Customer Identity and Access Management (CIAM): An overview of the main technology vendors

ANASTASIOS LIVERETOS, IVO DRAGANOV,
Technical University of Sofia,
8 Kliment Ohridski Blvd., Sofia, 1756
BULGARIA

Abstract: As more organizations undergo a digital transformation, they are exposing applications and services to customers and consumers at a much higher scale. This trend is seen across a variety of organizations, such as consumer services, government, education, and other. When building an approach for handling customer identities, many organizations think that they can treat these identities the same way as corporate ones. The truth is that they are very different.

Customer/Consumer identities greatly outnumber employee identities. Customers/Consumers today expect to be able to perform identity management tasks themselves without having to talk to a person (Self-Service). Requiring consumers to engage with a helpdesk with every identity management task will require to retain more help desk staff and it will result in lower customer satisfaction.

With the number of online applications and services, which people use, increasing, the number of user accounts that consumers are having to create and maintain is higher than ever. Therefore, many people are choosing to bring their own identity into the application. By integrating applications with established online Identity Providers (such as a Microsoft Account, Facebook, LinkedIn, etc.), enterprises can enable consumers to use the identities that they already have, instead of having to create yet another username and password.

Moreover, consumers do not want more than one account when working with an organization. They expect to have a single identity regardless of the application that they use – whether it is a web or a mobile device application.

Now more than ever, consumers are skeptical about what organizations will do with the identity data that they provide. Therefore, it is important to make sure that consumers understand how their identities are being used and consent to its use. Without this, the consumer will not trust the organization.

Finally, unlike employee identities, consumer identities can scale into the 100's of millions

Selecting the tool to address all beforementioned prerequisites is critical. This paper describes the four leading solutions for Customer Identity and Access Management and confirms that, to a great extent, they all cover adequately these prerequisites.

Keywords: Identity and access management, Customer identity and access management, Identity governance and administration, System integration.

Received: July 8, 2021. Revised: August 12, 2022. Accepted: September 11, 2022. Published: October 5, 2022.

1. Introduction

SEVERAL years ago, in 2007, Abad Shah, Amjad Farooq and Kashif Talib were presenting the challenges, which the then newly growing web-services were imposing to identity management. They were considering that an identity management system handles an activity that is undertaken by a service provider to provide and manage services and the user identities [1]. Since then, the on-line market has grown dramatically and the introduction of CIAM has become an absolute necessity for a lot of companies. Thus, an abundance of relevant solutions is the new reality.

Despite the big number of solutions, all of the currently available in the market ones cover the same high-level architecture (Fig. 1), as developed by the author.

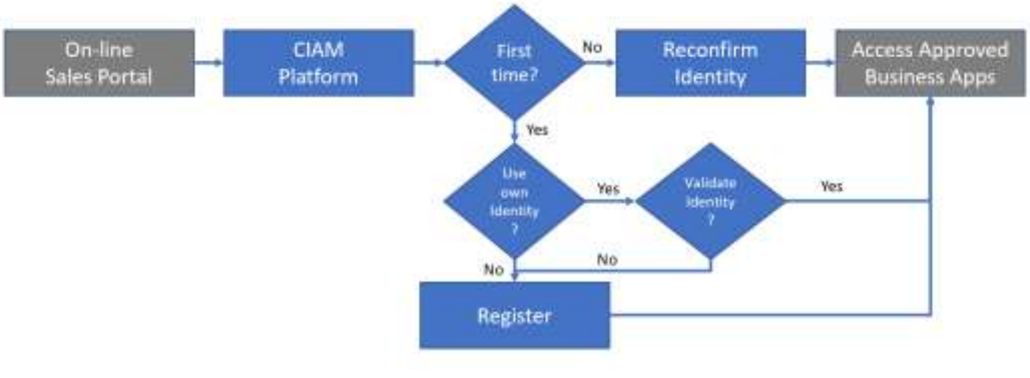

Fig. 1 High-Level CIAM architecture

The key driver for implementing a CIAM solution is the existence of a customer portal. Through this, customers are contacting the company, aiming to browse products, place orders, make payments, review delivery status etc. All these are referred to as "approved business apps".

Once the customer enters the portal, the CIAM solution kicks in, following specific steps:

- If the customer attempts to access the portal for the first time, they have the option to either bring their own identity from a recognized source (most likely a social identity from Facebook, LinkedIn, Twitter etc.), or register directly in the portal and create a new identity there.
- If it's a returning customer, the portal asks for the identity via which they had accessed the system before.

When the customer opts to bring their own identity, the identity is validated via federated identity management. Nowadays, there are many federated identity solutions, however, most of them covers different aspects of the identification problem, solving in some cases specific problems. Thus, none of these initiatives has consolidated as a unique solution and surely it will remain like that in a near future [2].

The validation of the identity is happening in the CIAM platform and access is provided based on the characteristics of the identity. In general, the cloud provider is responsible for enforcing the policies regarding authorizations and access controls, and the cloud user is responsible for defining the entitlements and also properly configuring them in the cloud platform [3].

2. Methodology

In June 2021, a questionnaire (Appendix 1) was purposely developed and shared with corporations worldwide. 24 replies were received from companies functioning in 17 different industries (Appendix 2).

With this survey, along with other focus points, we specifically targeted the CIAM area. CIAM requirements are very different to those for IAM. The key features of CIAM include: Cloud-based hosting, Platform-based functionality, Strong authentication and syndication, Integration, Scalability and Interface customability. These very particularities drive organizations into adopting additional solutions to support them with the management of their external identities.

14 of 22 (64%) of the participants leverage at least one CIAM solution, along with their IAM ones, to support the identities of their external personas/users.

5 of 14 (36%) of the respondents use SAP Customer Data Cloud (previously known as Gigya). Moreover, Company 2 (Pharmaceuticals), which is currently using MS Azure, is in the process of migrating to SAP Customer Data Cloud, too.

