UBISECURE™

Connecting Identity.
Transforming Digital Business.

BUILD VS BUY

Finding the Right Approach to Customer Identity and Access Management (CIAM)

Contents

Introduction

This white paper is about Customer Identity and Access Management (CIAM) and associated Identity APIs, a 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. Unlike traditional Identity and Access Management (IAM), CIAM goes beyond the scope and complexity of managing identities within a workforce or other closed system. It covers the identity management of external consumers, and this makes CIAM an inherently more complex topic than IAM.

CIAM solutions are used across a wide array of industries, such as when governments manage access requests to online tax-filing systems. Without a suitable verification infrastructure in place, online data exchanges like this could not take place in any reliable way.

Common use cases for CIAM are found in the banking, financial services and insurance (BFSI) sector. A good CIAM solution here can help for compliance with PSD2, which sets out that financial transactions should use strong authentication.

Many other sectors can also benefit from good CIAM, including education, healthcare and construction. The increasing array of online services in all sectors means that businesses and organisations need systems that allow them to support online registration, social media logins and authorisations, Internet of Things (IoT) and consent management. Concepts such as Multi Factor Authentication (MFA), Single Sign On (SSO) and Passwordless are at the root of the work that needs to be done to serve end user needs.

This white paper will primarily provide insights into:

- The business impact of an effective Customer IAM solution

- Objective comparisons between a build and buy process

- Top tips and critical considerations for implementation choices

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.

Why does identity management matter?

A fast, slick user experience is essential in improving the user experience for end users. 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.

Google and other search engines use this data as an SEO ranking factor. In short, giving users an effective login experience can produce better results for an organisation's discoverability on search engines.

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 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.

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

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

It is not always easy to quantify the effect of a good CIAM solution. However, any feature of your online service that has the potential to slow down or degrade the user experience will invariably have an impact on engagement.

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 optional.

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, without needing to have their identity checked at each door. It is like being in a hotel and having a single key card for your room. Your identity is checked once on arrival, and after that only a single point of authentication is needed to access all available amenities in the hotel. There is no requirement for multiple passwords. A single trusted identity manages your whole stay. This is what CIAM can offer for your organisation.

Along with a 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.

A CIAM solution lowers an organisation's risk by providing a robust, scalable means to process identities so that end users have a frictionless way of accessing online systems and services. Though a CIAM solution is essential to such activities, as with any good 'middleware' solution, it is characterised by its invisibility to the end user. A good CIAM solution helps to provide an unseen but essential stepping stone of trust that permits end users to perform actions with the minimum of disruption to the user experience.

> 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.

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.

These benefits should be held in mind when assessing the case for investing in a CIAM solution. Rather than being seen as a cost, this could be viewed instead as part of the infrastructure that drives long-term success for your organisation.

The growing need for reliable identity management services means that CIAM implementations are now found outside the traditional domain of B2B.

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.

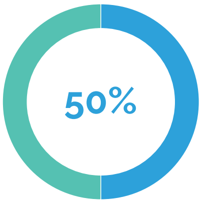
CIAM – Before and After Implementation Benefits

A before and after analysis for an effective CIAM solution should provide companies with:

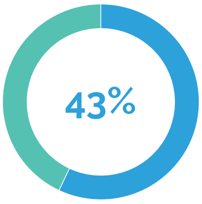
	BEFORE	AFTER
CUSTOMER EXPERIENCE	Multiple identities	Single identity
	Friction	Frictionless
	No personalisation	Personalised content
SECURITY	Data silos, breach risk	Consolidated secure data
	Identity fraud	Verified identities
	Unusable MFA	MFA suitable for situation
OPERATIONAL EFFICIENCY	Support desk overhead	Self-managed identity
	Manual workflows	Delegated admin
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

How a CIAM solution can save costs and accelerate business processes

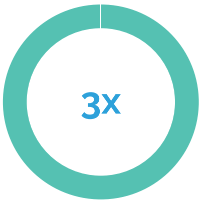
Many of our clients look for a CIAM solution because their internal development costs are too high and they need a streamlined IT process for managing consumer identities. Often, this is triggered by team changes, which can create or reveal gaps in your technical capability. The good news is that investing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



Top-performing companies are 50% more likely than their peers to 'have well-designed user journeys that facilitate clear communication and a seamless transaction' (69% vs 46%).



In terms of their tech setup, 43% of organisations report a fragmented approach with inconsistent integration between technologies.



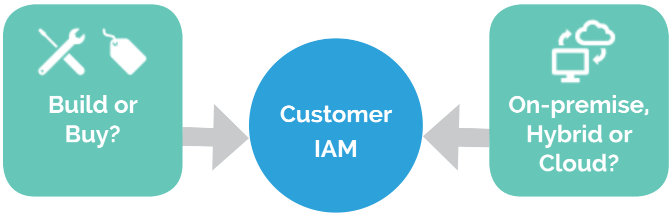
Top-performing companies are almost three times as likely as their mainstream peers to have invested in an integrated, cloud-based technology stack.

