KuppingerCole Report

WHITEPAPER

by Richard Hill | November 2019

Modern B2B Identity Management

With Business-to-Business (B2B) transformation comes digital initiatives to better connect B2B customer systems and supply chain services, and in doing so, Identity and Access Management (IAM) becomes a crucial consideration. IAM shares standard features that can be used in B2E or B2C use cases as well, but IAM in the B2B context has specific requirements that need to be addressed. B2B IAM services need to support customers, suppliers, and other partner organizations by providing capabilities such as support for multiple identity types, user delegation at different levels, strong authentication, self-service, and automation, to name a few. Ubisecure Identity Platform solution offers the right B2B capabilities to meet the challenge.

by **Richard Hill**
rh@kuppingercole.com
November 2019

Commissioned by Ubisecure

KuppingerCole Whitepaper
Modern B2B Identity Management
Report No.: **80135**

Table of Contents

List of Figures

Related KuppingerCole Research Documents

Executive View: Ubisecure Identity Platform – 79072

Leadership Compass: Access Management and Federation – 71147

Leadership Compass: Identity API Platforms – 79012

Leadership Compass: Adaptive Authentication – 71173

Leadership Compass: CIAM Platforms – 79059

1 Executive Summary

Identity and Access Management (IAM) solutions have continually evolved to meet the changing IT requirements. At first, IAM took root in business-to-employee (B2E) scenarios to address the business needs of an IT closed environment that ran within the walls of their perimeter. Identities were managed and stored on-premises and made available only to local access control systems to ensure individuals have access to resources they need through authentication & authorization, with the ability to audit user access.

As business needs extend beyond business-to-employee (B2E) to include business-to-business (B2B) and business-to-consumer (B2C), and more recently business-to-IoT (B2IoT) use cases, federation extended the reach of where identity and access controls reside. And Single sign-on (SSO) systems gave users the ability to authenticate not only across multiple IT systems but organizations too.

With the advent of cloud services (IaaS, PaaS, SaaS), organizations were given new options for their IT infrastructure, platforms, and software. Motivated by the business need to increase IT elasticity, flexibility, and scalability while reducing cost, businesses took to the cloud giving IT a new challenge to protect both identities and access to resources in a cloud environment.

IAM encompasses standard features that can be used in B2E or B2C use cases as well, but IAM in the B2B context has specific requirements that need to be addressed. B2B IAM services need to support customers, suppliers, and other partner organizations by providing capabilities such as support for multiple identity types, user delegation at different levels, strong authentication, self-service, and automation, to name a few.

Not all IAM solutions provide the capabilities needed to successfully meet all of the B2B requirements

Administrating user access within a single organization can be difficult enough without also trying to maintain customer or partner organization's user access as well. Managing access this way can often incur increased overhead costs and gaps in user access security. Through the use of automation and tiered delegated administration roles, this process can be improved by allowing the external organization to manage access to applications or other digital services they use at their partner organization.

Application Programming Interfaces (APIs) enable organizations to connect with partners and customers while providing a seamless experience by linking systems and services together. In order to accomplish this and to allow for better interoperability, common formats, protocols and standards should be used.

As an organization's infrastructure, platforms, software, and its data increasingly spans across the traditional enterprise boundaries into the cloud creating hybrid IT environment, so should IAM. Although cloud providers give varying levels of security and monitoring of users, the enterprise needs to have clear visibility on what users have access to and what they are doing with it, while applying consistent security controls regardless of whether it's in the cloud on or on-premise. The management of user identity, access, and its governance must evolve into a service that provides an "Identity Fabric" in order to provide all services in a standardized manner.

2 Highlights

- There are multiple types of identities that must be managed in a standardized way.
- B2B user onboarding processes can be complicated if manual, or simplified through automation.
- Maintaining B2B user lifecycles and can be difficult without the use of automation and allowing tiered delegation administration.
- APIs provide the ability to connect with partners and customers while providing a seamless experience by linking systems and services together.
- Successful B2B system integrations often requires the use of common formats, protocols and standards to maximize interoperability.
- Having the ability to delegate administrative tasks can improve process efficiency while reducing overhead costs.
- Support for common data formats, protocols and standards increases system integration flexibility and interoperability.
- Perform an architectural analysis of existing IAM infrastructure when considering a B2B IAM modernization project.

