UBISECURE®

Connecting Identity.
Transforming Digital Business.

SOLUTION BUYERS GUIDE

BUILD VS. BUY: CIAM

Evaluating the different approaches to adopting Customer Identity & Access Management

UBISECURE®

Contents

Introduction

Identity & Access Management (IAM) is a general domain that relates to verifying the authenticity of a person's identity so that the person may be granted access to online systems and services.

IAM is a mature defence against data breach attacks with most enterprises now employing some form of IAM to manage password policy (length, expiration, reset), authorisation policies (who can access what and when), and identity authentication policy (are you really who you claim to be?). The movement of the identity to the perimeter of the enterprise has caused the attack surface to be extended beyond the employee and to the customer and partner. Breaches, especially those attacking customer Personally Identifiable Information (PII), privileged credentials, and partner data via attacks on the supply chain, are increasing and expose the victim organisation to loss of customer trust, GDPR fines and lots of bad press.

This white paper is about making practical and secure design choices for the management of predominantly external identities – Customer IAM (CIAM). Unlike employee or internal IAM, CIAM goes beyond the scope and complexity of managing identities within a workforce or other closed systems. It covers the identity management of external users such as customers, consumers, partners, citizens and remote workers.

— SEE: IAM VS CIAM

CIAM solutions are used across a wide array of industries and many sectors benefit from effectively implemented CIAM. The increasing array of online services in all sectors means that businesses and other organisations need systems that allow them to support online registration, social logins and authorisations, Internet of Things (IoT) and consent management.

CIAM capabilities such as Multi-Factor Authentication (MFA), Single Sign-On (SSO) and Passwordless login help organisations achieve the necessary balance between security and usability.

CIAM is primarily standards-based. Whether you build or buy, you'll need a solution that supports standards including OpenID Connect, SAML, WS-Federation, and OAuth. Implementing standards requires engineering resource

and expertise to implement correctly. We discuss this critical point in detail later in this white paper.

This white paper will primarily provide insights into:

- The security benefits of a Customer IAM solution
- The business impact of an effective Customer IAM solution
- Objective comparisons between a build and buy process
- Top tips and critical considerations for implementation and deployment choices (do you deploy your solution to the cloud, on-premises, or a hybrid cloud/on-premises approach)

Throughout the white paper, we will look at why identity management matters and the critical considerations you need to make when evaluating a CIAM solution for your business or organisation.

Most data breaches are caused by compromised credentials, weak authorisation and access control implementations. Identity and Access Management is a core cybersecurity solution to prevent breaches. IAM security functionality can be extremely comprehensive, but for the purpose of this paper we'll draw attention to the following as critical IAM capabilities:

- **Single Sign-On (SSO)**
- **Multi-Factor Authentication (MFA)**
- **Authorisation policy management**
- **Acceptance for 3rd party Identity Providers (social, professional, federated)**
- **Self-service management of identity credentials at scale**
- **Identity data directories**
- **Privacy-by-design and adherence to privacy regulation**

> IDENTITY IS ITS OWN SOLAR SYSTEM. ITS OWN GALAXY.
>
> Robert Herjavec, CEO of global IT security firm Herjavec Group.

CIAM solutions can go way beyond functions like authentication and authorisation – they are the tools that enable your organisation to manage identity related data in a centralised manner.

UBISECURE

Why does CIAM matter?

A fast, slick user experience is essential. This will increase users' engagement with an online service, and that added 'dwell time' (a measure of how long users spend on a page) is a good indicator that the content is of value.

The cost of abandoned logins could be huge – customers may be less likely to return to using your systems and will be less likely to recommend your systems to others if they have had a bad user experience. The cost of implementing a reliable CIAM solution could therefore be seen as a long-term investment in the infrastructure of your operation. In fact, rather than being seen as a cost, it may instead be a way to drive more customer engagement and loyalty, thereby helping to generate more revenue.

Users no longer compare online service experiences within an industry – they compare them with the experiences they have when using all services online. In a world where users are used to one-touch payments, fingerprint and facial recognition, and apps that make authentication slick and invisible, a good CIAM solution becomes essential rather than nice-to-have.

The modern user wants and expects a simple system. They do not want to log into many different systems. Once they are in one ecosystem, they expect to move freely inside, from service to service.

