> CIAM helps you find the balance between security and usability

CIAM helps you find the balance between security and usability. For example, one solution to the potential friction of MFA security measures could be step-up authentication - introducing a second authentication factor only for certain resources.

CIAM is also key enabler to personalisation, which helps you to provide a great UX as well as helping you to understand your customers and tailor solutions to their needs. Personalised experiences and offers create upsell opportunities – as does federation, with the ability to move seamlessly between partner services. See: **CIAM for Customer Experience and Marketing**.

OPERATIONAL EFFICIENCY

Utilities services with multiple types of stakeholders require complex identity management workflows. With the correct CIAM solution, these workflows are digitised and seamless, enabling true operational efficiency.

Even core CIAM capabilities like a password-reset function can have a huge impact on your bottom line. According to **Forrester**, large organisations spend up to $1 million each year in staffing and infrastructure expenses to handle password resets – reduce this cost drastically by giving users control over their own account settings.

— FOR MORE ABOUT HOW CIAM SAVES ORGANISATIONS MONEY (AND INCREASES REVENUE), DOWNLOAD THIS GUIDE TO EVALUATING THE ROI OF CIAM.

Using a productised solution for CIAM frees existing in-house technical resource, enabling your developers to focus their efforts on business-specific and domain-specific projects. Login, authentication, password management, access rights management and approvals all become "part of the plumbing", not systems to be developed and maintained. When choosing to buy as-as-service, complex infrastructure management, monitoring and upgrading is no longer required, further freeing expensive resources.

As CIAM enables many integrations out-of-the-box, it is quickly adaptable to your desired environment. This makes such solutions effectively future proof, accelerating changes as the need arises. For example, the shift to remote working during the pandemic has seen many organisations' relationships with remote staff become more like their relationships with customers. CIAM enables seamless remote onboarding/offboarding and security features beyond the walls of in-office IT security.

Summary

In summary, CIAM is a key enabler to digital transformation for utilities service providers. The challenges that utilities are facing – including data security, regulatory compliance, user experience and operational efficiency – become significant opportunities for competitive advantage when leveraging CIAM capabilities.

Ubisecure CIAM supports utilities needs at scale. As a European CIAM provider, we understand European organisations' needs and have 20+ years of experience in delivering proven identity solutions – including to utilities organisations. Our Identity Platform can be deployed on-premises or in the cloud (Identity-as-a-Service, IDaaS), with flexibility to support hybrid IT environments and multi-cloud infrastructures.

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