KuppingerCole Report

EXECUTIVE VIEW

by John Tolbert | September 2017

iWelcome IDaaS and CIAM

IWelcome provides a complete solution for both Identity-as-a-Service and Consumer Identity and Access Management. As an EU-based company, iWelcome strives to help their customers with GDPR compliance, and as such as provides unparalleled consent management features.

by **John Tolbert**
jt@kuppingercole.com
September 2017

Content

Related Research

Executive View: iWelcome Identity & Access Management as a Service - 71205

Leadership Compass: CIAM Platforms - 70305

Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141

Leadership Compass: Identity as a Service: Cloud-based Provisioning, Access Governance and Federation (IDaaS B2E) - 70319

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. When GDPR takes effect in the EU in 2018, collecting clear and unambiguous consent from consumers for the use of their data will become mandatory. CIAM solutions are expanding their capabilities to 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. PSD2 also needs consent from the account holders and/or consumer on data exchange between the different parties defined in 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 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

iWelcome is a leading CIAM solution provider, headquartered in the Netherlands. The company is strongly focused on delivering IDaaS and CIAM solutions to help clients building frictionless customer journeys while complying with EU GDPR. Their offerings are 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 in its built-in MongoDB data store. iWelcome is built upon its CIAM designed flexible data model (non-relational) which includes, per attribute, a host of metadata for consent details, classification, data retention, and identity vetting. As an example of their scalability, iWelcome has dozens of customers in the insurance, finance, media, retail, transportation and logistics, manufacturing, and professional services industries. iWelcome hosts tens of millions of consumer identities. The company mission is to offer customers a complete, feature-rich IDaaS and CIAM solution with fine-grained consent management and audit response capabilities, supporting frictionless customer journeys at scale.

iWelcome allows for whitelabeling 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. Users may also register through custom SAML or any OpenID provider. In addition to the standard list of social logins, iWelcome supports username/password and SMS OTP authentication, and federation over SAML, Shibboleth, WS-Federation, and OAuth. As a competitive differentiator in certain markets, iWelcome accepts XING, BankID, PostNL, and iDIN credentials.

For mobile authentication, iWelcome provides Android and iOS Mobile Apps, which are available through online app stores. The Mobile App is an Out-of-Band (OOB) authenticator and/or transaction verifier. Users can push or 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 App can also be incorporated into consumer identity workflows. Developers can take advantage of the open API to create a facility to send messages to administrators or other users including notification requests.

For mobile app security, the Mobile App 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.

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. By supporting SAML, OAuth, OpenID Connect, and Kerberos, iWelcome can interoperate with IAM and SSO systems such as Oracle, Novell, IBM, Microsoft, ForgeRock, and others.

CIAM solutions today often utilize cyber threat and compromised credential intelligence to reduce misuse of accounts and fraud. The iWelcome risk engine processes geo-location and IP address information, and can trigger step-up events in 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 such as SMS/email OTP, mobile authentication, or others.

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. For advanced identity and marketing analytics, in-tenant instances of Tableau and Qlikview applications can access iWelcome's MongoDB data stores. 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. Customers can also use Native MongoDB connectors for Spotfire, Cognos, Microstrategy, or SAP Business Objects to develop additional reporting capabilities.

iWelcome is designed to be both user- and administrator-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.

GDPR compliance is a major concern for any company doing business either within the EU or with EU citizens. iWelcome provides fine-grained consent management mechanisms to enable their tenants to comply with GDPR, as understood today. iWelcome's built-in consent management functionality can also be integrated with existing IAM, CRM, or profile management systems in-house, offering Consent Lifecycle Management functionality while supporting IT eco systems already in place. 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. 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. 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 is quickly becoming the de facto standard for associating IoT device identities with consumer identities.

Within the solution, iWelcome IDaaS uses the 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 built for high availability. Their typical SLA guarantees 99.9% uptime, but can reach 99.99% with failover configured between multi-data center deployments.

3 Strengths and Challenges

As an EU-based company, iWelcome's service offering is strong in supporting GDPR. Their data centers are located in the EU and support full data localization by design. It provides very granular consent and privacy management functions. During registration using social network credentials, users can select which attributes they want to share with iWelcome clients. Also, at any point after registration, users may edit their choices. Moreover, if iWelcome client's privacy terms change, the users are notified and may decide on permissible uses of their PII. The solution also supports de-registration and deletion of data. iWelcome also supports family management. Users may define relationships and parents can govern children's' activities.

iWelcome is constantly innovating and delivering new features at customer request. In addition to registration-as-a-service, the company plans on offering an XACML-based authorization service for tenants on their near-term roadmap. iWelcome will also implement Kantara's Consent Receipt specification.

iWelcome has not branched out from Europe very much at present, but will likely expand in the months and years ahead. It has a small but fast-growing customer and support base. Additional authentication methods and built-in marketing analytics tools would make this already strong service even stronger.

Strengths	Challenges
• Very granular consent model • Strong support for GDPR compliance • Strong support for federation standards and social logins • Integration with local identification services such as BankID, iDIN • Very flexible data model with metadata at attribute level • OAuth2 Device Flow for IoT identity linking • Family Management • Support for Kantara UMA specification	• Small but growing partner ecosystem • Heavily centered on EU, no global reach yet • Limited identity and marketing analytics • Additional strong authentication mechanisms would be helpful

4 Copyright

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**

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

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