cidaas

CIDAAS - SECURITY

Security. Comfort. Value Add.

Whitepaper

CIDAAS: SECURITY - COMFORT VALUE ADD

Abstract

Today, users need secure, convenient, location- and device-independent access to their company's IT resources or cloud-based services. Digitalization makes the identification of a person on all channels one of the pivotal factors that determine the success of a business. Identification is crucial:

- to achieve a reliable personalized communication to the user;
- to ensure **secure access** to the resources respectively of the company and the user;
- for recognizing customers in order to provide customer-specific services and to address them personally.

cidaas, our Customer Identity Management is the solution designed to optimally meet these requirements and generate invaluable value add for businesses.

- How do we establish security?
- How reliable is the identification of the person?
- What do we offer in the context of the "user profile" for the user and the company?

These are the questions that are covered in this Whitepaper.

CIDAAS: HOW DO WE ESTABLISH SECURITY?

Cidaas is standard based and built using tested, verified identity standards, including - OAuth2 (+), OpenID Connect (+) and JSON Web Tokens (JWTs) (+)- all of the common and most popular industry standards used worldwide. Businesses can easily implement the solution in their existing IT systems to shield their own applications and APIs.

> Detect and Prevent Fraud and Anomalies

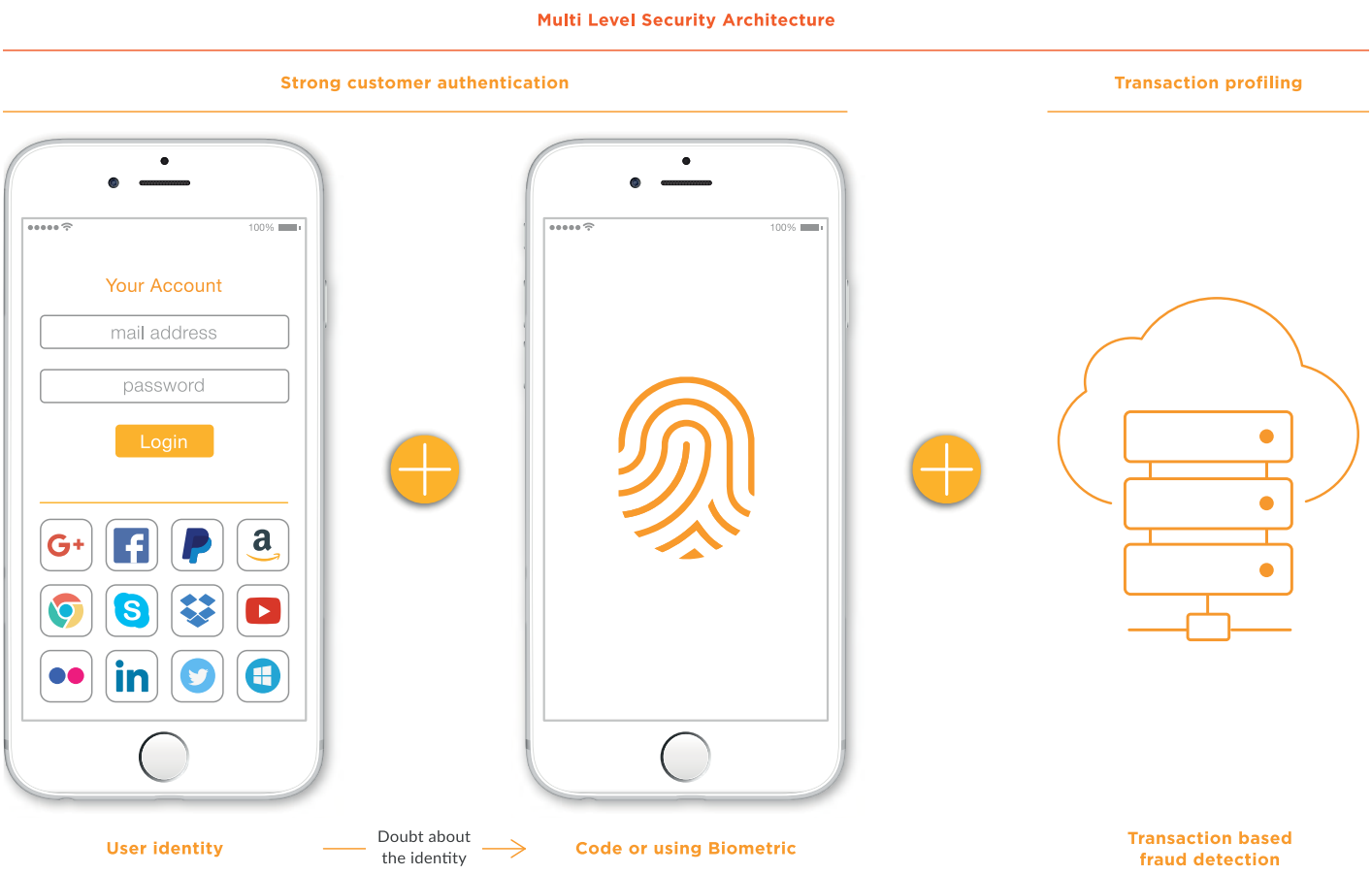
With cidaas, security is a default and is ensured in various ways. The primary goal is to keep the **protected resources** safe. So, even if a hacker got hold of the user's credentials somehow, he cannot access the protected resources.

