SECZAR · PRIVILEGED ACCESS MANAGEMENT

Regülasyon Uyumluluğu ve Teknik Yeterlilik Dokümanı

İhale Teknik Şartname Karşılama Beyanı

Ürün: **Seczar-PAM** · Sürüm: **1.3.0 (Appliance)**
Doküman Tarihi: 22.06.2026 · Sürüm: 1.0

Kapsam: ISO/IEC 27001:2022 · KVKK (6698) · Cumhurbaşkanlığı BİGR
PCI-DSS v4.0 · SOX · HIPAA · GDPR · PAM Teknik Şartname Maddeleri

Seczar-PAM — Regülasyon Uyumluluğu ve Teknik Yeterlilik Dokümanı

Bu doküman, Seczar-PAM ürününün kurumsal Ayrıcalıklı Erişim Yönetimi (PAM) ihale teknik şartnamelerinde aranan teknik kabiliyetleri ve ulusal/uluslararası regülasyon gerekliliklerini hangi düzeyde karşıladığını madde madde ortaya koyar.

1. Yönetici Özeti

Seczar-PAM; ayrıcalıklı hesapların **kasalanması**, erişimin **aracılanması (brokering)**, oturumların **kaydı ve izlenmesi**, riskli komutların **önlenmesi** ve davranışsal **analitik (UEBA)** yetenekleriyle uçtan uca ayrıcalık güvenliği sağlayan, Docker tabanlı **on-premise appliance** bir üründür.

Ürün; "kayıt + kontrol" katmanının ötesinde, otomatik ayrıcalık güvenliği (AAPM secret API, JIT ephemeral hesaplar, UEBA tehdit analitiği) sunan olgun PAM seviyesinde konumlanır. Tüm bileşenler tek sunucuda, dış dünyaya kapalı izole iç ağlarda, root'suz müşteri modeliyle çalışır; opsiyonel olarak active-passive Yüksek Erişilebilirlik (HA) ve otomatik failover desteklenir.

> **Uyumluluk Beyanı Notu:** Bu dokümanda her madde için karşılama durumu dürüstçe işaretlenmiştir. `TAM` üretimde devrede ve doğrulanmış kabiliyeti; `KISMİ` mevcut çekirdek karşılığı bulunan, kapsamı genişleyen / yol haritasında olan kalemleri ifade eder.

2. Ürün Mimarisi — Özet

Tek dış giriş noktası nginx reverse-proxy (80/443, TLS sonlandırma) üzerindendir. Çekirdek iş mantığı FastAPI backend'de toplanır; oturum aracılığı Apache Guacamole (RDP/SSH/VNC/telnet web brokering) ve native protokol proxy'leri ile sağlanır. Tüm veri tek PostgreSQL örneğinde (yalnız iç ağda, dışa kapalı) tutulur.

Katman	Bileşen / Kabiliyet
Sunum / Giriş	nginx reverse-proxy + TLS, React SPA yönetim arayüzü
Aracılık (Brokering)	Web (ajansız) Guacamole; Native (ajanlı) SSH bastion, RDP tünel, app launcher; DB wire-proxy (PG/MSSQL/MySQL); Web forward-proxy
Çekirdek	Kasa/kripto, parola rotasyonu, RBAC, talep-onay, UEBA, JIT, AAPM, raporlama, HA, imzalı güncelleme
Veri	PostgreSQL (PAM + Guacamole şeması), zarf şifreleme ile korunan credential deposu
Uç (Endpoint)	Windows/Linux iş istasyonu ajanı: native launch, ekran kaydı, DLP, discovery

3. PAM Teknik Şartname Maddeleri — Karşılama Matrisi

Aşağıdaki matris, kurumsal PAM ihalelerinin teknik şartnamelerinde standart olarak aranan gereksinimleri ve Seczar-PAM'in bunları karşılama biçimini içerir.

