UBISECURE®

Connecting Identity.
Transforming Digital Business.

Leverage CIAM for a better customer experience and more effective marketing

Customer Identity and Access Management (CIAM) for B2C, B2B and G2C

Introduction

Whoever your customers are - private, corporate, partners, citizens – a good user experience is critical to ensuring they use your digital apps and services on a regular basis.

To enable such a service to exist, you must consider how users will tell you who they are when they register and log in to your service, how you will verify those identities, and which parts of your service they can access. Such transactions have very specific Customer Identity and Access Management (**CIAM**) requirements and getting these wrong will mean customers go elsewhere to get what they need.

Traditional Identity and Access Management (IAM – aka legacy, internal, or employee IAM) is not designed to be customer facing at scale. Employees have little choice but to use whatever access control or IAM technology is mandated by IT Administration, and they will receive training on business systems. Customers, on the other hand, will quickly turn to your competitors in the case of a poor user experience with your app.

Further, Marketing and Customer Experience (CX) professionals know that customer trust in your brand is essential. Lack of robust identity practices will lead to a data breach – a.k.a. the marketing crisis of your year – making security a competitive benefit. Appropriate balancing of security and user experience is a fine art, which you can master with CIAM.

These are just some of the reasons why CIAM is a vital investment, and one that can provide a great ROI when leveraged correctly. Let's look at the CX and Marketing benefits by each CIAM feature.

CIAM features and benefits

ANCHOR CUSTOMERS TO THEIR EXISTING IDENTITES

Reducing abandonment through successful registration of new customers is a critical marketing goal. CIAM makes it possible to use both existing digital and real-world identities to simplify initial customer registrations, and as a positive side effect, reduce fraud.

CIAM allows customers to register and login with their digital identity from a wide-range of digital identity schemes including eIDs, BankIDs and Government issued digital IDs. Such digital identities are in wide usage throughout Europe in particular. For countries that do not yet offer standardised verified digital identities, let users verify themselves in realtime using their Government issued documents such as driving licenses, national identity cards and passports. CIAM solutions that support both digital and real-world identities will help reduce both fraud and user friction, making it easy to capture and convert new, verified customers.

CIAM also provides progressive profiling and personalisation capabilities. Building a profile allows you to link identity data sources, identity proofing levels, and attribute information for a centralised view of users, to build personalised experiences.

MULTI-FACTOR AUTHENTICATION (MFA)

MFA means that users must use more than one authentication method (usually something you know like a password + something you have like a mobile device) at the point of login. This means that even if a potential attacker can get through one authentication barrier (such as cracking a password), they are very unlikely to be able to get through two – greatly improving an app's security measures.

MFA is a security gold standard and no longer needs to be a CX disaster. MFA is fast becoming standard across apps and services, and customers are becoming more and more accustomed to the practice and understanding why it's in place.

TOP TIPS FOR MFA:

- Go passwordless – remove the burden of another set of credentials to remember and manage. Other authentication methods are stronger and more convenient.
- Ensure authentication methods are appropriate to your target audience and level of data sensitivity. E.g. social login is not as strong as using a verified bank ID, but using both together to 'step up' authentication levels when needed is even stronger.
- Even better, allow your users to choose which authentication method suits them best. They will likely choose to authenticate with identities they already own – known as BYOID (bring your own identity).
- Enable authentication with biometrics – a popular choice among consumers and already facilitated by most smart phones and laptops.

SELF-SERVICE ACCOUNT MANAGEMENT

— A SINGLE MANUAL PASSWORD RESET IS INCREDIBLY EXPENSIVE – COSTING AN ORGANISATION OVER £50, ACCORDING TO FORRESTER

Source

Users want to manage their own settings at any time of day, from any place. They don't want to wait on the phone on hold while a helpdesk technician updates credentials on their behalf. A key CIAM feature is self-service account management – enabling them to manage their own password resets, communication preferences etc.

