

Warum ImmoGenio auf Zitadel Cloud setzt: ISO- 27001-zertifizierter Login für Hausverwaltungen

ImmoGenio nutzt Zitadel Cloud als externen Identitätsprovider: ISO 27001 zertifiziert, passwortloser Login per Passkey, PKCE-Flow ohne Client-Secret. Was das für Hausverwaltungen bedeutet.

Inhalt

- 01 Was ist Zitadel Cloud?
- 02 Die ISO/IEC 27001-Zertifizierung — was sie bedeutet
- 03 Passwortloser Login per Passkey (FIDO2/WebAuthn)
- 04 PKCE-Flow: Warum kein Client-Secret
- 05 Was in den technischen und organisatorischen Maßnahmen (TOM) steht
- 06 Abgrenzung: Was Zitadel nicht übernimmt
- 07 Fazit



ER ALS HAUSVERWALTUNG EINE CLOUD-SOFTWARE EINSETZT, ÜBERGIBT DEM ANBIETER EINEN erheblichen Teil seiner IT-Sicherheitsverantwortung. Dazu gehört auch die Authentifizierung: Wie werden Zugangsdaten gespeichert? Wer haftet bei einem Passwort-Leak? Welche Standards gelten für das Credential-

Management?

ImmoGenio hat diese Frage mit einer klaren Architekturentscheidung beantwortet: Die Authentifizierung von Hausverwaltungs-Accounts wurde vollständig an **Zitadel Cloud** ausgelagert – einen auf Identity-as-a-Service spezialisierten Anbieter, der im Mai 2023 die **ISO/IEC 27001-Zertifizierung** erhalten hat.

Was ist Zitadel Cloud?

Zitadel ist eine Open-Source-Identitätsplattform, die als verwalteter Cloud-Dienst betrieben werden kann. Sie übernimmt alle Aufgaben rund um Nutzeridentitäten: Registrierung, Login, Passwort-Verwaltung, Multi-Faktor-Authentifizierung und Single Sign-On. Das Unternehmen hinter Zitadel – CAOS AG – betreibt die Cloud-Instanzen ausschließlich in europäischen Rechenzentren; ein Transfer personenbezogener Daten in Drittländer findet nicht statt.

Für Hausverwaltungen als Auftraggeber bedeutet das: Der Dienstleister, dem sie ihr Login-Management anvertrauen, unterliegt denselben DSGVO-Anforderungen wie ein deutsches Rechenzentrum.

Die ISO/IEC 27001-Zertifizierung – was sie bedeutet

ISO/IEC 27001 ist der international anerkannte Standard für Informationssicherheits-Managementsysteme (ISMS). Eine Zertifizierung belegt, dass der Anbieter:

- alle sicherheitsrelevanten Prozesse systematisch dokumentiert und überprüft,
- Risiken identifiziert, bewertet und mit definierten Kontrollen adressiert,
- regelmäßige externe Audits durch akkreditierte Prüfstellen durchläuft.

Für ein Unternehmen, das Login-Credentials für mehrere tausend Nutzer verwaltet, ist diese Zertifizierung kein Marketingsignal, sondern ein nachprüfbarer Nachweis. Zitadel veröffentlicht das Zertifikat auf seiner Website.

Passwortloser Login per Passkey (FIDO2/WebAuthn)

Die technisch bedeutsamste Änderung für ImmoGenio-Nutzer: Hausverwaltungsmitarbeiter können sich ohne Passwort anmelden. Stattdessen kommt ein **Passkey** zum Einsatz — ein kryptografisches Schlüsselpaar, das auf dem Gerät des Nutzers gespeichert wird (TouchID, FaceID, Windows Hello oder ein Hardware-Sicherheitsschlüssel).

Der Vorteil gegenüber klassischen Passwörtern ist fundamental:

EIGENSCHAFT	PASSWORT	PASSKEY (FIDO2)
Speicherort	Server (Hash) + Nutzer (Kopf/Notiz)	Ausschließlich Nutzergerät
Phishing-Anfälligkeit	Hoch	Nicht möglich (origin-gebunden)
Brute-Force	Möglich bei schwachen Passwörtern	Nicht möglich (kein Geheimnis auf Server)
Datenpanne beim Anbieter	Hashes können geknackt werden	Kein verwertbares Geheimnis vorhanden
Nutzerfreundlichkeit	Mäßig (Passwort merken, regelmäßig ändern)	Hoch (biometrische Entsperrung in Sekunden)

ImmoGenio speichert für Zitadel-authentifizierte Nutzer **keinen Passwort-Hash** in der eigenen Datenbank. Selbst wenn die ImmoGenio-Datenbank kompromittiert würde, gäbe es keine Zugangsdaten zu stehlen.