Statistic from the Adobe Digital Intelligence Briefing 2018.

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.

CIAM – two core decisions

There are two main decisions to take when considering how to implement a CIAM solution in 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:

- On-premise: a solution implemented in a trusted internal space where you have full control over deployment.
- Cloud or Hybrid: a solution that relies on a third-party cloud storage setup.

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. If your organisation specialises in financial services, your efforts should be focused on providing that core proposition, not on spending time to plan and implement 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.

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 aware from our core competences?	
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 in-house software development projects[1]:

- 27% exceed their timeline.
- 18% exceed their budget.

For large software projects[2]:

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

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 onboard 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-premise 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.

1 Source: OohLaLog [http://oohlalog.com/blog/2014-09-03-in-house-fail-successful-app-development-looks-outside-it-for-critical-timely-resources-and-skills]

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

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:

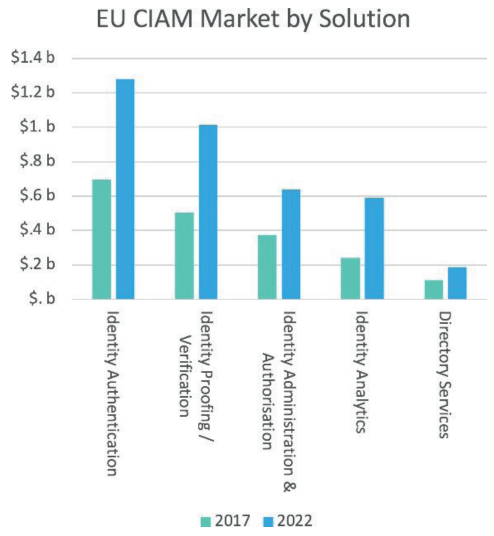
- You have 10K+ employees and in-house expertise in identity management.
- You have security requirements so strict that you cannot use any third-party solution.

Buying a CIAM solution

We have set out the significant negatives associated with building your own CIAM solution. The alternative to building your own CIAM solution is to buy one from an identity services management provider.

The trend is for increased investment in CIAM solutions, with MarketsandMarkets analysis in 2017 predicting that the global consumer IAM market would grow from USD 14.3 billion in 2017 to USD 31.75 billion by 2022, including a significant CIAM investment increase in the EU.

Ubisecure's specialist areas of Identity Authentication, Identity Proofing/ Verification and Identity Administration & Authorisation see some of the biggest increases in these projections.



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.

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.

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.

CIAM installation types

The second main consideration when choosing a CIAM solution is the type of installation or deployment. Most of our clients already have a clear idea of their installation requirements. It is useful to note that not all identity management providers can support both main types of CIAM solutions – and this may rule out some providers from your assessment phase.

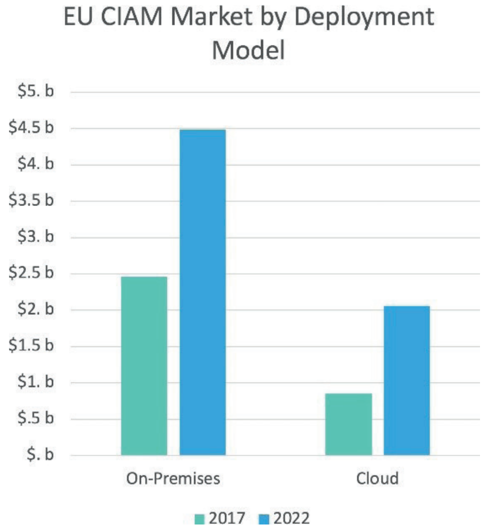
ON-PREMISE INSTALLATIONS

An on-premise CIAM installation means that the software runs on servers owned and operated by you.

While many services are moving to the cloud, identity management is one area where security-conscious organisations prefer to use an on-premise 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-premise-like experience, but with the safety net of infrastructure and support coming from an existing partner you know and trust.

The MarketsAndMarkets 2017 Customer IAM report shows that there is significant growth in both on-premise and cloud deployments of CIAM solutions. Note that on-premise deployments account for double the market share when compared with cloud – and this trend looks set to continue until at least 2022.



We see this as a clear sign that moving security to the cloud is not the preferred option for most businesses and organisations.

CLOUD INSTALLATIONS

A cloud-based CIAM installation involves the use of third-party servers that are not owned by you.

Management of identities is an area where some organisations will be understandably hesitant to introduce the use of a cloud system. Identity management is often treated under the umbrella of cybersecurity, and this is one of the last areas to see a move to cloud-based systems.

Organisations who have moved all services to the cloud face the risk of a ‘data repatriation’ request from their government. This is particularly relevant for organisations based in the US, where Federal orders could result in a requirement for data to be stored and processed on US territory.