TAM Devrede / doğrulanmış **KISMİ** Çekirdek karşılığı var / genişliyor

#	Gereksinim	Durum	Seczar-PAM Karşılığı
1	Ayrıcalıklı hesap kasalama (vaulting) — parolaların şifreli merkezi saklanması	TAM	Zarf şifreleme (KEK→DEK), AES-GCM ile parola şifreleme; parolalar plaintext saklanmaz. Keyring tabanlı KEK halkası.
2	Otomatik parola rotasyonu (periyodik + olay tetikli)	TAM	`auto_rotate_days` periyodik rotasyon + drift kontrolü + domain grup senkronizasyonu; oturum-kes sonrası otomatik rotate.
3	Çoklu platform parola yönetimi	TAM	Windows Local/Domain (AD), Linux (SSH key dahil), ağ cihazları (Cisco/Fortinet/Juniper/MikroTik/Aruba/HP/Palo Alto/Ubiquiti), DB (PostgreSQL/MSSQL/MySQL/Oracle), admin tanımlı özel platform şablonu.
4	Oturum aracılama (session brokering) — RDP/SSH/VNC/Telnet	TAM	Ajansız web (Guacamole) ve ajanlı native (SSH bastion, RDP tünel) modlarında çok protokollü erişim.
5	Veritabanı erişim aracılama ve denetimi	TAM	Wire-proxy: PostgreSQL :15432 (TLS), MSSQL :11433, MySQL :13306. SQL sniff + kayıt + komut bloklama.
6	Oturum kaydı (video + metin/komut)	TAM	Guacamole grafik kaydı + native ekran kaydı (DXGI) + SSH/DB transcript. Kural bazlı tetikleme.
7	Kayıtlarda içerik arama (OCR / metin index)	TAM	Tesseract (tur+eng) OCR ile grafik kayıtlarda kelime arama; SSH/DB transcript metin indeksi. 5 protokolde arama.
8	Canlı oturum izleme, devralma ve sonlandırma (shadowing)	TAM	Admin tüm modlarda (Guacamole/Web ext/Native) oturumu izle + kontrol al + sonlandır.
9	Komut / sorgu filtreleme ve engelleme	TAM	SSH bastion satır-tamponlu komut bloklama; DB proxy yıkıcı SQL (DROP/TRUNCATE/ALTER), WHERE'siz DELETE/UPDATE + özel regex bloklama.
10	Politika ihlalinde otomatik oturum sonlandırma	TAM	`auto_kill_threshold`: oturumda ≥N engellenen komut → otomatik sonlandırma + opsiyonel credential rotate.
11	Just-In-Time (JIT) erişim / Zero Standing Privilege	TAM	Talep anında hedefte geçici (ephemeral) hesap üretimi, TTL dolunca otomatik silme. 5 platform (Linux/Windows/PG/MSSQL/MySQL). Gerekçe zorunlu + audit + alarm.
12	Talep-onay iş akışı (çift / çok onaylı)	TAM	Talep→onay akışı, lider + admin çift onay; geçici/zamanlı paylaşım; erişim-anı risk kapısı.
13	Rol Bazlı Erişim Kontrolü (RBAC) / en az yetki	TAM	Rol→izin eşlemesi (admin/lider/operator + özel roller). Granüler izinler: `checkout`, `rotate`, `discovery`, `audit_view`, `jit_access` vb.
14	Çok faktörlü kimlik doğrulama (MFA)	TAM	TOTP + RADIUS challenge. (FIDO2/push genişlemesi yol haritasında.)
15	Dizin servisi entegrasyonu (LDAP/AD/RADIUS)	TAM	Yerel, LDAP/AD ve RADIUS kimlik kaynakları aynı oturum/token modeline düşer; LDAP grup→rol eşlemesi.
16	Uygulama/servis parolası yönetimi (AAPM / secret API)	TAM	Scope'lu API token (SHA-256 hash + prefix + IP allowlist); hardcoded parola çözümü. 3 referans uç nokta, CCP tarzı sorgu.
17	Ayrıcalıklı hesap keşfi (discovery)	TAM	Hesap/hedef keşfi (registry/GPO/privilege escalation), keşif sonuçları ve otomatik onboarding.
18	Merkezi denetim izi ve SIEM entegrasyonu	TAM	Merkezi `pam_audit_log` + syslog/SIEM aktarımı + e-posta alarmı. Tüm kritik işlemler (checkout, rotate, JIT, AAPM, risk) izlenir.
19	Uyumluluk raporlama (PDF/CSV export)	TAM	Data-driven raporlar (KVKK/ISO 27001/GDPR/SOX/PCI-DSS/HIPAA temalı) + PDF/CSV/TXT export.
20	Davranışsal analitik / anomali tespiti (UEBA)	TAM	Saatlik risk skorlama: cold-start kural eşikleri + kişisel istatistiksel baseline (z-score) + trend. Yüksek/kritik'te otomatik yanıt.