PKCE-Flow: Warum kein Client-Secret

Die technische Verbindung zwischen ImmoGenio-Portal und Zitadel folgt dem OAuth 2.0 Authorization Code Flow mit **PKCE** (Proof Key for Code Exchange, RFC 7636). PKCE wurde entwickelt, um OAuth-Flows sicher für Browser-basierte Anwendungen zu machen — ohne dass ein Client-Secret im Quellcode hinterlegt werden muss.

Der Ablauf in Kurzform:

1. Beim Klick auf „Mit Firmen-Account anmelden“ generiert das ImmoGenio-Backend einen zufälligen `code_verifier` und dessen Hash (`code_challenge`).
2. Der Nutzer wird zu Zitadel weitergeleitet; der Hash wird mitgegeben.
3. Nach erfolgreicher Authentifizierung leitet Zitadel mit einem `code` zurück.

4. Das Backend tauscht den `code` gegen Tokens, indem es den ursprünglichen `code_verifier` mitschickt – den nur es kennt.

Ein abgefangener `code` ist ohne den passenden `code_verifier` wertlos. Da dieser nur serverseitig existiert und nie übertragen wird, ist der Flow robust gegen Redirect-Hijacking.

Was in den technischen und organisatorischen Maßnahmen (TOM) steht

Die Entscheidung für Zitadel ist im TOM-Dokument von ImmoGenio (gemäß Art. 32 DSGVO, Rev. 1.3) dokumentiert. Relevante Aussagen:

„*Passwortloser Login via Passkey (WebAuthn/FIDO2) oder OTP – kein Passwort-Hash für Zitadel-authentifizierte Nutzer in der ImmoGenio-Datenbank.*“

„*Kein Passwort-Management in ImmoGenio: Passwörter, Passwort-Reset-Links und Credential-Speicherung liegen vollständig bei Zitadel Cloud; das Haftungsrisiko für Credential-Kompromittierung ist an einen ISO-27001-zertifizierten Spezialanbieter ausgelagert.*“

Auftraggeber, die einen Auftragsverarbeitungsvertrag (AVV) mit ImmoGenio abschließen, erhalten das vollständige TOM-Dokument als Anlage 2 des AVV.

Abgrenzung: Was Zitadel nicht übernimmt

Zitadel ist ausschließlich für die **Authentifizierung** von Hausverwaltungs-Accounts zuständig. Die **Autorisierung** – also welcher Nutzer welche Daten sehen und bearbeiten darf – verbleibt vollständig im ImmoGenio-Backend:

- Das rollenbasierte Zugriffssystem (RBAC) mit 12 definierten Rollen
- Row-Level Security (RLS) in PostgreSQL
- Tenant-Isolation (Mandantentrennung auf Datenbankebene)

Nach erfolgreichem Zitadel-Login prüft das ImmoGenio-Backend, ob die E-Mail-Adresse in der eigenen Nutztabelle registriert und aktiv ist. Nicht registrierte Adressen erhalten keinen Zugang – unabhängig davon, ob die Authentifizierung bei Zitadel erfolgreich war.

Fazit

Die Auslagerung der Authentifizierung an einen ISO-27001-zertifizierten Spezialanbieter ist für eine Hausverwaltungs-SaaS kein Luxus, sondern ein sinnvolles Risikomanagement. Credential-Management gehört nicht zum Kerngeschäft einer Hausverwaltungssoftware; es erfordert aber spezialisiertes Know-how und kontinuierliche Sicherheitsupdates.

Hausverwaltungen, die ImmoGenio einsetzen, profitieren davon ohne eigenen Aufwand: Der Passkey-Login ist ab dem ersten Anmeldetag verfügbar, ohne dass Passwortrichtlinien konfiguriert, Passwort-Resets bearbeitet oder HaveIBeenPwned-Abfragen integriert werden müssten.