cidaas

Buyer's Guide: Customer Identity and Access Management

What should be considered when choosing a CIAM solution?

Whitepaper

The Digitalization Effect
The world is transforming

About the Autor

Sadrick Widmann is the Chief Product Officer of cidaas, the first customer identity and access management solution completely developed and hosted in Germany. He knows and understands the requirements of a digitized world and helps customers build identity-based business models.

PROLOGUE

Everything today is becoming radically digital. Digital transformation is a buzz word that is heard often, and so is Digital Disruption. The rate at which new disruptive technologies are being introduced in the market is increasing day-by-day and is certainly changing the way we operate, including our personal and professional lives. This has given rise to new business models that are mostly data-driven & cloud-enabled and more importantly, customer-centric. And what play a fundamental role in such a customer-driven strategic business transformation are obviously, Customer Identities.

>The management of identities becomes a success factor

In a highly connected digital eco-system, managing millions of user identities, be it identities of employees or customers, i.e., storing and securing their identities and sharing them with appropriate consent across other applications pose technical and security challenges. Every point of interaction must be a consistent experience, while protecting consumers' sensitive data and complying with EU data protection regulations. But it is not only in the business-to-consumer (B2C) environment that delivery of the the right customer experience is important; it is also becoming increasingly established in the business-to-business (B2B) domian.
The IT market has responded to this change by introducing identity management solutions that can be easily integrated into existing IT infrastructures. There are two types: internal and external Identity and Access Management (IAM), the latter being called Customer Identity and Access Management (CIAM).

>Customer Identity and Access Management gears up business processes for the digital future

But what is the exact difference between IAM and CIAM? And which companies profit from such solutions? This guide gives you an overview of the differences and key features you should consider when choosing a CIAM solution.
However, we must have one thing in mind: an effectively implemented customer identity and access management system has become a must-have in the digitalization strategy of any company, regardless of its industry and size.

Hope you find this guide informative with interesting insights.
Happy Reading!
Sadrick Widmann

TABLE OF CONTENTS

>THE DIGITALIZATION EFFECT

> IDENTITY AND ACCESS MANAGEMENT IN GENERAL

> FACTORS TO CONSIDER WHILE CHOOSING A CIAM SOLUTION

> CIDAAS - CUSTOMER IDENTITY AS A SERVICE

> CONCLUSION

CUSTOMER IDENTITY AND ACCESS MANAGEMENT

In General

>Traditional IAM

Classic Identity and Access Management, or IAM in short, is a system for the Authentication and Authorization of all Individuals within a company.

The main function of IAM is to manage the identities, roles and privileges of the associated actors. Employees, freelancers, partners and all other stakeholders receive the right access to the digital resources of a company.

Based on "Need to Know“ principle, everyone has the accesses and privileges that correspond to their role in the company.

> The approach of a classical IAM

Conventional IAM solutions are developed with the following objec - tives:

- Verification of the identities of a known group of users
- Avoiding data protection violations through controlled access

This approach is effective as long as it involves the management of a defined number of users. Due to the digitalization effect and related networking, however, external stakeholders such as customers, suppliers, partners and even "things" are given their own identities, and demand access to apps, services and data. For example, it is common today for a customer or supplier to be able to manage their personal data in their customer account all by themselves.

In order to make access to sensitive data available outside the company, an external identity management system has emerged in addition to the internal identity management system. This is generally known as Customer Identity and Access Management, or CIAM, in short.

CIAM vs. IAM
Here are the differences

> CIAM as a technical enhancement of the classic IAM

CIAM changes and enhances the traditional IAM concept. Like before, technically oriented, modern identity and access management encompasses aspects such as the registration process and the collection and use of data and also forms the interface to marketing services in order to provide customers with targeted information.

CIAM solutions are developed with a focus on customer satisfaction, scalability and adaptability to constantly changing market trends and increasing security requirements due to increasing cybercrime.

This requires flexible workflows, extensive authentication procedures, high scalability, but also standardized processes to meet the growing legal and regulatory requirements.

> CIAM creates a 360° view of user data

In order for a CIAM solution to provide an all-round view of identities while maintaining a balance between marketing, security requirements and regulatory compliance guidelines, an out-of-the-box solution should include the following aspects:

- Access security using modern authentication procedures:
  The provisioning of sensitive data must be secured at all times. Modern authentication methods with biometric factors such as fingerprints, face scans, etc. should be available.