The potential for a data repatriation requirement means that many organisations prefer to handle identity access management via an on-premise installation of a CIAM solution.

> 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

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 or the risks your organisation is willing to take with its users' information, it may be worth using a CIAM provider who can offer an on-premise solution.

At Ubisecure, we offer both on-premise and cloud-based CIAM solutions. What suits one client will not necessarily suit another, so we cannot say that on-premise is always better than cloud or vice versa. We are happy to have this discussion with you and with your System Integrator to find the best option for your organisation.

Partnering with a System Integrator

When you buy a CIAM solution, you will probably need the help of a System Integrator.

The System Integrator is a third-party technical service provider that can implement the CIAM solution in line with your needs as the buying organisation. Each technical setup will differ between organisations, and so a bought CIAM solution needs to be configured.

> 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

System Integrators such as Capgemini and Accenture may take an on-premise installation from Ubisecure, deploy this to their datacentre and provide a private cloud solution to you.

We can run our cloud-based CIAM solution for you, but even in this case it is typical to use the services of a System Integrator.

We do provide best-practice training called IAM Academy for organisations who wish to learn how good CIAM integration works. Please review our Developer website for more information on the IAM Academy – www.ubisecure.com/developers.

At Ubisecure, our focus is on developing the software and tools that power identity management. For that reason, we recommend that you engage a trusted third-party System Integrator to perform the CIAM implementation.

Critical considerations for a CIAM solution

These are our recommended key considerations for assessing which CIAM solution best suits your organisation.

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? Would it be safer to use an on-premise installation instead? Could an on-premise 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

> 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

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?

We do one thing well: Other providers may offer services beyond identity management, such as system integration. Our strength is our knowledge of standards-compliant identity management, so that is the sole focus of Ubisecure. Our clients come to us because they want an expert in this area, not an agency that offers many other complementary services.

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.

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 nation-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.

15+ 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 since 2002 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.

Founded in Finland, now serving the greater European market: The domains of identity management and information security are highly developed and innovative in the Nordic region, and we integrate with services across Scandinavia and beyond. Finland is a leader in digital identity – the first European country to implement eID cards for citizens and SIM-based login solutions for public services.

Commitment to standards: We are represented in the technical working groups of the OpenID Foundation and GSMA. 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:

OpenID
kantara INITIATIVE
OIX OPEN IDENTITY EXCHANGE
GSMA
IETF
IDESG
LIGHTest
FINNISH INDUSTRIAL INTERNET FORUM
FISC Finnish Information Security Cluster

Case studies – CIAM buy scenarios

RETAIL

CASE STUDY: S-GROUP

S-Group is a retail chain operating in Scandinavia, Russia, and the Baltics with retail 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 sees S-Group using 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 benefits of the Ubisecure Identity Platform to S-Group are deep. Customer are 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

FINNISH GOVERNMENT

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, now known throughout Finland as Katso.

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 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. Since initial deployment Katso has become one of the largest examples 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.

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, 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.

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.

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.

With frictionless identity management, we see a future where smart use of technology produces a safer and more streamlined way for everyone to be an engaged digital citizen.

We genuinely believe that building your own CIAM solution is the weaker option when compared with buying a solution.

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.

We work with high-performing organisations who see the value of investing in greater simplicity and lower risk.

E-GOVERNMENT
Kela
VERO SKATT
Katso
kieku
Finnish Communications Regulatory Authority
Ulkoasiainministeriö Utrikesministeriet
Huoltovarmuuskeskus Försörjningsberedskapscentralen National Emergency Supply Agency
Väestörekisterikeskus
TULLI
tunnistus.fi
TEKES
TELECOMS
DNA
Telia
EnStream
FINANCIAL
etera
FIM
LähiTapiola
Eläketurvakeskus Pensionsskyddscentralen
Finnish Motor Insurers' centre
FINNVERA
RAHASTOPALVELU
ENERGY
Vantaan Energia
HELEN
loiste
ELLEVIO
HEALTHCARE
TALTIONI
KanTa
eHälsomyndigheten
visibacare
INDUSTRY
Metsä
NESTE
metso
PLANMECA
YIT
oilon
Halton
RETAIL
S GROUP
STOCKMANN
paf
ray
VIKING LINE
SERVICES
posti
GRANO
ADITRO
SILTA
CGI
INSTA
ac coun tor
ecraft

FURTHER RESOURCES

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

You can review Ubisecure Use Cases, White Papers and Case Studies at www.ubisecure.com/resources. Ubisecure operates a robust partner and developer program with training programs, detailed documentation for APIs, SDKs, single page applications, and much more.

Also sign up to our newsletter and blog at www.ubisecure.com/blog for the latest industry and technical information about identity management, legal entity identifiers and more.

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-team@ubisecure.com.

About 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.

UBISECURE™

www.ubisecure.com
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