Alongside cultivating an interoperable environment that leads to better end-user experiences, a good CIAM solution can help organisations with elements of GDPR compliance – specifically with consent management, user data management and minimum viable data.

The benefits of good CIAM go beyond the reduction of risk to your organisation. Giving users a better user experience can mean:

- More revenue from new users.
- Enhanced brand loyalty from existing users.
- Higher conversion rates for all users.

Identity management is fast becoming an essential part of many B2C services, such as family access to shared music subscriptions, the setting of parental controls for online systems and the setting of spending limits for online video and gaming accounts. CIAM is also increasingly recognised as necessary in B2B settings, such as managing privileged users in supply chain management, assisting with complex delegation of authority scenarios (such as online tax filing) and more.

UBISECURE

CIAM – before and after implementation

A 'before and after' analysis of an effective CIAM solution.

	BEFORE	AFTER
CUSTOMER EXPERIENCE	Multiple identities	Single identity
	Friction	Frictionless
	No personalisation	Personalised content
SECURITY	Breach risk, identity data silos	Breach protection, consolidated secure data
	Identity fraud	Verified identities
	Unusable MFA	MFA appropriate to situation
OPERATIONAL EFFICIENCY	Support desk overhead	Self-managed identity
	Manual workflows	Delegated administration
PRIVACY & COMPLIANCE	Compliance risk	Meets compliance
	No consent management	Consent management
SCALING	Data scaling issues	Stored at scale, structured access
	No sync with external services	IAM master of identity, CRM master of contracts
	Unpredictable, complex costs	Predictive, transparent, controllable costs

— SEE ALSO:

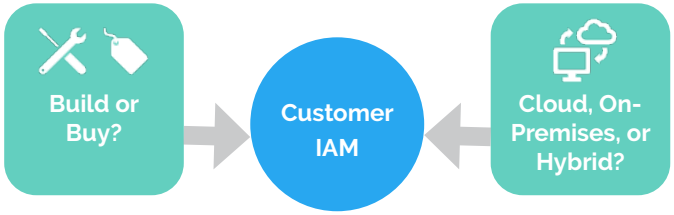
CIAM INVESTMENT AND ROI - A GUIDE TO THE VALUE OF CIAM PROJECTS

Many of our clients look for a CIAM solution because their internal development costs are too high and they need a streamlined IT process for managing consumer identities. Often this is triggered by team changes, which can create or reveal gaps in your technical capability. The good news is that investing in a CIAM solution can save your organisation money.

CIAM – two core decisions

DEPLOYMENT OPTIONS

There are two main decisions to take when considering how to implement a CIAM solution for your organisation.



The first decision is to decide whether to build your own CIAM solution or to buy one from an identity management provider:

- **Build:** use your existing internal resources and expertise to handle identity and access management.
- **Buy:** use external resources and expertise to handle identity and access management.

The principal aim of this paper is to help you make an informed decision about which of these options is best for your organisation.

The second decision relates to your mode of deployment and installation:

- **Cloud:** either private cloud, or next generation identity-as-a-service (IDaaS) pre-configured to accelerate deployment time.
- **On-premises:** a solution implemented in a trusted internal space where you have full control over deployment.
- **Hybrid:** flexible cloud + on-premises solution.

Building a CIAM solution

The concept of identity can be thought of as a collection of verified attributes – a set of name/value pairs that has to be corroborated before any system can trust that a person is who they say they are.

This sounds straightforward. And in a closed system of trusted employees, IAM presents only a moderate technical challenge. However, there is a significant jump in complexity from traditional workforce-focused IAM to the much broader landscape of CIAM.

While it may be natural to think that a CIAM solution is one of many tasks that you can assign to your in-house technical team, our experience of offering

identity management services since 2002 has shown us that the build process is not simple.

A self-build process diverts resources from your team and slows down your progress on your main line of business. For example, if your organisation specialises in financial services, your efforts should be focused on providing that core proposition, not on spending time planning and implementing a niche technical project around identity management.

The same applies to almost all organisations who have a need for a CIAM solution – the work required is so specialised that a bought solution will be quicker and more robust than a custom-made alternative that is developed in house.

If your core business does not relate to access management, you will start to find complexity if you look to build your own CIAM solution. Naturally, there is a cost associated with outsourcing the job to an external provider, but this far outweighs the risk of doing the work in house and ending up with a system that may not be robust, standards compliant or scalable.