- Compliance:
  EU-GDPR-compliant consent management for compliance with data protection requirements.

- Scalability:
  The number of users can increase rapidly and immensely - a CIAM should be able to accomodate this.

CIAM vs. IAM

Here are the differences

- Integration:
  Seamless and simple integration into existing software enviroment.

- User Self-Services:
  Users should be given the provision to do simple activities such as the first registration or changing passwords by themselves.

- Social Login and Single-Sign-On (SSO):
  Enable simple and convenient login by providing social login, where the user can register/login using common social media provider accounts. The Single Sign-On (SSO) function gives users access to all services and eliminates the need for multiple logins.

- Standards instead of customizing:
  Choose a solution that relies on standards such as OAuth2 or OpenID Connect. Since many heterogeneous systems have to be connected to each other, a standardized procedure and no in-house development is recommended.

- Marketing functionalities:
  For a direct and personalized interaction with the customer.

The selection of a software solution for Customer Identity and Access Management, however, only makes sense after a precise analysis of your own business processes.

The million dollar question
Make or Buy

Especially when a company has its own IT department, the question often arises as to which services can be developed by its own team and which should be purchased. In the course of digitalization, the old topic of "make or buy" is gathering momentum again.

As a company, however, you should always ask yourself whether there are clear competitive advantages in developing an in-house solution. Especially if companies already have an IAM system in place, it looks tempting to add more functionalities further, on top of the existing solution. At the first glance, in-house developments often seem simple, but in the end it usually turns out that proprietary solutions cost more time and money and are not as effective as standardized solutions. When it comes to identity management, which is always closely associated with highly sensitive data, special attention must be paid to the aspects of security, data protection and authentication and the associated requirements. In this light, it is advisable to rely on experts.

> The following points speak in favor of using a standardized CIAM solution:

- Low Costs:
  The implementation of a standard CIAM software is uncomplicated and individual functions can be enabled shortly. A good CIAM solution always comes with ready-made SDKs so that your team can concentrate on configuring the solution and not on programming it.

- Highest security for sensitive data:
  A CIAM manages highly sensitive data that must be protected from unauthorized access. When using a standard solution, it is the provider's responsibility to ensure that the latest security guidelines and certificates are always adhered to and that standards such as OAuth2, SAML, etc. are used.

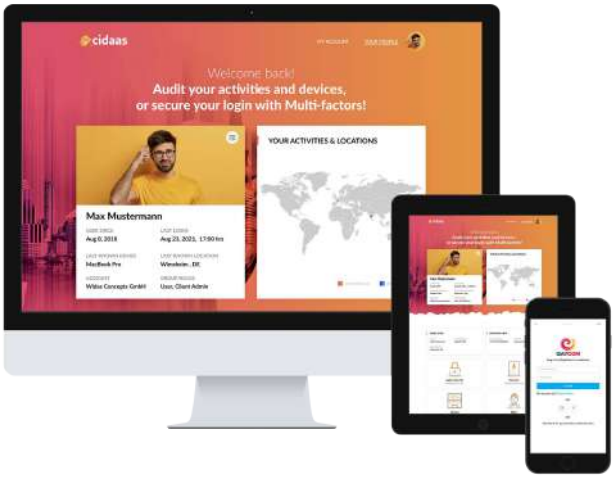
The million dollar question

Make or Buy

- High user acceptance:
  Standard CIAM solutions use the most common and user-friendly login and authentication methods and are therefore highly preferred by users.

- Scalability:
  Your business is not static - user numbers can grow rapidly. When using an external CIAM solu - tion, you do not have to worry about accomodating new users, but can leave it to the provider to manage it all.

- Expert support:
  Most vendors provide 24/7 support to their customers. The handling of questions or incidents is therefore not in the hands of your own company, but can be outsourced. This in turn relieves the burden on the company's own help desk, if one exists.



