EXTERNAL IDENTITY MANAGEMENT & NEW BUSINESS OPPORTUNITIES

EXAMINING THE E-SERVICE DIGITALIZATION MATURITY MODEL

WHITE PAPER

UBISECURE™

Connecting Identity.
Transforming Digital Business.

INTRODUCTION

What we've seen when we've been dealing with the online services or digitalization projects, where companies can offer always available, easy-to-use customer services to their own stakeholders, is that there's a certain development path for the service itself. This short paper discusses briefly about these steps from the identity management perspective in the development path and tries to explain and list the benefits that companies deploying online services can achieve by taking a simple or bigger step forward.

We saw very simple extranets years ago, where Internet facing services were deployed so that customers, partners and other stakeholders could access some data over the net. The first generation of extranets didn't offer too much in terms of functionality, mostly they were there just for sharing of information, such as price lists. But the modern multi-site digital services can offer so much more for customers, partners, or other stakeholders. Companies today are not just standalone islands, and the traditional borders between businesses are disappearing when different types of business ecosystems are formed.

The evolution in the online services can be also seen in how they are using digital identities as enablers. The first extranets were relying on very simple methods of verifying the user identity, whereas the modern counterparts can utilize several methods for verification, including identity federation and utilizing identities from other sites or resources. Access decisions are not made based on simple yes/no authentication, but according to what the user is authorized to do by evaluating role or attribute type of information delivered to the application.

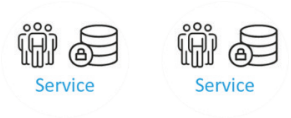
Digital services evolve through time. By reading this paper you can quickly see where you stand in the evolution path, and see what benefits lie ahead should you choose to further develop your own digital solutions. Identity can be a true enabler, not just an inconvenient mandatory security method.

THE DIGITAL SERVICE MATURITY MODEL

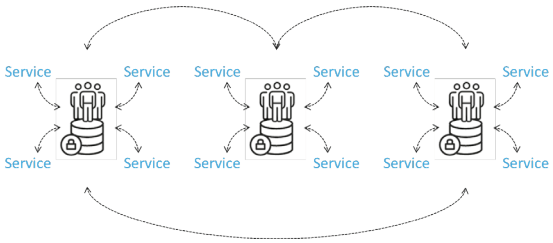
Ubisecure has been delivering authentication and identity management solutions to online services for more than a decade. From this experience we've come up with a maturity model that describes how services tend to develop, and how they integrate various authentication and identity management features when they evolve.

The maturity model can be divided into four distinct steps with major developments on how e-Services utilize identity information. Within these four steps there are mi-nor developments that can be described as well. Each evolution changes how the e-Service takes advantage of authentication, single sign-on, federation, roles, identity attributes and so on. The evolution path from the customer identity and access management (CIAM) perspective typically follows the growth of the service. The service can start with basic features and functions, and due to growth or regulatory demands, new features will be added. The CIAM functions should follow the same path, as the value of identity information for the service becomes much more tangible.

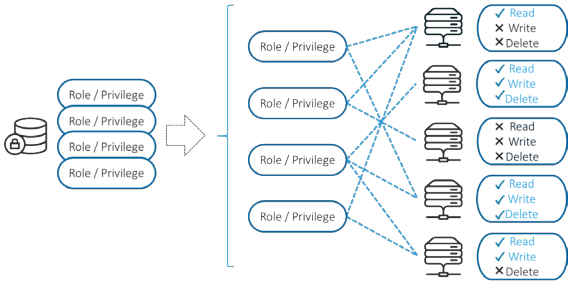
1 Stoneage



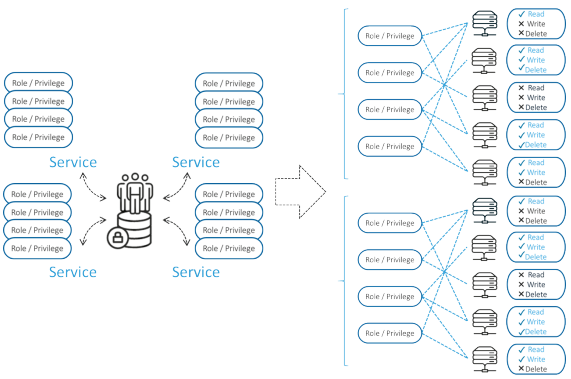
2 Medieval



3 Reneissance



4 Modern



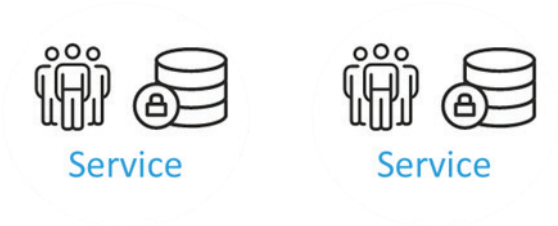
DIGITAL SERVICE 1.0– STANDALONE SERVICES