Good identity access management is essential to the running of a reliable digital service. A lack of investment in setting up the right identity management systems could have a long-term effect on your reputation and profitability. Failure to implement systems that achieve compliance with regulations and other security standards has the potential to put the viability of an entire business at threat.

BENEFITS OF BUILDING A CIAM SOLUTION	DRAWBACKS OF BUILDING A CIAM SOLUTION
✓ You can control and customise every part of the identity management process. ✓ Simple solutions may offer quick internal wins. ✓ The intellectual property of the internal solution may be strategically important.	✗ High level of technical expertise required. ✗ Complex and time-consuming to implement a custom system. ✗ No guarantee of compliance with industry standards. ✗ Scope creep – the risk of the project that never ends. ✗ Support is critical and must be well resourced.

Even the perceived benefit of the cost saving of doing identity management work in house is often a drawback in disguise. Unless you fully understand the complexity of the work needed, it is likely that you will underestimate the long-term cost of implementing and supporting your own CIAM solution.

UBISECURE®

CIAM self-build checklist

Ask yourself these questions when considering whether to build your own CIAM solution:

QUESTION	YOUR RESPONSE
What size of team do we need?	
How long will it take us to implement a robust solution?	
Can we keep up with technical and compliance changes as part of our ongoing operation?	
Do we have expertise available immediately in case something goes wrong?	
Can we afford all of the implementation, testing and support costs?	
Can we afford to divert resources away from our core competencies?	
Can we produce an interoperable system that is faster, better or cheaper than a bought solution?	
Do we have the resources to follow changes in the legal landscape around personal data management?	
Do we have the resources to follow and react to security developments in the various related protocols?	

The costs and challenges of developing an in-house CIAM solution

The main issue we see with the build option is that the process is technical by nature and complex. Expertise is needed to configure the setup, and your team requires significant knowledge about the domain of identity management and security.

This complexity can have a significant effect on the speed of implementation of any in-house CIAM solution. For large software projects:

- 33% exceed their schedule.
- 66% exceed their budget.
- 17% underachieve on expected benefits.

Source: McKinsey [**https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value**]

Building a CIAM solution is not a one-off project. If this work is done in house, your organisational responsibility will be to maintain the necessary IT expertise to support the identity management setup to ensure it functions as expected and interacts with other systems, including new systems you bring on board in future. This poses a significant technical challenge and can add a long-term cost to your IT budget.

Building and running your own CIAM solution involves costs such as data storage, data security, load balancing and the necessary staffing considerations – upskilling developers, managing teams, keeping training up to date, and so on. Good developers command high salaries, and a minimal enterprise-level development team may call for 6 or more such people. Consider also the need for 24/7 support for the enterprise, which would have to be managed in house, thereby adding a further financial burden.

Some of the implementation costs depend on whether you opt for an on-premises data centre or a private or public cloud solution. But in either case, the cost of developing your own CIAM solution is not to be underestimated.

Our experience tells us that, for most businesses and organisations, there is no compelling argument for building a CIAM solution in house. Consider the opportunity cost – the cost of choosing to develop your own in-house solution versus buying a CIAM solution. Picking this option means adding a non-core task to your workload, which comes at the expense of developing true expertise for your own domain.

Devoting resources away from your core services may not be a strategically wise move. Consider whether such an investment could be recouped elsewhere. For example, might it be possible to develop a platform that could be resold? Or could the development work lead to the creation of a new business arm? In most cases, these possibilities are unlikely to be realised. Rather than being an opportunity, such in-house development work tends to be a cost.

So, should any organisation ever build its own CIAM solution? Although we don't recommend this approach, there may be some scenarios where it could make sense:

- You have 10K+ employees and in-house expertise in identity management.
- You have security requirements so strict that you cannot use any third-party solution.

Buying a CIAM solution

The alternative to building your own CIAM solution is to buy one from an identity services management provider. By purchasing a configurable CIAM product, you devolve the task to a specialist whose one and only function is to provide a robust, standards-compliant identity management solution. The result is that you can spend the time, money and energy on development and specialisation within your own organisation.

