IPKC-E

IP Kripto Cihazı ve Güvenlik Yönetim Merkezi

TÜBİTAK
UEKAE
ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

YEREL ALAN AĞLARI ÜZERİNDEN GÜVENLİ İLETİŞİM

IPKC-E, güvensiz ağlar üzerinden haberleşen IP/Ethernet tipi yerel alan ağları (LAN) arasındaki traŞğin güvenliğini sağlar. Cihaz yerel ağ ile yönlendirici ya da geçit arasında bağlanır ve böylece bir güvenlik geçiti oluşturur. Cihazın sağladığı güvenlik hizmetleri şunlardır: Veri gizliliği, kimlik doğrulama, veri bütünlüğü ve traŞk akış gizliliği.

IPKC-E GÜVENLİK YÖNETİM MERKEZİ

IPKC-E Yönetim Merkezi IPKC-E cihazlarının konfigürasyon, gözetleme ve güvenlik yönlerinden merkezi yönetimini sağlayan yazılım çözümüdür.

IPKC-E Yönetim Merkezi kripto cihazlarının konfigürasyon işlemlerini uzaktan gerçekleştirir. Gözetleme ve olay mekanizmaları kullanıcıya alarmlar ve olaylar hakkında anlık bilgi sağlar. Kripto cihazlarının arasında güvenlik politikaları ve birlikleri Yönetim Merkezi kullanılarak kolaylıkla oluşturulur. IPKC-E Yönetim Merkezi aynı zamanda anahtar dağıtımı ve yazılım güncelleme işlerini gerçekleştirir.

IPKC-E ANAHTAR ÜRETİM CİHAZI

Anahtar Üretim Cihazı (IPKC-AÜC), IP Kripto Cihazları (IPKC) için kriptografik anahtar üretimi, saklanması ve dağıtımı işlevlerini yerine getirir.

Cihaz aynı zamanda, IPKC'lerin güvenli bir şekilde yazılım terfisininin gerçekleştirilmesinde IPKC yazılımı için kriptografik koruma sağlar.

IPKC-AÜC, donanımsal gerçek rassal sayı üretecine sahiptir ve güçlü milli algoritmalar ile veri şifreleme yapar. Cihazda fiziksel saldırılara karşı kurcalama koruması ve acil silme düğmesi mevcuttur.

IPKC-AÜC, kullanıcı arayüz yazılımı ile seri konsol bağlantısı ile yönetilir.

TÜBİTAK UEKAE

HABERLEŞME VE BİLGİ GÜVENLİĞİ

TEKNİK ÖZELLİKLER (IPKC-E)

Uygulama	IP/Ethernet ağlarının güvenli olmayan korumasız ağlar üzerinden güvenli olarak haberleştirilmesi
Güvenlik Hizmetleri	- Veri gizliliği (şifreleme) - Kimlik doğrulaması - Veri bütünlüğü - Trafik akış gizliliği
Algoritmalar	- Şifreleme : TÜBİTAK UEKAE onaylı milli algoritma - Kimlik doğrulama : HMAC-MD5 (RFC 2104, RFC 2085)
Anahtar Girişi	Anahtar yükleyici kullanılarak manual
Anahtar Belleği	- Güç kesintilerinde anahtarların korunması - En az 48 saate kadar saklama
Güvenlik Protokolleri	- IPSec: IP güvenlik mimarisi (RFC 2401) - AH: Authentication Header (RFC 2402) - ESP: Encapsulating Security Payload (RFC 2406)
Erişim Güvenliği	- Mekanik anahtarla acil-silme (güç beslemesi olmasa bile) - Konsol ile düzenlemede parola ile koruma - Yetki anahtarı
Haberleşme Protokolleri	IP, ARP, ICMP , TCP, UDP
Ağ Arayüzleri	Siyah ve Kırmızı: 10/100 Mbit/s Ethernet (IEEE 802.3), 100BaseFX (ST)
İzleme	- Olayların kaydı - Alarmların kaydı - İşlem bilgilerinin kaydı
Kullanıcı Arayüzü	- Ön-panel (butonlar, gösterge, lambalar v.b.) - Konsol portu üzerinden komuta-dayalı düzenleme
EMI/EMC	MIL-STD-461E, AMSG-720
Güç Beslemesi	- 110/220 VAC, 47...63 Hz - Güç harcaması en çok 60 VA
Çevresel Koşullar	- Çalışma sıcaklığı : 0 °C...+45 °C - Depolama sıcaklığı : -20 °C...+65 °C - Bağıl nem : +40 °C sıcaklıkta %90
Ağırlık	< 15 kg.
Boyutlar	- Masaüstü ya da 19" çekmeceye monte edilebilir - Genişlik : 427 mm - Yükseklik : 132 mm (3U) - Derinlik : 306 mm

Devam eden araştırma ve geliştirme çalışmaları sonucunda, önceden uyarı olmaksızın burada belirtilen özellikler değişebilir.

