Parola & API Key Yönetimi için Vault/KMS Planlama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu şablon; hassas kimlik bilgilerini (parola, API key, JWT token, veritabanı bağlantı metinleri ve TLS sertifikaları) kod depolarından (*Git repository*) ve yerel yapılandırma dosyalarından (*.env*) çıkarıp merkezi bir Vault/KMS mimarisine taşımak amacıyla hazırlanmıştır. Rol tabanlı erişim politikaları (RBAC) kurarak anahtar rotasyonu (*rotation*) ve iptal (*revocation*) süreçlerini otomatize eder. Otel PMS/OTA entegrasyonları, CRM ve sanal pos/ödeme sistemlerindeki kritik anahtar sızıntısı risklerini engeller, audit log'lar ile tüm erişimleri izleyerek KVKK/GDPR teknik tedbirlerini destekler.

Kim Kullanır?: DevOps ve Backend Geliştiriciler, Güvenlik / Ops Ekipleri, Otel IT Yöneticileri ve B2B Entegrasyon Ekipleri.

Nasıl Kullanılır?

1. Altyapınızda ve entegrasyonlarınızda kullanılan tüm hassas anahtarların envanterini çıkarın, kritiklik derecelerini (1–5) belirleyin.
2. RBAC rol politikalarını, uygulama çalışma zamanı (*runtime injection*) yöntemini ve CI/CD git-leak tarama kurallarını tanımlayın.
3. Otomatik/manuel rotasyon periyotlarını, olay anı iptal (*revocation*) runbook'unu ve audit log kurallarını devreye alın.

TEMPLATE — Parola & API Key Yönetimi İçin Vault/KMS Planı

1) Secret Envanteri ve Risk Matrisi

Secret	Tür	Kullanım Yeri	Ortam (Prod/Stage)	Sahip Ekip	Risk (1–5)
PMS API Key	API Key	Entegrasyon Servisi (PMS Entegrasyonu)	Prod	Integration / Backend	**5 (Kritik)**
CRM Token	OAuth Token	API Gateway / CRM Servisi	Stage	Core App Team	**3 (Orta)**

Payment Gateway Credentials	API Key / Private Key	Ödeme & Sanal POS Servisi	Prod	Payment / Finance	**5 (Kritik)**
DB Master Password	Parola	Primary Database Cluster	Prod	DBA / Infrastructure	**5 (Kritik)**
TLS / SSL Private Key	Sertifika Anahtarı	Nginx / Ingress Controller	Prod / Stage	Security / DevOps	**4 (Yüksek)**

2) Saklama ve Dağıtım Modeli

- **Vault/KMS Sağlayıcı:** HashiCorp Vault / AWS KMS / Azure Key Vault
- **Runtime Injection Yöntemi:** Environment Variable Injection via Kubernetes Agent Sidecar / Vault Secrets Operator (Kod içinde veya diske statik yazılmadan belleğe enjekte edilir).
- **Repo / .env Yasağı ve Denetimi (CI Scan):** Git commit/push süreçlerinde Gitleaks ve TruffleHog tarayıcıları zorunludur. Kod deposuna .env veya anahtar commit edilirse build otomatik engellenir.
- **Log Masking Kuralı:** Uygulama ve sunucu loglarında (stdout/stderr) hassas kelimeler (password, token, secret, bearer, key) otomatik olarak ***MASKED*** ifadesi ile maskelenir.

3) RBAC (Kim Hangi Secret'ı Görür?)

Rol	Erişim Seviyesi	Secret Kapsamı	Süreli mi? (TTL)	Onay Akışı
Backend-Prod (Service Account)	Read-Only (Bellek)	Yalnızca bağlı olduğu mikroservisin ihtiyaç duyduğu Prod Secret'lar	Sürekli (Dynamic Leases: 1 Saat)	Otomatik (AppRole / K8s SA)

DevOps / Admin	Admin / Full Control	Tüm Vault yolları ve KMS konfigürasyonu	Sürekli	MFA + İki Aşamalı Onay
Dış Mimar / Ajans / Entegratör	None / Limited Read	Sadece ilgili projenin Staging/Development secret'ları	**Geçici (8 Saat)**	BT Direktörü Onayı
Developer (Geliştirici)	Read / Write (Dev/Stage)	Yalnızca Dev ve Staging ortamı secret'ları	Çalışma Saatleri (12 Saat)	Takım Lideri Onayı

