

KRİPTO VARLIKLARIN SAKLANMASINA İLİŞKİN PROSEDÜR

Doküman Kodu: KVSP-PR-01

Yürürlük Tarihi: 09.04.2025

Revizyon No: 1.0

Hazırlayan: Uyum ve Hukuk Direktörlüğü

Onaylayan: Yönetim Kurulu

İlgili Birimler: Operasyon, BT Direktörlüğü, Risk Yönetimi, İç Denetim, Cüzdan Yönetim Ekibi

1. AMAÇ

Bu prosedürün amacı, Magician of Meta Kripto Alım Satım Platformu A.Ş. (Areonx) nezdinde **müşteri ve platforma ait kripto varlıkların ayrı, güvenli, izlenebilir ve mevzuata uygun şekilde saklanması** sağlamak, bu süreçte uygulanacak **teknik, operasyonel ve idari kontrolleri** düzenlemektir.

2. HUKUKİ DAYANAK

Bu prosedür, Sermaye Piyasası Kurulu'nun **III-35/B.2 sayılı Sermaye Yeterliliği Tebliği'nin 26 maddesi** kapsamında hazırlanmıştır. Ayrıca;

- **VII-128.10 sayılı Bilgi Sistemleri Tebliği,**
- **MASAK rehber ilkeleri,**
- **FATF VASP Rehberleri,**
- Uluslararası kripto varlık saklama standartları (CCSS, ISO/IEC 27001) dikkate alınarak oluşturulmuştur.

3. KAPSAM

Bu prosedür;

- Müşteriye ait kripto varlıkların ayrı saklanması,
- Soğuk ve sıcak cüzdan kullanım politikaları,
- Platform varlıklarının ayrıştırılması,
- Anahtar yönetimi ve yetki matrisleri,
- Saklama altyapısının güvenliği ve iş sürekliliği politikalarını kapsar.

4. TEMEL İLKELER

AreonX aşağıdaki saklama prensiplerine uygun hareket eder:

- **Müşteri varlıkları ile platform varlıkları ayrı cüzdanlarda saklanır.**
- **Her bir müşteri için bireysel izlenebilir kayıt tutulur.**
- **Soğuk cüzdanlar çevrimdışı ve donanımsal güvenlik altında korunur.**
- **Çoklu imza (multi-signature) ve çoklu yetki (multi-approval) sistemi uygulanır.**
- **Kritik anahtarlara erişim, rollere göre sınırlanır ve log'lanır.**

5. CÜZDAN TİPLERİ VE KULLANIM POLİTİKASI

5.1 Sıcak Cüzdanlar (Hot Wallets)

- Günlük müşteri para çekme işlemlerinin karşılanması amacıyla kullanılır.
- Maksimum sıcak cüzdan limiti, toplam rezervin %2'si ile sınırlandırılır.
- Sürekli izleme, anti-malware koruma ve saldırı önleme sistemleri (IDS/IPS) aktif şekilde uygulanır.

5.2 Soğuk Cüzdanlar (Cold Wallets)

- Çevrimdışı ortamda, donanımsal cüzdan cihazlarında veya HSM (Hardware Security Module) sistemlerinde saklanır.
- Cüzdanlara erişim, çoklu yetkili (2/3 veya 3/5 imza kuralı) sistemle sağlanır.
- Fiziksel cihazlar kurumsal kasada, izole kasalarda veya güvenli veri merkezlerinde tutulur.
- Soğuk cüzdanlardan sıcak cüzdanlara transfer yalnızca "çekim denetimi" sonrası yapılır.

5.3 Yedekleme Cüzdanları

- Kripto varlıkların kurtarılabilişliğini temin etmek amacıyla ayrı olarak yapılandırılır.
- Cüzdan tohumları ve özel anahtar yedekleri **şifreli biçimde fiziksel güvenlik altında** saklanır.
- Erişim sadece yetkili 3 yönetici ve 1 iç denetim sorumlusunun imzası ile mümkündür.

6. MÜŞTERİ VARLIKLARININ AYRIŞTIRILMASI

- Müşteri kripto varlıkları, platform adına tutulan varlıklardan **tamamen ayrı cüzdan yapısında izlenebilir biçimde** saklanır.
- Her bir kripto varlık için **müşteri bazlı alt cüzdan (sub-account) veya hesap kodu** üzerinden takip yapılır.
- Müşteri varlıkları üzerinde **platformun rehin, teminat, kullanım yetkisi yoktur**.

7. ANAHTAR YÖNETİMİ VE YETKİ MATRİSİ

7.1 Özel Anahtar Yönetimi

- Özel anahtarlar **şifreli donanım modüllerinde (HSM)** saklanır.
- Anahtarlar parçalara bölünerek (sharded key management) farklı kişilere dağıtılabilir.
- Anahtarlar hiçbir zaman düz metin olarak sistemde veya personel cihazında tutulamaz.

7.2 Yetki Matrisi

Yetki Türü	Görevli Birim	Onay Sayısı
Soğuk cüzdan erişimi	BT Direktörü, CEO, İç Denetim	En az 2/3
Sıcak cüzdan çekimi	Operasyon Yöneticisi + BT	En az 2
Anahtar yedek açılımı	BT + İç Denetim + Yönetim	3/3

Tüm erişim girişimleri, çok faktörlü kimlik doğrulama ile kontrol edilir ve kayıt altına alınır.

8. DENETİM, GÜVENLİK VE RİSK TEDBİRLERİ

- Günlük sıcak cüzdan dengeleri Uyum birimi tarafından kontrol edilir.
- Soğuk cüzdan içerikleri aylık olarak İç Denetim tarafından fiziksel olarak doğrulanır.
- Dış denetim firmaları tarafından yılda en az bir kez saklama sistemleri denetlenir.
- Cüzdan yazılımları açık kaynaklı olup, dış denetimden geçirilmiş olmalıdır.

9. İŞ SÜREKLİLİĞİ VE OLAĞANÜSTÜ DURUM YÖNETİMİ

- Soğuk cüzdanlara ilişkin yedek anahtarlar güvenli konumda tutulur.
 - Felaket durumunda alternatif kurtarma planı uygulanır (anahtar kurtarma, soğuk cüzdan swap).
 - Olay müdahale planı, anlık izleme sistemleriyle entegre olarak işler.
-

10. KAYIT VE RAPORLAMA

- Cüzdan hareketleri, işlem onayları, imzalar ve erişim log'ları **en az 5 yıl süreyle** güvenli biçimde saklanır.
- Raporlar İç Denetim'e, Uyum'a ve gerektiğinde SPK'ya sunulmak üzere hazırlanır.
- Saklama raporları aylık, soğuk cüzdan denetim raporları 3 aylık olarak üst yönetime iletilir.

11. SON HÜKÜMLER

İş bu prosedür yılda bir gözden geçirilir ve güncellenir.