

CIDAAS - SICHERHEIT

Sicherheit. Komfort. Mehrwert.

Whitepaper



CIDAAS: SICHERHEIT - KOMFORT MEHRWERT

Prolog

Die Benutzer benötigen heute einen sicheren, komfortablen, orts- und geräteunabhängigen Zugang zu den IT-Ressourcen ihres Unternehmens oder Cloud-basierten Diensten. Mit der Digitalisierung wird die Identifizierung einer Person auf allen Kanälen zum Schlüssel des Unternehmenserfolgs.

Identifikation ist hier entscheidend, um...

- zuverlässig und personalisiert mit den Usern zu kommunizieren;
- um **sicheren Zugriff** zu garantieren, sowohl auf die Ressourcen des Unternehmens als auch des Endnutzers;
- um Kunden zu erkennen, und ihnen maßgeschneiderte Leistungen in einer individuellen Ansprache näherzubringen.

Cidaas, unsere Customer Identity Management Lösung ist dafür gestaltet, dass diese Anforderungen optimal erfüllt werden und einen unschätzbaren Mehrwert für Unternehmen generieren.

- Wie stellen wir Sicherheit her?
- Wie verlässlich ist bei uns die Identifizierung der Person?
- Was bieten wir hinsichtlich des User-Profiles für den Benutzer und dem Unternehmen?

In diesem 'Whitepaper' erfahren Sie alles rundum diese Fragen.

CIDAAS: WIE STELLEN WIR SICHERHEIT HER?

Cidaas setzt modernste und zukunftsweisende Technologien ein und basiert auf getesteten, verifizierten Identitätsstandards, wie - OAuth2 (+), OpenID Connect (+) und JSON Web Tokens (JWTs) (+) - den weltweit gängigsten und am meisten geschätzten Industriestandards. Unternehmen können die Lösung einfach in ihre vorhandenen IT-Systeme implementieren und damit ihre eigenen Anwendungen und APIs schützen.

> Betrug und Anomalien erkennen und verhindern

Bei cidaas ist Sicherheit die Norm. Ein Qualitätsstandard, der auf verschiedene Arten erreicht und sichergestellt wird. Dabei ist das Hauptziel **geschützte Ressourcen** sicher zu halten. Also, selbst wenn Hacker an Nutzer-Login Daten gekommen ist, kann er auf die geschützten Ressourcen nicht zugreifen.

Der Cidaas-Check ist bei jeder Transaktion aktiv, basierend auf einer kontextbezogenen Strategie werden Änderung der benutzten Geräte, Benutzerstandort, Zugriffszeiten, Zugriffspunkte umfassend - in Millisekunden - geprüft.

Zu dieser Sicherheitsstrategie gehören weiter, die von cidaas in den Sicherheitsmodulen integrierten maschinellen Lern-Algorithmen und KI. Hiermit können mögliche Angriffe verhindert, und eine Benutzersitzung autonom deaktiviert, werden. Gleichzeitig geht an den User und die Administratoren eine Warnung in Echtzeit raus.

> Multi-Faktor-Authentifizierung

Starke Verifizierung der Identität mit der cidaas Multi-Faktor-Authentifizierung (+). Abhängig davon wie sensitive oder kritische Zugriffe sind, werden zusätzliche Authentifizierungen unerlässlich und verpflichtend. Das fortschrittliche biometrische Cidaas-Verfahren zur Identitätsprüfung per Gesichtserkennung, Spracherkennung, Touch ID, Mustererkennung, Smart Push - bietet hier als einziges Produkt am Markt diese Lösung an. Selbstverständlich werden auch andere gängige Verifikationsmethoden mit OTP, die per SMS, Sprachcomputer oder E-Mail versendet werden, unterstützt.

Starke Kundenauthentifizierung

Transaktions-Profilung



> Passwort-Komplexität

Starke Kennwörter können mit den fünf Ebenen der Kennwortkomplexität verstärkt (+), sowie mit benutzerdefinierten Regeln, die OWASP-Empfehlungen implementieren und erzwungen werden (+).

> Role, Scope and Group based access control

- **Scopes** sind zu einem Standard mit OAuth2 geworden. Mit Scopes können Sie den Zugriff einer Client-App auf Ihre Webressourcen steuern, z.B. Web-APIs, Portale. Cidaas unterstützt alle OAuth2- und OpenID-Sicherheitsströme;
- Neben dem kundenorientierten Konzept (Scopes von OAuth2), kann das Unternehmen die Zugriffskontrolle über **Rollen** auch benutzerorientiert einstellen und bewerten;
- **Gruppen** werden eingesetzt zur effizienter Benutzer-Verwaltung, besonders durch delegiertes Nutzer-Management von Geschäftspartner wird die Sicherheit deutlich erhöht, und damit auch qualitativ die Sicherheitsnorm. Gruppen helfen weiter dabei, die Nutzung von Client-Apps freizugeben oder zu verweigern, und können dazu verwendet werden, die Zugriffskontrolle in Nutzer-orientierter Weise neben dem Scope-Konzept, OAuth2 auszuwerten.

> Sichere und zuverlässige Unternehmens-Infrastruktur

WidasConcepts und alle seine DataCenter-Partner sind ISO27001: 2013 zertifiziert. Cloud-Dienste werden in Deutschland gehostet: Verantwortungsvoller Umgang mit Kundendaten nach dem Bundesdatenschutzgesetz und EU-DSGVO garantiert.

Eine hochautomatisierte Infrastruktur stellt sicher, dass die Systeme jederzeit auf dem aktuellsten Stand sind. Zum Beispiel werden Sicherheits-Patches ohne manuellen Eingriff schnell und präzise.