3 The Business-to-Business (B2B) Challenge

Identities are converging, IAM is converging. It is about enabling everyone to access every service in a controlled manner.

Changes in how businesses interact with their customers, suppliers, and other partner organizations are driving Digital Transformation at every level, including Identities. With the multitude of identity types in play across organizations and customers, having the ability to manage and control the access of every one to every service has become essential.

IAM must support all types of identities for the shared value and supply chains of today's businesses

3.1 Different Types of Identities

In order to succeed, the business will need to provide a robust digital identity backend that can deliver all the identity services required to support new digital services. The ability to support such digital services must also allow for the identity diversity necessary for the use of devices such as enterprise-issued mobile devices and IoT. To do this, an "Identity Fabric" is needed to provide all services in a standardized manner as well as ensuring integration with an organization's legacy IAM.

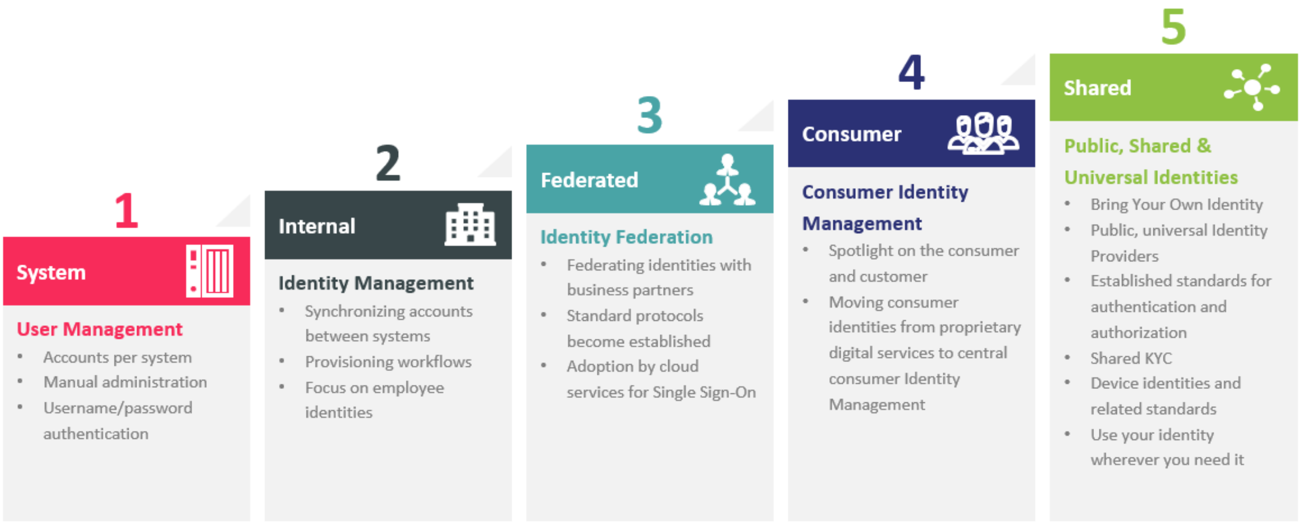
1
System
User Management
• Accounts per system
• Manual administration
• Username/password authentication
2
Internal
Identity Management
• Synchronizing accounts between systems
• Provisioning workflows
• Focus on employee identities
3
Federated
Identity Federation
• Federating identities with business partners
• Standard protocols become established
• Adoption by cloud services for Single Sign-On
4
Consumer
Consumer Identity Management
• Spotlight on the consumer and customer
• Moving consumer identities from proprietary digital services to central consumer Identity Management
5
Shared
Public, Shared & Universal Identities
• Bring Your Own Identity
• Public, universal Identity Providers
• Established standards for authentication and authorization
• Shared KYC
• Device identities and related standards
• Use your identity wherever you need it

Figure 1: Evolution of Identities

Digital identities associate information about a person or entity that can be used when interacting with digital services, systems or applications. This person or other entity may have one or more digital identities associated with them depending on their role or purpose at the time of use.

