kuppingercole ANALYSTS

Executive View Thales OneWelcome Identity Platform

John Tolbert

July 12, 2023

EXECUTIVE VIEW

This KuppingerCole Whitepaper looks at the Consumer Identity and Access Market and the key capabilities of vendors in this space. A technical review of the Thales OneWelcome Identity Platform is included.

Content

Figures

Introduction

Identity and Access Management (IAM) has been an integral part of IT security and computing in general for decades. The earliest IAM solutions were often built directly into applications, which created difficulties for organizations to manage. Dedicated, independent IAM systems began to emerge in the 1990s, generally constructed upon common user databases (based on the Lightweight Directory Access Protocol, or LDAP). This enabled organizations to simplify user account creation and maintenance.

These traditional IAM systems were designed to provision, authenticate, authorize, and store information about employee users. User accounts are defined; users are assigned to groups; users receive role or attribute information from an authoritative source, commonly at the employee or contractor onboarding phase. Traditional workforce-facing IAM systems are generally deployed in an inward-facing way to serve a single enterprise.

Starting in the early to mid 2000s, many enterprises found it necessary to also store information about their business partners, suppliers, and customers in their own enterprise IAM systems, as collaborative development and e-commerce needs dictated. Many organizations have built extensive identity federations to allow users from other domains to get authenticated and authorized to external resources.

By the late 2000s and early 2010s, consumer-facing enterprises began deploying separate instances of their IAM systems to house user accounts specifically for those consumer end-users. The types of information that can be obtained from and used in servicing consumer users can be quite different in nature and storage type requirements than those of enterprise workforce users. For example, organizations may want to collect information about other digital accounts a given consumer has, their demographic information, likes and preferences for consumer products, browsing and purchase histories, etc., as well as consumer generated content such as photos and videos.

The processes by which consumer and customer identities are created and maintained also differ significantly in many cases from those used for employee onboarding. Employees usually have digital accounts created for them soon after hiring in the onboarding process. Employees will be assigned to groups from which flow access entitlements. Human Resource (HR) departments validate employee identity documents and populate the user directory with relatively high assurance identity data.

Consumers and customers instead arrive at business web properties and must register for better, more personalized service. Guest checkouts which did not require registration were common in the early days of e-commerce, but as e-commerce grew, companies realized that digital identity has many benefits to offer. For the consumer or customer, registration allows personalization, including features such as retaining history of purchases to make repeat buying easier, and provides messaging options for interacting with brands of their choice. Most customers create accounts with email addresses (and passwords) or use social network login credentials. CIAM platforms have moved to accommodate many different privacy regulations globally, by offering consumer or customer users the facility to view, grant, and revoke consent for the use of their personal information.

For businesses, CIAM solutions are the means by which they can improve customer experiences through personalization. CIAM systems are also repositories of consumer identity, and browsing and purchasing information, which are valuable for organizations that are looking to maximize marketing potentials and revenue.

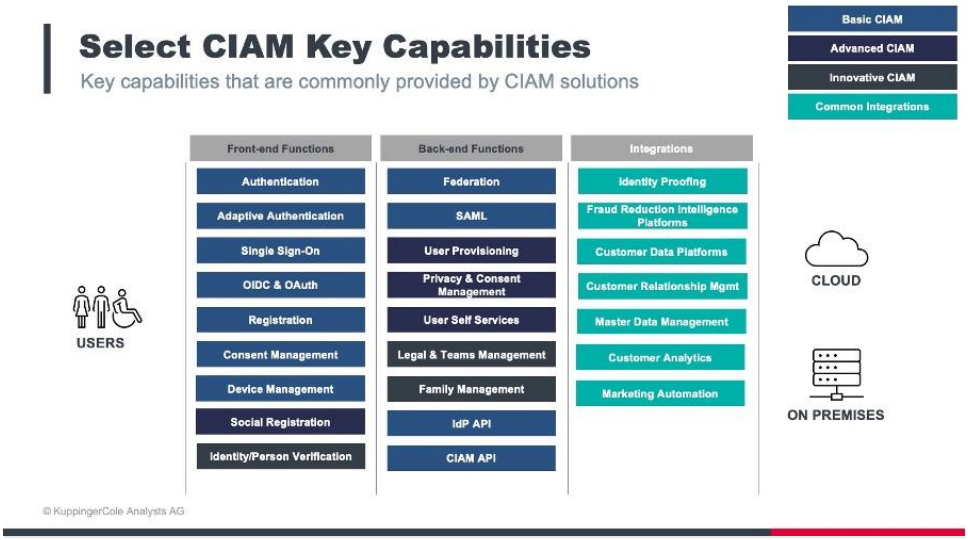

Figure 1: Selection of key capabilities for CIAM solutions

CIAM solutions allow users to associate devices and other digital identities with primary accounts, authenticate, authorize, collect, and store information about consumers from across many domains. Information collected about consumers can be used for many different purposes, such as authorization to resources or for transaction, or for analysis to support marketing campaigns, or Know Your Customer (KYC) and Anti-Money Laundering (AML) regulatory compliance. Moreover, CIAM systems must be able to manage many millions to even billions of identities, and process potentially tens of billions of logins and other transactions per day. SaaS delivery of CIAM services is the norm and will remain so.