21	Parolanın istemciye/iş istasyonuna düşmemesi	TAM	Bastion/proxy/cred-hiding mimarisi: gerçek parola hiçbir zaman istemciye inmez. Web extension placeholder-swap, app launcher klavye-enjeksiyonu.
22	Yüksek Erişilebilirlik (HA) / felaket kurtarma	TAM	Active-passive otomatik failover (WireGuard tünel + Postgres replication + VIP + self-fence daemon). Break-glass vault kurtarma + offsite FTP yedek.
23	İzole / on-prem dağıtım (air-gapped uyumlu)	TAM	Tek sunucu Docker Compose appliance; iç ağlar dışa kapalı; root'suz müşteri modeli; bulut bağımlılığı yok.
24	İmzalı / güvenli ürün güncelleme	TAM	RSA imzalı, image-based rolling update + rollback; pre-update snapshot (dosya + DB + image tag).
25	Veritabanı sonuç maskeleme / 4-göz sorgu onayı	KISMİ YOL HRT.	Komut bloklama + oturum-kes devrede; DB sonuç maskeleme ve sorgu-onayı (4-göz) yol haritasında.
26	Erişim sertifikasyonu (recertification kampanyaları)	KISMİ	Granüler erişim envanteri + denetim raporları mevcut; periyodik kampanya otomasyonu yol haritasında.

4. ISO/IEC 27001:2022 — Annex A Kontrol Eşlemesi

Seczar-PAM, bilgi güvenliği yönetim sistemi (BGYS) kontrollerinden özellikle erişim kontrolü, kimlik yönetimi, kayıt/izleme ve kriptografi alanlarındaki kontrollerin teknik uygulanmasını doğrudan destekler.

Kontrol	Başlık	Durum	Seczar-PAM Karşılığı
A.5.15	Erişim kontrolü	TAM	RBAC, sahiplik, paylaşım, talep-onay; hedef bazında en az yetki.
A.5.16	Kimlik yönetimi	TAM	Yerel/LDAP-AD/RADIUS kimlikleri; JIT ephemeral kimlik yaşam döngüsü.
A.5.17	Kimlik doğrulama bilgisi	TAM	Parola kasalama, rotasyon, zarf şifreleme; AAPM ile uygulama sırları.
A.5.18	Erişim hakları	TAM	Hak atama/geri çekme, zamanlı paylaşım, otomatik süre dolumu.
A.8.2	Ayrıcalıklı erişim hakları	TAM	PAM'in çekirdek amacı: ayrıcalıklı hesapların kasalanması, aracılanması, izlenmesi, JIT.
A.8.3	Bilgiye erişim kısıtlama	TAM	Granüler izinler, sahiplik/paylaşım modeli, risk kapısı ile erişim engelleme.
A.8.5	Güvenli kimlik doğrulama	TAM	MFA (TOTP/RADIUS), token TTL, bastion token-auth.
A.8.15	Kayıt tutma (logging)	TAM	Merkezi denetim izi, oturum kaydı, transcript, OCR index.
A.8.16	İzleme faaliyetleri	TAM	Canlı shadowing, UEBA risk skorlama, syslog/SIEM, alarm.
A.8.24	Kriptografi kullanımı	TAM	AES-GCM zarf şifreleme, 90 günlük otomatik KEK rotasyonu, TLS, iç PKI.
A.5.7	Tehdit istihbaratı / anomali	TAM	UEBA davranış analitiği, risk tabanlı otomatik yanıt.
A.8.7 / A.8.12	Zararlıya/veri sızıntısına karşı koruma (DLP)	TAM	Ajan DLP (SSL MITM kural motoru, clipboard kontrolü, session kill); izole proxy erişimi.

5. KVKK (6698 Sayılı Kanun) — Veri Güvenliği Tedbirleri

KVKK Madde 12 kapsamında veri sorumlusunun almakla yükümlü olduğu teknik tedbirlerin önemli bölümü, ayrıcalıklı erişimin kontrolü ve izlenmesiyle doğrudan ilişkilidir. Seczar-PAM bu teknik tedbirlerin uygulanmasını sağlar.