Such identities types can include:

- **Organization** – Identities by companies, enterprises, partners, or non-profit organizations as examples.
- **Customer** – person or partner organization that uses digital services from a business or other organizational type.
- **Government** – Government identities are used, for example, to access either government services or by entities that must comply with government agencies such as banks.
- **Application** – Some applications or services may require a user identifier to gain access to the applications or service that is not associated with any organization, but is used solely for the purpose applications or services use.
- **Machine** – Device, IoT or other types of machines that have their own identifiers such as a serial number.
- **Transactional** – A temporary identity that is created for the purpose completing a transaction.
- **Aggregated** – A collection of entity attributes that can be used identify the entity.

The management of identities, access, and its governance must evolve into a service that provides an "Identity Fabric" in order to provide all services in a standardized manner.

3.2 B2B User Onboarding

A B2B customer onboarding process involves multiple steps on both the part of the organization allowing access to their resources or services and another person or organization wishing to access them. Sometimes bilateral onboarding occurs when organization A onboards users at organization B while organization B onboards user from organization A in a business partnership relationship. At worst, this is a manual process on both ends requiring a lot of overhead and high user friction to onboard. At best, the onboarding process can be optimized through automation, reducing both overhead and user friction. But often, it's somewhere in between.

Typically, once agreements between organizations are in place, an organizational focal or representative is put in place on both sides to approval who has access to what resources or services. An individual in this role requires some level authority to make access decisions for their organization, which often requires delegation of approval powers from higher up in an organization. When these empowering individuals do not fully understand the user's access that is granted, recertified or doesn't have a clear insight into potential access violations, they can potentially approve access that is sometimes risky. Since this access approval process is usually conducted outside of the IAM system, it is therefore not captured and stored within an IAM system for later analysis. This lack of visibility to access approvals makes it less likely to be able to spot risky access or potential violations.

Once users at the partner organization have been identified and approved for access, the final steps involve creating and sending the user an invitation of some kind to access the other organization's resources or services. This invitation can be as manual as sending instructions on what steps need to be taken to register and gain access to the organization's user portal, or it can be as automated as sending an invitation email with a link that redirects the user to the user portal and completes the onboarding process.

3.3 B2B User Lifecycle

Organizations need well thought-out processes for Identity and Access Management that ensure that identities are managed correctly and all the challenges in particular of mover and leaver (JML) processes are handled correctly. This also requires periodic recertification processes to ensure that users still need access to resources or digital services and make entitlements base on any JML activity. This JML information is most often provided by Human Resource (HR) systems within the organization, such as a database or LDAP as examples.

An organization’s user lifecycle management can be expensive in the sense of the overhead needed to maintain systems and processes. Now imagine maintaining one or more partner organization's user lifecycles. This can often lead to user identity mapping, giving external partner business identities within the organization's HR system, and mapping that identity to the partner organization user. Without the use of automation and delegation at multiple tiers allowing partner organizations to maintain their own user, B2B user lifecycle management can be quite daunting, complex, and potentially put both sides of the partner organizations at risk for not changing user access when needed.

3.4 B2B System Integrations

Regardless of the organization size, B2B interactions often requires some kind of integration between business systems. This linking of systems and services together can include applications, the use of APIs, or integration platforms. To better support interoperability between systems and services, common formats, protocols, and standards should be used. New integration efforts gravitate to more modern protocols and standards looking to the future. But legacy systems should not be forgotten and must be supported until the modernization of systems is made on both sides of the B2B equation. Sometimes the impedance mismatch between systems can be overcome through integration platforms or federation types of hubs between partner organizations.

When considering a B2B system integration, organizations need to ask themselves:

- Which B2B systems are currently integrated and how well do those integrations work?
- Which business processes need to be put into place or improved?
- What data formats, protocols or standards promote the best interoperability?
- What legacy data formats, protocols or standards still need to be supported and is there a roadmap to modernize them?
- Are there platforms that can facilitate B2B integration security, reduces user friction, and lowers overhead costs?

3.5 B2B Supply Chain

An organization's supply chain depends on its network of people, organizations, resources, activities, and all the technologies required to make this interaction possible efficiently and securely. This also means providing the right access to the right individuals or organizations when they need access, such as in B2B or B2B2C scenarios.

