میزبانی شخصی · دانش‌صفر · ساده و راحت

مدیریت رازها، گذرواژه‌ها و حساب‌ها در یک سامانه.

رازدار یک پلتفرم کاملاً ایرانی (از پایه) است که سه مشکل اساسی در سازمان‌ها و تیم‌ها را در یک سامانه واحد به ساده‌ترین شکل ممکن حل می‌کند:

۱- نگهداری امن اطلاعات محرمانه و اشتراک‌گذاری اثربخش همراه با گردش‌کار و تأیید

۲- فرآیند ریست کلمات عبور یا از قفل در آوردن حساب‌کاربری در سامانه‌ها و پلتفرم‌های مختلف توسط خود کاربران به صورت امن

۳- مدیریت حساب‌های کاربری (ایجاد، حذف، تعلیق) به صورت متمرکز

AES-256-GCM	RSA-2048	تعداد ۶۰۰ هزار تکرار	بدون تله‌متری
رمزنگاری متقارن احرازشده	رمزنگاری کلید OAEP برای اشتراک	استخراج کلید PBKDF2-SHA256	میزبانی شخصی · بدون ارسال داده

رازدار چیست؟

معرفی

رازدار یک **مدیر گذرواژه‌ی دانش‌صفر (zero-knowledge) و خود-میزبان (self-hosted)** برای تیم‌ها و سازمان‌هاست. هر راز — در چندین نوع اعتبارنامه — پیش از رسیدن به سرور با الگوریتم AES-256-GCM در مرورگر رمزنگاری می‌شود؛ بنابراین متن ساده، گذرواژه‌ی اصلی و کلیدها هرگز از کنترل شما خارج نمی‌شوند. اشتراک‌گذاری با اعضای گروه، یکپارچگی با اکتیودایرکتوری، احراز هویت دومرحله‌ای، پیوست رمزنگاری شده، گزارش رخداد تغییرناپذیر و یک بازیابی اضطراری مبتنی بر حدنصاب (حداقلی از یک تعداد کلید توسط مدیران) را افزوده است که هرگز به سرور — یا هیچ مدیر تنها — دسترسی دائم نمی‌دهد. یک زنجیره‌ی تایید چندمرحله‌ای قابل‌تعریف توسط مدیر، اشتراک‌گذاری گروهی و بازنشانی گذرواژه را پیش از اجرا از تاییدِ افراد مشخص عبور می‌دهد. واسط کاربری انگلیسی و فارسی (راست‌به‌چپ) به‌صورت پیش‌فرض وجود دارد.

هر آنچه یک تیم نیاز دارد، نه چیزی بیشتر.

ویژگی‌ها

AES-256-GCM

گاوصندوق دانش‌صفر

هر اعتبارنامه پیش از رسیدن به شبکه در مرورگر شما رمزنگاری می‌شود. سرور تنها انبار متن رمزشده است — نمی‌تواند داده‌های شما را بخواند.

چند نوع آیتم

همه‌ی رازها، یک گاوصندوق

ورود، کلید SSH، کارت بانکی، هویت، یادداشت امن، اعتبارنامه‌ی API و اتصال پایگاه‌داده، هرکدام با فیلدهای اختصاصی.

RSA-OAEP

اشتراک کاربر و گروه

با افراد یا گروه‌ها به‌اشتراک بگذارید؛ کلید هر عضو با کلید عمومی خودش رمزنگاری می‌شود. می‌توان گروه‌ها و اعضای مختلف تعریف کرد.

M-OF-N · SHAMIR

دسترسی اضطراری

بازیابی حساب بر پایه‌ی حدنصاب. آستانه‌ای از مدیران، کلید سپرده‌شده را در سمت کلاینت بازسازی می‌کنند — سرور و هیچ مدیری به صورت تکی هرگز دسترسی نمی‌یابد.

LDAP / AD

یکپارچگی با دایرکتوری

با اکتیو دایرکتوری یا LDAP احراز هویت کنید. کاربران در نخستین ورود به‌صورت خودکار ساخته می‌شوند و امکان ورود کاربران و گروه‌ها به‌صورت انبوه وجود دارد.

TOTP · RFC 6238

احراز هویت دومرحله‌ای و کنترل نقش

احراز هویت دومرحله‌ای با برنامه‌ی احرازکننده، به‌علاوه‌ی نقش‌های مدیر/کاربر، سیاست قفل گاوصندوق و گزارش رخداد تغییرناپذیر.