The advantages of an existing, mature Identity Management System usually outweigh those of an in-house developed product

Factors to consider while choosing a CIAM solution

> CIAM is not just CIAM

The CIAM market has grown strongly in recent years and has become more complex. Finding the right product is not always easy, because one thing is clear- CIAM is not just CIAM. There are many differences with regard to individual functionalities offered and the technologies used. The topics Multi-Factor-Authentication (MFA) and Single Sign-On (SSO) still harbour a lot of growth potential. Since each product has its own focus areas and goes hand in hand with a wide variety of function sets, the "must-haves" and "nice-to-haves" for the company's own processes must be crystallized.

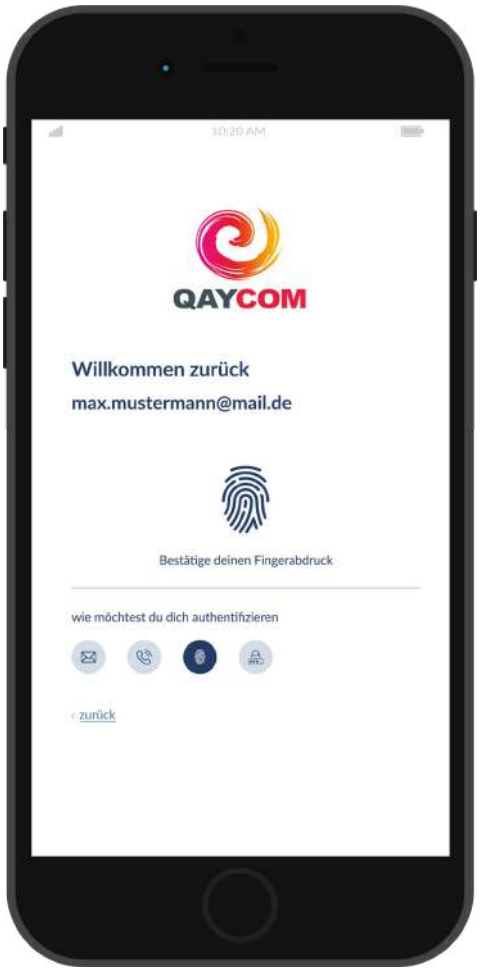
In the following section we present the functionalities that are absolutely necessary for a CIAM system in order to advance the digital future of your company.

Onboarding and Authentication of users

The primary goal of a customer identity and access management system is to create a unified digital identity to deliver a consistent, personalized user experience across all channels. To achieve this goal, the login and authentication processes should be as convenient as possible for the user.

>Password-less Login / Social Login for user registration and login

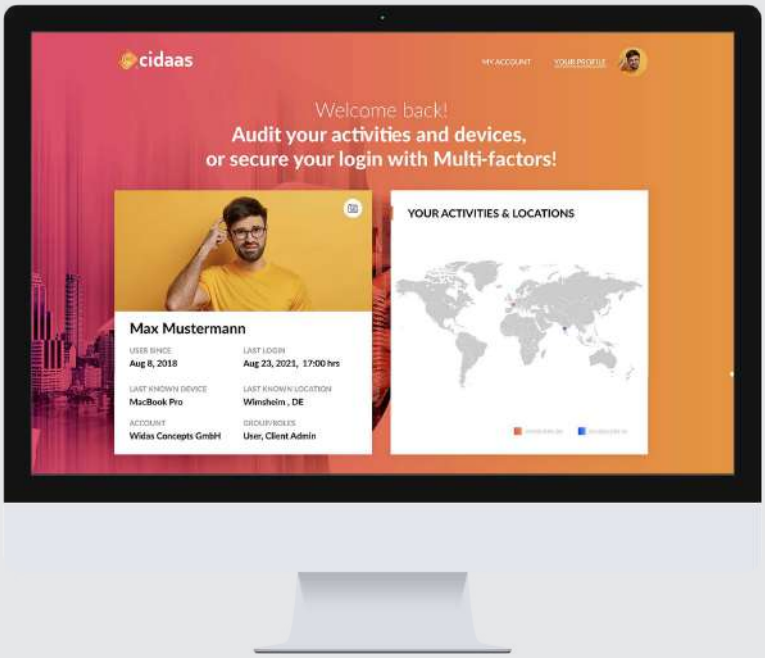
A good CIAM solution should support all common identity providers. In the business environment Office 365 or Active Directory and in the consumer environment all common social media platforms (Google, Twitter, Facebook,...) should be supported. Passwordless authentication could be achieved using biometric factors such as touch ID, voice, face or by using conventional methods such as E-Mail, SMS or FIDO-based verifications.