Cyber attacks are proliferating throughout the world, and B2B supply chain services are not an exception. As organizations tighten security controls for their employees, cybercriminals find new attack surfaces through vulnerable third-party access to supply chain networks, as seen by the increase of third-party data breaches.

Organizations can mitigate these risks when engaging in B2B activities using a supply chain identity management approach, such as:

- Establishing trusted B2B relationships through trusted Organization Identity, using Legal Entity Identifiers to establish the authenticity of suppliers when possible.
- Managing supply chain users through multi-tier delegation of authorization rights, including authentication methods and identity proofing.
- Maintaining accurate user accounts that reflect the current needs for access rights.
- Building systems that scale to large numbers of sub-organizations or subtenants to isolate partner data pools and optimize delegation capabilities.

4 Core B2B Capabilities

Partner onboarding is easier than offboarding. Have a well-defined process at both the organization and the individual level to ensure that there are no unexpected risks.

IAM solutions should provide features and capabilities to meet use case requirements in which it's used. IAM in the B2B context has specific requirements that need to be addressed. B2B IAM services need to support customers, suppliers, and other partner organizations by providing capabilities such as support for multiple identity types, user delegation at different levels, strong authentication, self-service, and automation, to name a few.

4.1 Identity Management

Identity is at the core of any information security system and Identity and Access Management (IAM) gives the capabilities to manage these identities, and their access privileges, ensuring that they only have access to rights to resources for the right reasons. Traditional IT environment ran within the confined eco system of the organization and were developed to address the business needs of this closed environment.

Initial cloud IAM offerings included the same IAM capabilities as on-premise IAM while targeting new capabilities required to meet the use case of their time. Where traditional on-premise IAM sought to address the access control to the web-based application of the day, cloud IAM also needed to address the demands of more current access requirements such as mobile uses cases, providing programmatic APIs for integrations and automation, and adaptive or more contextual access controls. Single-Sign-On (SSO), once an add-on or separate on-premises offering, now comes frequently as a baseline cloud IAM capability.

Once an identity has been established, it can be used at authorization time to gain access to systems, applications and data. The Authenticator Assurance Level (AAL)[1] of a user credential should be used to ensure that the level of authentication is high enough given the potential risk or sensitivity of resource accessed by the user.

The use of federation extended the reach of where identity and access controls reside and allow for the secure exchange user information. This could be between divisions with organizations or between organizations in the same industry sector. This works in some B2B scenarios and allows organizations and their partners to access each other's services while minimizing administrative overhead and avoiding security issues such as the synchronization of identities and passwords.

[1] https://pages.nist.gov/800-63-3/sp800-63b.html

4.2 User Self-Service

In the context of B2B interactions, it is helpful to reduce costs and user friction by providing customers the tools that they need in an easy to use way. Typically, self-service is provided through an organization's user portal that offers some kind of dashboard and user account information. Customer roles such as an administrator for their organization, buyer, or approver of products or services also need to be supported by the portal system. When given access, and based on user roles, user self-service portals should provide the ability for business to be conducted. Business interactions can include such things as providing access to applications or other services or enabling users to make purchase orders, invoicing, or facilitated user onboarding and administration.

There are multiple models of self-service and delegation, specifically around partners. You must support them all in a flexible manner.

More advanced self-service capabilities can provide the ability to customize or configure the self-service workflow. Other functionality may include the ability to allow for delegated administration, support user registration through user identity verification, or linking accounts during the provisioning process.

4.3 User Management and Delegation

Having the ability to perform user management is a key capability of IAM. This can be accomplished through account management in which you can create, change, or disable user accounts, although difficult to do for federated identities when you do not have control over the identity source. Here, accounts are tied to a user's identity and associated with the group, permissions, etc. These accounts often tie user entitlements to resources and digital services to the user identity to allow access once properly authenticated.

The administration of user accounts is core to the maintenance of user access to the resources and digital service that they need to perform the jobs. Before a user account can be created, an approval from someone on the organization's management hierarchy such as a manager is required. Often, managers will need to delegate their approval powers to someone trusted in the organization, which allow the manager to maintain business continuity if they are unavailable or need to reduce their workload so they can perform other duties.