The sites that are initially deployed may rely on a simple model, where everything is concentrated into the single architecture. This could be a simple web application server with a database attached to it to store the users and their passwords and some simple data about them. Most likely, the user identities (username + pass-word) are stored to the platform's own user database.

Benefits	Drawbacks
Simple, quick	Managed by IT
	Password reset costs
	Only password

DIGITAL SERVICE 1.1 – SEPARATE STANDALONE SERVICES

A natural evolution might occur, when another site spawns, with a similar architecture. This is just a minor upgrade to the service hierarchy and might not require anything new. If you can keep things simple, this might be a workable solution, but here the user identities are separate, which makes it a bit inconvenient for the end user if they have to have accounts in both sites.



Benefits	Drawbacks
Just like 1.0 – simple, quick	Managed by IT
	Password reset costs
	Only password

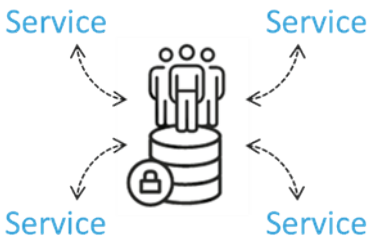
DIGITAL SERVICE 1.2 – SINGLE USER REPOSITORY

When users start to complain about having to maintain two accounts, or the IT department gets fed up with two separate databases, a merge can happen, where the user identities are handled in a single database. This can ease the registration pain for the customers, but still they need to login separately to each site, even if they have a single identity.

Benefits	Drawbacks
Just like 1.0 – simple, quick	Scaling issues
Centralized logging	Password management issues
	Multiple logins (no SSO)
	Only password

DIGITAL SERVICE 2.0 – INTRODUCING SINGLE SIGN-ON

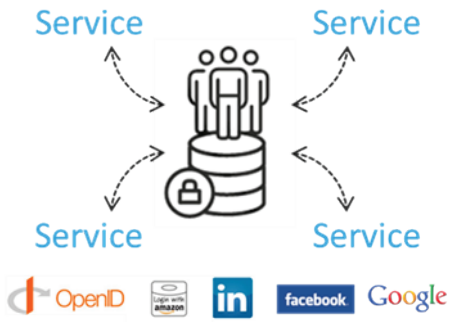
Once the number of sites grow, and the inconvenient multiple logins start to deter customers, it's time to introduce a single sign-on (SSO)solution such as Ubisecure Identity Platform. When using Ubisecure Identity Platform, services can benefit by having a single user repository, and single sign-on between services. The main benefit of SSO in this case is user convenience. Other tangible benefits include cost savings in password and identity management, centralized policy control and improved risk mitigation.



Benefits	Drawbacks
Easy for the end-users	Scaling issues
Single identity for all connected e-Services	Password management issues
Single sign-on and single logout	Multiple logins (no SSO)
Centralized logging	Only password

DIGITAL SERVICE 2.1 – SOCIAL IDENTITIES

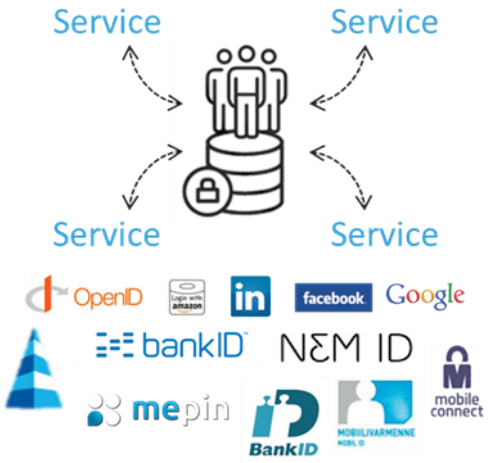
Social is all the rage now. And there's good reason for that. The chances are that almost all your customers have a social identity that they are comfortable with. When using Ubisecure Identity Platform, the service solution can integrate external authentication mechanisms to the services. The biggest benefit of having a social identity integration is in the convenience and easiness of registration and login. As we saw before, social identities with a strong identity can be used to strengthen the weak identity, while at the same time retaining the ease of use and wide acceptance by the end-users. This translates easily into lower cost for the service as the credentials are issued and managed by an external party, and better customer satisfaction as users can utilize their preferred social identity.