3 of 14 (21%) use Okta and another 3 use Ping Identity. Of the latter 3, Company 9 (HR Services) is also using CA Siteminder and Company 18 (Pharmaceuticals) is using SailPoint.

Amongst the Companies that are not currently using any CIAM solution, Company 7 (Automotive) is looking into Azure AD and Company 22 (Energy) is investing into building a home-grown solution for managing external identities.

This paper provides an in-depth analysis of the four main identified vendors: SAP, Microsoft, Okta and Ping.

3. Results

3.1 SAP

SAP is one of the world's leading producers of software for the management of business processes, developing solutions that facilitate effective data processing and information flow across organizations. Founded in 1972, the company was initially called System Analysis Program Development (Systemanalyse Programmentwicklung), later abbreviated to SAP. With the introduction of its original SAP R/2 and SAP R/3 software, SAP established the global standard for Enterprise Resource Planning (ERP) software. Now, SAP S/4 HANA takes ERP to the next level by using the power of in-memory computing to process vast amounts of data, and to support advanced technologies such as artificial intelligence (AI) and machine learning.

One of the primary concepts that emphasizes on the Customer Identity and Access Management (CIAM) is SAP S/4HANA [4]. Based on its ideas a related framework has been developed encompassing secure access with identity authentication based on enhanced user management and granting the related permissions. The abstract layers within it assure functionalities connected to service provisioning and the appropriate business roles, cataloguing processes and implied restrictions on information objects. Mohammed [5] propose a model for identity and access management (IAM) based on cloud infrastructure. The author starts building his model from the general structure for cloud services where the users and supplied services are stacked in different groups. They are interconnected by permissions, acting as bridges to groups of users with similar roles. Both the federated and non-federated models for IAM are considered within this study. Given these assumptions a broker-model has been proposed for cloud identity framework with the following main components – identity and attribute providers, home and Service Provider (SP) brokers, and user applications, connected through the element of trust. One of the main advantages of the model is the independence from the accuracy of the identity brokers. The model is foreseen as a base for SAP Cloud Identity Access Governance. Another study by Kunz et al. [6] pose attention on the attribute quality that needs separate management when access is granted to dynamic identities. Correlation among users' data attributes on one hand, and the information domain attributes, using SAP Enterprise Resource Planning (ERP) permissions, on the other are the foundation of this model and pointed out as an advantage. The large number of control parameters remains problematic in most of the systems of this type, reaching over 1500, as Stankov and Tsochev [7] show for a particular SAP Customer Relationship Management (CRM) implementation.

SAP's proposed solution for Customer Identity and Access Management consists of the SAP Customer Data Cloud Solutions: SAP CIAM for B2C and SAP Enterprise Consent and Preference Management (ECPM).

SAP Customer Identity and Access Management (CIAM) for B2C allows to

- provide frictionless points of entry for customers across brands, regions, and properties, with customizable and secure registration and social log-in screens and flows
- securely identify online visitors from any touch point, with data federation and single-sign-on functionality and flexible user authentication options
- orchestrate unified profiles across the business to deliver personalized, trusted experiences at every customer engagement

SAP Customer Identity and Access Management (CIAM) for B2B adds capabilities for

- organization management
- delegated administration and
- policy-based access control

SAP Enterprise Consent and Preference Management (ECPM) provides

- Best-practice workflows to transparently present, collect, and manage customer consent and preferences for terms of service, privacy policies, marketing communications, and any data processing requirements
- A system that enables brands and properties to offer clear, intuitive customer control of profile data, preference choices, and consent settings
- Secure, centralized, and audit-ready consent records that can be used to enforce customer decisions about their personal data and synchronized in near-real time with downstream systems such as commerce, marketing, sales, and services applications

The SAP Customer Data Cloud Solutions, SAP CIAM and SAP ECPM, are SaaS, Public Cloud Solutions that provide services to be integrated into any company's customer facing applications and backend solutions. To allow implementation/utilization of the respective services, in accordance with regional data protection regulations, the solutions are available globally, with datacenters in Australia, the European Union and the United States of America (incl. the CIAM for B2B Add-On), as well as in Russia and China (excl. the CIAM for B2B Add-On). For the European Union an additional option exists, to utilize the MS Azure based data center.

Comprised of the three integrated products SAP Customer Identity, SAP Customer Consent and SAP Customer Profile, the SAP Customer Data Cloud Solutions SAP CIAM and SAP ECPM help businesses securely identify consumers across devices and channels to drive registrations and engagement, manage their customers' preference and consent data across the entire lifecycle, transform data into unified customer profiles that are centrally and securely governed and analyzed, and then orchestrate changes with downstream applications through the advanced extract, transform, and load (ETL) functions of the IdentitySync feature.

The main functionalities, as shown in Fig. 2, are:

SAP Customer Identity: Provides the functionality of the SAP CIAM solution for helping clients transform unknown online visitors into known, loyal customers, engage them earlier in their journeys, and reduce friction while increasing security by minimizing risky password-based transactions.

− *Registration and Authentication*: Build and manage registration, authentication, and profile management workflows across client Web sites and mobile applications. Leverage a wide range of capabilities, including lite registration, traditional registration and social login, multi-factor authentication, risk-based authentication, profile update flows, and password reset flows.

− *Social Login*: Use an existing identity from more than 30 social networks and identity providers (IDPs) – including Facebook, Twitter, LinkedIn, Google+ and more – to quickly log in to Web sites and applications.

− *Progressive and Conditional Profiling*: Enable progressive and conditional data flows that gather new attributes from customers as they return after initial registration, leading to more complete profiles that can be used to drive contextual marketing strategies and highly personalized customer experiences.

− *Single Sign-On (SSO) & Federation*: Synchronize a user's login state across multiple Web properties that share a back-end repository. Enable SSO with applications, which do not share a database, with support for SAML 2.0 and OpenID Connect.

