Veri Tipi Bazlı Şifreleme & Key Management Planlama Şablonu — Yazılım / Crypto (v1.0)

Asset Amaç: Bu şablon; işlenen verileri kritiklik seviyelerine (yüksek/orta/düşük) göre sınıflandırıp her veri türü için doğru şifreleme katmanını (aktarımda TLS, durağan/at-rest, alan bazlı/field-level) belirlemenizi sağlar. Kriptografik anahtar yönetimini KMS (Key Management Service) veya Secrets Manager altyapıları üzerinden RBAC, MFA ve silinemez audit log standartlarıyla kurgular. Otel ve B2B yazılım mimarilerinde sürdürülebilir, denetlenebilir ve yüksek güvenlikli bir kripto hijyeni oluşturmayı hedefler.

Kim Kullanır?: IT / BT Yöneticileri, Yazılım Mimarları & Geliştiricileri, Bilgi Güvenliği Ekipleri.

Nasıl Kullanılır?

1. Envanterdeki veri türlerini çıkararak risk sınıflarını (Yüksek, Orta, Düşük) tanımlayın.
2. Veri türüne göre TLS, At-Rest ve Field-Level şifreleme gereksinimlerini belirleyin; yedek (backup) ve log katmanlarını plana dahil edin.
3. Anahtar yönetimi (KMS) politikasını; saklama, erişim rolleri, rotasyon sıklığı, iptal (revoke) ve denetim adımlarıyla doldurun.

TEMPLATE — Veri Tipi Bazlı Şifreleme & Key Management Planlama Şablonu

1) Veri Tipi Bazlı Şifreleme Tablosu

Veri Türü / Kategorisi	Kaynak Sistem (Web / PMS / CRM / Docs / BI)	Risk Sınıfı (Yüksek / Orta / Düşük)	TLS Zorunlu? (E/H)	At-Rest Şifreleme? (E/H)	Field-Level Şifreleme? (E/H)	Backup Şifreli mi? (E/H)	Log Minimizasyonu / Maskeleme? (E/H)	Notlar / Ek Güvenlik Tedbiri
Özel Nitelikli Veri *(Kredi Kartı / Pasaport No)*	_____ _____ _____	[ ] Yüksek	[ ] Evet	[ ] Evet	[ ] Evet	[ ] Evet	[ ] Evet	_____ _____ _____
Müşteri Kimlik & İletişim	_____ _____ _____	[ ] Yüksek	[ ] Evet	[ ] Evet	[ ] Evet	[ ] Evet	[ ] Evet	_____ _____ _____

(TCKN / Tel / E-posta)								
Rezervasyon & Konaklama Geçmişi	_____ _____ _____	[ ] Orta	[ ] Evet	[ ] Evet	[ ] Hayır	[ ] Evet	[ ] Evet	_____ _____ _____
Personel / IK Verileri	_____ _____ _____	[ ] Yüksek	[ ] Evet	[ ] Evet	[ ] Evet	[ ] Evet	[ ] Evet	_____ _____ _____
Sistem / Uygulama Logları	_____ _____ _____	[ ] Orta	[ ] Evet	[ ] Evet	[ ] Hayır	[ ] Evet	[ ] Evet	_____ _____ _____
Genel Şirket / Kataloğ Verisi	_____ _____ _____	[ ] Düşük	[ ] Evet	[ ] Evet	[ ] Hayır	[ ] Evet	[ ] Hayır	_____ _____ _____

2) Key Management (Anahtar Yönetimi) Politikası

- **KMS / Secrets Manager Altyapısı:** _____ *(Örn: AWS KMS, HashiCorp Vault, Azure Key Vault)*
- **Erişim Rolleri & RBAC Yetkileri:** _____ *(Anahtar oluşturma, okuma, şifre çözme yetkilerinin ayrıştırılması)*
- **MFA Zorunluluğu:** [ ] Evet | [ ] Hayır *(Anahtar yönetim paneli ve kritik decrypt yetkileri için)*
- **Anahtar Rotasyon Periyodu:** _____ *(Örn: Otomatik 90 Gün / 365 Gün)*
- **Anahtar İptal & Revoke Prosedürü:** _____ *(Açık / sızıntı durumunda pasife alma ve re-encryption adımları)*
- **Merkezi Decrypt & Access Audit Log:** [ ] Evet | [ ] Hayır *(Tüm anahtar kullanım ve deşifreleme olaylarının kaydedilmesi)*

- **Break-Glass Prosedürü:** _____ *(Acil durumlarda kilit açma yetkisi ve güvenli anahtar kasası protokolü)*

3) Operasyonel Kontroller

- [ ] **Sertifika Yenileme Otomasyonu:** TLS/SSL sertifikalarının süresi dolmadan otomatik yenilenmesi (Let's Encrypt / Vault Cert Manager vb.).
- [ ] **Şifreli Backup Restore Test Planı:** Şifrelenmiş yedeklerin periyodik olarak geri yükleme (restore) testlerinin yapılması ve anahtar erişiminin doğrulanması.
- [ ] **Field-Level Decrypt Logları:** Hassas alan deşifre etme (field-level decryption) işlemlerinin kullanıcı ve zaman bazlı izlenmesi.
- [ ] **Aylık Anahtar Erişim Gözden Geçirme:** KMS erişim yetkilerinin ve rollerinin ayda bir kez güvenlik ekibince taranması.