EMAIL / SMS OTP

بازنشانی خودکار گذرواژه

یک لایه‌ی جدا برای پشتیبانی IT: کاربر با کد یک‌بارمصرف ایمیل یا پیامک هویت خود را اثبات می‌کند و گذرواژه‌ی حساب‌های خارجی (AD، سرور و...) را بدون تیکت پشتیبانی بازنشانی می‌کند.

APPROVAL ENGINE

گردش‌کار تایید چندمرحله‌ای

مدیر می‌تواند زنجیره‌ای از تاییدکننده‌ها را برای اشتراک‌گذاری گروهی یا بازنشانی گذرواژه تعریف کند؛ هر مرحله قاعده‌ی خودش (هرکس، همه، یا حدنصاب) را دارد.

SMTP · IN-APP

اطلاع‌رسانی خودکار

درخواست‌های در انتظار تایید و نتیجه‌ی آن‌ها به‌صورت خودکار از طریق ایمیل و صندوق پیام درون‌برنامه به افراد مرتبط اطلاع داده می‌شود.

سرور چه می‌بیند و چه نمی‌بیند.

امنیت

سرور ذخیره می‌کند	سرور هرگز نمی‌بیند
خروجی Argon2id	گذرواژه‌ی اصلی
Salt و پارامترهای KDF	کلید رمزنگاری
کلید عمومی RSA	کلید خصوصی RSA
متن رمزشده‌ی AES-GCM	متن ساده‌ی اعتبارنامه
کلیدهای AES بسته‌بندی‌شده با RSA برای هر کاربر	کلیدهای خامِ AES
بلوکِ سپردهٔ بازیابی با RSA	کلیدِ بازساختهٔ بازیابی
رازِ TOTP	کدهای TOTP

اگر به سرور نفوذ شود، مهاجم تنها **بلوک‌های رمزشده** به‌دست می‌آورد که بدون گذرواژه‌ی اصلی هر شخص بی‌فایده‌اند — هیچ در پشتی و هیچ بازنشانی سمت سرور وجود ندارد. بازیابی اضطراری یک فرآیند اختیاری است و به **حدنصابی از مدیران** همراه با کلید اختصاصی نیاز دارد، نه به سرور یا یک نفر، بنابراین هیچ مدیری به تنهایی نمی‌تواند بازیابی انجام دهد.

مشخصات فنی

مشخصات

رمزنگاری

درهم‌سازی گذرواژه / KDF	**Argon2id**
استخراج کلید گاوصندوق (کلاینت)	**PBKDF2-SHA256**
رمزنگاری متقارن	**AES-256-GCM**
بسته‌بندی کلید نامتقارن	**RSA-2048-OAEP**
تقسیم کلید بازیابی مدیر	**Shamir M-of-N**
ذخیره‌ی توکن نشست	**SHA-256**
تولید IV	تصادفی، برای هر مورد

قالب‌های ورودی

Bitwarden	JSON · CSV
1Password	1PUX · CSV
عمومی	نگاشت فیلدها + CSV / Excel

معماری و استقرار

بک‌اند	**Go**
فرانت‌اند	**React · TypeScript**
پایگاه داده	**PostgreSQL**
استقرار	**Docker**
پراکسی معکوس	**Nginx**
تله‌متری (ارسال اطلاعات به خارج)	ندارد

خروجی و کنترل دسترسی

قالب‌های خروجی	.svault · Bitwarden · CSV
نقش‌ها	admin · user (RBAC)
بازیابی اضطراری	حدنصاب M از N مدیر
سیاست قفل گاوصندوق	هر کاربر + سقف مدیر

رمزنگاری پیش از خروجِ داده از مرورگر شما انجام می‌شود.

چگونه کار می‌کند

۱

گذرواژه‌ی اصلی

`PBKDF2-SHA256` با ۶۰۰٬۰۰۰ تکرار یک کلید اصلی استخراج می‌کند. گذرواژه‌ی شما هرگز از مرورگر خارج نمی‌شود.

۲

دو کلید استخراج می‌شود

یک Hash احراز هویت برای ورود به سرور می‌رود؛ کلید رمزنگاری تنها در حافظه‌ی مرورگر می‌ماند.

۳

زوج‌کلیدRSA ساخته می‌شود

کلید خصوصی با کلید رمزنگاری توسط AES رمز می‌شود. تنها کلید عمومی به‌صورت متن ساده ذخیره می‌شود.

۴

کلیدِ AES برای هر مورد

هر اعتبارنامه کلید مخصوص خود را دارد که با `RSA-OAEP` برای کلید عمومی گیرنده رمزنگاری می‌شود.