4) Rotation (Rotasyon) & Revocation (İptal) Stratejisi

Anahtar / Secret Türü	**Rotasyon Periyodu**	**Revocation Prosedürü (Olay / İhlal Anında)**	**Eski Secret Geçiş Planı (Grace Period)**
DB Parolaları	30 Gün (Otomatik)	Vault CLI ile anında revoke_lease + DB kullanıcı şifresini sıfırlama	15 Dakika paralel geçerlilik (*Zero-downtime*)
PMS / OTA API Keys	60 Gün (Yarı-Otomatik)	İlgili servis sağlayıcı portalından key'i iptal etme + Vault path güncelleme	24 Saat eski key aktif (Kademeli geçiş)
Sanal POS / Ödeme Key	90 Gün (Manuel)	Banka/Pos sağlayıcı paneli üzerinden instant revocation	Geçiş penceresi yok (Anında anahtar değişimi)
TLS / SSL Sertifikası	90 Gün (Let's Encrypt / Auto)	Certificate Revocation List (CRL) yayını + Yeni sertifika deployment	Eski sertifika anında silinir

5) Audit Log & KVKK Uyum Yönetimi

- **Audit Log Saklama Yeri:** Tüm Vault/KMS okuma, yazma, rotasyon ve deneme logları değiştirilemez (*append-only*) biçimde **S3 Immutable Log Bucket / Central SIEM** üzerinde toplanır.
- **Saklama Süresi / Erişim Yetkisi:** Loglar en az **2 Yıl** saklanır; erişim yetkisi sadece Güvenlik Denetçisi (*Security Auditor*) rolüne aittir.
- **KVKK Uyum Notu:** Kimlik doğrulama anahtarları ve veritabanı erişim bilgileri KVKK Teknik Tedbirleri / ISO 27001 gereğince en az AES-256 / RSA-4096 standartlarında şifrelenmiş (*Encryption-at-rest & In-transit*) olarak saklanmak zorundadır.

6) Denetim ve Kontrol Listesi (Checklist)

- [ ] **Secret'lar Repo / .env Dosyasında Değil:** Kod depoları taranıp hardcoded yazılmış tüm şifre ve key'ler temizlendi.
- [ ] **Prod / Stage Ortam Ayrımı Var:** Prod ve Test ortamları için tamamen farklı Vault path'leri ve anahtarlar kullanılıyor.
- [ ] **RBAC Rol Matrisi Hazır:** Kimlerin ve hangi servislerin hangi secret'lara erişebileceği en küçük yetki (*Least Privilege*) prensibiyle yapılandırıldı.
- [ ] **Rotation Takvimi Var:** Tüm API key, parola ve sertifikalar için otomatik/planlı rotasyon periyotları tanımlandı.
- [ ] **Revocation Runbook Test Edildi:** Sızıntı senaryosunda anahtarların nasıl anında geçersiz kılınacağı tatbikatla doğrulandı.
- [ ] **Audit Log ile Erişim İzleniyor:** Kimin ne zaman hangi secret'a eriştiği silinemez loglar üzerinden 7/24 izleniyor.

Deliverables (Teslim Edilecek Çıktılar)

- **Vault / KMS Mimari & Mimaride Secret Dağıtım Planı (v1.0):** Secret saklama, enjeksiyon ve izolasyon mimarisini tanımlayan teknik doküman.
- **CI/CD Git-Leak Tarama & Runtime Injection Konfigürasyonu:** Gitleaks, TruffleHog ve Kubernetes Sidecar entegrasyon kural dosyaları.
- **RBAC Yetki Matrisi & Dynamic Secrets Politikası:** Rol bazlı erişim politikalarını ve dinamik süre tanımlarını içeren matris.
- **Acil Durum Key Revocation Runbook'u:** Anahtar ihlallerinde uygulanacak anlık iptal ve değişim rehberi.
- **KVKK & ISO 27001 Uyumlu Audit Logging Konfigürasyonu:** Erişim kayıtlarının izlenmesi ve güvenli arşivlenmesi kılavuzu.

[Deliverables / Proof Card]

DevOps mühendisleri, güvenlik mimarları ve yazılım liderleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Secrets Management Deliverables Kartı. Koyu karbon gri ve parlak neon mor/altın sarısı tonlarındaki teknolojik zemin üzerinde; şifreli kasa (Vault) simgesi, dijital anahtar ve API token akış şeması, RBAC yetkilendirme rozetleri ve otomatik rotasyon döngü simgeleri yer alıyor. Kartın üzerinde; "Centralized Vault/KMS & Runtime Secrets Injection", "Least Privilege RBAC Policy & Dynamic Leases", "Automated Rotation & Instant Revocation Runbook" ve "KVKK Compliant Immutable Audit Logging" teslimat kalemi başlıkları, yanlarında parlak mor onay işaretleriyle scannable ve kurumsal bir proof-card formatında sergileniyor.