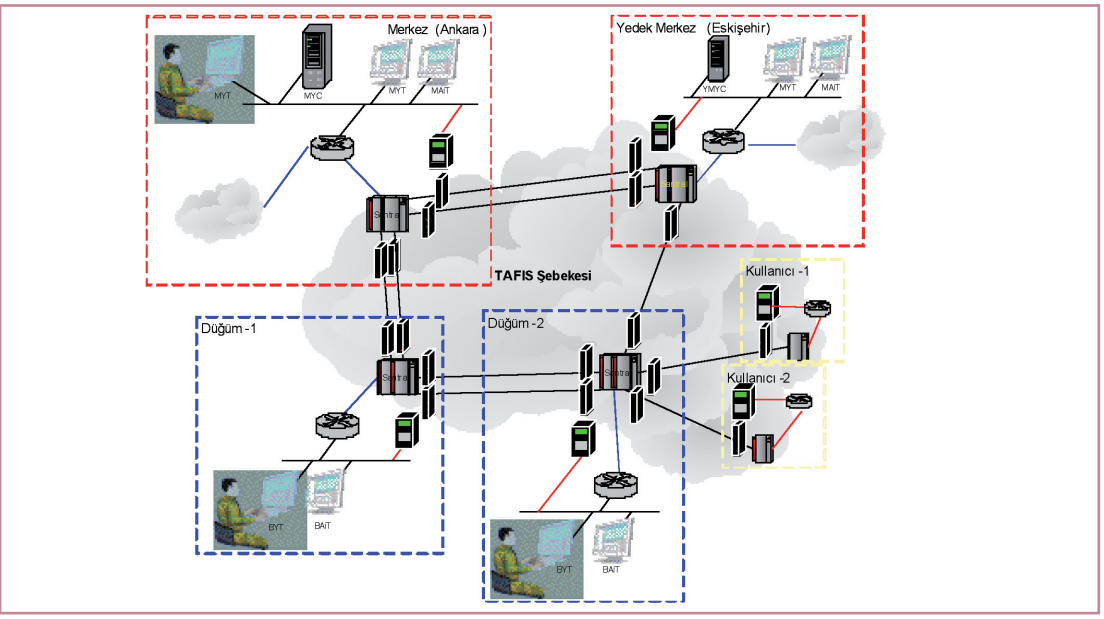
TELAYS

TAFICS Elektronik Anahtar Yönetim Sistemi

TÜBİTAK
UEKAE
ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ



TAFICS ANAHTAR YÖNETİMİ İÇİN ULUSAL ÇÖZÜM

TELAYS (TAFICS Elektronik Anahtar Yönetim Sistemi), TAFICS kripto cihazlarının (MILON ailesi ve SVKC-Senkron Veri Kripto Cihazı) ihtiyaç duyduğu kripto anahtarlarını üreten, çevrim-içi ve çevrim-dışı güvenli yollardan uç noktadaki kripto cihazlarına(MILON ailesi ve SVKC) dağıtan ve muhasebe bilgilerini saklayan yönetim sistemidir.

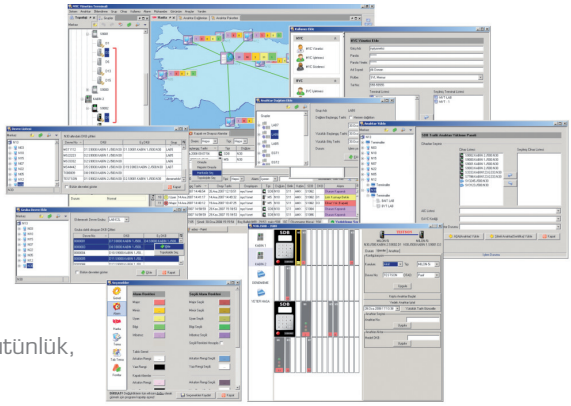
TELAYS anahtar yönetimi, alarmları ve cihaz arızalarına ilişkin durumlar merkez ve düğüm terminallerinde anında izlenir.

