PassGrid Enterprise

Souveräne Geheimnisverwaltung

durch radikale Autarkie und "Privacy-by-Architecture"

1. Executive Summary

In einer Bedrohungslandschaft, die durch Supply-Chain-Angriffe auf Cloud-Anbieter und zentrale Identitätsdienste geprägt ist, bietet PassGrid eine Gegenstrategie: **Vollständige technologische Unabhängigkeit.** PassGrid Enterprise ist eine rein Web-basierte, self-hosted Lösung, die auf maximale Datensouveränität ausgelegt ist. Durch den bewussten Verzicht auf externe Abhängigkeiten wie SSO oder Cloud-Logging eliminiert PassGrid kritische Angriffsvektoren ab Werk.

2. Kernarchitektur & Sicherheitsprinzipien

2.1 Client-Side AES-256 (Zero-Knowledge)

Sicherheit beginnt beim Nutzer. Alle Daten werden lokal im Browser verschlüsselt. Der Server speichert lediglich verschlüsselte Blobs. Selbst bei einem physischen Diebstahl des Servers bleiben alle Geheimnisse ohne den individuellen Master-Key wertlos.

2.2 Radikale Autarkie: Warum wir auf SSO/LDAP verzichten

PassGrid wurde für Hochsicherheitsumgebungen entwickelt. Der bewusste Verzicht auf Single-Sign-On (SSO) und LDAP-Anbindungen ist ein strategisches Sicherheitsfeature:

Blast-Radius-Minimierung: Ein kompromittierter zentraler Identity-Provider (z.B. Azure AD) führt nicht zum Zugriff auf PassGrid.

Resilienz: Das System bleibt autark funktionsfähig, auch wenn zentrale Netzwerkdienste ausfallen oder kompromittiert sind.

2.3 Konsequente No-Logging-Policy

Datenschutz ist bei PassGrid kein Prozess, sondern Architektur. Das System führt keine nutzerbezogenen Logs.

Maximale DSGVO-Konformität: Da keine Bewegungsprofile oder Zugriffsprotokolle existieren, können diese weder missbraucht noch entwendet werden.

Privacy by Design: PassGrid schützt die Privatsphäre der Mitarbeiter durch das Fehlen jeglicher Überwachungsmetadaten.

3. Exklusive Enterprise-Sicherheitsfunktionen

3.1 IP-Stealth Mode (Infrastruktur-Schutz)

Die Enterprise-Edition ermöglicht die strikte Zugriffskontrolle auf Netzwerkebene (Whitelisting). Dies schützt die Instanz vor unbefugten Zugriffen aus unbekannten Netzwerken und minimiert die Sichtbarkeit der Anwendung für potenzielle Angreifer.

3.2 Smart-Forwarding für Unbefugte

Einzigartig in der Enterprise-Version: Unbefugte oder nicht autorisierte Zugriffsversuche werden durch intelligentes Forwarding neutralisiert. Angreifer erhalten keine Fehlermeldungen, die auf die Existenz der Software hindeuten könnten, was gezielte Sondierungen (Reconnaissance) erschwert.

3.3 White-Labeling & Corporate Compliance

Vollständige Integration in das Corporate Design bei gleichzeitiger Hoheit über die Rechtstexte (Impressum/DSGVO). Dies stellt sicher, dass das Tool nahtlos in die interne Compliance-Struktur des Unternehmens passt.

4. Investitionsschutz durch Perpetual Fallback License

4.1 Faire Lizenzierung ohne Vendor-Lock-in

PassGrid verfolgt ein Lizenzmodell, das echte Datensouveränität garantiert. Jährliche Lizenzen berechtigen zum Erhalt von Updates und Support während der Laufzeit. Nach Ablauf der Lizenz wird Ihre Installation auf der letzten lizenzierten Version "eingefroren" – diese läuft dauerhaft weiter, ohne Funktionsverlust.

Perpetual Fallback bedeutet:

Keine Datengeisel: Ihre Geheimnisse bleiben zugänglich, auch ohne Lizenzverlängerung.

Volle Kontrolle: Sie entscheiden, wann und ob Sie upgraden möchten.

Faire Kosten: Sie zahlen für Innovation und Support, nicht für die Nutzung.

4.2 Self-Hosted auf bewährter Technologie

PHP/MySQL: Betrieb auf bewährter Standard-Technologie, die in fast jeder IT-Infrastruktur ohne Zusatzkosten betrieben werden kann.

Installation in 5 Minuten: Einfaches Setup vergleichbar mit WordPress – kein komplexes Deployment nötig.

Keine versteckten Kosten: Kein Cloud-Hosting, keine User-Fees, keine Überraschungen. Sie behalten die volle Kostenkontrolle.

PassGrid – Datensouveränität durch Technologie, nicht durch Marketing.