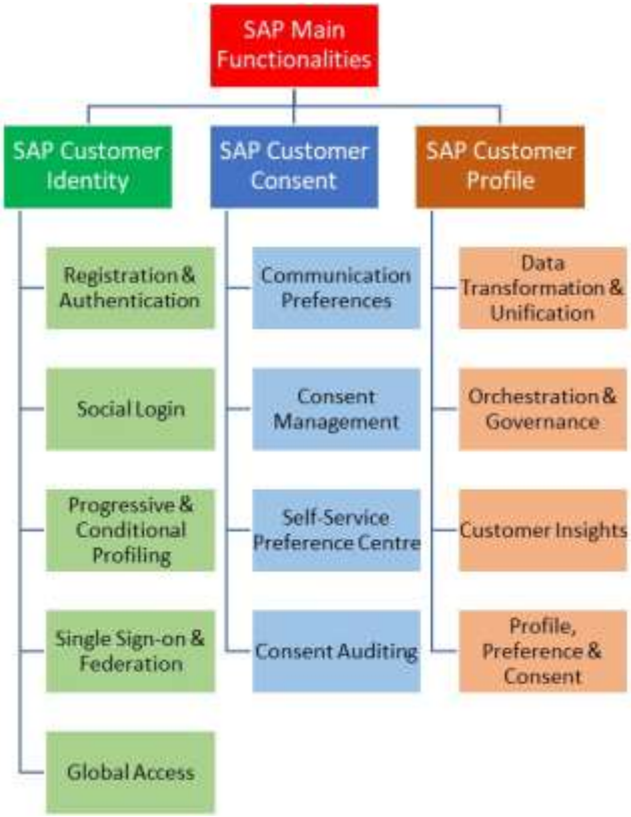
SAP Main Functionalities
SAP Customer Identity
SAP Customer Consent
SAP Customer Profile
Registration & Authentication
Social Login
Progressive & Conditional Profiling
Single Sign-on & Federation
Global Access
Communication Preferences
Consent Management
Self-Service Preference Centre
Consent Auditing
Data Transformation & Unification
Orchestration & Governance
Customer Insights
Profile, Preference & Consent

Fig. 2 SAP CIAM main functionalities

− *Global Access*: Allows businesses to store the data of users from across regions in the data centers they are originally registered, regardless of their location when they authenticate, helping the businesses achieve compliance with applicable data residency requirements.

SAP Customer Consent: Provides the functionality of the SAP ECPM solution for managing customers' preferences and consent settings, including opt-in and communications preference data, in a centralized and audit-ready vault. SAP Customer Consent includes:

− *Communication Preferences & Opt-In Management*: Allow unregistered and registered users to opt-in to newsletters and other marketing subscriptions or promotions and to set associated preferences. Support double opt-in flows for subscriptions in regions, where this is a requirement.

− *Consent Management*: Implement customizable, out-of-the-box workflows to present clear consent requests for terms of service, privacy policies, cookie consent (ePrivacy), or any other permission-based activities. Automatically trigger requests to renew consent every time terms and policies change.

− *Self-Service Preference Centre UIs*: Allow customers to view their consent to legal terms, policies, and opt-ins to marketing communications, and to update their consent, opt-ins, and preferences on a self-service basis.

− *Consent Auditing*: Capture all consent-related actions in a read-only, audit-ready Consent Vault. Run queries easily via a dashboard interface or the API and maintain all consent related transaction data for seven years.

SAP Customer Profile: Provides the profile management functionality for the SAP CIAM and SAP ECPM solutions, for volunteered, first-party user data, eliminating segregated data silos and transforming user data into unified profiles that can be orchestrated across every downstream application and service. It allows you to govern customer accounts and data centrally to enable a more stable and integrated digital ecosystem and analyze data to drive more effective in-moment marketing. SAP Customer Profile includes:

− *Data Transformation & Unification*: Transform consumer identity, profile, and account status data captured from online users into a unified profile for each customer.

− *Orchestration & Governance*: Orchestrate data from each profile – or specific attributes only – in real time or batch mode to any application, service, or data lake using the built-in ETL service, Webhooks, REST API, or any of more than 50 pre-built integrations with the most popular third-party customer engagement technologies in use today. Govern all customer accounts and data from a centralized location and gain access to an audit trail of all administrator- and customer-initiated updates. Meanwhile, advanced error and exception handling helps address anomalous activities and behaviors.

− *Customer Insights*: Analyze customer identity, profile and account status data to gain a deeper understanding of audiences and drive more accurate segmentation with cross-platform analytics, social data insights, and flexible reporting.

− *Profile, Preference, & Consent Data Store*: Store all social user data and attributes gathered through progressive and conditional profiling, as well as traditional profile information, consent and opt-in data, associated preferences, and behavioral data, with a fully indexed dynamic schema database designed to store an unlimited number of fields on the user record.

3.2 Microsoft

Microsoft Corporation (Nasdaq "MSFT" @microsoft) was founded in 1975 and it was incorporated in the State of Washington. The company generates revenue by developing, manufacturing, licensing, and support of software products and services for different types of computing devices worldwide. Microsoft's mission is to empower every person and every organization on the planet to achieve more.

Microsoft Azure Active Directory (AD) is a service, offering the next level for authentication which provides seamless single sign-on functionality according to Subbarao et al. [8]. It keeps away sensitive data from handled applications, e.g. passwords, and uses other means for authentication, e.g. biometrics. Conditional access has been improved using multi-factor authentication according to the authors of this study while they apply the new .NET functionalities through Visual Studio 2019 on a Security Assertion Mark-up Language (SAML) request-response basis. Bhardwaj et al. [9] investigate further the Azure security practices. Information Security Management System (ISMS) has been developed which allows a set of security policies to be introduced along with the definition of data safety. Scaling abilities with conformance to generated data traffic emerge from these efforts while performing extensive computing and encryption, resulting in equalization of the data loads and reducing the risk of a data loss. As Herath [10] reveal one of the first thing to configure during the successful usage of Azure AD is the (Business to Customer) B2C tenant. As a set of identities that is going to be used with the connected applications it is the starting point for providing security. Soh et al. [11] emphasize on the importance of introducing the Global Administrator and the Privileged Role Administrator into the delegation of the roles for administrative purposes to given number of users. All key roles have been summarized in a complete classification.

