KuppingerCole Report

EXECUTIVE VIEW

by John Tolbert | April 2019

Ubisecure Identity Platform

Ubisecure Identity Platform is an integrated consumer identity and access management suite for on-premise or cloud deployment. Ubisecure features strong federation capabilities, innovative standards support, and the ability to leverage some bank and national IDs. RapidLEI provides a way to manage organizational identity.

by **John Tolbert**
jt@kuppingercole.com
April 2019

Content

Related Research

Executive View: Ubisecure Identity Server - 70838

Leadership Compass: Access Management and Federation - 71102

Leadership Compass: CIAM Platforms - 79059

1 Introduction

Consumer Identity and Access Management (CIAM) is the fastest growing specialty in Identity and Access Management (IAM) that has emerged in the last few years to meet evolving business requirements. Many businesses and public-sector organizations are finding that they must provide better digital experiences for and gather more information about the consumers who are using their services. Enterprises want to collect, store, and analyze data on consumers to create additional sales opportunities and increase brand loyalty.

To reduce money laundering, cyber-crime, terrorist financing, and fraud, regulators are requiring banks and financial service providers to put into place mechanisms for “Knowing Your Customer”. Having IAM systems dedicated to hosting consumer identities and their associated profiles is a good first step toward KYC.

CIAM systems can aid in other types of regulatory compliance. Now that the General Data Protection Reguation (GDPR) is in effect in the EU, collecting clear and unambiguous consent from consumers for the use of their data is often mandatory. Many CIAM solutions provide this capability, plus offer consumers dashboards to manage their information sharing choices. Moreover, CIAM systems can help corporate customers implement consistent privacy policies and provide the means to notify users when terms change and then collect acknowledgement.

The Revised Payment Service Directive (PSD2) in the EU will require banks, financial institutions, and other payment service providers to offer strong customer authentication (SCA) and perform user behavioral analysis to authenticate and authorize monetary transactions. Sophisticated CIAM solutions can provide these necessary functions. Additionally, the improved customer experience possibilities that CIAM offers will facilitate brand loyalty and give a competitive advantage to those financial companies that deploy it.

Common features of Consumer Identity solutions include:

- Self-registration for customers, usually via social network registration
- Consent mechanisms for users to control the use of their data
- Single Sign-On (SSO) across all digital properties
- Multiple authentications options for customers, depending on risks and policies
- Customer profile storage
- SaaS application integration
- Fine-grained access control to resources and data

Ubisecure is based in Finland and has offices in the UK, Sweden and Germany. They released their first CIAM product in 2006 with a focus on SSO and privacy. Their current offering, Ubisecure Identity Platform, is an API based offering incorporating CIAM functionality 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. It provides robust federation options, advanced mobile authentication using the GSMA Mobile Connect standard, and can integrate with several national e-IDs. 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.

2 Product Description

Ubisecure currently supports directly provisioned customers for both Identity Sever and Identity Cloud models as well as a wide variety of industry verticals through their Partner Program. Ubisecure plans to refine deployment model options in 2020, including microservices, containers, and virtual images. Ubisecure Identity Server leverages external PostgreSQL database servers for user information. For high utilization deployments, a Redis database can be used to store SSO session information to improve transaction speed and scalability; this model is in already in use for systems with millions of users.

Ubisecure customers can authenticate with a number of different mechanisms, including:

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

A CIBA based Authentication Adapter microservice exists within the platform for quick addition of other standards-based authentication methods and Identity Providers.

Ubisecure was an early adopter of GSMA's Mobile Connect. Mobile Connect is a mobile phone-based strong authentication solution available today in 32 countries, including Denmark, Finland, France, Italy, Norway, Spain, and Switzerland. Mobile Connect users register their phones with their service provider's Mobile Connect service. A binding is created between the user's identity and the phone, enabling the "something you have" portion of passwordless authentication. After registration, when a user navigates to a site that accepts Mobile Connect, they only need to swipe the Mobile Connect button. For stronger authentication, users can register a PIN on their device. The PIN validation is local to the device; it is not transmitted over the air. Financial apps can require the use of this PIN for access, thereby achieving Strong Customer Authentication, as defined by EU PSD2. If users give consent, apps can obtain additional attributes, such as full name, street address, city, state, country, postal code, phone number(s), email address, DOB, and national ID. GSMA Mobile Connect is up to version 1.1, and Ubisecure supports the latest iteration of the standard.

Ubisecure Identity Platform in both on-premise and cloud configurations supports using national IDs, such as from Estonia, Denmark, and Finland, and is well-positioned for eIDAS implementations. The product can also authenticate users with their bank IDs, for example, in the Nordic countries, and utilize basic information from national and bank IDs to perform attribute queries against other identity repositories to obtain additional and/or more current information about the subject users.

Ubisecure supports OpenID Connect's Client-Initiated Backchannel Authentication (CIBA) specification, which allows Relying Parties (RPs) to request authentication by OpenID Providers (Ops) of end-users via their devices, providing the end-user consents. A common example given is a call-center employee requesting authentication of the current caller.