KVKK Teknik Tedbiri (Md.12 / Rehber)	Durum	Seczar-PAM Karşılığı
Yetki matrisi ve erişim yetkilerinin sınırlandırılması	TAM	RBAC + en az yetki + sahiplik/paylaşım + talep-onay.
Kimlik doğrulama ve güçlü yetkilendirme	TAM	MFA (TOTP/RADIUS), AD/LDAP entegrasyonu, oturum token TTL.
Kişisel veriye erişimin loglanması / iz kaydı	TAM	Merkezi denetim izi + oturum kaydı + OCR'lı içerik araması.
Şifreleme (kriptografik koruma)	TAM	AES-GCM zarf şifreleme, KEK rotasyonu, TLS, TLS'li DB proxy.
Sızma testi / saldırı tespiti / izleme	TAM	UEBA anomali tespiti, komut/SQL bloklama, otomatik oturum-kes, alarm.
Yedekleme ve veri kurtarma	TAM	Vault ciphertext yedeği + break-glass recover + offsite FTP + HA.
Veri minimizasyonu / erişim ihtiyaç bazlı	TAM	JIT/Zero Standing Privilege, zamanlı paylaşım, otomatik süre dolumu.

6. Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi (BİGR)

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi, kamu kurumları ve kritik altyapı işletmecileri için tedbir setleri tanımlar. Seczar-PAM, Rehber'in özellikle **erişim/yetki yönetimi, ayrıcalıklı hesaplar, kayıt yönetimi ve kriptografi** alanlarındaki tedbirlerinin teknik uygulanmasını sağlar.

BİGR Tedbir Teması	Durum	Seczar-PAM Karşılığı
Ayrıcalıklı (yetkili) hesapların merkezi yönetimi ve denetimi	TAM	Tüm ayrıcalıklı hesaplar kasada; erişim aracılı, kayıtlı, onay/denetim altında.
Merkezi kimlik doğrulama ve çok faktörlü doğrulama	TAM	AD/LDAP/RADIUS entegrasyonu + MFA (TOTP/RADIUS).
Erişim kayıtlarının (log) tutulması ve merkezi log yönetimi	TAM	Merkezi audit log + syslog/SIEM aktarımı + oturum kaydı.
Uzaktan erişim güvenliği ve izolasyon	TAM	Ajansız izole web erişimi (istemci hedefe doğrudan ulaşmaz) + bastion + forward-proxy.
Kriptografik tedbirler / şifreleme	TAM	AES-GCM zarf şifreleme, KEK rotasyonu, TLS, iç PKI.
Yerli/yerinde (on-prem) çözüm, yurt dışı veri çıkışının olmaması	TAM	Yerli ürün; tamamen on-prem appliance; bulut/yurt dışı bağımlılığı yok; air-gapped uyumlu.
Olay yönetimi ve otomatik müdahale	TAM	UEBA risk + otomatik oturum-kes/rotate + alarm + JIT acil erişim izi.
Yedekleme, süreklilik ve felaket kurtarma	TAM	HA active-passive failover + vault yedeği + offsite yedek.
Sızma testi ve güvenlik doğrulaması	TAM	Bağımsız sızma testi raporu mevcut; tasarımda no-backdoor/no-SQLi/no-XSS ilkeleri.

Not: BİGR uygulaması varlık kritiklik derecesine göre Seviye 1/2/3 tedbirleri içerir. Seczar-PAM, ayrıcalıklı erişim alanındaki tedbirlerin teknik karşılığını sağlar; idari/süreçsel tedbirler kurumun BGYS'si ile birlikte uygulanır.

7. Uluslararası Regülasyonlar — PCI-DSS, SOX, HIPAA, GDPR

Ürün, finans, sağlık ve uluslararası uyum gerektiren ihaleler için aşağıdaki çerçevelerin ayrıcalıklı erişimle ilgili maddelerini karşılar ve bu çerçeveler için hazır uyumluluk raporları üretir.

7.1 PCI-DSS v4.0

Gereksinim	Durum	Seczar-PAM Karşılığı
Req 7 — İhtiyaç bazlı erişim kısıtlama	TAM	RBAC, en az yetki, hedef bazlı paylaşım, JIT.
Req 8.2/8.3 — Kimlik, MFA, güçlü doğrulama	TAM	Benzersiz kimlik, MFA (TOTP/RADIUS), oturum yönetimi.
Req 8.3.x — Parola politikası ve rotasyon	TAM	Parola politikası kuralları + otomatik rotasyon.
Req 8.6 — Uygulama/sistem hesapları	TAM	AAPM scope'lu token, hardcoded parola eliminasyonu.
Req 10 — Tüm erişimin loglanması/izlenmesi	TAM	Merkezi audit log, oturum kaydı, syslog/SIEM.