Microsoft operates a comprehensive partner network. However, they recommend that it is their own internal resources that engage directly to deliver certain key foundational components of the Customer Identity and Access Management Solution. This allows Microsoft to utilize their internal architects, engineers and intellectual property (IP) to ensure this initial foundation is established and delivered successfully and in line with Microsoft's Best Practices.

Microsoft has extensive experience in delivering large, complex solutions that are spread over multi-year development and Deployment life cycles. With decades of experience on several projects implemented worldwide, Microsoft provides solutions and specific consultancy services to Retails, Consumer services, Aerospace, Financial, Health, Government, Chemical and Agrochemical, Discrete Manufacturing, Education Media and Entertainment, Mining Oil and Gas, Power and Utilities, Public Safety, Telecommunications, and Travel and Transportation globally.

Microsoft proposes a four pilar strategy, when it comes to CIAM implementation. The four digital transformation pillars (Engage Customers, Empower Employees, Optimize Operations and Transform Products) and their digital feedback loop (Fig. 3), allow its customers to conceptualize, refine, and implement their business transformation ideas.

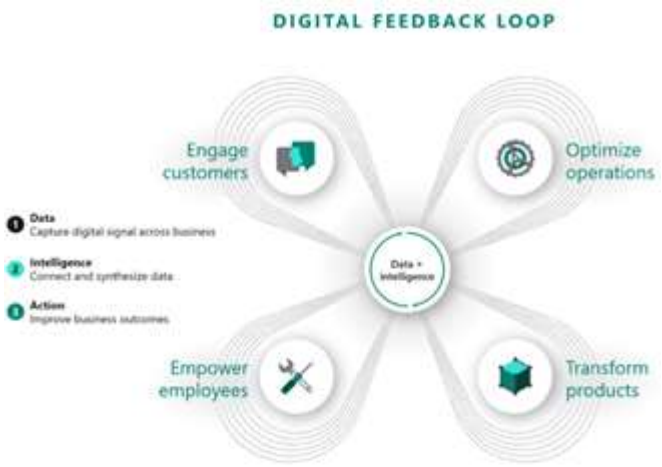

Fig. 3 The digital feedback loop, https://cloudblogs.microsoft.com/industry-blog/en-au/skills-culture/2019/03/14/transforming-organisational-culture-and-experience-by-creating-a-digital-feedback-loop/

To solve current industry challenges pertaining to consumer identities, Microsoft has built a new type of consumer identity service on top of Azure Active Directory (AD).

Azure AD is a cloud-scale identity service that already handles billions of user authentications for Microsoft's online services, such as Office 365.

Azure AD B2C is a consumer version of an Azure AD tenant, built with consumers and citizens in mind. It enables consumer and citizen identities to be used in web applications, mobile device applications, and web services, and these applications and services do not need to live in the Microsoft cloud. They can live anywhere – in on-premises systems, in Azure, or in other non-Microsoft clouds such as Amazon Web Services.

As they are leveraging the Azure Active Directory service, Microsoft's B2C service has already been proven to scale to 100's of millions of identities. Unlike on-premises systems, Microsoft measures its services capacity in terms of 'millions' rather than 'thousands'. And with that high of a user volume, it's important to provide self-service capabilities—and in Azure AD B2C, self-service is a primary consideration.

Microsoft's CIAM provides self-service experiences for user registration, account management, and password reset. The built-in user experience customization capability allows Microsoft's customers to customize the branding and theme the end-user interfaces to their preference. Another feature provided through Microsoft's CIAM is the ability to enable a custom domain to the service, so that users don't see a microsoftonline.com address in the URL bar of the B2C web pages.

Within the Microsoft technical solution considerations several attributes are included:

- *Embrace social media identities*

Azure AD B2C enables users to use their existing social identities This reduces application sign-up friction and facilitates a better sign in experience.

- *Let developers focus on end-user experience and productivity*

Most public-facing applications need to perform two primary identity functions:

(1) authenticating users and

(2) managing user identities.

These tasks have traditionally been left up to the application developers, laying the burden on them of having to secure and manage user identities. With the constantly changing threat landscape, one needs top notch security experts filling this role. Microsoft does not let a breach of the user's password create an entry to the customer's system. Instead, it enables developers to use a cloud identity service, which is continuously being hardened against emerging threats.

- *Know who's really accessing each application*

Azure AD B2C isn't a typical cloud identity service. Using the power of Azure AD B2C's trust framework engine, one can define policies for users of their applications. These policies can leverage 3rd party attribute providers and attribute verifiers, which can increase the confidence in the user's identity being genuine.

- *Scale to hundreds of millions of users*

Most organizations attempt to manage external user identities with complex systems that reside on their corporate network. These systems are often fragile and difficult to manage. What is more, legacy on-premises identity systems often struggle to scale, when user volume demand rises, during a busy season. Azure AD B2C scales to billions of users and takes that burden off of the on-premises identity systems.

Key Differentiating Points of Azure:

- *Availability Zones*

In addition to a vast catalog of products and solutions, Azure meets resiliency requirements by launching in Availability Zone architecture, which is a high availability offering that protects applications and data from datacenter failures.

- *16,000 offers on Azure*

Microsoft has a complete set of integrated cloud offerings, from infrastructure as a service (IaaS), to Platform as a Service (PaaS) to Software as a Service (SaaS). With a broad partner ecosystem of over 60,000 partners, they offer solutions and services to their customers through App source. In addition, the Azure Marketplace is a rich catalog of over 16,000 products and solutions ranging from open source and community software to enterprise applications, which have been certified and optimized to run on Azure.

