KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert

August 27, 2021

Widas ID GmbH cidaas

Widas ID GmbH offers a complete cloud identity and access management solution: cidaas. cidaas is developed and hosted in Germany. cidaas contains most standard and many innovative features, such IoT integration and consent management. It is based on a micro-services architecture which enables continuous deployment of service enhancements.

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

Content

1 Introduction

Consumer Identity and Access Management (CIAM) continues to be a fast-growing area in Identity and Access Management (IAM) that has emerged in the recent years to meet evolving business requirements. CIAM solutions are designed to meet evolving technical requirements for businesses and other organizations that deal directly with consumers and citizens. They are designed to provide better digital experiences for and gather more information about the consumers who are using their services. Enterprises want to collect, store, and analyze data on consumers to create additional sales opportunities and increase brand loyalty.

Consumer IAM systems are designed to provision, authenticate, authorize, collect, and store information about consumers from across many domains. Unlike workforce IAM systems though, information about these consumers often arrives from many unauthoritative sources. Information collected about consumers can be used for many different purposes, such as authorization to resources, or for analysis to support marketing campaigns, or Anti-Money Laundering (AML) initiatives. Moreover, CIAM systems must be able to manage many millions of identities, and process potentially billions of logins and other transactions per day. SaaS delivery of CIAM services is trending upwards and will likely remain the default choice for most organizations.

CIAM systems can aid in many types of regulatory compliance, e.g., when banks and financial service providers are required to put into place mechanisms for "Knowing Your Customer" (KYC). EU-GDPR requires collecting clear and unambiguous consent from consumers for the use of their data. Many CIAM solutions provide this capability, plus offer consumers dashboards to manage their information sharing choices. Moreover, CIAM systems can help corporate customers implement consistent privacy policies and provide the means to notify users when terms change and then collect acknowledgement.

The top features CIAM services provide are

- **Social logins**
  Allow users to login via Facebook, LinkedIn, Twitter, Google, Amazon, etc.
- **Multi-factor authentication (MFA)**
  Email/phone/SMS OTP, mobile biometrics, behavioral biometrics, mobile push apps, FIDO, risk-adaptive and continuous authentication, etc. Simple SMS OTP is not secure and is not recommended.
- **Risk adaptive authentication**
  Evaluation of runtime environmental parameters, User Behavioral Analytics (UBA), and fraud/threat/compromised credential intelligence to match the appropriate authentication mechanism to the level of business risk or as required by regulations.

- **Account recovery mechanisms**
  When consumers forget passwords, lose credentials, or change devices, they need ways to get access to their accounts. Account recovery techniques include Knowledge-Based Authentication (KBA; but it is recommended to avoid this method as it is usually even less secure than password authentication), email/phone/SMS OTP (also not recommended), mobile push notifications, and account linking.

- **Inclusion of 3rd-party fraud and compromised credential intelligence**
  Runtime evaluation of internal or external cyber threat or fraud information, such as known bad IP addresses/domains, compromised credentials, accounts suspected of fraud, fraud patterns, botnet behavior, etc., for the purpose of reducing the risk of fraud at the transaction level.

- **Identity analytics**
  Dashboards and reports on common identity attribute activities including failed logins, consumer profile changes, credential changes, registration tracking, etc.

- **Business intelligence for marketing**
  Transformation of data about user activities into information for marketers.

- **Privacy and consent management**
  Explicit user consent must be received for the use of their information. Consumer account dashboards are common mechanisms for providing users with consent monitoring, granting, and withdrawal options. Compliance with EU GDPR, Canada's PIPEDA, and California's CCPA are notable drivers.

- **IoT device identity association**
  As IoT devices increase in popularity, consumers and business customer users will have greater need to associate their IoT devices with their digital identities. These identity associations between consumer and IoT objects will allow for more secure and private use of smart home, wearables, medical, and even industrial devices.