Having the ability to delegate the administration of user access becomes even more powerful when it can be applied to organizations in a B2B relationship. In this scenario, a person or group in each organization can manage access for their users, eliminating the need for one organization to manage all access to resources. Individuals with a delegated role must only have the ability to perform specific tasks and given the least privilege to perform those tasks.

4.4 APIs

Many different factors are driving Digital Transformation in the market today. One factor is the change in how businesses interact with their consumers requiring changes in the services they provided to their customers. Another factor is more on the technical side that addresses the implementation of new Digital Services that have become more complex due to the different environments and the many integration points to consider. This is driving the rapidly growing demand for exposing and consuming APIs. APIs are enabling organizations to create new business models, connect with partners and customers while providing a seamless experience by linking systems and services together.

These changes in which services expose and consume APIs are also enabling agile paradigms and DevOps by providing a well-defined set of APIs to security services instead of creating their own identity and security (and other) services in each and every application again and again.

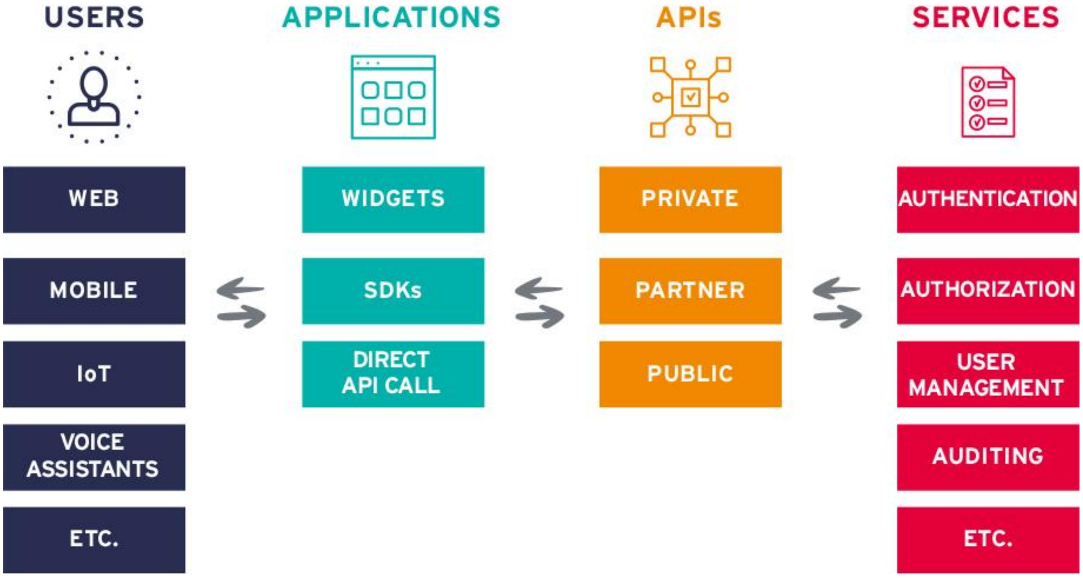

Figure 2: High level architectural overview of IAM API usage

The need for APIs is driven by the need to meet emerging IT requirements such as hybrid environments that span across on-premises, the cloud, even multi-cloud environments supporting the different functional requirements of B2E, B2B and B2C, as well as the ability to select these capabilities a la carte as needed. By exposing key functionality via APIs, it allows for workflow and orchestration capabilities across environments as well as better DevOps support through automation.

APIs are enabling organizations to create new business models, connect with partners and customers while providing a seamless experience by linking systems and services together

Identity platforms that provide APIs must expose the basic functionality of identity and user management, authentication, authorization, and support for auditing. Other capabilities available through APIs can be added based on the solutions target market use cases such as capabilities found in CIAM to support consumers like user consent management workflows, federation in IDaaS, or more intelligent authentication as seen with Adaptive Authentication as well as support for compliance and access governance offered by IGA solutions. Beyond these capabilities available through APIs, evolving requirements such as IoT, workflows and orchestration, DevOps, and API security functionality should also be taken into account.

5 The Ubisecure Approach to Solving B2B Challenges

In order to build a solid foundation in which B2B partners, suppliers, and customers can interact, identity as the basis of trust must first be established.