CIAM systems can aid in other types of regulatory compliance. Many governments around the world have enacted privacy regulations that empower citizens and residents to control what kinds of information organizations can collect, how it can be obtained, how it must be treated, and how it must be dispositioned upon consumer request. Many CIAM solutions provide these capabilities, plus offer consumers dashboards to manage their information sharing and management 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.

Improving the consumer experience is often a key goal in deploying or upgrading CIAM solutions. With the increasing digitization of Business-to-Consumer (B2C) interactions, consumers are asked to create and use more and more accounts and passwords. Managing the escalating numbers of digital accounts can be burdensome for consumers if the CIAM systems with which they are engaging are not optimally designed, implemented, and continuously tuned.

Product Description

OneWelcome launched as a new brand in 2021 after iWelcome and Onegini (both founded in 2011) joined together. They are headquartered in the Netherlands. OneWelcome specializes in CIAM and B2B IAM. OneWelcome acquired Scaled Access, a dynamic authorization product, in early 2022. Thales Group then acquired OneWelcome in October 2022. Organizational integration was completed in March 2023. All Thales IAM products, including SafeNet Trusted Access, have been rebranded under the product family name “OneWelcome”. The scope of this Executive View is the CIAM offering, OneWelcome Identity Platform.

The Thales OneWelcome Identity Platform provides foundational IAM capabilities enhanced with Identity Apps to fulfill the needs of specific scenarios for different user groups like Workforce, Consumers, Business or Gig-workers for different verticals like Banking, Insurance, Manufacturing and more. The OneWelcome Identity Platform is composed of the following modules: the Identity and Access Core, User Journey Orchestration, Delegated User Management, Externalized Authorization, Consent and Preference Management, Mobile Identity and Identity Broker. The solution is a multi-tenant SaaS hosted in two public IaaS providers, leveraging multiple data centers for high availability and scalability. OneWelcome Identity Platform runs in IaaS data centers in several countries across Europe as well as in the Americas and APAC and offers in-country data residency. The roadmap for the platform will be around 3 main topics: 1. Orchestration of the customer journey, 2. Authorization in addition to identity and access and 3. Sovereignty for the user, the organization and the geo-political area.

Migrating customers and consumers from prior CIAMs is facilitated via LDAP and SCIM. Customers may also register using their email addresses, social network credentials, or any OAuth/OIDC compliant Identity Provider (IdP). Registration workflows are easily customized in the User Journey Orchestration interface. Features that may be selected in the User Journey Orchestration include targeted brands, languages, SMS and email confirmation options, password policies, attribute lookup requirements (including definition of API connectivity to external sources), trusted IdPs and wallets, document consent, account linking, device association, duplicate account checks, account recovery options, and cross-provisioning to CRM. All registration, login, and user portal pages can be white-labeled by customers for seamless branding for B2C as well as B2B scenarios. The User Journey Orchestration module helps customers build user-friendly journeys employing the progressive profiling concept, in which consumer information is collected on an as-needed basis, with consent, and in a way that does not impede providing service to the user.

For authentication, OneWelcome Identity Platform accepts username/password, email/phone/SMS OTP, mobile push notifications, mobile app, Android and iOS biometrics, and FIDO U2F and 2.0 authenticators. Thales also provides a secure SDK for customers to

develop and integrate their authentication capabilities to their platform. In terms of security features, the SDK can detect application tampering, phone jailbreak and rooting; it can also collect device information for risk decisions and require step-up authentication. Risk scores and associated actions can be set by customers. The risk engine and weighting of individual risk factors in policies are configurable by the Thales delivery team; a customer-exposed GUI will soon be released.

OneWelcome Identity Platform interoperates with many external ID proofing, attribute services, and biometric services including BankID, Experian, FranceConnect, GBG, IDIN, ID.me, IDNow, iProov, MitID, OnFido, ReadID, Signicat, Speed, Verimi, WebID, and Yes. The solution recognizes and works with all eIDAS compliant identities. Adding identity proofing functions to the registration workflow can help customers comply with Know Your Customer (KYC) regulations. The ability to interoperate with many IdPs including national eIDs and BankIDs permits OneWelcome to act as an identity broker for their tenants.

