

TRANSFER EMİRLERİNİN GERÇEKLEŞTİRİLMESİ POLİTİKASI

Doküman Kodu: TEGP-PL-01

Yürürlük Tarihi: 09.04.2025

Revizyon No: 1.0

Hazırlayan Birim: Uyum ve Hukuk Direktörlüğü

Onaylayan: Yönetim Kurulu

İlgili Birimler: Operasyon Departmanı, Bilgi Teknolojileri Direktörlüğü, Risk Yönetimi Departmanı

1. Amaç

Bu politikanın amacı, AreonX Kripto Para Borsası müşterileri tarafından iletilen kripto varlık transfer emirlerinin gerçekleştirilmesine ilişkin süreçleri düzenlemek, müşteri varlıklarının güvenli, yasalara uygun, izlenebilir ve zamanında transfer edilmesini sağlamak ve FATF'in Travel Rule yükümlülüklerini içeren operasyonel çerçeveyi tanımlamaktır.

2. Kapsam

Bu politika; AreonX nezdinde tutulan kripto varlıkların:

- Müşterinin harici bir cüzdan adresine transfer edilmesi,
- Müşteriler arası iç transfer (peer-to-peer) işlemleri,
- Platformdan diğer VASP'lara (Virtual Asset Service Provider) yapılan transferleri,
- Geri ödeme ve iade süreçlerini kapsar.

3. Hukuki Dayanak

- 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun
- 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanun
- MASAK Yükümlülük Rehberi
- FATF R.16 / "Travel Rule" Rehber İlkeleri
- Sermaye Piyasası Kurulu düzenlemeleri ve SPK'nın III-35/B.2 sayılı tebliği

4. Temel İlkeler

AreonX aşağıdaki ilkelere uygun şekilde transfer emirlerini gerçekleştirir:

- **Kimlik Doğrulama:** Transfer talebinde bulunan müşterinin kimliği, çift aşamalı kimlik doğrulama dahil olmak üzere doğrulanır.
- **Varlık Sınırı Kontrolü:** Transfer talebi öncesinde cüzdan bakiyesi, varlık blokajı ve günlük/aylık limitler kontrol edilir.
- **Kaynak Sorgulama:** Belirli tutarların üzerindeki transferlerde kaynak ve amaç beyanı alınır.
- **Uygunluk Denetimi:** Adres, IP ve karşı taraf VASP bilgileri, kara liste (sanctions) ve coğrafi risk taramasından geçirilir.
- **Kayıt ve İzlenebilirlik:** Her transfer işlemi detaylı biçimde kayıt altına alınır ve denetime hazır formatta saklanır.

5. Transfer Süreci ve Aşamalar

5.1 Müşteri Talebi

- Müşteri transfer işlemi kullanıcı arayüzü veya API üzerinden iletir.
- Transfer miktarı, varlık tipi, hedef cüzdan adresi ve açıklama bilgisi alınır.

5.2 Teknik ve Operasyonel Kontroller

- Cüzdan adresi biçimsel doğrulama ve ağ uyumu kontrolünden geçer.
- Transfer edilen varlık tipi ile hedef ağ tipi (örn. ERC-20, TRC-20) eşleşmesi yapılır.
- Sistemsel olarak minimum/maximum transfer limitleri ve saatlik yoğunluk analizleri uygulanır.
- AML risk skoru ve adres etiketleme sistemi (örneğin Chainalysis veya TRM Labs) tarafından değerlendirilir.

5.3 Travel Rule Uygulaması (VASP ↔ VASP)

- 1.000 USD ve üzeri transferlerde alıcı VASP bilgisi talep edilir.
- Gönderici adı, soyadı, adresi ve gönderilen varlık tutarı, transfer mesajıyla birlikte şifreli biçimde karşı tarafa iletir.

- Alıcı VASP bilgisi eksikse işlem ertelenir ve müşteri bilgilendirilir.
- AreonX, gerekli veri aktarımını TRP (Travel Rule Protocol), IVMS 101 veya benzeri FATF uyumlu protokollerle sağlar.

5.4 Onay ve Gerçekleştirme

- Tüm kontrollerin olumlu tamamlanması hâlinde sistem işlemi onaylar.
- İşlem blockchain ağına gönderilir ve hash değeri ile birlikte müşteri panelinde görüntülenir.
- Transfer süresi, blok ağ yoğunluğuna göre değişkenlik gösterebilir.

6. İç Transfer İşlemleri

- AreonX içi kullanıcılar arası transferler sistem içinde, zincir dışı (off-chain) olarak gerçekleştirilir.
- Bu işlemler Travel Rule kapsamı dışındadır ancak AML taramasına tabidir.
- Sistemsel eşleşme ve bakiye güncellemesi anlık olarak tamamlanır.

7. Reddedilen veya İptal Edilen Transferler

Aşağıdaki durumlarda transfer emri reddedilir veya durdurulur:

- Alıcı adresin yüksek riskli veya kara listede olması
- Transferin şüpheli işlem kriterlerine takılması
- Adresin VASP olarak doğrulanamaması (Travel Rule uyumsuzluğu)
- Transfer emrinde çifte giriş veya yetkisiz cihaz kullanımı
- Transfer emrinin düzenleyici kurumlarca bloke edilmesi

Reddedilen işlemler sistem kayıtlarında ayrı olarak tutulur ve müşteri bilgilendirilir.

8. İzleme, Kayıt ve Raporlama

- Tüm transfer işlemleri, zaman damgalı şekilde sistem günlüklerine kaydedilir.
- 1.000 USD ve üzeri VASP transferleri için giden ve gelen tüm bilgiler 5 yıl süreyle saklanır.

- Transfer işlemleri aylık olarak Uyum ve Risk Yönetimi tarafından analiz edilir.
 - Gerekli durumlarda SPK ve MASAK'a bildirim yapılır.
-

9. Politikanın Gözden Geçirilmesi

Bu politika yılda en az bir kez gözden geçirilir. Mevzuat değişiklikleri, FATF güncellemeleri veya iç denetim sonuçlarına bağlı olarak güncellenir. Güncellemeler Yönetim Kurulu onayına sunulur.