Widas ID GmbH, as part of the WidasConcepts group, develops and operates cidaas, a secure cloud identity and access management solution headquartered in Europe. cidaas was launched in 2015 and was able to achieve continuous growth to around 120 employees.

2 Product Description

cidaas is a full-featured CIAM SaaS solution by Widas ID GmbH. The solution is fully multi-tenant. cidaas offers various plans for businesses, which include packages for discrete ranges of numbers of users and devices. Enterprise licensing options are also available. Though primarily meant for cloud-based delivery, cidaas can be run on-premises by large enterprise customers.

cidaas allows for white labeling and seamless branding. Corporate customers can easily build portals for consumer self-registration. cidaas allows bulk identity import from LDAP. cidaas can interoperate with other CIAM and IDaaS solutions over OIDC. A mobile SDK allows customers wanting to do so to create their own apps, including adding their own MFA functionality.

Standard username/password authentication is available with cidaas as well as innovative passwordless authentication options. The solution supports traditional OTP methods, such as email/phone/SMS OTP. More than 15 authentication methods including FIDO are supported which allows Multi-Factor Authentication flows (MFA). cidaas has mobile apps for authentication and can do mobile push notifications. A wide variety of social logins can be used for registration and authentication, such as Facebook, Google, LinkedIn, Amazon, and Microsoft. cidaas interoperates with 3rd party authenticators, including Google Authenticator, and others which allow for utilization of built-in biometrics such as Touch ID, FaceID, and FIDO U2F. Voice recognition biometric authentication is also possible.

cidaas supports federated authentication and authorization protocols including SAML, JWE, JWT, OAuth2 (including the IETF OAuth2 Device Flow specification), and OIDC. These enable interoperability with other common services and many SaaS apps. cidaas supports delegated administration within the customer console. This feature enables to map even complex organization structures in customer relationships. A common example would be to give a B2B customer the possibility to self-manage the users related to the including administrative access to read and edit user information.

The latest versions of cidaas add eIDAS compliance for verified onboarding processes for employees and consumers alike. Officially issued ID documents, including passports and driver's licenses can be validated using the cidaas ID Validator app by scanning them, followed by face recognition and liveness detection. This data is compared to the photo on the ID document and functionality has been developed by cidaas to read the ID chip data (via NFC) for stronger validation on both mobile devices (phones, tablets) and laptops. The ID validator has been certified as eIDAS compliant (identity verification and AutoIdent).

Consumer identity solutions are increasingly under attack by fraudsters. cidaas utilizes the expertise and techniques of WidasConcepts' data analytics line of business to look for signs of attempted fraud and prevent exploitation within the cidaas customer network, particularly for banking and insurance customers. Fraud detection is enhanced by identity proofing and device fingerprinting functionality. cidaas smart MFA uses User Behavioral Analysis (UBA), based on geo-location, device fingerprint and more, as triggers for

step-up authentication.

Server-based bot detection counters increasing attacks from botnets, which are commonly used in credential stuffing attacks that come with Account Takeover (ATO) fraud attempts. Machine learning (ML) detection models are deployed, including recurrent neural networks and semi-supervised ML algorithms, assessing source IP, user behavior, and device fingerprints.

Compromised credential intelligence can be added in but is not enabled by default. Risk analysis and decisioning process information is viewable by customer organizations. However, as of now customers do not write their own authentication policies. A Security Dashboard is integrated in cidaas' admin UI to help customers secure their applications, the dashboard provides functionalities to monitor and manage security and fraud protection, as well as provides insights into the cidaas configuration of clients or the instance (wrong scopes on a client). The Security Dashboard does not yet allow customers to edit policies directly.

Progressive profiling is supported to gather growing insights into cidaas' flexible consumer profile storage during their identity lifetime. The system can respond to dynamic schema change requests and changes to consumer profiles can be configured to send alerts for confirmation. cidaas provides more than 25 identity analytics reports out of the box, which includes information on devices and browsers used, user locations, new vs. returning users, most active users, social logins used, MFA events, and login failures. On the marketing analytics side, cidaas can provide some insights about per-client and per-user API usage. For more detailed analyses, cidaas allows REST API access to customer activity logs from customer sites. Customers can then use other applications for data analytics.

