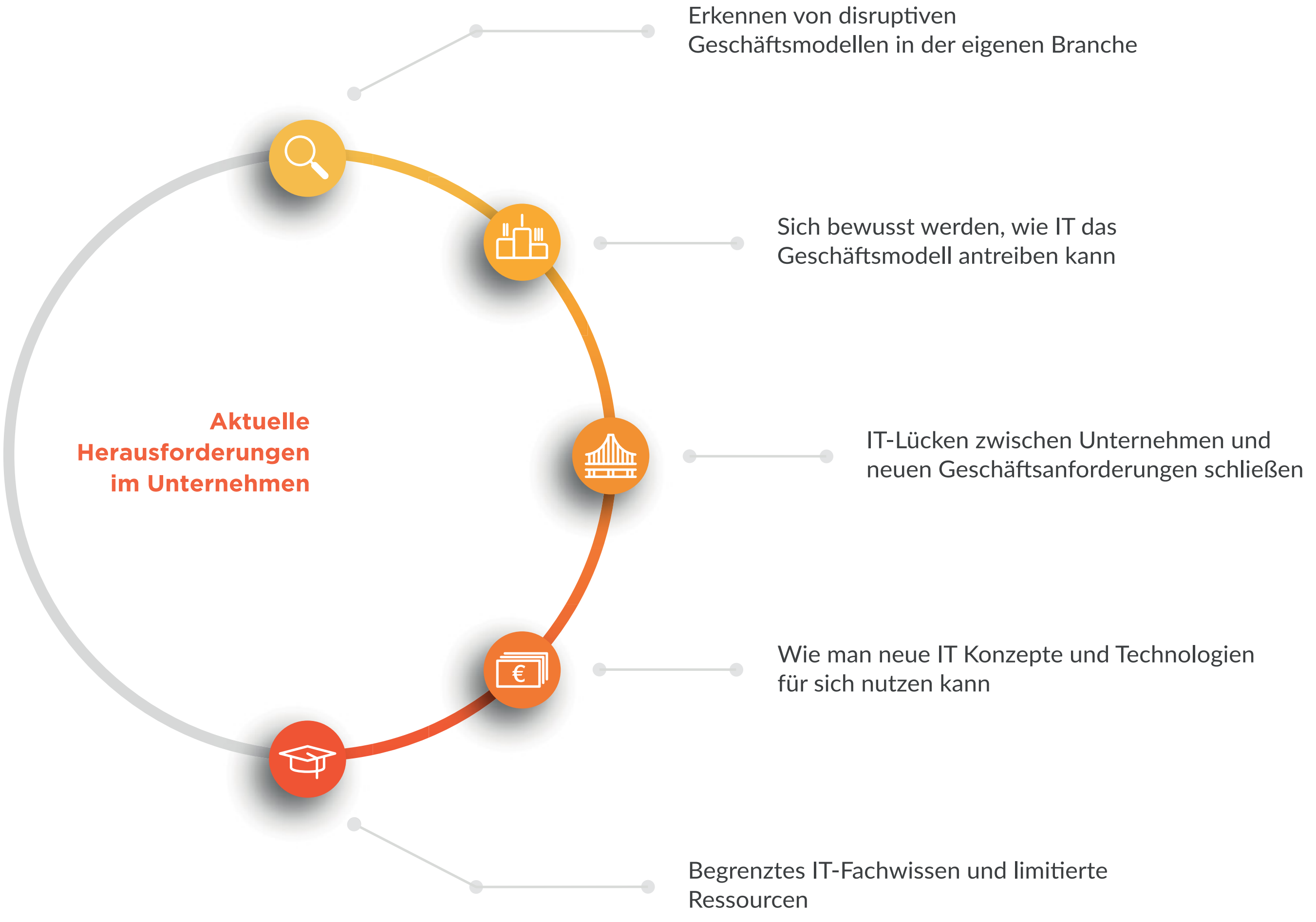
cidaas

CIDAAS – TECHNICAL INTEGRATION

Innovative Customer Identity Management – secure, fast and unmatched

Whitepaper . October 30, 2017

CIDAAS: MOTIVATION AND VISION


Aktuelle Herausforderungen im Unternehmen
Erkennen von disruptiven Geschäftsmodellen in der eigenen Branche
Sich bewusst werden, wie IT das Geschäftsmodell antreiben kann
IT-Lücken zwischen Unternehmen und neuen Geschäftsanforderungen schließen
Wie man neue IT Konzepte und Technologien für sich nutzen kann
Begrenztes IT-Fachwissen und limitierte Ressourcen

Today, users need **comfortable, efficient, secure, flexible, location-and-device-independent access to digital services** - IT resources or cloud-based services accessible over APIs, applications or devices.

If companies don't provide those digital services it could be a stony path to sustain in a digitalized world.

The software technology stack changes dramatically thanks to JavaScript, web services, mobile apps and the Internet of things. Software is very distributed today.

At the same time, the possibilities for user identification are continually changing - biometric procedures are top in the race.

