KuppingerCole Report

EXECUTIVE VIEW

by John Tolbert | January 2022

OneWelcome Customer Identity and B2B identity

OneWelcome is the combined brand after the merger of iWelcome and Onegini, two leading Identity as a Service providers that are based in the Netherlands. OneWelcome offers a full-featured IDaaS for B2C use cases and B2B relationship management. As a European headquartered identity service provider, OneWelcome is uniquely attuned to the business and regulatory compliance requirements of GDPR. OneWelcome has extensive privacy and consent management features and data residency compliance.

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

Content

Introduction

Consumer Identity and Access Management (CIAM) continues to grow as a segment within the overall IAM space. The reasons for CIAM growth are multi-faceted: digital transformation is picking up speed, consumer expectations for sophistication and ease-of-use in their digital experiences are rising, and regulations requiring more secure processing and handling of consumer data are coming into force in more jurisdictions globally.

The digital transformation is well underway, with almost every kind of business finding it necessary to offer better experiences not only to acquire new customers, but also to retain their current consumer bases. The global pandemic has accelerated the digital transformation even in industries that had been lagging technically, such as retail, health care, insurance, etc.

The solutions within the market are evolving rapidly in response to customer demands, new and changing regulations, and advent of new technologies. Consumer demand and satisfaction are evidenced by increased business. Pleasant and secure user journeys lead to repeat site visits and higher revenue. Unpleasant or insecure user interactions will drive consumers to competitors. Consumer and/or customer identity management is pivotal in this scenario. Getting CIAM right can mean the difference between profit and loss, and between expansion vs. closing down.

CIAM is a field characterized by innovation. New authenticators, risk analytics, fraud detection intelligence, device identity integration, API accessibility, and privacy management are key areas in which CIAM solutions are showing new developments.

Everyone knows – consumers included – that passwords are insecure authenticators. Consumers prefer authentication mechanisms that do not require creating, memorizing, or maintaining more passwords. Much ecommerce is transacted via smartphones, and even typing in passwords on smartphones is frustrating. Smartphone-based biometrics have long been embraced by consumers, and most CIAM solutions interoperate with mobile authenticators.

Risk-adaptive authentication solutions are more commonly found within CIAM systems today, allowing the evaluation of multiple risk factors and providing higher levels of authentication assurance. Risk-adaptive authentication is a pre-cursor for continuous authentication, which can reduce the need for explicit authentication events from customers while improving the customer experience.

Fraud rates are increasing as fraudsters rapidly evolve new techniques. Cybercriminals attack not only financial institutions, but also ecommerce, insurance, travel/hospitality, and most every industry. Fraud Reduction Intelligence Platforms (FRIP) offer the means to integrate with many CIAM solutions so as to help their customers detect fraud attempts at both registration time as well as transaction time.

SmartHome, wearable, and other IoT device types are proliferating. Almost all such devices have identities of their own that need to be associated with consumer or customer users. CIAM solutions are expanding their capabilities to serve the more complex needs of managing device identities in conjunction with user identities.

CIAM systems are not islands unto themselves, and as such API connectivity is a must. Some CIAM specialists have concentrated on making their solutions developer-centric, providing robust APIs that

allow integration with related tools and services, such as Customer Data Platforms (CDP), Customer Relationship Management (CRM), and FRIP services.

The EU General Data Protection Regulation (GDPR) has been in effect for four years, and most solution providers have adapted their products to accommodate the technical requirements for gathering and managing consumer and customer consent. However, differences between products in this space can be significant, with some providing more intuitive administrative interfaces and consumer self-service portals. Moreover, other regions of the world have been enacting privacy regulations, which increases complexity for both CIAM vendors and their customers.

Product Description

OneWelcome is the union of iWelcome and Onegini, two CIAM, B2B IAM, and authentication service specialist companies headquartered in the Netherlands. Both companies were founded in 2011 and merged in 2021. iWelcome was known for its deep relationship and consent management, GDPR compliance features, and focus on API interoperability; and Onegini was known for its advanced risk-adaptive authentication services, multi-factor authenticator support, and mobile SDK. Their combined offerings are full-service Identity as-a-Service solutions uniquely positioned to meet the needs of the European market. OneWelcome has a large and growing customer base with many customers in regulated industries like insurance, finance and government. As a horizontal solution, OneWelcome also serves customers across media, retail, transportation and logistics, manufacturing and professional services industries, with up to tens of millions of consumer identities per customer.