Benefits	Drawbacks
Extremely easy onboarding	Still only for one e-Service
Social identity for registration and authentication	

DIGITAL SERVICE 2.2 – MULTI-FACTOR AUTHENTICATION

Ubisecure Identity Platform can connect and support multiple identity repositories or providers from social identities to national eID infrastructure. Banks have been issuing credential (TUPAS in Finland, Bank ID in Sweden etc) to their customers for a long while now, and in most countries the chosen method is one-time password (OTP). Some banks use a device which will generate an OTP with a push of a button, or a paper based list, or SMS (text message) based. Then another strong identity category is the government issued eIDs that can also come in multiple formats including smart cards and mobile based PKI identities. These can be used to enrich other identities, and if needed, to implement step-up authentication when security and confidentiality is of outmost importance.

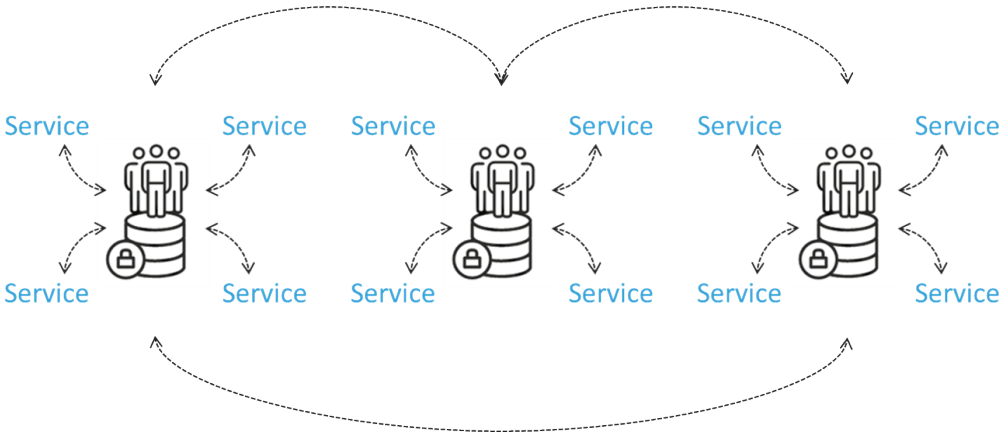


Benefits	Drawbacks
Social identity for registration	
Step-up authentication only when needed	

DIGITAL SERVICE 2.3 – ECOSYSTEMS

A natural step forward in the business ecosystem building is to enable your business partners and stakeholders to gain access to your service resources through identity federation. This means that once they have authenticated themselves in their own domain, they can quickly move to your domain without any extra logins. The necessary identity information is delivered as part of the process and for the end-user the transition is transparent. This convenience combined with the inclusion of social identities makes customer or partner on boarding extremely easy and convenient.

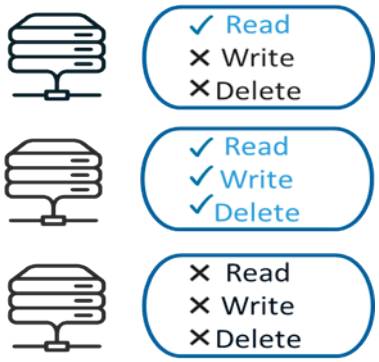
One of the easiest ways to build business oriented federation into your applications and services is to allow your business partners to use their existing IDs. Ubisecure Windows AP can provide SSO from a corporate Windows AD network to your services, or Ubisecure Identity Platform can be used to create single sign-on from Office365/Azure AD and Google Apps into your services. Joining your services when your customer is already using e.g. Azure AD can be done in minutes – this is business federation on steroids.



Benefits	Drawbacks
Identity integration across business domains	
Multiple domains linked with single sign-on	

DIGITAL SERVICE 3.0 – MANAGING THE IDENTITY

In the previous steps, we covered issues around authentication. The next step happens when identity information of the user can be better leveraged in the services. There can be a lot of information attached to a user identity that the service can utilize to offer better customer experience through personalization. Role and attributes delivered to the service can be used to improve security when the service can determine access level privileges on a more, fine grained level compared to the yes / no information based on authentication alone.

