UKİS 2 Serisi

Akıllı Kart İşletim Sistemi

TÜBİTAK
BİLGEM
BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

AKILLI KART

İçerisinde mikrobilgisayar (mikroişlemci), bellek ve şifreleme makinası (kriptoişlemci) barındıran ve oldukça az elektriksel güç tüketerek dış dünya ile temaslı veya temassız olarak iletişim kuran, tek bir yongadan (chip) oluşan modüle akıllı kart modülü, bu modülün bir PVC, PET veya PC üzerine yapıştırılması ile elde edilen karta da Akıllı Kart denir.

Akıllı Kart donanım birimleri

* Mikrodenetleyici (mikrobilgisayar) birimi
* ROM bellek (İşletim Sistemini barındırır)
* Dosyaların bulunduğu işlem belleği (kalıcı EEPROM, geçici RAM)
* Şifreleme işlemleri için Şifre Makinası (Kripto İşlemci)
* Dış çevre ile temaslı iletişim birimi

AKILLI KARTIN YAYGIN KULLANIM ALANLARI

Akıllı kartların kullanıldığı yaygın uygulama alanları;

* Kimlik Kartı,
* Sürücü Belgesi,
* Elektronik (Sayısal) İmza Kartı,
* Cep telefonu SIM Kartı,
* Banka Kartı,
* Cihaz Kartı,
* Kurumlara Özel Kartlar (ödeme sistemleri, toplu taşıma sistemleri, otomatik geçiş sistemleri vb.)

TÜBİTAK BİLGEM

AKILLI KART İŞLETİM SİSTEMİ VE UKİS

Akıllı Kart İşletim Sistemi, akıllı kart donanımını kullanarak dış dünya ile belli standartlar çerçevesinde (ISO 7816) güvenli veri alışverişinde bulunulmasını sağlayan ve çeşitli şifreleme yöntemlerini kullanarak modül içerisindeki bilginin uygun bir yöntemle gizlilik içersinde saklanmasını, yönetilmesini gerçekleştiren ve ROM / EEPROM bellek içerisinde bulunan bellenim (firmware) programıdır.

UKİS (Akıllı Kart İşletim Sistemi), akıllı kart yongaları üzerindeki bilgi güvenliği, kimlik tanıma, sayısal imza ve güvenli bilgi taşıma uygulamalarını çalıştıran, TÜBİTAK BİLGEM UEKAE tarafından geliştirilmiş milli bir işletim sistemidir.

UKİS GENEL ÖZELLİKLERİ

Dış dünya ile ISO-7816 standart mesaj kümeleri ile iletişim kurma
Bilgilerin EEPROM'daki bellekte şifreli olarak saklanması
Çeşitli şifreleme yöntemleriyle güvenli mesajlaşma
Değişik şifreleme yöntemleri (3DES, AES, RSA)
Özgün Dosya Yönetim Sistemi (MF, DF, EF'lerin yönetimi)
Özgün Bellek Yönetim Sistemi
SPA / DPA Saldırılarına karşı koruma (donanım seviyesinde)
Yapısal Güvenlik Mimarisi ve Güvenli Anahtar Yönetimi
PC / SC, PKCS#11 / CSP ve mini driver uyumlu, CT-API

UKİS GÜVENLİĞİ VE KRİPTOGRAFİK SERVİSLER

* Gerekçeklenen Algoritmalar: RSA 1024 /2048 Bit (PKCS#11), SHA-1, SHA-256, Triple-DES (ECB, CBC, MAC, CMAC), AES (ECB, CBC, MAC, CMAC)
* Donanımsal 3DES makinası: Yazılım ile gerçekleştirilenden çok daha güvenli ve hızlı
* "Bellcore-Attack" Saldırılarına karşı koruma
* 3DES ve RSA için Sample Power Analysis (SPA) ve Differential Power Analysis (DPA) saldırılarına karşı koruma
* ISO 7816'da tanımlı zincir komut yapısı desteği (Command Chaining)
* Yonga içerisindeki ROM üzerinde yer alan kütüphane ile birlikte gerçek rasgele sayı üreticisi kullanılarak rasgele sayı üretme (FIPS 140-2)
* "On-chip" sayısal imza işlevleri
* CC EAL4+ güvenlik sertifikası