The expectations of the customers and digital service providers are huge:

- Secure and easy to use authentication;
- **Once** authenticated, the customer wants to access **all** the company's digital services;
- The service provider wants to control and authorize the service access on a fine-grained, and in a personalized way;
- Fraud attacks should be detected;
- The service provider wants to know the customer in detail across all channels to personalize the access and to continuously improve the offered digital services.

Our answer therefore is cidaas!

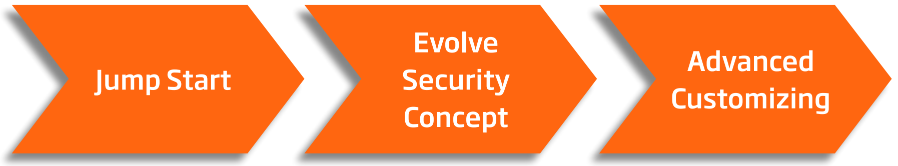
cidaas (customer identity as a service) - is a cloud based service that abstracts how users authenticate to applications. Developed by WidasConcepts, our Customer Identity solution provides out-of-the-box social login, registration and single sign on components. Built using OAuth 2.0 and Open ID connect standards, cidaas is designed to offer scalability, security, transparency and flexibility to manage customer identities and data.

For developers and architects OAuth2 and OpenId Connect are de-facto standards for security protocols and enable easy technical integration of cidaas into the business software.

CONTENTS

CIDAAS: TECHNICAL INTEGRATION

With cidaas, it is only a matter of asking the right questions to choose the best suited plan for your business and to know what is involved in integrating a such a solution. The three basic steps are outlined here:



> Jump Start

Connect your first app to see how easy it is to connect with cidaas and get in touch with the various options cidaas provides.

- Configure Social Login providers, if needed;
- Create one App to enable access for one client;
- Use appropriate SDK or web-APIs (docs.cidaas.de -> Developer Guide) to:
  - Connect with cidaas;
  - Protect your resources.
- Implement basic webhooks to recognize new users and logins.

> Evolve Security concept

Once jump start is done, security considerations might be essential to give client apps access to your resources and you may require an additional level of role based security.

- Define scopes: canonical subject + verb expressions are recommended;
- Apply scopes: tag your resources with required scopes and grant clients access to specific scopes;
- If some of your systems require role based security, go ahead and apply the same in admin dashboard.

> Advanced Customizing

One of the next steps are following tasks which you most likely setup once and apply accordingly. While custom layouts are optional, at least legal setup is highly recommended. cidaas links with your terms and privacy policies which users shall accept when registering.

- Define Custom Layout(s) for login and registration;
- Prepare Terms of Use and Privacy Policy Links (+) (can be configured in the App settings);
- You may use (+) custom fields to have additional info at hand;
- Enable and promote (+) 2-FA resp. (+) passwordless Login Options;
- Implement advanced (+) webhooks to KYC.

CIDAAS: SELECT PLAN

cidaas plans are built on required feature-sets, business maturity and favourable prices.

cidaas free	This plan is meant for evaluation and startup businesses with the comprehensive feature set of cidaas. It could be used in real life business scenarios, but since it is free we grant very limited service levels
cidaas essentials	A plan which could fit best for small businesses, ideally as a starter to grow their business
cidaas standard	Standard allows to implement a broad usage of use cases on an excellent service support during business hours.
cidaas free	Pro plan fits best for businesses who are going to broaden their digitalized channels and/or expecting lots of users and systems to interact with. This plan enables 24x7 support
cidaas enterprise	Enterprise plan is recommended for large businesses with integration of legacy authenticators.

As a quick guide, these selected few questions can decisively lead you to the Plan that would best suit your business. You can even simply get started with the free plan!

Questions	Cidaas Free	Cidaas Essentials	Cidaas Standard	Cidaas Pro	Cidaas Enterprise
How many end points to I have? No. of Portals, mobile Apps, Long running Processes?	Max 10	Max 4	Max 6	Max 10	Unlimited
Which and how many Social Logins would I like to use?	Max 2	Max 2	Max 4	Unlimited	Unlimited
How many users do I have?	500	2000 (1*50 for 50k users)	5000 (n*50 for 50k users)	1000,000 (n*50 for 50k users)	Contact us
Do I plan to use JWE Tokens?	yes	No	No	Yes	yes
Do you plan to integrate with your LDAP?	No	No	No	No	Yes
Do you plan to have multi factor authentication?	Yes	No	Yes	Yes	Yes
Which Support Level do you need? Basic, Business Hours, 24x7	Basic	Basic	Business hours	24/7	24/7

Note: All of the cidaas plans are detailed here complete with the feature list: www.cidaas.com/pricing

FAQ

What is SSO and how is it supported?

The Single Sign On (SSO) principle that allows users to access different services with only a single login – this is possible because cidaas internally generates different access tokens for each of the different services, facilitating the different app-scopes.

What kind of preparations do I have to make (setting up an authorization model (scopes, roles), guidelines for URLs, etc.)?

Initially the company decision makers together with the technical team gather requirements that fundamentally answers the questions:

1. What resources must be protected?
2. Who must be allowed to access them?
3. What is the functionality scope of the several business applications? – does the application involve interaction with users? etc.