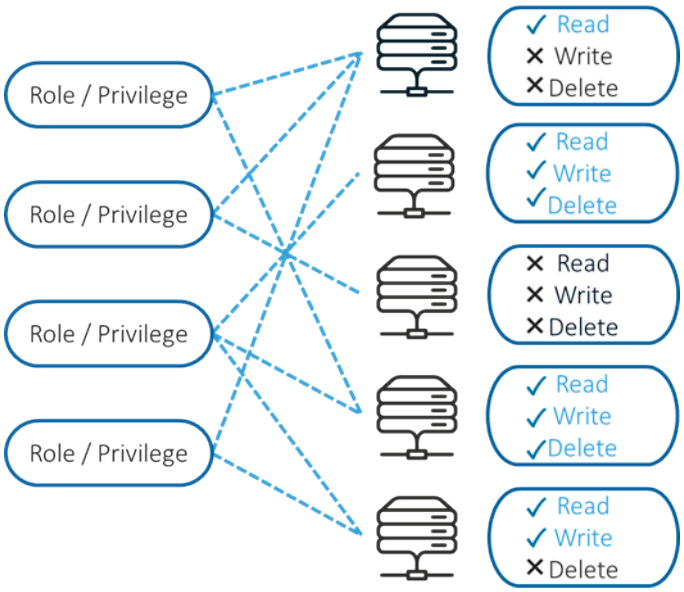


Each service might have a different structure how they model what the end-users can actually do within the site. Authentication provides the proof of identity, but it does not include any kind of information of what the user can or more importantly cannot do.

All web facing applications have database tables or similar methods of arranging information. When you create these tables, you also define how those tables can be modified, i.e. what the user can do the data stored in that table. This set of privileges will define how your application data is utilized.

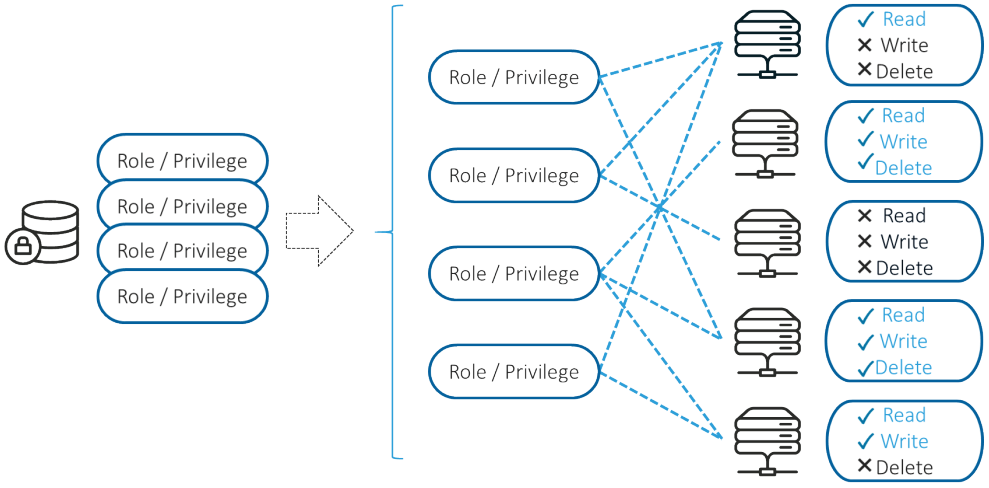
It is almost impossible to manage access privileges on a file or table-to-table level. Therefore, modern applications rely on roles to enable more intelligent management of user privileges. A role is typically application specific, as it is tied to the internal privileges of the application itself. Naturally there are quite a bit of generic roles such as “employee” or similar. But, these won’t cut it when we’re talking about application roles. Sure, they can be a part of the role set, but if application specifics need to be taken under consideration, each application might have their own unique role set.

People who manage access privileges won’t have to worry about the complexity shown, they just have a simple set of access roles that need to be assigned to the end-users. If you manage these roles application per application, you can manage quite easily with a small number of users, and a very limited set of applications. Once the number of either category grows, you’re faced with the management challenge.