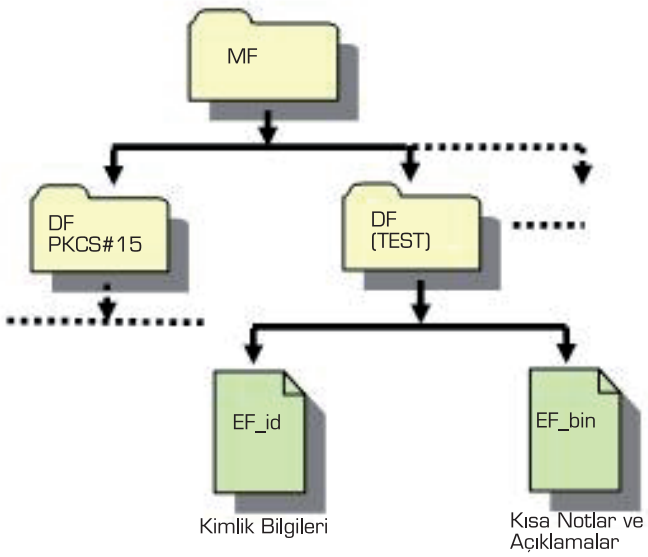
UKİS, Linux Yazılım Kütüphaneleri
Linux Thunderbird
Linux SmartCard Logon

UKİS, CSP Yazılım Kütüphaneleri
Microsoft's CAPI® yi destekleyen tüm uygulama yazılımları
Microsoft SmartCard Logon®
Microsoft Outlook ®
Microsoft Outlook Express®

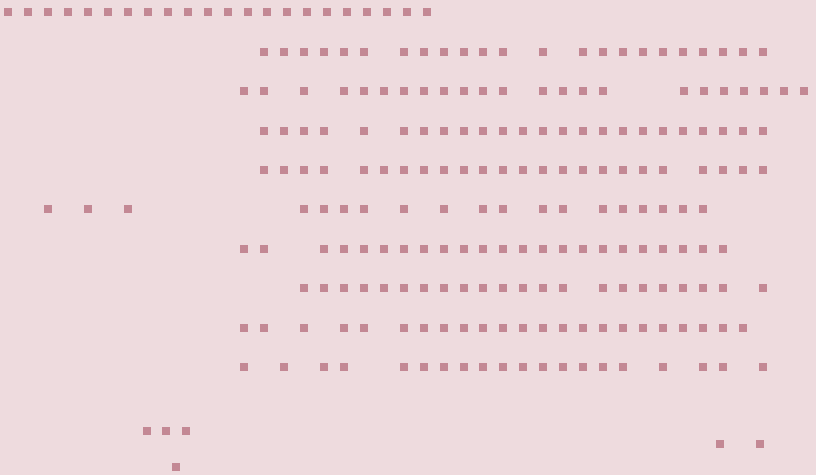
HABERLEŞME VE BİLGİ GÜVENLİĞİ

UKİS DOSYA / BELLEK YÖNETİM SİSTEMİ ÖZELLİKLERİ

* UKİS işletim sistemi yongaya özgü kripto mekanizmalarıyla korunmuş esnek, dinamik bellek ve dosya yönetim sistemine sahiptir.
* Bağımsız sayıda Dizin (DF) / Dosya (EF) oluşturulabilmektedir (En fazla 127 adet EF, DF).
* DF ve EF sayısı yonganın EEPROM belleğinin sığasına bağlıdır.
* UKİS, Dinamik bellek yönetimi ile varolan EEPROM bellek alanının kullanımını en verimli şekilde düzenler.
* UKİS, enerji dalgalanmalarından veya farklı fiziksel koşullardan dolayı EEPROM'daki bozulmaları düzelten bir mekanizmaya sahiptir.



* Farklı sertifikalar için farklı erişim hakları tanımlama olanağına sahiptir (Rol tabanlı erişim kuralları).
* Her komut veya veri nesnesi kendi erişim kuralları ile korunmaktadır.
* Tüm anahtarlar ve güvenlik nesneleri, uygulama dizinine bağlı sistem dosyası içerisinde güvenli olarak saklanmaktadır
* Şifreleme / Deşifreleme ve asıllama (Authentication) anahtarları birbirlerinden tümüyle ayrılmıştır.



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