TELAYS (TAFICS ELEKTRONIK ANAHTAR YÖNETİM SİSTEMİ)

Merkezi Yönetim Cihazı (MYC Sunucu), Merkezi ve Bölgesel Yönetim Terminalleri (MYT, BYT), Merkezi ve Bölgesel Alarm İzleme Terminalleri (MAİT, BAİT), Anahtar Üretim ve İşleme Cihazları (AİCÜ, AİC&Ü), Elektronik Kripto Anahtar İletim ve Yükleme Cihazı (MİLAY), VPN Cihazlarından (IPKCE) ve SDB (veya SVKC) den oluşan TELAYS, TAFICS'in güvenliğini sağlayan cihazların tüm anahtar ihtiyaçlarına çözüm sunar.

TELAYS'ın üstün özellikleri şunlardır:

- Otomatik Anahtar Üretimi ve Dağıtımı
- Milli Kriptografik Algoritmalar
- Elektronik ve Manuel Anahtar Dağıtımı
- Uzaktan, Kripto Cihazı Konfigürasyon Yönetimi
- Kripto Cihazları ve Terminallerin Çevrim-içi İzlenmesi
- Etkin Alarm Yönetimi ve Uyarı Sistemi
- Kullanıcı İşlem Kayıtları ve Muhasebe Bilgilerinin Arşivlenmesi
- Cihazlar Arası Güvenli Haberleşme (Kimlik Doğrulama, Gizlilik, Bütünlük, Trafik Doldurma)
- Rol Tabanlı Kullanıcı Erişim Denetimi
- Sistemin Güvenirliğini Artıran Yedek MYC (YMYC) Üzerinde Anında Veritabanı Yedekleme ve Arşivleme.



TÜBİTAK UEKAE

HABERLEŞME VE BİLGİ GÜVENLİĞİ

TELAYS TEKNİK ÖZELLİKLERİ

Genel Özellikler	- Kullanımı kolay ve esnek kullanıcı arayüzü sayesinde gelişmiş pencere yönetimi ve kişisel kullanıcı arayüzü profili oluşturma - Kullanıcı ve sistem hareketlerinin loglanması - Çok sayıda terminal bağlantısı olanağı - Etkin Alarm Yönetimi ve Uyarı Sistemi
Anahtar Yönetim Servisler	- Cihazların ve terminallerin kriptografik ilklendirilmesi - Anahtar dağıtım grupları oluşturma - İletişim anahtarlarının ve sertifikalarının üretimi, dağıtımı - Otomatik ve manuel anahtar dağıtımı
Konfigurasyon Yönetimi	- Kripto cihazlarının bölgesel yönetimi - TAFICS iletişim devrelerinin tanımlaması ve gruplanması - Cihaz konfigürasyon değişikliklerini izleme - Kripto cihazlarının uzaktan konfigurasyonu - Terminal yazılımlarının uzaktan otomatik güncellenmesi
Alarm Yönetimi	- Kripto cihazlarının alarmlarını çevrim-içi izleme - Alarmların terminallerde harita üzerinde ve liste olarak yansıtılması - Alarmların filtrenmesi, onaylanması ve arşivlenmesi - Alarm önceliklerini ve renklerini değiştirebilme
Güvenlik	- Şifreli anahtarların Kriptolu hatlar üzerinden iletilmesi - TÜBİTAK Kripto Analiz Merkezi onaylı algoritmalar ve protokoller - SSL ve kripto kartını kullanan çift yönlü kimlik doğrulama ve şifreli iletişim - Rol tabanlı kullanıcı erişim denetimi - Kullanıcıların aktivitelerinin sistemde kayıtlanması - Yedek MYC(YMYC) merkezine veritabanı yedekleme ve arşivleme
Platform Gereksinimleri	Sunucu - Windows XP/2000/2003 - Oracle 10g - JBoss Application Server - Intel(r) Pentium(tm) 4 İşlemci (min) - 4 GB hafıza (min) - 80 GB Sabit Disk (min) - 2 adet Ağ Kartı - CD-RW/DVD-ROM 24X Sürücü - AİC&Ü (Anahtar İşleme ve Üretim Cihazı) - IPKC Kripto Cihazı - UEKAE Kripto Kartı (PCI-X) - Yedekleme Teyp Kartuşları
Terminal	- Windows Professional XP/2000 - Intel Pentium 4 işlemci, 1 GB hafıza (min) - 20 GB sabit disk (min)

