KuppingerCole Report
EXECUTIVE VIEW

By John Tolbert | March 23, 2020

iWelcome IDaaS and CIAM

iWelcome provides a mature Identity-as-a-Service platform with extensive support for B2C (Customer Identity & Access Management – CIAM) and B2B use cases with interfaces for end-users as well as app developers. As an EU-based company, iWelcome strives to fulfill regional requirements such as interoperability with various national IDs and GDPR compliance, and as such provides unparalleled consent management features. Although iWelcome provides a horizontal solution, it has a strong customer base in regulated industries.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

Consumer Identity and Access Management (CIAM) is now a well-established specialty in Identity and Access Management (IAM). 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". CIAM solutions are an enabler for KYC and AML.

CIAM systems can aid in other types of regulatory compliance. When GDPR took effect in 2018, collecting clear and unambiguous consent from consumers for the use of their data became mandatory. CIAM solutions have expanded their capabilities to offer consumers dashboards to manage their information sharing choices. Moreover, CIAM systems 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 requires banks, financial institutions, and other payment service providers to offer strong customer authentication (SCA) and perform User Behavioral Analysis (UBA) to authenticate and authorize monetary transactions. PSD2 also involves collecting consent from the account holders and/or consumer on data exchange between the different parties defined under PSD2. 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 CIAM solutions include:

- User self-registration capabilities, including interoperability with social network credentials, and national digital ID systems, eIDAS, and Bank IDs
- Consent capture and management mechanisms for consumers to select which types of information they want to share and with whom.
- Capabilities for interoperating with other applications, such as CRM and marketing systems. Interoperability is best achieved via the use of well-documented APIs and webhooks
- Management of consumer users, including associated directory services and profile databases, supporting high-scalability requirements, often in the millions of users,

events, and logins. Many vendors have moved or are moving to micro-services architectures to achieve optimum scalability

- Support for Single Sign-On, allowing seamless connections with business partners and cloud services using industry standard protocols such as OAuth, Open ID Connect, and SAML
- Authentication services, including support multiple forms of MFA and risk-adaptive authentication; especially mobile authentication features, such as the provision of SDKs for customer app development and support for FIDO.

iWelcome is a leading CIAM solution provider, headquartered in the Netherlands. The company is focused on helping clients building frictionless B2C and B2B customer journeys for omni-channel on-boarding and authentication while complying with strict privacy regulations like EU GDPR. With its roots in enterprise identity and security, iWelcome has a strong customer base in regulated industries, like finance, insurance and utilities. Their offerings are developer friendly, cloud-based, scalable solutions hosted in 14 data centers across the EU, with two additional data centers in the USA and two more in the APAC region.

2 Product Description

iWelcome is offered as a micro-services-based SaaS, with the ability to store complex consumer profiles. iWelcome has a flexible data model (non-relational) which includes, per attribute, a host of metadata for consent details based on the US NISTIR 8112 standard with multiple processing purposes, classification and KYC, data retention, and identity vetting. As an example of their scalability, iWelcome has a sizable customer base in the insurance, finance, media, retail, transportation and logistics, manufacturing, government and professional services industries, with up to tens of millions of consumer identities per customer. The company mission is to offer customers a complete IDaaS for consumers and business users solution with fine-grained consent management and audit response capabilities, supporting frictionless customer journeys at scale. iWelcome aims to be the single source of truth for consumer data for their customers.

The iWelcome suite comprises Customer Journey Management, Mobile, Consent & Preference Management, eID, and RITM (Relationship, Identities, Things, and Mandates) for B2B and B2B2C relationship and delegation of authority management. Its platform is API-first with a flexible configuration engine.

iWelcome allows for white labeling and seamless branding. Tenants can easily build portals for consumer self-registration. Users may register and authenticate via social networks such as Facebook, Twitter, Google, or LinkedIn. iWelcome supports OAuth, Open ID Connect, and SAML enabling connections with almost any ID provider. iWelcome allows for registration and authentication via the eID module, which supports BankID's, eIDAS, eHerkenning (they report that more than 70% of eHerkenning authentications are handled by iWelcome), France Connect, and iDIN.