GDPR compliance is a major concern for any company doing business either within the EU or with EU citizens. cidaas offers consent collection and management for its customers. The interface can host a user dashboard facility, where users can review and edit their consents for data use aligned with Kantara Initiative's Consent Receipt specification. Users can granularly select which attributes from social networks will be shared and revoke consent through the dashboard. Users can export their data, and the solution adheres to data deletion requests, as mandated by GDPR. The solution does permit the definition of family groupings and gives parents control over the use of their children's data.

cidaas can facilitate SSO to any on-premises or SaaS application based on OIDC and SAML2. This provides easy setup for many major cloud services. It can interoperate with Microsoft Azure AD or other IDaaS systems. Due to its support of REST APIs and Webhooks, it can allow integration with popular LOB applications such as big data / data analytics and CRMs, as well as key security infrastructure systems such as SIEMs.

The melding of consumer identities with consumer-owned devices is a high priority and growth area. This is reflected in both current cidaas capabilities as well as their roadmap. cidaas today allows consumers to associate certain types of devices, particularly door openers and cameras, with their cidaas-hosted identities. cidaas also facilitates some leading-edge consumer-centric use cases. By incorporating facial recognition from stationary cameras, on-location beacons, and Bluetooth technologies, cidaas customers can recognize, authenticate, track consumer physical locations, and push notifications to consumers' mobile devices. Most recently a "ticket management" feature has been added, allowing authentication and physical access (e.g., to a soccer stadium) for users and user groups based on issued tickets or loyalty cards.

cidaas operates in data centers within Germany. The micro-services architecture allows for rapid manual scaling and de-provisioning to accommodate heavy or unexpected loads, with auto-scaling. As of mid-2021, cidaas manages more than 150 million user identities. Additionally, cidaas asserts that it can process 250,000 logins and 250,000 registrations in parallel per second on a single instance. Upcoming releases are expected to allow customers to choose their IaaS providers and geographic locations for hosting, while adding high availability and failover options.

3 Strengths and Challenges

cidaas provides an easy-to-deploy CIAM or IDaaS solution. It offers many of the basic features required by many kinds of businesses today. The product evolved and benefited from their experience working with large prominent companies in Germany.

Mobile SDK, eIDAS compliance and the modern, scalable architecture are examples that Widas is constantly evolving the system to meet current and future requirements. The emphasis on incorporating IoT device identities with consumer identities shows that the vendor is aware of and responding to this important technical trend.

Widas is still a relatively small company mainly based in the European market. However, they customer base is constantly growing, they have plans to expand within the EU and Asia, and they do have a base of operations in India.

The service would benefit by adding 3rd party fraud/risk/threat intelligence integration capabilities and building in additional identity and marketing analytics. ISO 27001 and OpenID certifications demonstrate high performance and security standards. However, expanding to non-EU regions would be made significantly easier if internationally relevant certifications, such as SOC2 type 2, or CSA Star are achieved and made available to prospective customer organizations.

Strengths

- Easy to deploy and integrate with common SaaS applications
- Good consent collection and management capabilities
- Robust eIDAS compliance implemented within own code base
- Micro-service architecture allows for rapid and dynamic scaling and continuous deployment of service enhancements
- Forward-looking support for CIAM and physical access use cases
- Remote ID validation app facilitates consumer onboarding and stronger identity assurance

Challenges

- Need to promote GDPR-compliant, privacy-preserving fraud, risk, and threat intelligence with existing integrations among their customer base
- Small, but growing customer base and geographic presence
- No international certifications (SOC 2) for non-European markets available

4 Related Research

Leadership Compass CIAM Platforms - 80040

Leadership Compass Access Management - 80257

Advisory Note Identity Authentication Standards - 71106

Advisory Note Future of Identity Management - 71303

Copyright

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

KuppingerCole, 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.