4) Şablon Doldurma Kuralları (5 Altın Kural)

1. **Aktarımda ve Durağan Şifreleme Varsayılandır:** TLS (aktarım) ve At-Rest (durağan) şifrelemeyi tüm sistemler için standart kabul edin; uygulanmadığı durumları istisna olarak gerekçelendirin.
2. **Field-Level Şifrelemeyi Hedefli Kullanın:** Veritabanı performansını korumak için alan bazlı şifrelemeyi yalnızca Kredi Kartı, TCKN, Pasaport No gibi yüksek riskli kritik alanlara uygulayın.
3. **Hardcoded Key Kullanmayın:** Şifreleme anahtarlarını, API secret'larını asla kaynak koda veya konfigürasyon dosyalarına yazmayın; mutlaka KMS veya Secrets Manager kullanın.
4. **Rotasyon ve Revoke Prosedürünü Dokümante Edin:** Anahtarların çalınması veya periyodik yenilenmesi durumunda verinin yeniden nasıl şifreleneceğini (re-encryption) adım adım yazın.
5. **365 Günlük Periyodik Güncelleme:** Şifreleme algoritmalarını (Örn: AES-256) ve anahtar politikalarını yılda en az bir kez güncel standartlara göre gözden geçirin.

5) Kontrol Listesi (Checklist)

- [ ] **Veri Sınıflandırması Tamamlandı:** Tüm veri tipleri risk derecelerine göre kategorize edildi.
- [ ] **Tam TLS Kapsaması:** Tüm API, web ve mikroservis haberleşmeleri güncel TLS standartlarıyla koruma altında.
- [ ] **At-Rest & Backup Şifreleme Aktif:** Veritabanları, diskler ve tüm yedekleme alanları AES-256 veya dengi yöntemlerle şifrelendi.
- [ ] **Güvenli Key Management Mimarisi:** KMS/Vault kullanımı ile RBAC, MFA ve audit log kontrolleri sağlandı.
- [ ] **Aktif Rotasyon Planı:** Anahtarların otomatik rotasyon takvimi ve acil durum iptal (revoke) prosedürü hazır.

Deliverables (Teslim Edilecek Çıktılar)

- **Veri Tipi Bazlı Şifreleme Matrisi (v1.0):** Tüm veritabanı ve servisler için katmanlı şifreleme rehberi.
- **KMS & Secrets Manager Mimari Standardı:** Anahtar yönetimi, RBAC yetkileri ve rotasyon politikası dokümanı.

- **Kriptografik İptal & Re-Encryption Runbook'u:** Sızıntı anında veya periyodik rotasyonda veri yeniden şifreleme prosedürü.
- **Sertifika & Anahtar Yönetimi Operasyonel Denetim Takvimi:** 365 günlük periyodik kontrol ve test rehberi.

[Diagram / Flow]

Verinin istemciden sunucuya aktarımından (TLS 1.3), uygulama içi alan bazlı şifrelemeye (Field-Level Decryption), veritabanı disk şifrelemesine (At-Rest AES-256) ve KMS/Secrets Manager anahtar kasası mimarisine kadar tüm katmanları gösteren, 16:9 formatında yüksek çözünürlüklü bir Kriptografik Şifreleme Katman Diyagramı. Koyu şık zemin üzerinde; mavi, yeşil ve mor katman hatları, kilitli veri blokları, KMS anahtar senkronizasyon okları ve silinemez denetim izi (Audit Log) simgeleri profesyonel bir mimari şema olarak sergileniyor.

[Checklist / Framework Card]

IT yöneticileri, yazılım mimarları ve siber güvenlik uzmanları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Kriptografi & Key Management Checklist Kartı. Koyu karbon gri zemin üzerine yerleştirilmiş; şifreleme kalkanı, KMS anahtar simgesi, AES-256 rozeti ve rotasyon zamanlayıcısı. Kartın üzerinde; "Data Classification & Multi-Layer Encryption (TLS, At-Rest, Field-Level)", "Centralized KMS & Secrets Manager with RBAC & MFA", "Automated Certificate & Key Rotation Procedures", ve "Encrypted Backup Restore & Decrypt Event Audit Logging" teslimat kalemi başlıkları, yanlarında yeşil onay rozetleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.