TEKNİK ÖZELLİKLER (IPKC-E GÜVENLİK YÖNETİM MERKEZİ)	
Yönetim Özellikleri	- Kimlik Doğrulama ve Yetkilendirme: Kullanıcılar için değişik erişim hakları. - Kolay Kullanıcı Arayüzü: Cihaz konfigürasyonu ve gözetleme için kullanışlı gruplama ve gösterim mekanizmaları. - Alarm Filtreleme: Yönetim Merkezi alarm incelemesini kolaylaştıran gelişmiş filtreleme özellikleri. - Alert Filtering: Alarmlar için farklı uyarılar kurulabilir. Yönetim Merkezi kullanıcı tanımlı uyarı filtrelerine uyan bir alarm oluştuğunda mesaj, ses ve e-posta ile uyarı verebilir. - Otomatik Yoklama: Yönetim Merkezi yönetilen bütün cihazların yönetim bağlantısını öğrenmek için cihazları periyodik olarak yoklar. - Sistem Jurnal: Yönetim Merkezi kullanıcı hareketlerini jurnaller.
Platform Gereksinimleri	Windows 2000 Professional , Windows XP Professional
Yazılım Gereksinimleri	MSSQL 2000
IPKC-E Konfigürasyon Yönetimi Yönetim Servisleri	- IPKC-E kaydı, değiştirme ve silme - Grup oluşturma, değiştirme ve silme - Sürekli konfigürasyon ve alarm loglarını toplama ve gösterme - IPKC-E Yönlendirme tablosu yönetimi - Paket izleme, trafik MIB sayaçlarının gözlenmesi - Uzaktan IPKC-E'ye ping attırma ve ARP Tablosu görüntüleme - Uzaktan IPKC-E konfigürasyon yedeği alma
IPKC-E Güvenlik Yönetimi ve Anahtar Dağıtımı Yönetim Servisleri	- Güvenlik Birlikleri, IKE Tanımları, Kripto Haritası ve Güvenlik Politikası ekleme, değiştirme ve silme - IPKC-E'nin anahtar konfigürasyonlarını görüntüleme - IPKC-E'lere güvenli trafik ve sistem anahtarları dağıtımı - Anahtar dağıtımı envanteri - IPKC-E'lerin güvenli uzaktan yazılım güncellemesi
Devam eden araştırma ve geliştirme çalışmaları sonucunda, önceden uyarı olmaksızın burada belirtilen özellikler değişebilir.	

TEKNİK ÖZELLİKLER (IPKC-E ANAHTAR ÜRETİM CİHAZI)

Uygulama	IPKC ağ güvenliği sistemi için kriptografik anahtar üretim ve dağıtımı
Servisler	- Anahtar Üretimi - Anahtar Saklama - Anahtar Dağıtımı - Anahtar Silme - IPKC yazılım terfisi için güvenlik
Algoritmalar	- Simetrik fiifreleme: Milli algoritma - Hash: SHA - İmzalama: DSA
Anahtar Üretimi	- IKE önpaylaşımlı anahtarlar - Şifreleme anahtarları - Kimlik doğrulama anahtarları
Dağıtım	Milay, CD, Disket
Erişim Denetimi	Kullanıcı kimliği ve parola ile
Yönetim Arayüzü	RS-232 Seri Port
Kayıt Tutma	- İşlem bilgisi - Alarm ve sistem olayları
Kullanıcı Arayüzü	- Ön Panel ekranı ve lambaları - Grafiksel Kullanıcı Arayüzü Yazılımı
TEMPEST/EMI/EMC	MIL-STD-461, MIL-STD-462, AMSG-720
Güç Beslemesi	110/220 VAC, 47…63 Hz
Çevresel Koşullar	- Çalışma Sıcaklılğ: 0 °C…+45 °C - Depolama Sıcaklığı: -20 °C…+65 °C - Bağıl Nem: +40 °C'de %90
Ağırlık	10 kg
Boyutlar	Genişlik: 470 mm Yükseklik: 88 mm Derinlik: 306 mm

Devam eden araştırma ve geliştirme çalışmaları sonucunda, önceden uyarı olmaksızın burada belirtilen özellikler değişebilir.

TÜBİTAK UEKAE
T: 0262 648 1000 • F: 0262 648 1100 • E: uekae@uekae.tubitak.gov.tr
W: http://www.uekae.tubitak.gov.tr • A: PK.: 74, 41470, Gebze, Kocaeli