Ubisecure originates from Finland and has offices in the UK, Sweden, and Germany with strong regional support in the Nordic region. Their current offering, Ubisecure Identity Platform, provides IAM and CIAM functionality supporting B2E, B2B, and B2C use cases that can be deployed on customer-owned or managed infrastructure, both on-premises or cloud, as Identity Server or hosted by Ubisecure in dedicated private cloud instances as Identity Cloud. Ubisecure currently supports directly provisioned customers for both Identity Server and Identity Cloud models as well as a wide variety of industry verticals through their Partner Program.

5.1 Ubisecure Overview

In a B2B context, Ubisecure provides strong federation capabilities, innovative standards support, as well as flexibility through workflow automation and APIs. Ubisecure offers a unique ability to handle complex delegation scenarios in B2B2C relationships, sharply differentiating them from other solutions in the market place.

Ubisecure features strong federation capabilities, innovative standards support, and the ability to leverage some bank and national IDs.

Ubisecure's relationships with banks and governments, as well as their ability to directly leverage existing strongly-vetted identity credentials from Nordic banks and national governments makes it easier for customers in those areas to quickly integrate with the Ubisecure Identity Platform solution.

5.2 Ubisecure Capabilities

Ubisecure Identity Server allows for the storage of identities within Redis, LDAP, and SQL clusters. For high utilization deployments, the Redis database can be used to store SSO session information to improve transaction speed and scalability. Logging and reporting capabilities are also available within their storage architecture. Their Identity Broker allows for the aggregation of identity attributes from multiple sources as well as providing federation, multifactor, access, and authorization (via roles and policies), consent, and trust relationship management capabilities.

The platform can handle organizational identity as a primary identity class, and when coupled with Ubisecure's Legal Entity Identifier solution, branded as RapidLEI, enables management of highly assured organizational identity and an Individuals' right to represent said organization. LEI[2] is backed by the G20 giving both momentum and the potential of global adoption.

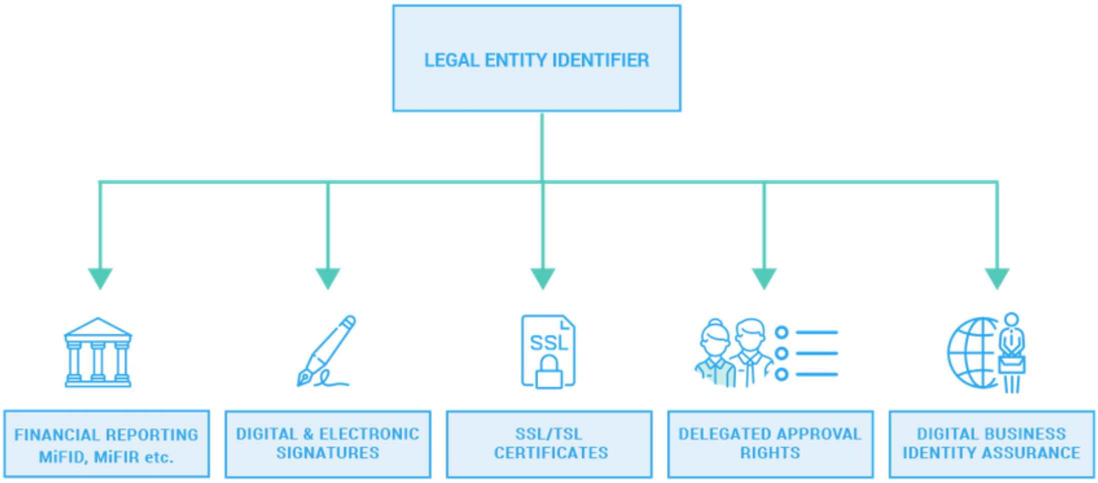
LEGAL ENTITY IDENTIFIER
SSL
FINANCIAL REPORTING MiFID, MiFIR etc.
DIGITAL & ELECTRONIC SIGNATURES
SSL/TSL CERTIFICATES
DELEGATED APPROVAL RIGHTS
DIGITAL BUSINESS IDENTITY ASSURANCE

Figure 3: LEI (Source Ubisecure)

To help with reducing the overhead cost and security risks, Ubisecure supports user self-service through configurable workflows that facilitates the sending of invitations to users as well as the user registration process and role requests. Workflow automation is also possible by sending back-end requests to other systems. During the registration process, verification of a user's identity is also possible through the use of external IdPs. Self-service password management including password verification and recovery is given out-of-box. Support for self-service email and phone number verification at registration time, as well as the ability to manage the authentication methods used is also provided.