۵

اشتراک = رمزنگاری دوباره

برای اشتراک، مرورگر کلید هدف را برای هر عضو دوباره رمزنگاری می‌کند. سرور هرگز متن غیررمزنگاری شده را نمی‌بیند.

بازنشانی خودکار گذرواژه، بدون تیکت پشتیبانی.

بازنشانی خودکار (Self-Service)

این یک لایه‌ی **جدا و آگاهانه غیر دانش‌صفر** است، مکمل گاوصندوق شخصی — نه جایگزین آن. اینجا خودِ سرور اعتبارنامه‌ی اتصال‌دهنده‌های ممتاز را (رمزنگاری‌شده در حالت سکون) نگه می‌دارد تا از طرف کاربر روی سامانه‌های خارجی مانند اکتیودایرکتوری عمل کند. کاربرِ قفل‌شده، هویت خود را با کدِ یک‌بارمصرفِ ایمیل یا پیامک اثبات می‌کند، سپس حساب‌های خارجیِ متصل به خود را می‌بیند و گذرواژه‌ی آن‌ها را بدون دخالت تیم پشتیبانی بازنشانی می‌کند.

اتصال‌دهنده‌های ممتاز (Connectors)

HTTP عمومی	قالب درخواست + متغیر کاربر/گذرواژه
LDAP / Active Directory	Password-Modify یا unicodePwd
SSH (لینوکس)	chpasswd روی stdin
cPanel · DirectAdmin	بازنشانی حساب ایمیل
ownCloud / Nextcloud	OCS Provisioning API

شناسایی هویت با کد یک‌بارمصرف

کانال ارسال کد	ایمیل + پیامک (SMS)
درگاه پیامک پشتیبانی‌شده	ملی‌پیامک · کاوه‌نگار
ذخیره‌سازی کد	هش‌شده + دارای انقضا و سقف تلاش
نگاشت کاربر ⇄ حساب خارجی	مدیریت از پنل ادمین
حالت اعمال بازنشانی	فوری یا پس از تایید پشتیبانی

زنجیره‌ی تاییدِ چندمرحله‌ای برای عملیات حساس.

گردش‌کار تایید (Workflow)

یک موتور تاییدِ عمومی و قابل‌تعریف توسط مدیر که پیش از اجرای عملیات حساس، درخواست را از یک زنجیره‌ی مرحله‌به‌مرحله عبور می‌دهد. نخستین کاربردِ آن، اشتراک‌گذاری گروهی است؛ بازنشانی خودکار گذرواژه نیز از همین موتور بهره می‌برد.

۱

تعریف زنجیره‌ی مراحل

مدیر برای هر مرحله یک گروهِ تاییدکننده (کاربر، نقش، یا گروه) و یک قاعده تعیین می‌کند.

۲

قاعده‌ی هر مرحله

`هرکس`، `همه`، یا `حدنصاب` — درخواست‌کننده هرگز جزو تاییدکنندگانِ خودش نیست.

۳

رد = وتوی کامل

رد از سوی هر تاییدکننده‌ی واجدشرایط، کل درخواست را فوراً متوقف می‌کند.

۴

تایید نهایی = اجرا

با عبور از آخرین مرحله، عملیات به‌صورت خودکار اعمال و در گزارش رخداد ثبت می‌شود.

تاییدکنندگان و درخواست‌کنندگان از هر رویداد — درخواست جدید، تایید، رد — از طریق **پیام درون‌برنامه‌ای و ایمیل (SMTP)** مطلع می‌شوند؛ اطلاع‌رسانی هرگز مسیر اصلی عملیات را کند یا متوقف نمی‌کند.

// فلسفه‌ی لوگو — چرا «رازدار»؟

نماد رازدار، علامت سکوت در موسیقی، بیانگر فلسفه‌ای عمیق در امنیت سایبری است: بهترین محافظت، حضوری مطمئن و بی‌صدا دارد. همان‌گونه که سکوت در موسیقی بخشی ضروری از نظم و هارمونی است، امنیت نیز زمانی در بهترین حالت خود قرار دارد که بدون ایجاد پیچیدگی، از دارایی‌های حیاتی محافظت کند. از مهم‌ترین ویژگی‌های شخص رازدار، سکوت است. عبارت انگلیسی معادل در موسیقی Rest است، زمانی که شما استراحت می‌کنید و هیچ‌کاری انجام نمی‌دهید. نگهداری امن اطلاعات را به رازدار بسپارید.