>Modern multi-factor authentication methods

The use of a second authentication factor is intended to ensure that only the real owner of the account has triggered an activity. The prompt to key-in a second authentication factor could be triggered either at each login or only in case suspicious activity is detected, i.e., when it is assumed that it was not the actual account owner who initiated the activity. These anomalies should be detected by the CIAM system through behavior-based clustering such as location data or common device usage. The most secure variant of multi-factor authentication is the use of biometric features (fingerprint, face scan,...) to identify a person.

Authentication methods - The choice is crucial



Cidaas offers a variety of modern, passwordless login options and ensures secure authentication.

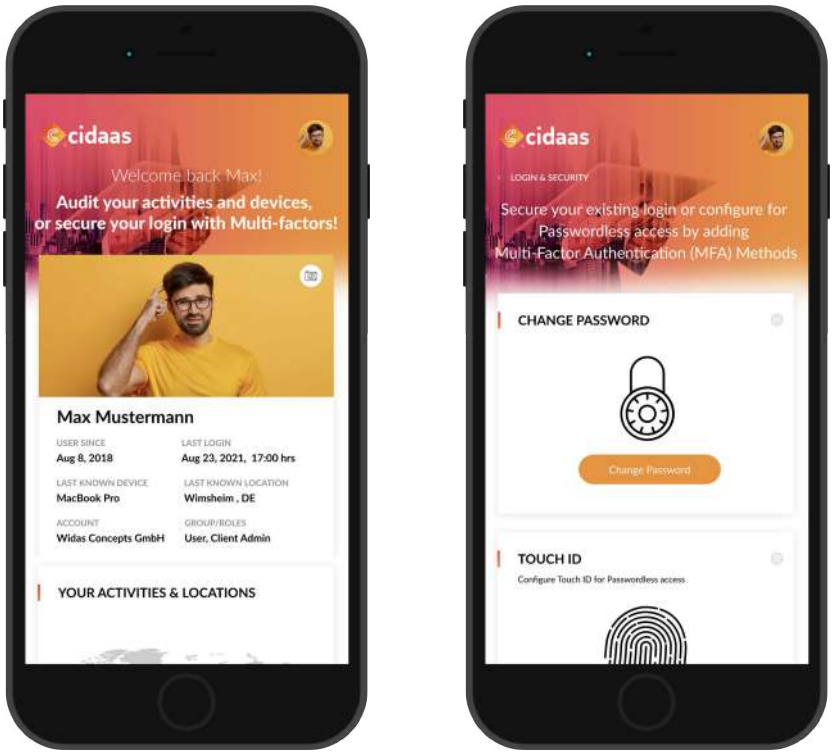
Discover now

> Single Sign-On across all company channels

Single sign-on or SSO, ensures a consistent login experience. The customer logs in once and can use all the digital channels of the company without having to log in again or indi - vidually into each of the channels.

> User-Self-Services for managing user accounts

User self-services enable customers to manage, update or delete their stored data all by themselves.



Data Protection and Security

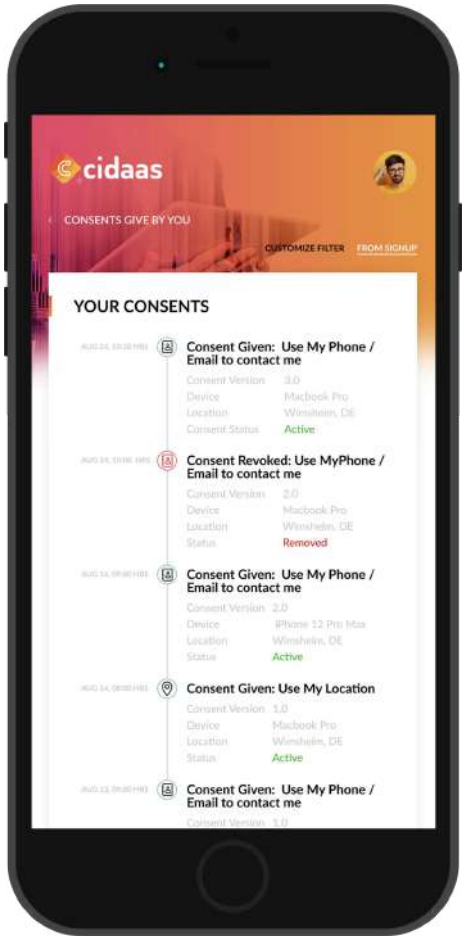
Increasing cybercrime and privacy requirements have made the topic “security” a top priority. Today's digital enterprises therefore do enough to create a centralized access layer for all data.