This means, to set up an authorization model for a business, achieved by defining the scopes and roles in the cidaas admin dashboard.

OAuth2 Scopes

The cidaas scopes conform to the OAuth2 standards which is the essential access management element. It is introduced to restrict access to resources (e.g. web services, web pages) to clients.

Some advice on on how to use scopes:

1. Define scopes canonically: <product>:<entity/service>:read or write.
2. Since resources get tagged with scopes, you can easily cross check if scope are robust.
3. Please do not create App definitions for clients and assign plenty of scopes. Cidaas asks users of public apps for consent for every scope required. This could be a mess for users.

Advice on how to use roles:

1. In cidaas you can manage roles and assign roles to users in order to restrict accessibility/ visibility of entities/objects even if you are able to access the resource server.
2. JWT access_token contains the roles of user
3. Most commonly, roles have to be evaluated by the business software ideally by using a separate framework.

Guidelines for URLs

Basic guidelines for the structure of the URLs of the different service portals must be laid. What the base URL should be, and so on.

How to implement webhooks

Cidaas provides a well-known approach to integrate with business software just by implementing webhooks. Business software can act in case a particular event occurs.

Need to define what business specific actions must be executed at the time of certain events - for e.g. when a new user registers, logs in, etc. webhooks are triggered by the cidaas system which must be handled appropriately in the business logic – be it create an enriched user profile using his social details, or be it delighting an active customer with targeted offers. For information on (+) cidaas webhooks.

We are happy to guide you further with specific business requirements. Because once this is clear, integrating cidaas is a matter of only a few days. Your existing business can continue as normal and your corporate brand will remain the same!

What is JWT and why should I use it?

JWT (Json Web Token) is an open standard that defines a compact and self-contained way for securely transmitting information between parties in the web as a JSON object. This Token can be verified and trusted because it is digitally signed using another standard JWS (Json Web Token Signature). In the payload of the token could be placed further information in self-defined fields, which content can be decrypted transferred using a further standard JWE (Json Web Encryption), see below.

JWT is used in the Web as standardized way to realize SSO and a secure transfer of information between parties (API consumers, applications, …).

When do I use JWE?

When there is a need to pass sensitive/private information as payload in a token, then to achieve a secure level of protection from attackers, there is a need to encrypt and guard the claims data using JWE - JSON Web Encryption.

Why do I need to define multiple apps?

Depending on each business scenario, there may be several applications that need access to the resources that must be protected. And where clear identification of the logged in user is important to establish.

- Front end web applications to which customers login;
- Services provided via mobile application (iOS, Android, Windows Mobile) with the same user base / larger user base;
- Web application portals to which distributors and sales and partners login.
- Corporate internal network to which employees login;
- There could be service based applications which do not involve user interactions.

Each of the several application scenarios require a separate client/app to be defined in the cidaas system. This is because, each of these clients can have specific scopes defined – for e.g. the service based app will not have the "register" scope. There could be different redirect locations to be defined in each case – as to where the user must be redirected to after logging in.

These are individual App-level settings which can be configured in the cidaas Admin Dashboard.

Who should get access to the admin dashboard? How can I restrict the permissions in the admin dashboard? Are there specialist admins and tech admins?

The cidaas Admin dashboard is user friendly and designed to be a central management console of all the cidaas services. The technical team member, who has a fair understanding of the IT landscape of your business can be the primary admin, who can in turn allocate/invite other team members as secondary admins, giving them full/ restricted access.

This decentralized administration approach aka delegated Admin can help a growing organization simplify their user management workflow by giving subordinate accounts access to create, edit, and further manage various user accounts throughout the organization. For example: an organization wishing to grant specific access to various departments: IT Support would be able to view, edit, and delete all organizational accounts, while Customer Support would only have access to customers.

Which APIs can I use from cidaas? Who should use them?

cidaas API service is a REST-like interface, supporting multiple environments so that developers can easily use them in their applications. The APIs allows you to manage every aspect of your cidaas account, or to build your authentication UI manually. For e.g. you can use the cidaas API to automate the configuration of your user environments or for runtime tasks such as user creation. For the API documentation: https://api.cidaas.de/

What do the cidaas scopes mean and who / which app should/ should not receive these scopes?

Cidaas scopes are nothing but the oAuth2 standard based scopes that define authorization for a particular app. Does the application functionality require read access to the user information? Write/update authority to the user profile? Separate scope to delete, and so on. For e.g.: (Service based app should not be allowed to register). There are 4 basic scopes that cidaas offers by default - cidaas:register , cidaas:login , cidaas:userinfo and cidaas:userupdate. More can be defined using a canonical representation.

A great use of scope is to selectively enable access to client app based on the functionality needed. For example, Google offers a set of scopes for their various services such as Google Drive, Gmail, YouTube, etc. This means apps that need to access the YouTube API won't necessarily also be able to access the user's Gmail account.

WIDASCONCEPTS GMBH

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

cidaas

Tel: +49(0)7044 95103-100
Mail: sales@cidaas.de
Web: www.cidaas.com