OneWelcome's service offerings are composed of the IDaaS Core plus four applications:

- **IDaaS Core** contains the directory, APIs, identity federation capabilities and Single Sign-On
- **Customer Journey** allows the definition of the user life cycle, including identity verification actions and general onboarding
- **Delegation & Relations** enables management of relations between entities
- **Consent Management** for supporting GDPR privacy requirements
- **Mobile** offers MFA options, a pre-built app and SDK

Customer Identity is their CIAM service, and B2B Identity handles IDaaS for complex business relationships. OneWelcome's services are hosted in the public cloud in EU data centers. Their deployments are ISO 27001 and SOC 2 Type 2 certified. Licensing is per active or registered user per month/quarter/year.

OneWelcome allows seamless branding for customers through white-labeling of registration and login pages. Consumers can register using social network credentials from Facebook, Google, LinkedIn, and Twitter. Apple ID support is planned. Any OIDC conformant identity provider can be incorporated. Customers who are migrating from another CIAM or IDaaS solution will find multiple mechanisms for quicily creating accounts; for example, OneWelcomecan bulk import user information using SCIM. Customers can integrate their Microsoft Active Directory (AD) and Azure AD with OneWelcome services. OneWelcome supports a broad range of eIDs, including EU's eIDAS; Netherlands' DigiD, DigitaalPaspoort, and eHerkenning; Belgium's Itsme and BelgianID; FranceConnect; Nordic BankIDs and the Finnish Trust Network (FTN). Netherlands' iDIN attribute service can also be invoked from OneWelcome. The solution is extensible, and other eID schemes can be supported as needed. OneWelcome's support for OAuth2, OIDC, and SAML enable Single Sign-On to and from other IdPs and relying party applications.

Fraud is a major concern that both operators of consumer-facing businesses and B2B partners face today. Identity proofing, the process of verifying that credentials are issued to the proper entities, is a recommended preventive measure that can boost identity assurance levels and reduce account opening or synthetic fraud. Identity proofing is required for certain industries and jurisdictions, such as for AML and KYC compliance, and is a desirable option in other use cases such as in the retail and hospitality sectors. To that end, OneWelcome interoperates with identity proofing service providers GBG, ID R&D, iProov, Onfido, ReadID, and Signicat. Customers can choose to add identity proofing steps engaging these providers via the User Journey Orchestration module. Moreover, OneWelcome can work with customers to add other identity proofing services if needed.

OneWelcome accepts username/password, email/SMS OTP, Google and Microsoft Authenticators for browser-based authentication. OneWelcome has integrations for MessageBird and Twilio, and other SMS providers can be connected via API. OneWelcome provides a mobile authenticator for Out-of-Band (OOB) authentication and/or transaction verification. Upon receiving push notifications, users can simply swipe for authentication or to authorize a transaction or be required to scan their fingerprints or enter a PIN in order to authorize events that need higher assurance, such as a high-value financial transaction. QR code reading can be used for registration and in lieu of asking for username/password for logins. FIDO authentication is supported, but none of the components are certified. Android and iOS biometric authentication are supported as well.

For cases where customers want to add OneWelcome authentication and integration into their own apps, OneWelcome has an SDK that works with Android, iOS, Appian, Cordova, Flutter, Mendix, OutSystems, and React Native. Customer developers can create API-level integrations for custom authenticators and use the open API to send secure messages and enable transaction signing. OneWelcome's mobile SDKs utilize the standard security features within the underlying OSes, such as the Trusted Execution Environment (TEE) in Android, to prevent rogue applications from observing or tampering with consumer transactions. The SDK can detect if a consumer's phone has been rooted, jailbroken, or is in debug mode.

OneWelcome aids implementation of risk adaptative authentication schemes. The risk engine processes geo-location, IP address, and other data points 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 from users via SMS/email OTP or the mobile authenticator. External fraud risk intelligence sources can be queried and considered within OneWelcome, although API connectivity must be configured.

Consumer and B2B customer devices have identities that must be associated with user identities. If users agree, OneWelcome can store consumers' device information, such as wearables, 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. OneWelcome supports the IETF OAuth2 Device Flow specification, which has become a de facto standard for associating IoT device identities with consumer identities.

OneWelcome's Delegation & Relations module is focused on the fast expanding area of business-to-business and B2B2C relationship management. It allows for complex relationships to be modeled for power-of-attorney, business customers, or business ecosystem. It supports not only B2B users, but any delegated user manager, delegation of authority, and power user roles. 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. Customers can design portals that allow their CISOs and DPMs to monitor access by 3rd-parties. Delegation & Relations can generate organization and access structures automatically or these can be maintained by (delegated) admins. It enables the creation of custom attributes, metadata, actions, request approval routings, and workflows that better meet the needs of the increasing varieties of roles in business environments today, especially for non-technical personas. Delegation & Relations can be used to centralize and orchestrate identities between other IDPs and SaaS apps. Delegation & Relations allows customers to define time-limited accounts, roles, and permissions.