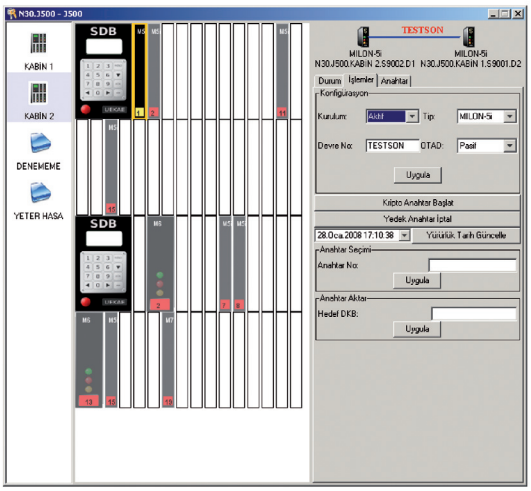
Devam eden araştırma ve geliştirme çalışmaları sonucunda, önceden uyarı olmaksızın burada belirtilen özellikler değişebilir.

SDB (SİSTEM DENETİM BİRİMİ)

SDB cihazları, uç kripto cihazlarının alt yönetim birimidir. Uç kripto cihazlarının yönetimi, SDB üzerinde bulunan tuştakımı (HMI) ile ya da uzaktan TELAYS terminalleri aracılığı ile (merkez ya da düğüm) elektronik olarak yapılır.

SDB cihazları, anahtar yönetimi ve cihaz/ iletişim arızalarına ilişkin alarmları TELAYS merkez ve düğüm merkezi terminallerine anında iletir.

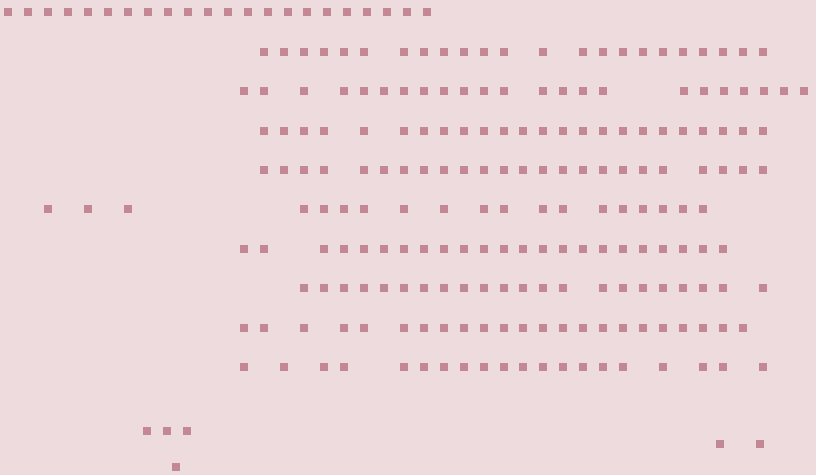
Ayrıca anahtarların uç kripto cihazlarına dağıtılması ve alarmların toplanıp merkeze yollanması ve uç kripto cihazlarına yerinde müdehale edilmesini sağlar.



SDB TEKNİK ÖZELLİKLERİ

Genel Özellikler	- TELAYS ile çevrim-içi bağlanma - Kripto cihazlarının uzaktan veya elle kontrolü - Kullanıcı ve sistem hareketlerini arşivleme - Alarm Durumlarını Anında Bildirme - En fazla 30 adet DKB(Demet Kripto Birimi) kontrol etme
Anahtar Yükleme	- TELAYS ile otomatik olarak anahtar yükleme - MILAY-1(Milli Elektronik Anahtar Yükleyici) ile şifreli veya açık anahtar yükleme - Tuş takımında anahtar yazma - Özel bakım anahtarları
Anahtar Belleği	- Güç kesintilerinde anahtarların korunması - En az 48 saate kadar saklama - Milon-5 ve Milon-6 için 188, Milon-7 için 94 adetlik anahtar kapasitesi
Güvenlik	- Filtreli giriş-çıkış bağlantıları - Mekanik anahtarlarla acil-silme(besleme gerilimi olsun veya olmasın) - Sistem parametrelerinin korunması için kalıcı bellek - TELAYS ile şifreli ağ bağlantısı (ilklendirme-sertifika)
EMI/EMC	- MIL-STD-461, MIL-STD-462, AMSG-720
Güç Beslemesi	- - 48 VDC (36 - 72 VDC aralığı)
Çevresel Koşullar	- Çalışma sıcaklığı : 0 C...+50 C - Depolama sıcaklığı : -30...+70 C - Bağıl Nem : +40 C sıcaklıkta %95

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