— LINK SELF-SERVICE ACCOUNT MANAGEMENT WITH YOUR CRM:

- → Increase accuracy of customer data across your systems, ready to be leveraged for progressive profiling.
- → Ensure data is always up to date, allowing for better planning of marketing, other aspects of CX and personalisation of communications/services.
- → Put customers in control of communication preferences to help with GDPR compliance.

SINGLE SIGN-ON (SSO)

SSO allows your customers and partners to sign into your web application once, to then automatically be logged in to all connected services and applications that they have the right to access. Think Google – you don't need to repeatedly sign in to access Mail, Drive, Analytics etc.

Watch this short explainer video on SSO

This is a key customer experience asset, as well as a security asset, as a user only needs one set of credentials to verify their identity, rather than a separate login for each application. SSO provides a seamless user journey through all of your services and even to external services if you leverage federation (see Federation feature below).

— HOW COULD SSO BE USED IN PRACTICE? ENERGY COMPANY EXAMPLE:

- → A customer uses their chosen identity provider (e.g. Bank ID, Mobile Connect) to log into the company's app.
- → The customer can now access different services – electricity reporting, gas usage, service status. No need to log in again for each area.
- → The customer now wants to access more sensitive information such as payment history, for which higher assurance is needed. They must re-

authenticate with another chosen strong identity provider (e.g. bank ID).

- Customer logs out once – they are now logged out of all services.

FEDERATION

Federation allows organisations to build links between their own services and external third parties services.

WHY FEDERATE?

- Raise awareness of your brand through federated third-party services.
- Already invest in strong KYC assurance practices? Other services will pay for use of your system – build new revenue streams.
- SSO to other federated services is a big win for CX – remove the frustrations that come with different credentials for multiple apps and services.

DELEGATED AUTHORITY

Delegated Authority is a solution to enable individual or organisation users to simply delegate the right to use digital services on their behalf in B2B, B2C and B2B2C applications. Digitalise otherwise admin-heavy, insecure ways of granting account access.

Watch our short explainer video on Delegated Authority

WHERE CAN DELEGATED AUTHORITY MAKE A BIG DIFFERENCE? (EXAMPLES)

- B2B - make supply chain and partner access to your services seamless. Insufficient measures lead to data breaches, which can destroy your brand's reputation. Don't take that risk.
- B2C – delegate allowances within family mobile contracts. Surprise and delight customers.
- B2B2C – outsource corporate tax admin to another company. Allow them to delegate access within their own company to avoid time-intensive manual workflows.
- G2C (government to citizen) – delegate power of attorney not just for sensitive data, but sensitive situations too (e.g. pensions, healthcare).

> 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

kuppingercole ANALYSTS

Ubisecure CIAM

Ubisecure's Identity Platform makes it simple, fast and cost effective to build CIAM capabilities into your apps and services. Help your developers get applications to market faster by plugging-in proven identity management:

1. Acquire, retain and grow customers with improved omni-channel registration, login, and engagement.
2. Reduce breach risk by upgrading authentication options, appropriate authorisation policies, and protection of identity data. Avoid being in the news for the wrong reasons.
3. Level up your customer experience and marketing operation with self-service and marketing insights.
4. Flexible deployment options - IDaaS (SaaS IAM), Private Cloud, or on-premise software. Always your choice of geographical data residency.

Ubisecure listens to your individual requirements and makes recommendations based on its many years of experience providing successful, flexible solutions to customers in all verticals (both private and public sector).

See case studies here.

ubisecure.com/demo
sales@ubisecure.com

UK: +44 (203) 974 2504
US: +1 (617) 917-3577
Finland: +358 8 415 41715
Sweden: +46 70 603 34 83
Germany: +49 89 20190980

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, Cloud, or on-premise 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
UK: +44 203 974 2504

UBISECURE FINLAND
Vaisalantie 2
FI- Espoo, 02130
Finland
FI: +358 8 415 41715

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

UBISECURE DACH
Franz-Joseph-Str. 11
80801 Munich
Germany
DE: +49 89 20190980