- *Hybrid cloud management*

Among the hybrid cloud offers, Azure launched Arc, which is an offer for customers who want to simplify complex and distributed environments across on-premises, edge, and multi-cloud. Azure Arc enables deployment of Azure services anywhere and extends Azure management to any infrastructure

- *Datacenters* in more than 60 regions
- *Azure's Virtual Machine (VM)* uptime Service Level Agreement (SLA) is best in industry at 99.99% if using Availability Zones.
- *Comprehensive set of compliance offerings*

Microsoft is committed to the highest levels of trust, transparency, standards conformance, and regulatory compliance with the most comprehensive set of compliance offerings of any cloud service provider. Security is foundational for Azure and Microsoft leads the industry in establishing and consistently meeting security and privacy requirements. Azure is built with customized hardware, has security controls integrated into the hardware and firmware components, and added protections against threats such as Distributed Denial of Service (DDoS).

- *85% of global systemically important financial institutions (GSIFI) rely on Microsoft Azure & Office 365.*

3.3 Okta

Okta (iC Consult) was founded in Munich in 1997. Today they have offices in Germany (Hamburg, Essen, Frankfurt am Main, Stuttgart and Munich) as well as in Switzerland, Austria, UK, Spain, USA and China. Besides iC Consult GmbH with focus a on IAM implementation and integration, the other specialized brands of iC Consult Group are xdi360 GmbH (IAM Business Consulting and GDPR), IAM Worx GmbH (IAM Support and Operations) and Service Layers GmbH (Custom-fit IAM as a Managed Service).

Okta's vision is to be the platform that enables any company to adopt any technology. Okta is a 100% multi-tenant cloud service, which is one of the foundational innovations that sets Okta apart from both legacy IAM and IDaaS competitors.

Okta relies on ambitious model for Corporate Social Responsibility (CSR) [12]. It has in-depth framework which renders an account on social impact, which is being synchronized with its core business services and thus becoming one of the leaders in market of IAM solutions. Its model is taken into consideration by Thakur et al. [13] in their study on data security of directory servers. They describe the structure of a directory as a tree information entity where a suffix, distinguished name and relative distinguished name are the main 3 branches. As Azhar [14] points out, the purchase of Auth0 by Okta is one of the driving forces into the fusion of identity and access management with customer-centric identity and access management. Kumar et al. [15] explore the data security issues within the solutions for cloud computing, also considering the Okta product. They focus on the cloud computing actors put in a single unified structure and naming them as consumer, auditor, broker, provider and carrier. Then, the issues that arise from any of these elements are being classified as related to confidentiality, integrity and availability, to authentication and access control, to sessions and the actual access, and to other processes. Each one of them deserves closer look in order to tighten the overall security.

According to Okta, the selection of a suitable CIAM vendor is one thing – but delivering an end-to-end positive journey and experience to your customer involves more. The ease of use for onboarding of new users, self-registration or self-services represents key factors having a direct impact on the adoption of new digital services and offerings and thus on the resulting revenues. A strong expertise not just on technology but also on comprehensive understanding of the customer journey and underlying processes are thus essential. In addition, a state-of-the-art consent management is a must for any successful digital business.

Within the iC Consult Group, xdi360 GmbH is dedicated to consulting, conception and implementation of innovative solutions in the areas of customer, things and digital business. Xdi360 supports customers in gaining a 360° view of their data - manufacturer-independent, focused and competent.

• Customer Data Management and Consent Management as a corporate focus: xdi360 has been on the market as a specialist for Customer Data Management since 2012 and has completed many projects very successfully and with great customer satisfaction during this time.

• Outstanding professional and technical competence: xdi360 has outstanding professional and technical expertise in all topics relevant to CCH.

• Long-standing service provider and partner in financial services industry: xdi360 has been active as a service provider in the financial services segment for many years already.

• Comprehensive understanding of consent management: xdi360 has a deep and comprehensive understanding of Consent Management and counts on the experience of many projects with a focus on consent management, data protection and customer data management.

The Okta service provides directory services, single sign-on, strong authentication, provisioning workflows, API access management, server access management, and built-in reporting. It runs in the cloud on a secure, reliable, extensively audited platform and integrates with on-premises applications, directories, and identity management systems.

Comprehensive service: offer full IAM functionality, including standards-based authentication and authorization (SAML, OpenID Connect, OAuth 2.0, WS-Fed, Kerberos, Headers-based, etc., as per Fig. 4), a cloud directory, MFA, user provisioning / de-provisioning, and detailed reporting and analytics.

Ease of use: transform enterprise IAM into a simple to use service with an intuitive UI for users accessing cloud services online and provide very fast time to deployment and value.

Service: 100% on-demand with no HW or SW to maintain. Further, all app integrations are developed, tested, and maintained as part of its service. This helps customers to integrate easily with existing systems and applications.

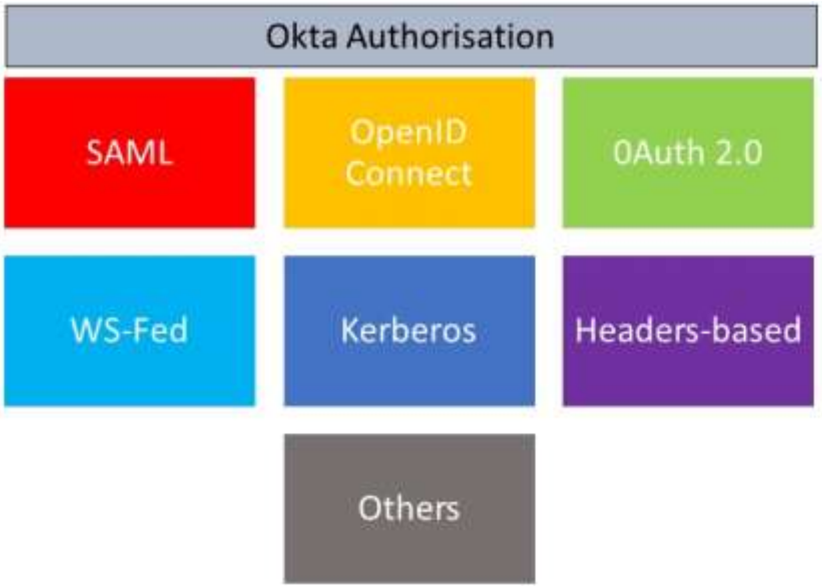

Fig. 4 Okta’s supported authorization standards

Integration: Support over 6500 apps in its catalogue. Additionally, customers can add other applications not supported in the catalogue by using templates or wizard-style configuration steps. Users can also make use of Okta’s password vaulting to provide SSO to all web-based applications that do not support federation standards.