There are a number of different authentication methods that Ubisecure customers can use, as well as step-up authentication capabilities when needed. Authentication methods includes:

- ETSI MSS
- GSMA Mobile Connect
- Meontrust MePIN smartphone biometrics authenticator app.
- NemID
- OTP TAN
- Passwords
- SMS OTP
- Social logins from Facebook, Google+, LinkedIn, Twitter, VKontakte, Yahoo, Amazon, Microsoft, and GitHub
- FTN (TUPAS)
- X.509

[2] https://www.gleif.org/en/about-lei/gleif-management-of-the-global-lei-system

Ubisecure is a member of Kantara Initiative, and an early supporter of their Consent Receipt specification, which provides a standard format for collecting and storing individual consent actions to facilitate compliance with GDPR. Ubisecure also supports a large number of identity protocols and standards, including:

- SAML 2.0
- OpenID
- OAuth 2.0
- OpenID Connect
- Mobile Connect
- WS-Federation
- FTN / TUPAS
- ETSI MSS (ETSI TS 102 204)

Ubisecure APIs not only support the most common authentication standards, but they also support some not so common standards such as Certification Authentication Protocol (Cert AP) and the Swedish BankID (OIDC CIBA). Also, application SSO integration APIs are provided as a base functionality for Ubisecure SSO. REST APIs give the ability to use identity management functionality within a customer's own application as well as for bulk provisioning. APIs are also available for the linking of user accounts during provisioning using an external integration tool. In addition, Ubisecure Identity Server allows the harvesting of user data via REST APIs and via log extraction, for example using LogStash, for transformation into business intelligence (BI).

The Ubisecure Delegated ID gives both individuals and organizational users the ability to delegate their right to use a digital service on their behalf. Delegated ID's supports complex combinations of delegated rights and roles between different permutations of individuals and/or organizations allowing for multi-tier delegation of authority, or e-power of attorney, to manage access and authority given to third-party service providers. This allows organizations to delegate access and authorization rights, invite new users, and control onward-delegation rights.

The power of delegated role management has been demonstrated in multiple case studies. In one case study, the Finnish government used Ubisecure's Delegated ID with their nationwide platform called Katso. The Katso platform allows citizens to go online and create an ID as a representative of an organization to manage different types of authorizations, organizational data, and Sub-IDs. This allows representatives of organizations in the Katso system to log into over 100 government applications. Katso supports over 400,000 organizations and user IDs. In another case study, a large company in the energy sector used Delegated ID to allow their B2B customers to delegate access and authority within their accounts.