In addition to the previously mentioned SDKs and low-code development environments, OneWelcome provides a well-documented set of APIs for their IDaaS Core, Delegation & Relations module, Mobile Identity, and Consent Management modules. API security is achievable via integration with Apigee, Mulesoft (Salesforce), and nginx. Any service that supports API endpoint authentication over OAuth could also be configured.

OneWelcome has good capabilities in the areas of identity and marketing analytics. OneWelcome can track key user activities per-tenant including registrations, logins, failed logins, etc. in its 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, 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, OneWelcome can abstract and obscure underlying attribute details when required.

Customers can integrate their OneWelcome instances with various 3rd-party marketing analytics services to obtain additional insights. For example, OneWelcome has connectors for Adobe Experience Cloud and Tag Manager, Google Analytics, Marketo, Tableau, and Thallium.

OneWelcome provides fine-grained attribute consent management mechanisms to enable their clients to comply with GDPR. OneWelcome's Consent Management module, like the Delegation & Relationship and Mobile modules, can also be integrated with existing IAM, CRM, or consumer profile management systems. For example, OneWelcome provides consumer self-service portals and dashboards. OneWelcome Customer Identity also stores proof of consent within the customer profile. OneWelcome supports the right to export data, data deletion upon request, and data age/retention policies. OneWelcome has multiple data centers within Europe for localizing user data in the most compliant way.

OneWelcome has a flexible, non-relational data model which includes, on a per-attribute basis, 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. OneWelcome 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. Support for Kantara Initiative's Consent Receipt specification is planned.

Family management is supported under OneWelcome Customer Identity. The family management features are implemented as a delegated administration model. The OneWelcome user interface allows parents and guardians to establish family relationships with their children or dependents for the purpose of controlling minor access and to collect consent for or disallow the use of underage consumers' attributes.

OneWelcome uses the ELK stack for processing security intelligence and allows customers to export security event information and send to customers' SIEMs over syslog. All customer and consumer data is encrypted both at rest and in-transit.

Strengths and Challenges

The merger of iWelcome and Onegini has resulted in an IDaaS solution that is greater than the sum of its parts. iWelcome brought a well-designed set of interfaces, for both customer administrators (B2B delegation) and consumers, and a well-documented set of APIs that cover all the platform's major functions. iWelcome also brought top-notch consent and privacy management features for GDPR compliance. Onegini's contributions include MFA support, a highly flexible mobile SDK, and support for multiple development environments to facilitate integration into customer environments. Together, OneWelcome's combined CIAM, B2B, and B2B2C services have the security, scalability, and extensibility needed to meet the requirements of enterprises, mid-sized businesses, non-profit organizations, and government agencies.

Identity proofing is an important method for reducing fraud and is required for AML and KYC compliance in the financial industry. OneWelcome has built-in integrations with many EU eIDs, attribute providers, and identity proofing service providers. Having additional connectors to Fraud Reduction Intelligence Platforms would be advantageous for customers. OneWelcome supports a good number of authenticator types and provides risk-adaptive techniques to deliver higher authentication assurance when dictated by regulations and customer security policies. Their mobile SDK makes it easy to integrate with customer applications. The ability to collect additional device intelligence data points would make the solution even more robust.

OneWelcome's innovative approach to customer identity and relationship management allows their customers to build more efficient supply chains, facilitates management of temporary workers, and provides a framework for managing customer and consumer identities across complex business models in industries where dealers, resellers, channel distributors, licensees, and tenant arrangements must be made. OneWelcome's services enable their clients to address advanced use cases with ease.

OneWelcome has been in the forefront of GDPR compliance. Their Consent Management module provides all the features needed to help their customers deliver pleasant user journeys while enabling adherence to GDPR. Support for Kantara Initiative Consent Receipt is planned. Any EU-based organization that is looking for comprehensive customer and B2B relationship management should further investigate OneWelcome's solutions.

Strengths

- Excellent consent lifecycle management features promote GDPR compliance
- Support for many EU eIDs and attribute providers
- Integrations with multiple identity proofing service providers
- Intuitive customer admin and consumer interfaces
- Mobile SDK provides the flexibility to work well in multiple types of development environments
- Sophisticated relationship management enables customers to tailor working relationships and supply chain interactions as needed
- Good built-in identity and marketing analytics which can be extended with 3rd-party services
- Complete and well-documented APIs for all major functions

Challenges

- Connectors for Fraud Reduction Intelligence Platforms should be present
- Mobile SDK should collect more device intelligence for risk analytics
- FIDO is supported but the platform is not certified
- Small but growing partner ecosystem
- Sales and marketing centered on EU, no global reach yet

Related Research

Leadership Compass - CIAM Platforms
Executive View - iWelcome IDaaS and CIAM
Executive View - Onegini Connect

Copyright

KuppingerCole Analysts support 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, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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