BENEFITS OF BUYING A CIAM SOLUTION	DRAWBACKS OF BUYING A CIAM SOLUTION
✓ Pre-built, robust, highly tested and future-ready system. ✓ No need to delay other projects and core services. ✓ External support means no ongoing in-house support requirement. ✓ Focusing on your main service will drive your business forward. ✓ Compliance with relevant rules and regulations. ✓ Better security – the CIAM solution provider abides by strict policies to keep data safe.	✗ Initial costs may seem high. ✗ You may overlook in-house skills.

In the world of cybersecurity and IAM specifically, standards rule, and resource is expensive. In most cases, it makes little sense for your organisation to fight for expert development resource from a limited pool, when even general software development resource is scarce.

UBISECURE

CIAM installation types

The second main consideration when choosing a CIAM solution is the type of installation or deployment. It is useful to note that not all identity management providers can support all types of CIAM solution deployment – and this may rule out some providers from your assessment phase.

ON-PREMISES INSTALLATIONS

An on-premises CIAM installation means that the software runs on servers owned and operated by you. Some organisations prefer or have to use an on-premises solution so that they can retain full control and responsibility for security and data sharing with the outside world.

A System Integrator may take the CIAM solution from an identity management provider and host it for you, which has the benefit of offering an on-premises-like experience, but with the safety net of infrastructure and support coming from an existing partner you know and trust.

IDAAS & CLOUD INSTALLATIONS

IDaaS (Identity-as-a-Service) makes deployment somewhat simpler by pre-configuring many of the standard IAM functions. This makes for a less customisable system, but accelerates the time to value.

Cloud-based data storage offers more flexibility and scalability than on-premises storage, and is more cost-effective than on-premises storage, but it may raise questions on how data residency issues are handled due to the organisation not having complete control over which jurisdiction the data is stored under.

HYBRID CLOUD/ON-PREMISES INSTALLATIONS

A hybrid cloud/on-premises IAM solution generally means maintaining the core user directory and legacy applications on-premises, whilst running the IAM capabilities from a SaaS infrastructure.

This allows you to realise the benefits of cloud IAM – such as faster time to market and lower TCO – even if you want/need to host some applications on-premises.

WHICH TYPE OF INSTALLATION TO CHOOSE

Note that some identity services providers may be able to offer nothing but a cloud-based CIAM installation. If this does not suit your governance model, it may be worth using a CIAM provider who can offer an on-premises, or hybrid cloud/on-premises, solution.

Ubisecure offers cloud-based, on-premises and hybrid CIAM solutions. What suits one client will not necessarily suit another, so we cannot say that one deployment option is better. We are happy to have this discussion with you and with your System Integrator to find the best option for your organisation.

At Ubisecure, our focus is on developing the services, software and tools that power identity management. These are our recommended key considerations for assessing which CIAM solution best suits your organisation...

> UBISECURE IDENTITY PLATFORM HAS HELPED US REALISE A UNIFIED IAM SOLUTION FOR BOTH CONSUMERS AND CORPORATE CUSTOMERS, CREATING AN ENVIRONMENT WHERE YOU ONLY NEED ONE IDENTITY.

Taneli Ropponen - Director of IT-production, DNA

Critical considerations for a CIAM solution

> AS A SYSTEM INTEGRATOR OUR MAIN GOAL IS TO DELIVER HIGH QUALITY SOLUTIONS TO OUR CUSTOMERS ON TIME AND ON BUDGET. UBISECURE IDENTITY PLATFORM MADE IT POSSIBLE FOR US TO DEPLOY A COMPREHENSIVE IDENTITY RELATIONSHIP AND ACCESS MANAGEMENT SOLUTION TO OUR CUSTOMER IN LESS THAN FOUR WEEKS. UBISECURE IDENTITY PLATFORM TRULY LIVES UP TO ITS NAME AS WE WERE ABLE TO RAPIDLY DEPLOY THE PLATFORM AND INTEGRATE THE CUSTOMER'S CRM AND E-SERVICE PLATFORMS TO THE CIAM SOLUTION.

Ville Särmälä - CEO, Knowit Oy

SECURITY: You need a solution that puts security at the core, with strong authentication, reliable transmission encryption and tight access management. All of this needs to work across all use cases for the organisation, while abiding by all compliance regulations. Use cases and compliance may change in future, and the solution needs to be highly configurable to cater for this. CIAM is not a 'set and forget' activity.