Platform: Help provide a centralized Identity and Authentication service where users authenticate once (typically via their trusted AD authentication for workforce use cases and typically via Okta's cloud Universal Directory for customer use cases) and then gain SSO to all other applications with the option to use the integrated, context-based Okta Adaptive Multi-Factor Authentication (MFA) integrated service. All these features are available for the desktop, laptop and mobile devices (including phones and tablets supporting the Android and iOS operating systems).

Security: Focus on a secure and reliable architecture. The company has been verified against the industry's toughest standards (SOC 2 Type 1 and Type 2 audited, FedRAMP).

Key benefits of the Okta platform:

- Cloud-first architecture leads to increased operational efficiency (lower TCO).
- One Single Service to meet all Universal Identity Profile Management requirements; no need to install & manage multiple servers across cloud, on-prem, and directory services.
- Built in high availability, scalability, and security with 99.99% uptime for every customer. Avoid building out and supporting own infrastructure (load balancers, HA, etc.).
- No-code / Low-code offering: Rapid development through pre-built, customizable widgets and SDKs with detailed supporting documentation.
- Comprehensive APIs (registration/extensible profile management, authentication, Multifactor Authentication, lifecycle management, policies & entitlements).
- Broadest and deepest application network for single-sign-on and user lifecycle management.
- Real-time policy-driven automated provisioning capabilities.
- Manage all users and applications from One Single Interface. No requirement for users to be managed in different directories, DBs, apps, etc.

3.4 Ping

IPG Group (Ping) has been delivering comprehensive, fully customizable online payment gateways since 1997 for independent sales organizations (ISOs), payment facilitators (PFs) and payment processors (PPs). As an expert for Identity & Access Management for 20 years, Ping offers solutions for the administration and comprehensive protection of user data and access rights for companies and organizations in the entire economy and public administration. Their experience ensures top performance and forms the basis for innovative and sustainable solutions. Ping supplements its own methods with innovative products from selected technology partners. It thus achieves decisive competitive advantages, realizes tailor-made solutions and ensures the highest quality.

Ping Identity use Artificial Intelligence (AI) for Application Programming Interface (API) behavioral security [16]. AI is a top-notch approach in the monitoring of the corporate APIs. One of the aspects that needs improvement is the reliability of such methods. False Rejection Rate (FRR) of users remains problematic in some cases as well as the blocking of certain applications from authorized access to data. On such grounds Rasouli and Valmohammadi [17] propose conceptual framework for CIAM. Focusing on the connectivity with the users at the stage of access to information systems, both centralized and distributed, the authors pay attention to all the steps of the process – from registration to track. The results from content analysis of these researchers indicate that customer identity management, customer access management and business management are mostly affecting the identification procedures within CIAM solutions. Customized products could be partially selected based on the application of the conceptual model that emerges from these studies. According to Ng [18], Ping describe the system security as dynamic, adaptable to user's location and also dependent on time, the network and related devices' behavior. The complexity of the security assurance becomes even higher with the introduction of multi-cloud platforms [19]. In that study it's been shown that interoperable identity could be handled successfully through management protocol. Such an identity could be not only associated with a single person but with a cloud consumer in general. Elliptic curve cryptography (ECC) tends to be a suitable candidate for securing tool to use with the proposed protocol.

Ping's customers benefit from a comprehensive, holistic IAM competence. The IPG Group offers cross-product IAM consulting and, as an integration specialist, supports the planning and implementation of IAM solutions. It also ensures the operation of IAM solutions and offers a variety of IAM-related training courses.

By having multiple Directory back-ends in different countries and dynamically routing data to the appropriate place with the Ping Identity Platform Solution, the data residency requirements are addressed. Thanks to the support for hybrid deployments, customers can store data exactly where they are needed. This is typically not achievable with pure SaaS IAM vendors that are limited to some locations and changes in the regulations cannot be quickly addressed. Moreover, partial data synchronization ensures that customers can replicate only the necessary entities and attributes across borders, to make sure that sensitive information is never sent to remote locations if not needed.

Solution architecture is the fundamental difference between Ping and other vendors. Legacy architectures represent heavyweight agent server topologies, designed and developed in the previous century and targeting the enterprise, single-domain Web SSO requirements of that time. The Ping Identity Platform solution is designed to embrace standards and avoid vendor lock-in. Customers can simplify and improve user access to integrated web, mobile and API services in a secure manner but at a fraction of the cost and complexity of alternative solutions, including the option of in-house developed capability.

The key requirements (Fig. 5), which the architecture of this solution should cover are:

User authentication: The solution first authenticates users according to the configured policies; validates the user provided credentials against the connected identity data store and enforces any MFA requirements either using Ping MFA or any other third-party MFA solution, depending on the configured policies and the context of the request.

Self-Service: The solution provides self-service registration, profile management and password management capabilities.

Delegated Administration: Delegated administrators, designated by user or groups, have access to other user identities per hierarchical position or group memberships, with varying access levels on an attribute level.