iWelcome provides passwordless authentication. For mobile authentication, iWelcome accepts SMS and email OTP, and offers their Mobile Authenticator, which is an Android/iOS app available through online app stores. The Mobile Authenticator is an Out-of-Band (OOB) authenticator and/or transaction verifier. Users can swipe for authentication or to authorize a transaction, such as a high-value financial transaction. iWelcome supports the OpenID Connect SDKs for both Android and iOS, which can be found on GitHub. The Mobile Authenticator can also be incorporated into consumer identity workflows. Developers can take advantage of the open API to send secure messages and support transaction signing.

For security, the Mobile Authenticator uses TLS with Forward Security (to protect against MITM attack), open source white-box cryptography in the App for key protection, and the Double Ratchet Algorithm / Axolotl for push message protection. Customers can use the SDK to brand the Mobile Authenticator for consistency.

Identities can be synchronized between iWelcome and other identity systems, even in cases where an OOTB integration does not yet exist. iWelcome supports LDAP and SCIM for bulk provisioning, Just-In-Time provisioning, and synchronization. iWelcome provides integration to Microsoft Active Directory (AD) and Azure AD.

CIAM solutions today often utilize cyber threat and compromised credential intelligence to reduce misuse of accounts and fraud. The iWelcome platform is extensible and the risk engine processes geo-location, IP address, and other information accordance with client-defined policies. For example, if the score returned by the risk engine is deemed too low, the risk engine can request step-up authentication mechanisms via SMS/email OTP or the Mobile Authenticator.

iWelcome has strong capabilities in the areas of identity and marketing analytics. iWelcome can track key user activities per-tenant including registrations, logins, failed logins, etc. in its static dashboard as well as via tag-manager integration. Customers can also use Native MongoDB connectors for Spotfire, Cognos, Microstrategy, or SAP Business Objects to develop additional reporting capabilities. Customized reports covering user population analyses, including geo-location, frequency of login, social network attributes, authentication method, inactive users, new users created in the last year/month/week/day, demographic information, languages, interests, sex, and age can be generated. Administrators can build queries to aggregate information based on any combination of attributes available. In order to preserve anonymity in reports, iWelcome can abstract and obscure underlying attribute details when required.

iWelcome is designed to be both user-, administrator-, and developer friendly. All common functionality is available without the need for customization, only configuration. However, iWelcome can be extended with functionality that is available to a subset of customers using feature toggling, depending on the market in which they operate or specific geographic regions. For example, if tenants decide to implement new threat intelligence feeds for evaluation by the risk engine, or add new authenticators, such features can be added to the standard product and made available to relevant customers. iWelcome provides full documentation to support custom integration with the iWelcome platform by partners and customers.

GDPR compliance is a major concern for any company doing business within the EU or with EU citizens. iWelcome provides fine-grained attribute consent management mechanisms to enable their tenants to comply with GDPR and to ICO guidelines. iWelcome's Consent & Preference Management module can also be integrated with existing IAM, CRM, or consumer profile management systems in-house. For example, iWelcome provides consumer profile and privacy dashboards. It also stores proof of consent with the consumer profile. iWelcome supports the right to export data, data deletion upon request, and data age/retention policies. iWelcome has multiple data centers within Europe for localizing user data in the most compliant way.

iWelcome instantiates opt-in-based consent flows. The interface provides transparency for the user about the attributes retrieved with consent and the associated processing purposes. It also offers full traceability of which attributes are gathered, when they have been gathered, including the reason that the tenant asks for consent. This is visible to both the user on their personal dashboard, as well as for the organization, in accordance with the GDPR requirement. The solution gives users the ability to change the consent parameters and the ability to withdraw the consent, via the self-service pages. Historical login, back-tracing attribute gathering, and consent actions can also be viewed as a timeline in the user's personal information page. As another example of iWelcome's leading-edge consent management features, they support Kantara Initiative's User Managed Access (UMA) specification. iWelcome was an initial sponsor for Kantara's Consent Receipt working group as well.