SCALE: Can your chosen solution scale well and handle peaks in usage? Users access services continuously throughout the day, making smooth identity management a critical point in the infrastructure. Some enterprise systems may need to support 50 million users. While home-grown systems may work well in small test cases, they are unlikely to remain stable at scale or handle instances of high demand (e.g. tax peaks once a month, or Monday morning spikes). Can the system be adapted and well tuned for all of your use cases?

DEPLOYMENT: How do you want to deploy your CIAM solution? Is a cloud-only solution suitable for your organisation? Do you just need core IAM capabilities implemented into your application quickly? In which case an IDaaS solution may make most sense. Would it be safer to use an on-premises installation instead? Could an on-premises plus cloud hybrid model work? What options can your identity management provider or in-house development team offer?

SUPPORT COSTS AND EXPERTISE: An effective CIAM solution is crucial to your infrastructure, so you need a system you can rely on and that can be updated or fixed quickly should anything go wrong. Choosing open source means no support and no safety net if your system lets down end users.

PAST EXPERIENCE: Before investing in a CIAM solution, due diligence will involve asking whether a service provider has engaged in work that matches your use case. Clearly, this is not possible if you are building your own solution. In Ubisecure's case, we are happy to share case studies for our many client use cases since 2002.

Top tips for CIAM success

- Identity management is essential to the long-term success of your organisation. Think of it as an investment rather than a cost.
- It is better to focus on your core service than to devote internal resources to identity management.
- Any bought CIAM solution is significantly better than an incomplete or absent internal solution.

Choosing your CIAM solution provider

Our business – and that of every other reputable CIAM provider – is to remove complexity from your environment. Not only does this make things easier for your end users but also it means you can focus on developing and operating your core service.

Our clear view is that you can best remove this complexity by buying a CIAM solution instead of building your own. So why might you choose Ubisecure when there are other providers on the market?

European focused: With our origins in the Nordics and over a decade of involvement in European-specific digital identity initiatives, we remain focused on helping organisations protect identity data and benefit from the European identity ecosystem. Our regional presence means Ubisecure's experts are easily available when needed, and data residency requirements can meet country-specific geo-regulation.

Adaptable system: We handle tier-delegated administration well. Rather than creating a single account and giving it to everyone, our flexible system empowers

users to do things for themselves, so there is less reliance on other expert users. This leads to easier management and fewer support requests. It also leads to increased use because it reduces friction – and this can lead to greater sales for the end customer. Our systems can support all forms of individual and company delegations:

- Individual to individual.
- Individual to company.
- Company to company.
- Company to individual.

> WE ARE THRILLED TO BE WORKING WITH UBISECURE ON THIS EXCITING CUSTOMER PROJECT, WHICH IS DEMANDING A HIGH DEGREE OF INTEGRITY, MULTIPLE METHODS OF STRONG AUTHENTICATION AND FEDERATED ACCESS.

Greger Wikstrand, CTO and Head of Cloud Services, Capgemini Sweden

Government-level trust and national scale: We have experience of dealing with 3.6 million tax entities that interact with government through the Finnish Katso project. This implementation of our Identity Platform requires national-level scale and supports organisation and citizen authentication for 100+ government services. The solution also manages the complex delegation of authority to allow third parties to represent individuals and companies, making it one of the largest relationship management solutions deployed globally. With experience of dealing with financial systems that are of critical national importance, we can deliver first-class identity management for any type of organisation at even the highest levels of global security.

20+ years' experience: Identity management is complex and it is important for CIAM providers to have a broad and deep understanding of the topic so that they can offer a reliable solution that works now and that is ready for the future. We have worked in identity management for many years and have dealt with enough identity authentication and security scenarios to understand our clients' challenges. That means we can provide the right options quicker, with less time, effort and money wasted by you and your System Integrator.

> THE CONFIGURABLE WORKFLOWS ENABLED US TO REALISE OUR BUSINESS REQUIREMENTS FOR THE DELEGATED IDENTITY MANAGEMENT, EMPOWERING OUR CUSTOMERS TO TAKE CONTROL OF THEIR IDENTITIES. THE APIs HELPED US MASS IMPORT CLOSE TO A MILLION ENTRIES TO THE IDENTITY PLATFORM AND INTEGRATE THE IAM TO OUR CRM SYSTEMS.

Laura Lätti - Development Manager, DNA

Cloud, On-Premises or Hybrid - our customers can choose how their CIAM is deployed based on their budget, resource level, expertise level or even just company culture. We have deep experience will all levels of implementation.