Thales has a strong reputation in the financial sector, particularly in the areas of banking and payment services (BPS). Thales offers a range of essential functionalities such as Identity Verification, Strong Customer Authentication, and Fraud Detection. These functionalities are included in the OneWelcome Identity Suite and will be rebranded as such, will be offered as add-on fraud detection and prevention services. To further enhance its functionality, OneWelcome supports APIs, such as REST, Webhooks, Websockets, and WebAuthn API types, allowing customers to extend their connections to third-party Fraud Reduction Intelligence Platforms (FRIPs).

The OneWelcome Consent and Preference Management module was designed to help customers meet the rigorous requirements of the EU General Data Protection Regulation (GDPR). Stiff penalties can be imposed by member states for non-compliance with GDPR. GDPR put the notion of consent collection, profile editing, and “the right to be forgotten” front and center for all businesses that may collect information on EU citizens and residents. Consent collection (as one of the six legal bases under GDPR for processing personal information) and enforcement is required across all communication channels, including web, mobile devices, keyboard-less devices like Smart TV, tablets, email, and phone interactions. Thus, CIAM systems are, in many cases, the primary consent collection, profile editing, and compliance mechanisms. In Thales’s solution, self-service portals are provided, which allow users to granularly select which attributes they want to share from social network operators; to opt-in or out of data collection processes; to edit or delete their accounts and profiles; and to submit Data Subject Access Requests. OneWelcome’s CPM has well thought out data schema with per-attribute metadata. OneWelcome CPM is addressable via API directly from customer applications, such that their front-end applications can collect consent and pass it for record-keeping by the platform. OneWelcome Identity Platform supports the Kantara Consent Receipt format.

In addition to comprehensive EU GDPR support, customers will find that OneWelcome’s Consent and Preference Management module facilitates compliance with other privacy

regulations globally, such as California's CCPA. OneWelcome CPM is built into their own SaaS and can be licensed separately and run alongside other popular CIAM solutions.

The OneWelcome Delegated User Management module provides delegated administration and identity management, including complex, time-based roles and accounts, invitation-only account creation for B2B and B2B2C use cases; and family management for B2C use cases.

The Delegated User Management module also provides lightweight Identity Governance and Administration features. Users can set specific dates for when accounts should be activated or deactivated based on the type of account. The module also allows for defining access workflows. OneWelcome can identify and handle duplicate accounts by merging or deleting them.

OneWelcome Externalized Authorization module supports advanced fine-grained authorization scenarios, based on the Open Policy Agent (OPA). Customers use it to manage subscriptions and secure access to sensitive information such as patient records in a modern services-based architecture. The Externalized Authorization module also enables secure interactions with third-party identity platform providers, offering an added layer of control and protection.

OneWelcome Identity Platform facilitates consumer IoT device identity management via the OAuth2 Device Flow specification. Web-connected and user input-constrained devices can be linked with user identity accounts managed by OneWelcome tenants. Examples include Smart Home, consumer electronics, and wearable devices. Users can see and, if desired, disconnect paired devices. The solution also supports IoT device management in the B2B context.

OneWelcome Identity & Access Core tracks identity events and provides analytics reports, including failed login attempts, user profile changes, changes to credentials and devices, consent grants and revocations, changes to group memberships, etc. Organizational customers can define "front-end" events, i.e., user interactions on tenant web properties, using tag managers (such as Google Tag Manager, Tealium, etc.) which can then be reported on in OneWelcome's console, as well as streamed via API or syslog. The console support drill-down analysis to the event level. Customers can configure event streams for Customer Relationship Management (CRM) solutions. Out-of-the-box connectors are available for Kibana and Grafana data analysis and visualization services.

OneWelcome Identity & Access Core is built on LDAP and NoSQL databases, which allow customers to extend the schema and store a wide array of attributes as well as other file types. The solution interoperates with other IAM and IDaaS platforms by supporting OAuth, OIDC, and SAML. The solution's cloud-hosted architecture enables maximum scalability, utilizing microservices and serverless functions, and leveraging the elastic scaling capabilities of the underlying IaaS infrastructure. Thales offers zero downtime service level agreements. Moreover, Thales reports very low latency. Their Identity Platform is protected against DDoS and bot attacks at the service level.

OneWelcome (now Thales) is known for its innovation in CIAM. Thales was quick to address the growing B2B and B2B2C market segment by enabling complex relationship management. They have added features for consumer and B2B customer identity lifecycle

management. Today, tenants are using their platform in novel ways to allow their consumers to integrate their real-world purchases with their avatars in the metaverse.