Benefits	Drawbacks
Role based access control	Scaling issues
Access based authorization	Work done by e-service Admins
Finer access decision possible	Roles managed in applications

DIGITAL SERVICE 3.1 – EXTERNALIZE THE IDENTITY INFORMATION



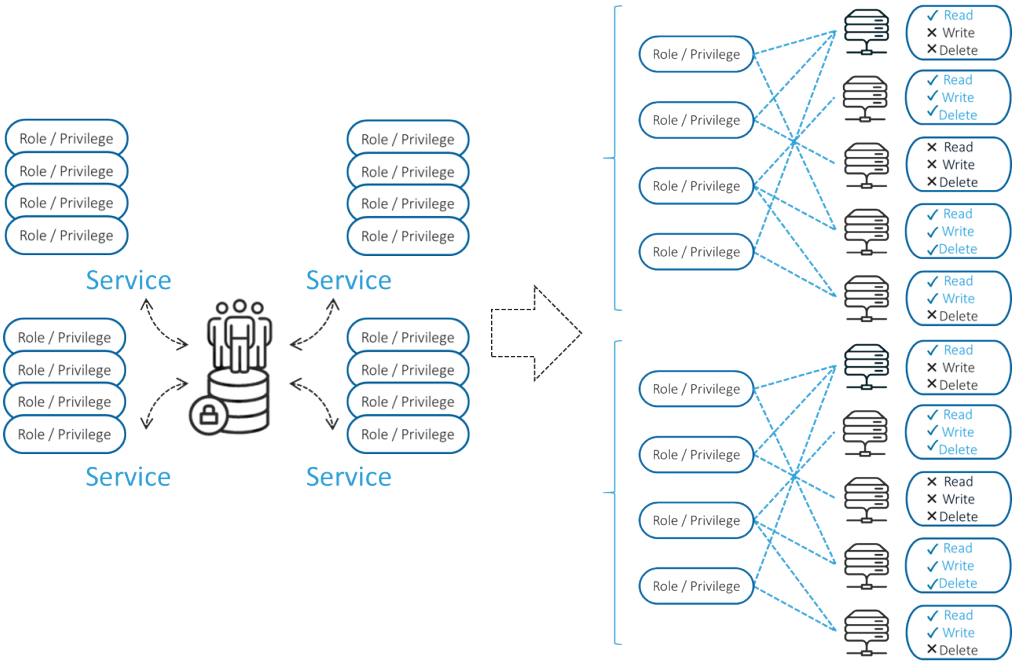
One step to alleviate the management challenge to a degree is to use an external or centralized system, which can deliver this role information to applications. This way, you don't have to build in the role management to each and every application you develop or deliver. All you need to do is to create the ability to utilize the role information coming from the centralized resource.

This is also typical for a federation use case, where identities travel from one identity domain to another. In federation however, there should be some kind of hub that has enough intelligence to translate the roles from one identity domain to roles understood in the other. This is what Ubisecure Identity Platform.

At this point, we are also talking about a central repository of identity information, not just role/privilege information. A load of identity attributes such as addresses, phone numbers, delivery addresses, loyalty information, etc. are stored for each user. Some of the information can come from external sources, such as the social security number, or from the back-end systems of the company running the solution. Naturally, this type of information can be present in the earlier stages of the Maturity Model, but we're trying to keep things simple and introduce the identity attribute management at this stage, where it's most obvious.

Benefits	Drawbacks
Role Based Access Control rules managed separately	Scaling issues
Ability to use external identity information from federation	Still managed by the e-service Admins on the service desk

DIGITAL SERVICE 3.2 – CENTRALIZED IDENTITY MANAGEMENT



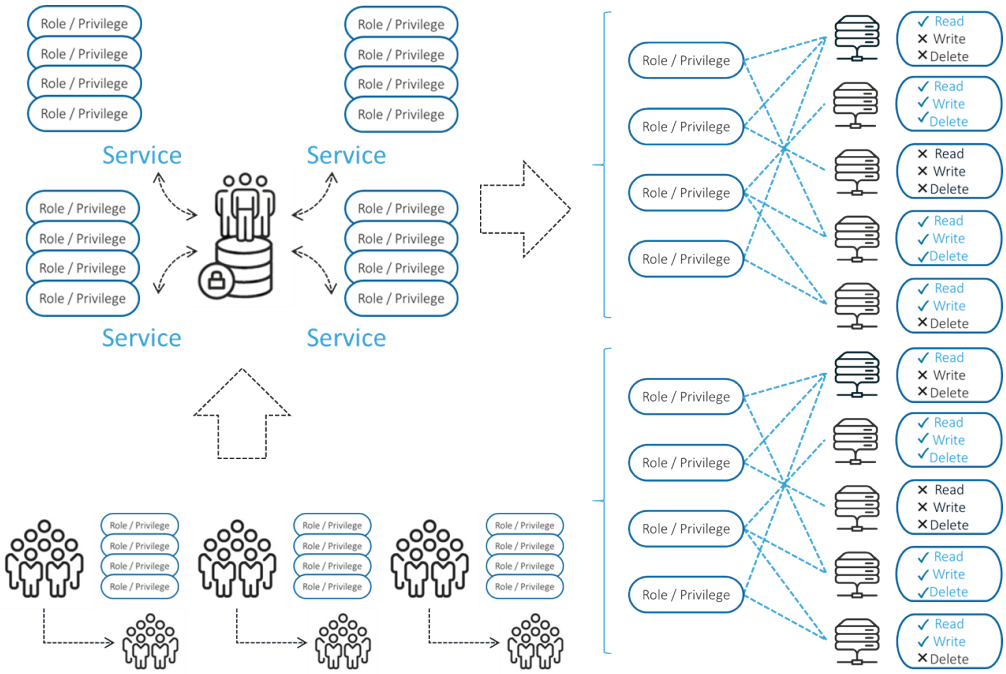
Transferring the role information to a centralized resource does not however take away the management burden if you are running several applications with hundreds or thousands of users. You are still trying to manage the identities and role information of all your incoming customers, partners, stakeholders, employees, etc. The complexity grows quickly with new applications, and especially the identity management of external identities might become something of a pain. This pain can be so severe that you might consider simplifying access roles so that the whole thing can be managed. Simplification can be one way to reduce the burden, but it might lead to compromises in terms of security and traceability.