> Regional, industry-specific or operational data protection regulations

A CIAM solution helps to implement the various data protection regulations and provides the technical prerequisites needed to manage consents and data usage regulations centrally, in one place. Be it EU-GDPR or other internal compliance requirements, the CIAM solution should provide the necessary tools.

> Handling personal data

The provisions of the EU-GDPR mandate that personally identifiable information (PII) should be allowed to be viewed and edited at any time. If updates or changes, for e.g. passing on data to third parties, are necessary, the customer is pro-actively requested to provide his consent. In addition, care must be taken to ensure that the user's personal data is made available to the user or can be deleted. When using a CIAM, the users themselves have full control over their sensitive personal data and can view and revoke consents at any time. At the click of a button, all the data that is stored at the given point in time can be made available.



> Securing Identities

The safeguarding of identities is an essential component of a CIAM system. This is ensured by secure data encryption and the triggering of two-factor authentication in the event of suspicious activities.

> Identity standards used

While evaluating an identity system, care should be taken to ensure that standard protocols such as OAuth2 or OpenID Connect are used for authentication and authorization.

Integration and Scalability

Since IT infrastructures today are very heterogeneous in most cases, the integration of an additional software component should be made possible without extensive programming efforts. Furthermore, scalability plays an important role, especially in times when digital value-added services are the main focus.