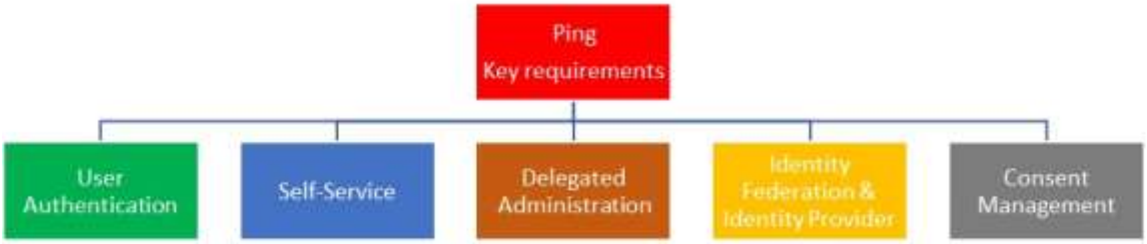

Fig. 5 Key requirements for Ping

Identity Federation & Identity Provider: Trust relationships between the solution and the external identity providers and applications are established. The solution is responsible for the identity linking between the identities in the IAM Platform and the external identities. It works both as an Identity Provider, to issue the necessary tokens, and as a Service Provider to receive and validate tokens from any configured external Identity Provider.

Consent Management: The solution displays a consent screen that gathers and stores the user consent to distribute a token with specific permissions attached to the token. Consent is stored in the solution directory, via the provided consent APIs.

Key advantages of Ping are:

- Single Platform and authentication authority with federated SSO, adaptive MFA and more to address diverse use cases and secure customer, partner and workforce identities.
- Seamless Digital Experience with a directory that synchronizes and aggregates identity data from multiple sources to increase user productivity and personalize customer experiences.
- Secure, centralized access across web applications, single page applications and APIs, that leverages identity intelligence to detect and block cyberattacks, prevent security breaches, and meet regulatory requirements.
- Rapid extensibility with standards support, integration kits and adapters to leverage existing investments and connect users to SaaS, cloud, mobile and on-premises resources.
- Deployment flexibility to accelerate cloud strategy with options for IDaaS, cloud, on-premises and hybrid IT.
- IAM expertise and world-class partners to support current and future requirements, including migrations from legacy IAM infrastructures and enterprise CIAM deployments.

4. Conclusions

Customer Identity and Access Management is nowadays covered adequately with strong solutions, supported by reputable vendors, who are eager to invest on their platforms and continuously improve them. Thus, the most relevant criteria based on which the solution should be chosen are:

- The CIAM solution should support the long-term vision of the company. The workflows must be flexible enough to meet current and anticipated needs.
- The CIAM solution is one item of the overall technology architecture of a company. It is crucial that CIAM is well integrated to the overall IT environment.
- As the needs change over time, it’s fundamental to define from the beginning the support structure for the CIAM solution. The choice between internally developed and vendor-driven enhancements may lead to choosing a different solution.
- The specificities of the industry and the geographical context drive regulatory, tax and legal considerations, which are often too significant to ignore.
- The security questions in terms of access and, most importantly, bring-your-own-identity are equally addressed by all available solutions. Still, defining who is the end-user (B2B, B2C, B2B2C etc.) drives different relationship requirements, which should be analyzed and covered.
- In all cases, a CIAM platform implementation should offer a complete customer journey, bolster user security experience and contribute to effective fraud reduction [20].

Having reviewed several of the available solutions for CIAM, the author confirmed that the material world is currently well covered. Looking into the expected developments in the near future, the author suggests further research to be made for critical CIAM capabilities in the area of Metaverse and on how identities may travel from the virtual to the material space and vice versa.

APPENDIX I

QUESTIONNAIRE

QUESTION: Do you currently leverage at least one central IGA solution as part of your overall IAM strategy?

_ Yes
_ No (If selected, you have completed the survey.)

1. What central IGA solution are you currently using? Please list the supplier and product name.

2. Your central IGA solution:

a. Which of the following main systems are used and integrated with your central IGA solution?

_ SAP ERP
_ Microsoft Azure Active Directory
_ Janrain
_ Auth0
_ ForgeRock
_ IBM Security Access Manager
_ Okta Customer Identity
_ Ping Identity
_ Salesforce
_ Other. Please specify:

b. What percentage of systems are currently operating with your primary IGA tool in the organization today?

_ <30%
_ Between 30%-50%
_ Between 51%-80%
_ >80%

3. Identity management operating model:

a. Briefly, please describe the management model of your IAM solution(s) (i.e., is your solution on-premises or SaaS-based? Is it managed internally or being outsourced? Etc.)

b. If applicable, what is the breakdown of the IAM solutions that are managed internally and being outsourced?

_% managed internally
_% outsourced

c. If your IAM solutions are outsourced, what (if any) benefits are you experiencing?

d. More specifically, what IAM sub-processes have you outsourced and insourced?

4. How many resources does your IAM team have in each of the following categories?

_ # of internal resources
_ # of contractors

5. For systems where access is managed manually (i.e., directly in the system by the user administrator, rather than by the IAM system), there may be a greater risk of error (e.g., excessive access, continued access for employees no longer with the organization, etc.). To what extent has this been a challenge in your organization?

_ Major challenge
_ Minor challenge
_ Not a challenge

How (if at all) have you changed your IAM program to adapt to zero trust principles? Please briefly describe any short-term and long-term initiatives you have planned.

6. Customer identity and access management (CIAM):

a. Have you added any customer identity and access management (CIAM) solutions to your current IAM infrastructure to support external identities?

_ Yes
_ No (If selected, please skip to Question 10.)

b. What CIAM solution are you using? Please list the supplier and product name.

c. What were your primary business drivers for adopting a CIAM solution? Please select (or identify) the top 3 drivers.