When you externalize the roles out of the application or service you have the chance to create more business oriented roles. Some technology platforms, such as MS SharePoint have built in roles that are technical in nature. Now, you can create business roles that are translated to technical roles understood by SharePoint.

Benefits	Drawbacks
Supporting multiple services	Scaling issues
Business orientated roles	Still managed by the e-service Admins on the service desk

DIGITAL SERVICE 4.0 – TRUE CUSTOMER IDENTITY AND ACCESS MANAGEMENT

The biggest step in the Maturity Model from the identity management perspective happens when you enable your own customer and partners to manage their own identities, identity attributes, and assign roles to those identities. This will completely remove your management challenge, improve customer satisfaction, give better compliance (GDPR), improve loyalty and trust, reduce churn, and improve security among other things. The trick is to allow your customer organization to take control of the identities you have for them. Your customer can invite people into the site, activate new services through self-service functions, authorize their own employees properly, or even authorize people from other organizations to represent your organization in the service. This can be site specific or on a project- by-project basis. Your customers, partners and stakeholders will also maintain accurate information about their identity attributes by themselves.



Benefits	Drawbacks
Utilization of role / attribute information	
Business oriented roles	
Proper authorization of users	
Accurate identity information	
Close to zero management cost for the e-Service provider	

CONCLUSIONS

The Digitalization Maturity Model can give clues on where your services stand as of today, and where you could develop those services. Customer Identity and Access management can be used to cut cost and deliver new business-related services to your customers.

There is a path or common steps in all the digitalization projects that we are seeing. The services evolve through time, and will gain new functions and the usage of the services will grow. All of these changes also have an impact on the identities that are using them. Identities are assets to any business, and assets need to be taken care of. Identity Relationship and Access management solutions can be used to maximize the potential of user information in your services.

Improving your services and customer satisfaction is the key to your success. This paper showed one view on developing services by modelling the growth of the digital identity from a mere zero utility username to a valuable asset that can help your business grow.

DELIVERY MODELS

How you deploy your Customer Identity and Access Management solution is very important. Experience has shown us that it is best to start with a handful of applications/services and then extend the CIAM solution to cover more services, include additional authentication methods, new workflows, and back-end integrations. The easiest way to implement CIAM would be to sign up with an Identity as a Service (IDaaS), available also from Ubisecure. With IDaaS, you get a fixed set of functionalities, authentication methods and other features. If you need something out-of-scope of the IDaaS provider, you can opt for a managed cloud delivery model, or have the CIAM solution installed on-premise.

For private cloud and on-premise installations, Ubisecure can offer the quickest and risk-free delivery model with a pre-configured CIAM solution. With 10 years of experience in delivering CIAM solutions to various customers, we have created this best-practice deployment model, which can be up-and-running in weeks instead of months. After the initial deployment, the delivered CIAM solution is fully configurable, and can be extended and modified to accommodate new services, authentication and federation needs, RESTful API integrations, customized workflows, etc. With Ubisecure products, no coding is required, not even when integrating the online services to the CIAM solution thanks to our extensive support for industry protocols and off-the-shelf integration components.

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.

To learn more about Customer IAM and Company Identity solutions visit www.ubisecure.com or contact us at sales-team@ubisecure.com