CIDAAS: WIE VERLÄSSLICH IST BEI UNS DIE IDENTIFIZIERUNG DER PERSON?

Cidaas Identity Service ist ganz im Sinne von Kunden aufgebaut. Der Schutz der Identität ist entscheidend und die gesamte Datenkommunikation über das Netzwerk ist verschlüsselt. Die Kontobestätigung umfasst folgendes:

Verhaltensanalyse: Zugriffstoken, die für Benutzer ausgegeben werden, werden mit fortschrittlicher Big-Data-Technologie überwacht und können somit eindeutig einem Benutzer zugeordnet werden. Eine intelligente Lösung durch die potentielle Betrüger erkannt werden.

Opt-in: Nach erfolgreicher Registrierung erhält der Benutzer eine Opt-In-E-Mail oder SMS vom System. Das Cidaas-System generiert automatisch eindeutige, aber temporäre Links und Codes und stellt die Kommunikation mit dem Benutzer her. Sobald der Opt-in ausgeführt wird, wird der Benutzer auf eine Landing-Page geleitet, cidaas benachrichtigt die Business-Software.

User- De-Duplikation: Unsere Analyse-Tools lernen von den Benutzerprofilen und erkennen doppelte Benutzerprofile gleich während der Registrierung. Nur eine, einzige Identität des Benutzers wird gespeichert.

CIDAAS: WAS BIETEN WIR HINSICHTLICH DES USER-PROFILS FÜR DEN BENUTZER UND DEM UNTERNEHMEN?

cidaas bietet die richtige Balance zwischen **Sicherheit und User Convenience**.

> Für die Kunden:

- Benutzerfreundlichkeit über das Self-Service-Portal, wo Benutzer
 - Passwort / Profilinginformationen bearbeiten können
 - erweiterte **passwortlose Authentifizierungs / Multi-Faktor** - Verifikationsmethoden (Sprach-, Gesichts-, Mustererkennung, Touch-ID, TOTP, Smart-Push, IVR, E-Mail, SMS und Backup-Codes) konfigurieren können
 - Konten, die mit verschiedenen Anbietern erstellt wurden, verknüpfen- bzw. aufheben können
 - Überblick über Aktivitäten erhalten - Datum und Uhrzeit der Anmeldung und andere Login-bezogene Aktivitäten, z. B. wann das Passwort geändert wurde, wann die E-Mail überprüft wurde, wann der Administrator das Konto aktiviert hat, wann der Benutzer sich abgemeldet hat, und mehr ...
- SSO: Endbenutzer können sich mit einer einzigen Identität über alle Kanäle und Dienste des Unternehmens anmelden.

> Für das Unternehmen:

- Einfach zu bedienende Administratorkonsole (+) mit umfassenden Konfigurationsoptionen und fein optimierten Verwaltungszugriffsstufen.
- cidaas WebHooks: Modernes managen von Ereignissen durch die Verwendung von WebHooks.
- Benutzerdefinierte Felder in der Benutzerregistrierung: cidaas bietet seinen Kunden eine Vielzahl frei definierbarer kundenspezifischer Felder zur Erfassung vielfältiger Kundendaten an.
- Optionale Integration in Ihre bestehenden AD / LDAP-Systeme: cidaas bietet die Möglichkeit, LDAP-Systeme als Login-Provider zu integrieren. Zunächst mit der Option, Mitarbeiter und Legacy-Systeme zu integrieren und schließlich einen reibungslosen Übergang zu den defacto Standards OpenId-Connect und OAuth2 zu erreichen.
- Erkenntnisse: Daten von verschiedenen Social Providern geben Einblicke in Kundeninteressen, Hobbys, Verhaltensmuster, Aktivitäten, demografische Informationen, Medienpräferenzen - cidaas verwandelt diese Informationen in nützliches Wissen für Ihr digitales Geschäft.

CIDAAS: MEHRWERT

Mit der cidaas Kundenidentitäts- und Zugangsmanagement-Lösung erhalten Unternehmen noch vieles mehr:

- Für Banken bietet cidaas ein vorgefertigtes PSD2-Entwickler-Portal, das den Zugriff auf Bank-APIs durch Dritten ermöglicht;
- cidaas sichert den Zugang zu Gebäuden und Räumen durch die Verwendung genau derselben Identitäten, Berechtigungsnachweise und biometrischen Daten;
- cidaas bietet digitales Consent-Management (Zustimmungsmanagement). Dadurch können Unternehmen die Einwilligung zur Datenschutzrichtlinien, die Nutzungsbedingungen gleich während der Registrierung oder des Logins anfordern sowie die aktionsbasierte Einwilligung in die eigene Unternehmenssoftware integrieren;
- Da sich cidaas stark bei verschiedenen IoT-Sicherheitsinitiativen engagiert, empfiehlt cidaas Unternehmen, auch IoT-Geräte von Benutzern aktiv zu verwalten.

CIDAAS: FAZIT

Wir von cidaas haben ein innovatives Sicherheitsprodukt entwickelt, mit dem unsere Kunden moderne Funktionen und all deren Vorteile erfolgreich nutzen können. Die Lösung stellt den Schutz von Benutzern und Unternehmen in Vordergrund. Deshalb haben wir das gesamte Produkt, mit all seinen Funktionen und Prozessen, auf Best Practices für Sicherheit ausgelegt. Unsere Systeme entsprechen den Industriestandards und demonstrieren damit unser anhaltendes Engagement für Sicherheit und Datenschutz.

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