The cidaas-check is present at every transaction, which uses contextual strategies which includes device changes, user location, access times, access points and much more.

On top of these strategies, machine learning algorithms and AI built into the cidaas security core, mitigates potential attacks and can autonomously by deactivating access of a user session, sends intelligent real-time alerts to the user, administrators.

> Multi factor Authentication

Strong fool-proof verification of identity with the cidaas Multi factor Authentication (+). Verifications are made mandatory depending on the sensitivity of the access request. Cidaas is the only product in the market that offers **advanced biometric techniques** for identity verification - Face Recognition, Voice Recognition, Touch ID, Pattern recognition, Smart Push. Of course, other common methods of verification using OTP sent via SMS, voice computer or Email are also supported.



> Password Complexity

Strong passwords can be enforced with the five levels of password complexity (+) , as well as custom rules implementing OWASP recommendations (+).

> Role, Scope and Group based access control

- **Scopes** have become a standard with OAuth2. Scopes allow you to control access of a client app to your web resources, e.g. Web-APIs, Portals. Cidaas supports all OAuth2 and OpenID security flows;
- Using **roles** a company can set and evaluate access control in a user centric way, besides the client centeric scopes concept of OAuth2;
- **Groups** are introduced to manage users efficiently, especially management of users of business customers can be delegated, which increase the security by default. These groups shall be used to allow/deny usage of a client app and can be used to evaluate access control in a user-group centeric way besides the scope concept OAuth2.

> Secure and reliable company Infrastructure

WidasConcepts and all of its DataCenter partners are ISO27001:2013 certified. Cloud services are hosted in Germany: Responsible handling of customer data in accordance with the German Data Protection Act.

Highly automated infrastructure ensures that systems are up to date at any time. For instance, security patches are applied rapidly without any manual intervention.

CIDAAS: HOW DO WE ESTABLISH SECURITY?

Cidaas identity service is architected with customer in mind. Safeguarding identity is critical and all data communication over network is encrypted. Account verification involves:

Behavioral Analysis: Access tokens issued for users, will be monitored using advanced Big Data Technology and can thus be clearly assigned to a user respectively potential fraudsters shall be recognized.

Opt-in: After successfully registering, the user receives an opt-in Email or SMS from the system. The cidaas system automatically generates unique but temporary links and codes and establishes communication with the user. Once the opt-in gets executed user is guided to a landing page, cidaas notifies the business software, all in one go.

User De-Duplication: Our analytics tools learn from the user profiles and recognize duplicate user profiles, during the registration itself. Only a single identity of the user is stored.

CIDAAS: WHAT DO WE OFFER IN THE CONTEXT OF THE "USER PROFILE" FOR THE USER AND THE COMPANY?

cidaas delivers the right balance between **Security and User Convenience.**

> For the customers:

- Ease of use via the self-service portal, where users can
  - Edit password/profile information
  - Configure advanced **passwordless Authentication / Multi Factor** verification methods (voice, face, pattern recognition, Touch-ID, TOTP, Smart-Push, IVR, Email, SMS and Backup codes)
  - Link/unlink accounts created using different providers
  - Overview of activities – date and time of login, and other login related activities such as when the password was changed, when the email was verified, when the Admin activated the account, when the user signed out, when the email address changed, etc.
- SSO: End users can login using a single identity across all channels and services of the company.

> For the company:

- Easy to operate administrator console (+) with a comprehensive set of configuration options and fine grained administration access levels.
- cidaas Webhooks: Advanced Event handling through the use of Webhooks.
- Custom Fields in the user registration: cidaas offers its customers a multitude of freely specifiable custom fields for capturing varied customer data.
- Optional Integration into your existing AD/LDAP systems: cidaas offers the possibility to integrate LDAP systems as login provider. Initially with the option to integrate employees and legacy systems and eventually get a smooth transition to the defacto Standard OpenId-Connect and OAuth2.
- Insights: Data from diverse Social Providers give insights on customer interests, hobbies, behavior pattern, user content, activities, demographic information, media preferences - cidaas transforms this information into useful knowledge for your business!

CIDAAS: VALUE-ADD

With cidaas Customer identity and access management company gets even more features

- For Banks cidaas provides a pre-built PSD2-Developer portal to allow access to Bank-APIs by 3rd parties.
- cidaas secures access to buildings and rooms by using exactly the same identity, credentials and biometrics.
- cidaas provides digital consent management. This allows companies to get consent for privacy policies, terms of services while registration and login as well as action-based consent to be integrated in your business software.
- Since cidaas works heavily in various IoT security initiatives, cidaas encourage companies to manage IoT devices of users.

CIDAAS: SUMMARY

At cidaas, we have built an innovative security product so that customers can take advantage of modern features designed to make protecting users and businesses hassle-free. We have based the entire product, its features and its processes on security best practices. Our systems are compliant with industry standards, clearly demonstrating our ongoing commitment to security and privacy.

WIDASCONCEPTS 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