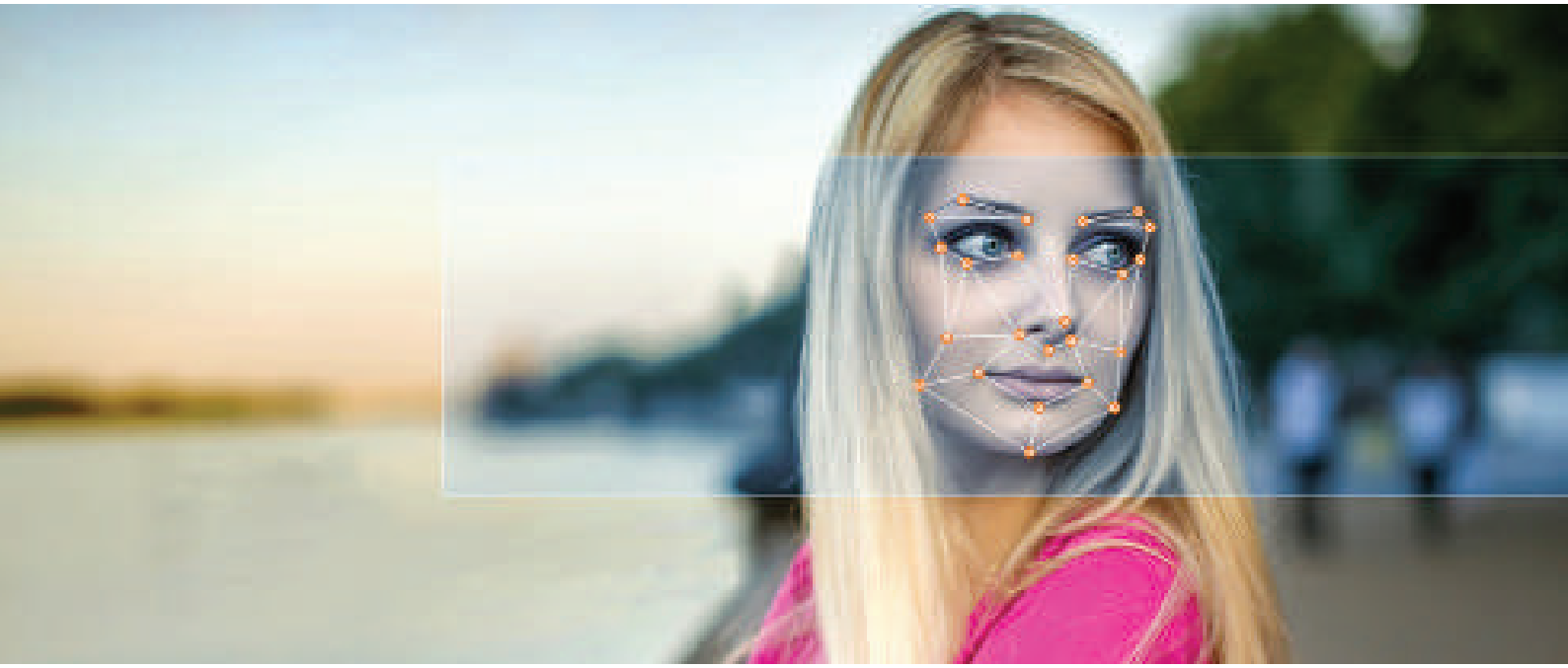
> Integration into existing IT systems

Regardless of how the current IT environment is operated, a CIAM solution should always provide open APIs to ensure easy technical integration of the identity solution into the existing business software. Often, ready-made SDKs (Software Development Kits) are also available to quickly integrate all existing applications.

> Expected user base

The growth of organizations is often difficult to predict. When selecting a CIAM provider, it is important not only to ensure that the service performs well during peak usage, but also to confirm that it can be scaled to support an almost unlimited number of users.

cidaas - Customer Identity as a Service



> The very first solution completely developed and hosted in Germany for efficient customer identity and access management.

As the previous chapter have shown, many factors play a key role in choosing an identity management solution.

Widas ID GmbH, based in Wimsheim, Germany, has been offering "Software made in Germany" since 1997 and has developed a highly scalable and seamlessly integrable customer identity and access management with the cloud service cidaas. Based on the OpenID Connect and OAuth2 standards, cidaas provides the highest level of security for interface authentication. The cloud service is developed and hosted in Germany and has been awarded the "Software hosted in Germany" seal of quality. Strong multi-factor authentication methods (MFA), including biometric ciphers (fingerprints, face scans,...), are used to distinctly verify user identities.

IN A NUTSHELL

CIDAAS - CUSTOMER IDENTITY

Cidaas contains out-of-the-box a comprehensive range of functions, which includes the following features:

- Multi-Factor-Authentication
- Social Login
- Single Sign-On
- Highest access security through integrated fraud and suspicion case detection
- Data governance through EU GDPR-compliant consent management
- Securing your portals and Web APIs through the standards OAuth2 and OpenID Connect
- User Self-Services
- Group management (B2B module) for simple role and privilege man - agement of your business partners
- Continuous scalability according to your requirements
- Modular Microservices architecture ensures maximum agility
- Different service packages that cater to individual requirements
- 24/7 Expert Support

cidaas thus offers flexibility, scalability, security and transparency and can be seamlessly integrated into any existing software landscape. The cloud software is available in 5 service packages to cater to individual requirements.

The cidaas entry-level service package is free of cost.

Get in Now

CONCLUSION

The question of whether to use identity management or not will no longer arise for most companies in the future. Regardless of whether customers, partners, employees or even "things" are involved- everything is digitally networked and a smooth and authorized access to applications, services and data as well as compliance with data protection regulations is expected.

> A customer identity platform secures your identities

With Customer Identity and Access Management, you not only reliably secure your identities and channels and thus minimize security risks, but also build the foundation for all data protection-relat - ed topics with regard to the EU-GDPR.

Don't wait any longer and schedule a free consultation - we will be happy to provide you with our expertise for your digital transformation.

In the age of digitalization, the protection of digital identities and portals has become immensely important, because every organization now has a digital presence in some form or other.

With cidaas, we provide companies with powerful software that provides all relevant security requirements with regard to authentication and authorization out-of-the-box, as well as guarantees the legally compliant storage and provisioning of personal data.

Sadrick Widmann . Chief Product Officer cidaas

Book your preferred date/time now

WIDAS ID GMBH

Maybachstraße 2
71299 Wimsheim
Tel: +49(0)7044 95103-100
Email: contact@widas.de

cidaas

Phone: +49 (7044) 95103 – 100
Mail: sales@cidaas.de
Web: www.cidaas.com