7.2 SOX (Sarbanes-Oxley) — ITGC

Kontrol Alanı	Durum	Seczar-PAM Karşılığı
Ayrıcalıklı erişim kontrolü	TAM	Kasalama + aracılama + kayıt + denetim izi.
Görevler ayrılığı (SoD) / self-approval engeli	TAM	Çift onay (lider+admin), self-approval kontrolü.
Değişiklik yönetimi izlenebilirliği	TAM	Tüm ayrıcalıklı oturum/komut kaydı + raporlama.

7.3 HIPAA

Madde	Durum	Seczar-PAM Karşılığı
§164.312(a) Erişim kontrolü	TAM	RBAC, benzersiz kimlik, otomatik oturum sonlandırma.
§164.312(a)(2)(ii) Acil erişim	TAM	JIT break-glass acil erişim (gerekçeli + denetimli).
§164.312(b) Denetim kontrolleri	TAM	Merkezi audit + oturum kaydı + OCR arama.
§164.308(a)(4) Erişim yönetimi	TAM	Hak atama/geri çekme, paylaşım, recertification raporları.

7.4 GDPR

Madde	Durum	Seczar-PAM Karşılığı
Art. 32 — İşlemenin güvenliği	TAM	Şifreleme, erişim kontrolü, kayıt, dayanıklılık (HA), kurtarma.
Art. 25 — Tasarımdan gizlilik	TAM	Parolanın istemciye düşmemesi, izolasyon, en az yetki, JIT.
Art. 30 — İşleme faaliyeti kayıtları	TAM	Erişim/işlem denetim izi + raporlama.

8. Güvenlik Tasarım İlkeleri

- **Parola izolasyonu:** Gerçek parola hiçbir zaman istemciye / iş istasyonuna düşmez (bastion / proxy / cred-hiding mimarisi).
- **Zarf şifreleme:** KEK→DEK→veri; AES-GCM; 90 günlük otomatik KEK rotasyonu; crash-safe staged uygulama; break-glass kurtarma.
- **Merkezi denetlenebilirlik:** Tüm ayrıcalıklı işlemler tek audit izinde; syslog/SIEM aktarımı; e-posta alarmı.
- **En az yetki ve onay:** RBAC, çift onay, geçici/zamanlı erişim, JIT / Zero Standing Privilege.
- **Önle–Tespit–Yanıt:** Komut/SQL bloklama (önle) + UEBA (tespit) + otomatik oturum-kes/rotate (yanıt).
- **İzolasyon:** Web proxy / Guacamole ile istemci hedefe doğrudan erişemez; iç ağlar dışa kapalı.
- **Bütünlük:** Root'suz appliance, RSA imzalı güncelleme, iç PKI, lisans kilidi.
- **Güvenli geliştirme:** No backdoor / No SQL Injection / No XSS / No XML attack ilkeleri; backend kod koruması (Nuitka derleme).

9. Sonuç ve Beyan

Seczar-PAM, kurumsal PAM ihale teknik şartnamelerinde aranan temel ve ileri seviye kabiliyetlerin tamamına yakınını **üretimde devrede** olarak karşılamakta; ISO/IEC 27001:2022, KVKK (6698), Cumhurbaşkanlığı BİGR ve PCI-DSS / SOX / HIPAA / GDPR çerçevelerinin ayrıcalıklı erişimle ilgili teknik gerekliliklerini sağlamaktadır. Yol haritasında belirtilen kalemler (DB sonuç maskeleme, 4-göz sorgu onayı, erişim sertifikasyon kampanyaları, MFA genişliği) ürünün çekirdek karşılıklarının üzerine planlı geliştirmelerdir.

> Bu doküman, ürünün 22.06.2026 tarihli mevcut (Sürüm 1.3.0) kabiliyet durumunu yansıtır. Belirli bir ihalenin teknik şartnamesine madde-madde özel karşılama matrisi talep edilmesi halinde, ilgili şartname maddeleri bire bir eşlenerek ayrıca düzenlenebilir.