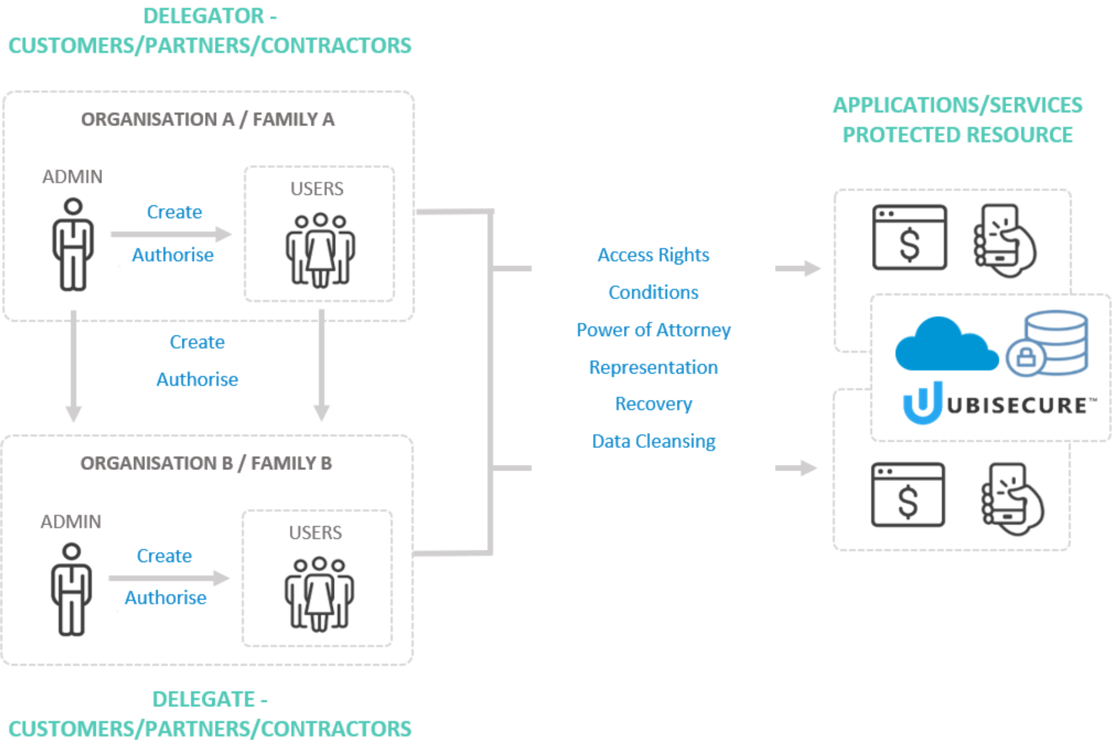
DELEGATOR - CUSTOMERS/PARTNERS/CONTRACTORS
ORGANISATION A / FAMILY A
ADMIN
Create
Authorise
USERS
Create
Authorise
ORGANISATION B / FAMILY B
ADMIN
Create
Authorise
USERS
DELEGATE - CUSTOMERS/PARTNERS/CONTRACTORS
Access Rights
Conditions
Power of Attorney
Representation
Recovery
Data Cleansing
APPLICATIONS/SERVICES PROTECTED RESOURCE
UBISECURE

Figure 4: Delegated ID (Source Ubisecure)

Ubisecure takes the ability to delegate even further by combining both Delegated ID and LEI to provide a new offering called *Right to Represent*. By using the LEI as verified organization attributes and the Delegated ID, identities of individuals can be connected to organizations. Ubisecure's Right to Represent reduces the risk of working with fraudulent organizations when provisioning new services, onboarding customers or performing high risk transactions as well giving the ability to automate workflows such as verification and KYC processes.

6 Summary and Recommendations

Traditional IAM is no longer enough for fulfilling the demands of the business-to-business scenarios of today. Shift the focus from using IAM for just protecting the business to an IAM that also supports the needs of your customers, suppliers, and other partner organizations too.

IAM is a core component of cybersecurity. With the rapidly changing business requirements and mandated government regulation, flexibility, and rapid delivery of IAM capabilities to meet these challenges will be essential for secure business collaboration to succeed.

Below are some concrete recommendations for consideration on how to proceed with IAM upgrades or new implementations on your roadmap.

6.1 Recommendations for architectural analysis

- Inventory existing IAM infrastructure and document architectural gaps.
- Consider how a modernization strategy will impact existing legacy IAM.
- Consider what the integration points will be needed for services on-premises and the cloud.
- Inventory externally facing APIs and their security and document deficiencies.

6.2 Recommendations for B2B IAM modernization

- Consider the advantages and disadvantages of IDaaS solutions.
- Plan for identity diversity that supports the digital services and the use of devices such as enterprise-issued mobile devices, and IoT.
- Evaluate Identity Platforms that will also facilitate privacy management services.
- Consider the use of analytic and intelligence tools to assist in lowering your access and compliance risks.
- Select an appropriate solution that will support all of your requirements and address your challenges, then create a roadmap fulfill what is still missing.
- Engage neutral, third-party expertise to perform IAM and cybersecurity assessments, requirements analysis and roadmap strategy.

7 Copyright

All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole ANALYSTS

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Deutschland

Telefon +49 (211) 23 70 77 - 0
Fax+49 (211) 23 70 77 - 11
www.kuppingercole.com