_ Unify user experience
_ Drive digital initiatives
_ 360-degree view of customer
_ Streamline operations
_ Replace homegrown systems
_ Other(s). Please specify:

7. What have been the key benefits and challenges you have encountered since adopting your CIAM solution?

a. Benefits:
b. Challenges:

8. Managing internal and external identities:

a. What types of user groups are considered internal identities and are therefore managed by your central IGA solution? And conversely, what types of user groups are considered external identities and are therefore managed by your CIAM solution? Please briefly explain.

b. Which of the following identities are being managed by your central IGA tool and your CIAM tool? Please mark an X in the appropriate column.

Identities	Managed by IGA	Managed by CIAM
Worker types		
Personas		
Privileged IDs		
Non-human		
Others		

APPENDIX II
PARTICIPANTS

(coded for GDPR purposes – data available by the author)

Company	**Industry**	**Employees***	**Revenue $bn***
Company 1	Food & Drinks	28,000	8.3
Company 2	Pharma	110,000	48.7
Company 3	HealthCare	n/a	n/a
Company 4	Hardware	28,000	16.5
Company 5	Bank	90,000	33.7
Company 6	Luxury Items	9,200	3.3
Company 7	Automotive	4,300	17.7
Company 8	HealthCare	7,500	80.4
Company 9	HR Services	58,000	14.6
Company 10	Winery	4,400	4.8
Company 11	Financial Services	n/a	n/a
Company 12	Cosmetics	33,400	1.4
Company 13	Petroleum	105,500	140.7
Company 14	Insurance	17,000	41.9
Company 15	HealthCare	300,000	268.7
Company 16	Wholesale	41,000	179.6
Company 17	Power Systems	60,000	19.8
Company 18	Pharma	27,000	7.9
Company 19	Food & Drinks	134,000	16.6
Company 20	HealthCare	49,600	29.4
Company 21	Tobacco	46,000	19.0
Company 22	Energy	14,300	100.0
Company 23	Animal Health	11,300	6.3
Company 24	Tobacco	n/a	n/a

*Latest publicly available data

References

[1] A. Shah, A. Farooq, and K. Talib, “User-oriented identity management model for web-services,” In 2007 International Symposium on High Capacity Optical Networks and Enabling Technologies, IEEE, November 2007, pp. 1-8.

[2] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. Garcia-Blas, “Federated identity architecture of the European eID system,” IEEE Access, 6, 2018, 75302-75326.

[3] J. Lampikari, “Secure Cloud Implementation in Governmental Organisations”, 2020

[4] S. Sarferaz, “Identity and Access Management,” In Compendium on Enterprise Resource Planning, Springer, Cham, 2020, pp. 485-498.

[5] I. A. Mohammed, “Cloud Identity and Access Management – A Model Proposal,” International Journal of Innovations in Engineering Research and Technology, vol. 6, no. 10, 2019, pp. 1-8.

[6] M. Kunz, A. Puchta, S. Groll, L. Fuchs, and G. Pernul, “Attribute quality management for dynamic identity and access management,” Journal of information security and applications, 44, 2019, pp. 64-79.

[7] I. Stankov and G. Tsochev, “Vulnerability and protection of business management systems: threats and challenges,” Problems of Engineering Cybernetics and Robotics, 72, 2020, pp. 29-40.

[8] D. Subbarao, B. Raju, F. Anjum, and B. M. Reddy, “Microsoft Azure active directory for next level authentication to provide a seamless single sign-on experience,” Applied Nanoscience, 2021, pp. 1-10.

[9] N. Bhardwaj, A. Banerjee, and A. Roy, “Case Study of Azure and Azure Security Practices,” Machine Learning Techniques and Analytics for Cloud Security, 2021, 339.

[10] P. Herath, “Introduction to Azure Active Directory,” In Azure Cloud Security for Absolute Beginners, Apress, Berkeley, CA, 2022, pp. 37-69.

[11] J. Soh, M. Copeland, A. Puca, and M. Harris, “Microsoft Azure and Cloud Computing,” In Microsoft Azure, Apress, Berkeley, CA, 2020, pp. 3-20.

[12] A. M. Isaacs, N. C. i Coromina, and A. Rosenzweig, “Okta for Good: Pursuing Innovation and Impact in Corporate Social Responsibility,” The Berkeley-Haas Case Series. University of California, Berkeley. Haas School of Business, 2019.

[13] M. A. Thakur, T. J. Parvat, and V. S. Walunj, “Data Security Using Directory Server in Identity and Access Management System,” In ICT Analysis and Applications, Springer, Singapore, 2021, pp. 73-84.

[14] I. Azhar, “A literature review on the application of AI to Identity Access Management,” International Journal of Emerging Technologies and Innovative Research (www.

jetir.org| UGC and issn Approved), ISSN 2349-5162, 2018.

[15] P. R. Kumar, P. H. Raj, P. Jelciana, "Exploring data security issues and solutions in cloud computing," Procedia Computer Science, 125, 2018, pp. 691-697.

[16] I. A. Mohammed, "The Interaction between Artificial Intelligence and Identity and Access Management: An Empirical Study," International Journal of Creative Research Thoughts (IJCRT), ISSN 2320(2882), pp. 668-671.

[17] H. Rasouli and C. Valmohammadi, "Proposing a conceptual framework for customer identity and access management: A qualitative approach," Global Knowledge, Memory and Communication, 2019.

[18] A. C. K. Ng (Ed.), "Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities," IGI Global, 2018.

[19] T. Chaudhary and S. Kalra, "Interoperable identity management protocol for multi-cloud platform," International Journal of Big Data Intelligence, vol. 6, no. 2, 2019, pp. 69-85.

[20] A. Cser, S. Ryan, M. Maxim, E. Pikulik, P. Dostie, "Forrester Research Inc. Best Practices: Customer Identity And Access Management," 2021.

Contribution of individual authors to the creation of a scientific article (ghostwriting policy)

Anastasios Liveretos prepared the questionnaire, processed the results from it and made conclusions. He also made in-depth analysis of the properties of SAP, MS Azure, Okta and Ping platforms.

Ivo Draganov made survey on the topic of the study.