As part of Thales, OneWelcome leverages key capabilities like Public Key Infrastructure (PKI), biometrics, key management, digital wallets, sovereignty, and software monetization, having therefore diversified its capabilities and transitioned from being a single-focus entity to a multifaceted solution provider.

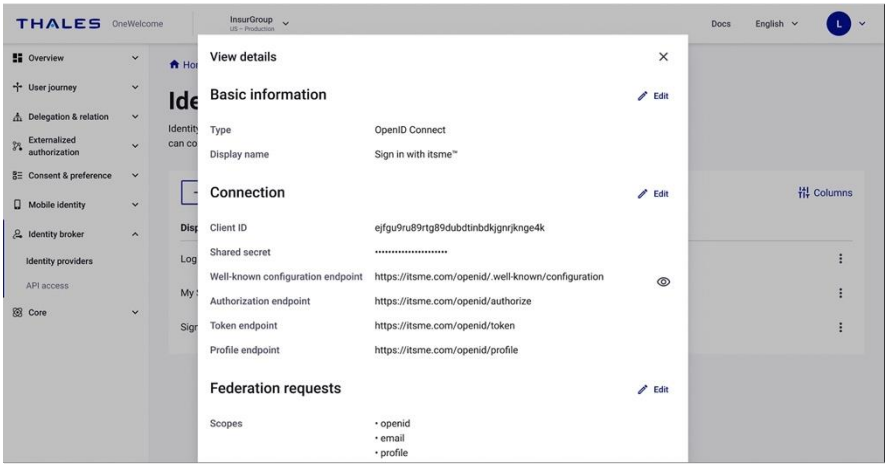

Figure 2: Thales OneWelcome User Journey Orchestration configuration (used with permission)

Strengths and Challenges

Thales strengths have been in the areas of consent and privacy management, data localization and EU GDPR compliance, B2B delegation, and authorization. The pairing of Thales SafeNet Trusted Access with OneWelcome adds strong authentication, more MFA options including FIDO, identity proofing, document verification, high assurance credential issuance, and fraud protection.

Going forward, OneWelcome will be the combined eponymous brand combining CIAM with the former Thales SafeNet offering, which is primarily for enterprise and workforce use cases. Whereas OneWelcome had been focused on the EU market, Thales is a global company. Thales will leverage their global sales and support network to grow their market share in CIAM in the Americas and APAC.

OneWelcome has been consistently recognized as a Product and Innovation Leader in KuppingerCole Leadership Compasses in CIAM. Thales Digital Identity and Security was also determined to be an Overall, Product, Innovation, and Market Leader in both the Reusable Verified Identity and Providers of Verified Identity Leadership Compasses. Thales SafeNet is an Overall, Product, and Market Leader in Passwordless Authentication.

Additionally, Thales CipherTrust was rated as Overall, Product, Innovation, and Market Leader in the Data Security Leadership Compass.

Additional connectors for CRM, data analytics, and marketing automation tools would be useful, as would the ability for tenant admins to be able to modify authentication risk factor weightings. These items are on their roadmap.

Any organization looking for a feature-rich CIAM service with excellent consent and privacy management, B2B relationship management, strong authentication and MFA capabilities, and extensibility through APIs should consider the OneWelcome Identity Platform.

Strengths

- Built-in identity proofing capabilities and many integrations with 3rd-party ID proofing and attribute services; eIDAS support
- Identity brokering services
- Strong privacy compliance features for GDPR including EU data localization as well as for CCPA and others
- Excellent consent and privacy management capabilities, available as standalone service that works in conjunction with other CIAM products
- Thales union brings support for many strong authentication methods including FIDO 2.0 and Passkeys
- Kantara Consent Receipt format conformance
- Support for SmartHome device identity management
- Fine-grained authorization functions enable complex B2B customer and consumer access control use cases
- B2B, Lightweight IGA, and consumer identity lifecycle management functions

Challenges

- Does not leverage in-network compromised credential intelligence
- Passive biometrics not utilized
- Additional out-of-the-box integrations with marketing automation and data analytics tools would be helpful
- Changing risk policies and risk factor weighting requires OneWelcome staff support; a GUI for customer admins is in work

Related Research

Leadership Compass CIAM Platforms 2022
Leadership Compass CIAM Platforms 2020
Leadership Compass CIAM Platforms 2018
Leadership Compass Privacy and Consent Management Platforms
Leadership Compass Passwordless Authentication
Leadership Compass Reusable Verified Identity

Executive View OneWelcome Customer Identity and B2B Identity
Executive View iWelcome IDaaS and CIAM

About KuppingerCole

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.

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.