Commitment to standards: We are represented in several technical working groups. Our team includes working group chairs in the specific interest groups that our represent the domains of our customers where we are a member of, and a community contributor for, the industry associations shaping the identity management ecosystem.

Case studies – CIAM buy scenarios

RETAIL

CASE STUDY: S-GROUP

S-Group is a retail chain with sales of over € 11 billion (2014). S-Group operates in over 1,600 locations and employs over 40,000 people. Its main businesses and brands include supermarkets, hotels, banks and retail.

S-Group has a wide range of both internal and external services operating under different brands, infrastructure and teams making it very difficult for customers to see and use all of the services easily. With each S-Group company often operating several brands each with their own online services, customers were unable move easily between services and websites and S-Group was unable to effectively engage its customers with all available services. Many S-Group services also offer online product sales and promo discounts to loyalty members and the group needed a way to easily apply discounts to encourage offer uptake. Other S-Group digital services included digital receipt and warranty management, management of the two million client-owner loyalty program members and annual bonus payments.

The solution saw S-Group deploy the Ubisecure Identity Platform to achieve a wide range of Customer IAM functionality designed around providing customers with a single identity for all S-Group company applications and services:

- Registration and login using social, business and S-Group's accepted strong identities
- Workflows for situational multi-factor authentication (step-up auth) and authorisation based on profile
- Single-sign on (SSO) across all group applications and services
- Personalised customer journeys based on single identities
- 24/7 self-service

The Ubisecure Identity Platform brought deep benefits to S-Group. Customers became happier and more loyal thanks to the use of a single identity: SSO across many different services; faster registration, login, engagement and checkout; personalised content and product promotions based on profile; easy access to receipts, warranties and bonus information; self-managing identity data and functions 24/7.

For S-Group, the use of the Ubisecure Identity Platform to achieve Customer IAM benefits was a core component of S-Group's digitalisation initiatives leading to improved customer journey and engagement; lower support costs; enriched customer identity data, attributes and profiles; improved security and privacy controls around identity data.

PUBLIC SECTOR

CASE STUDY: FINNISH GOVERNMENT

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.

Part of the national initiative was to implement a standards-based identity management system to enable the strong identification of organisations in government e-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).

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

The system enabled an enormous user base, as all Finnish companies needed to have the ID in order to use the online services provided by the Finnish government. Since initial deployment, the system became one of the largest examples of digital identity management, authentication and attribute distribution solutions in the world. It became the de-facto identity management solution used by all Finnish organisations to use Finnish online government services.

The primary transformational driver for the system was 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 cost between 20 – 50 Euros. The online service transaction cost was estimated to be 10 – 50 Cents, meaning 99% reduction in cost - equating to hundreds of millions of euros potential savings. The ID platform enabled the online services, by ensuring strong authentication of organisations and their representatives. Without proper authentication, the services could not be made available online.

The system 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, with over 444,000 organisations using it as their main identity solution when dealing with government institutions.

Final Thoughts

The future of identity management is to make authentication and personal identity management a seamless process to end users. By removing the friction, we want to help create a digital landscape where services are easy to access but also secure and respectful of the level of information that needs to be processed.

We genuinely believe that building your own CIAM solution is the weaker option when compared with buying a solution, especially when SaaS-based solutions, like IDaaS, offer streamlined IAM functionality quickly, easily and at a lower cost.

The cost, complexity and long-term support burdens of such projects are easy to underestimate. Often, our software is selected to replace an in-house-developed solution that becomes unmanageable when significant team members leave the organisation.

Think carefully about the problem you solve for your clients and user users. If security and identity management is part of your core proposition, building your own CIAM solution may make sense.

For most organisations, your core proposition relates to a different field. It therefore makes sense to focus on that core part of your business and to use an expert provider to handle all of the complexity of dealing with external identities. This results in a simplified operation and a reduction in risk to your organisation.

For more examples of how other companies utilise Ubisecure solutions, please visit **www.ubisecure.com/customers**.

Contact Ubisecure

If you would like to reduce your risk and remove the complexity of identity management, contact us to find out how we can help you implement the right CIAM solution for your organisation.

To learn more about Customer IAM and company identity solutions visit **www.ubisecure.com** or contact us at **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