Ubisecure supports a large number of identity protocols and standards, including OAuth, OIDC, SAML, WS-Federation. It supports LDAP and REST for bulk provisioning. 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.

GDPR compliance is a major concern for any company doing business both in the EU; or with EU citizens. Ubisecure provides consent management mechanisms to enable their customers to better comply with GDPR. For example, Ubisecure Identity Platform facilitates the development of consumer consent dashboards. Ubisecure are participating in the development of the Kantara Consent Receipt standard which will be implemented within Identity Server and Identity Cloud when the standard becomes formalized. The Consent Receipt will support the right to export data, and data deletion upon request. The Identity Broker Engine, found within the Identity Platform, can also anonymize sensitive data attributes, such as Date of Birth, into a simple "Yes/No" answers to questions such as "Is subject over the age of 18?".

Ubisecure supports 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. This service is in place throughout the Nordics and in use within the Finnish Tax Authority. Family management can be achieved in Ubisecure Identity Platform by modeling parent/guardian to child relations as a service contract.

Ubisecure's RapidLEI solution can provide assignment and maintenance of Legal Entity Identifiers (LEIs). LEI, an ISO standard[1], is a global identifier for companies, specified by the EU eIDAS regulation, and endorsed by the G20. LEI is a relatively new standard to aid in compliance for Anti-Money Laundering (AML) and Know Your Customer (KYC) initiatives.   An LEI is a 20-digit alphanumeric code. Individuals can be entrusted to represent organizations under the LEI framework. Typically, country registrars have been issuing them, but private sector organizations can do so if accredited by governments. Ubisecure was accredited to issue LEIs in June 2018, launch a same-session LEI issuance API in February 2019 and has quickly become a large issuer of LEIs. Ubisecure's RapidLEI is independent of their Identity Platform currently but will be joined together with the Identity Platform stack to deliver a new "Right to Represent" (RtX) proposition incorporating components of CIAM, delegation of authority and Identity Provider federation later in 2019.

[1] https://www.iso.org/standard/59771.html

CIAM solutions today often utilize cyber threat and compromised credential intelligence to reduce misuse of accounts and fraud. Ubisecure currently only looks at a small number of risk factors. The Ubisecure solution can also be connected to a 3rd party system that returns authorization decisions or backend-provided attributes; and access control decisions in Ubisecure SSO can be tied to such internal or external information. Ubisecure is actively working with cyber intelligence providers to integrate such capabilities. In this way, external cyber threat or compromised credential intelligence feeds may also be utilized and integrated. However, it does not yet have the ability to utilize external cyber threat or compromised credential intelligence feeds. Building these risk-adaptive authentication capabilities is on their 2019 roadmap.

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). Ubisecure has limited built-in reporting capabilities for identity and marketing analytics, but they do ship with capabilities for Pentaho Data Integration. Ubisecure is working with other BI vendors and system integrators to deliver identity and marketing analytics information to customers.

Ubisecure allows for whitelabeling of the solution and allows self-registration and self-service. Customer access is managed and modeled as a CRM customer contract. The solution can integrate with SaaS applications, such as Office 365, Salesforce, and Google Suite, as well as Amazon AWS and Microsoft Azure platforms. Ubisecure also supports integration to several other SaaS services and applications, such as Aditro, Atlassian Confluence, Atlassian Jira, SAP Successfactors, etc.

IoT device information can be linked to consumer identities via an app management API or through command line interface tools.

3 Strengths and Challenges

The company has strong regional support in the Nordics, and is expanding to other areas within the EU, as well as in some countries in North and South America. They have a growing partner and system integrator ecosystem. Capgemini, CGI and Tieto are among their leading partners.

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.

Ubisecure’s alignment with Mobile Connect is an important feature. Mobile Connect will become an increasingly popular identification and authentication method, and organizations operating in those areas should consider Mobile Connect integration as a near-term option. Moreover, GSMA Mobile Connect will assist customers in meeting EU PSD2 Strong Customer Authentication requirements.

The extensive federation options that Ubisecure Identity Server has, including OAuth, OIDC, OIDC CIBA, SAML, and WS-Federation, facilitate customer connections with popular IaaS and SaaS applications, as well as subsidiaries and business partners.

Though it does not have built-in identity and marketing analytics, it does allow the data it produces to be mined by BI and SIEM type applications. Ubisecure is branching out to offer its solutions in the cloud, but it is mainly deployed on-premises today.

Strengths

- Comprehensive identity federation support
- Mobile Connect 1.1 and OIDC CIBA authentication
- Support for selected bank IDs
- National ID support in Nordic region
- Good consent management features, including Kantara Consent Receipt
- RapidLEI for h**igh assurance** organizational identity management
- Growing partner and integrator network
- Unique connection between Legal Entity Identifiers and Individuals managed via CIAM

Challenges

- No built-in identity and marketing analytics
- Mostly Nordic regional customer base
- Risk-based, adaptive authentication needed
- Admin UI should be feature-enhanced and redesigned
- Limited IoT support

4 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.

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
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com