True family management is supported by their CIAM service. The family management features are implemented as a delegated administration model. The iWelcome user interface allows parents and guardians to establish family relationships with their children or dependents for the purpose of access control and consent for the use of underage consumer attributes.

iWelcome can store users' device information, such as wearable IoT, SmartHome products, and IoT entertainment devices, with their consumer profiles. Users can add, remove, and manage their associated devices through their dashboard. Devices which use certificate-based identities or federation tokens are the most straightforward to integrate. iWelcome supports the IETF OAuth2 Device Flow specification, which has become a de facto standard for associating IoT device identities with consumer identities.

iWelcome's RITM module is focused on B2* relationship management. It allows for complex relationships to be modeled, and supports not only B2B users, but any delegated user manager, delegation of authority, power user roles, and C2C mandating. For example, delegated user managers enroll and control other business users, while power users can nominate the delegated user managers and publish/revoke applications, or consumers can mandate caretakers. RITM enables the creation of custom attributes, metadata, actions, and workflows that better meet the needs of the increasing varieties of roles in business environments today, including non-technical personas. RITM can also be used to centralize and orchestrate identities between other IDPs and SaaS apps.

Within the solution, iWelcome IDaaS uses the Amazon version of ELK stack (Elasticsearch, Logstash, Kibana) for security intelligence. It also supports integration with external SIEM systems via secure syslog forwarding. iWelcome encrypts all customer data at rest and in transit, and also provides the option (additional fee) to also support data field encryption for PII information and log data encryption if required by the customer (not mandatory for GDPR).

iWelcome is moving to AWS PaaS and is built for high availability. As part of its AWS PaaS strategy, iWelcome utilizes native Amazon components like DocumentDB and MariaDB for storage. This SaaS offering is fully multi-tenant. Their typical SLA guarantees 99.9% uptime but usually reaches 99.99% with failover configured between multi-data center deployments.

3 Strengths and Challenges

As a Netherlands headquartered company, iWelcome's IDaaS and CIAM offering is strong in supporting the regional needs of European companies, especially with GDPR. Their service is hosted in data centers that are located in the EU and support full data localization by design. It provides very granular consent and privacy management functions. iWelcome provides a good selection of authentication mechanisms. Their support for eIDAS, national IDs, and Bank IDs makes it easy for their EU customer organizations to integrate with large IDPs.

iWelcome is constantly innovating and delivering new features at customer request. iWelcome has been a longtime sponsor of industry standards and is a member of Kantara. They were an early adopter of Kantara's UMA and will also implement Kantara's Consent Receipt specification.

iWelcome's new RITM module is the next logical evolution of their product. Whereas they have had excellent B2B IDaaS and B2C CIAM solutions for years, RITM addresses the changing needs of the business marketplace by providing comprehensive and customizable relationship management which includes coverage for B2B2C and C2C use cases.

iWelcome supports users all over the world, has not branched out from Europe. It has a fast-growing customer and partner support base, including KPMG, PwC Capgemini, and local identity specialists in almost every European country. iWelcome's AWS native strategy makes this more attractive for customers with an AWS strategy and provides a basis for a global roll-out. Additional authentication methods would make this already strong service even stronger.

Strengths

- Very flexible data model with metadata for every attribute
- Excellent granular consent model for GDPR support
- Strong support for federation standards and social logins
- Interoperability with BankID, eIDAS, FranceConnect, iDIN, and others
- OAuth2 Device Flow for IoT identity linking
- Highly extensible via developer friendly APIs and mobile SDKs

Challenges

- Small but growing partner ecosystem
- Sales and marketing centered on EU, no global reach yet
- Limited built-in identity and marketing analytics
- Entry level pricing is not attractive for start-ups

4 Related Research

Executive View: iWelcome IDaaS and CIAM - 70298
Leadership Compass: CIAM Platforms - 79059
Leadership Compass: Identity API Platforms - 79012
Leadership Compass: Identity as a Service: Cloud-based Provisioning, Access Governance and Federation (IDaaS B2E) - 70319

Copyright

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

KuppingerCole Analysts, 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.