AKİS
e-Pasaport Uygulamaları

TÜBİTAK
BİLGEM
BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

ELEKTRONİK PASAPORT

Ülke sınırlarından giriş/çıkış işlemlerinin elektronik olarak konrol edilmesi amacıyla içerisine yonga (chip) yerleştirilmiş olan pasaportlara elektronik pasaport (e-Pasaport) denir.

Elektronik pasaport ile geleneksel pasaport arasındaki en önemli fark içerisinde barındırdığı elektronik yongadır. Bu yongaların standartları ICAO (International Civil Aviation Organization) olarak adlandırılan Uluslararası Sivil Havacılık Organizasyonu tarafından belirlenmektedir.

ELEKTRONİK PASAPORT YONGASI İÇERİSİNDE BULUNAN BİLGİLER

Elektonik pasaport yongasının içerisinde Logical Data Structure (LDS) olarak adlandırılan veri grupları (DG) bulunmakta olup bunlardan DG1, DG2, COM ve SOD veri gruplarının elektronik pasaport içerisinde bulunulması zorunludur. Geri kalan veri grupları ülkelere göre değişim gösterir. Zorunlu veri gruplarından (DG1), elektronik pasaport üzerinde yazılı olan MRZ bilgisini bulundurur. DG2 veri grubunda ise pasaport sahibinin elektronik olarak yüz fotoğrafı bulunmaktadır. COM ve SOD veri dosyalarında ise elektronik pasaportun güvenliği ile ilgili bilgiler bulunmaktadır.

HABERLEŞME VE BİLGİ GÜVENLİĞİ

AKİS İŞLETİM SİSTEMİ ÜZERİNDE ÇALIŞAN e-PASAPORT UYGULAMASININ ÖZELLİKLERİ

ICAO 9303 LDS v1.7

ICAO Basic Access Control (BAC)

ICAO Active Authentication (AA)

ISO/IEC 14443-3 Type A

424 kbps / 848 kbps iletişim hızı

RSA şifreleme

SHA-1, SHA-256 özet alma algoritmaları

Güvenlik Onayı BSI-CC-PP 0055 (CC EAL 4+)

Standartlara uygun bütün e-Pasaport okuyucuları desteklenmektedir.

AKİS V1.4 ICAO SDK

- AKİS Yazılım Geliştirme Kit'i (SDK), bilgisayar üzerinde çalışan API, dll ve yazılım kütüphaneleri (AKİS CIF, PKCSS#11, CSP) aracılığıyla kolay yazılım geliştirilmesine olanak sağlamaktadır.

DESTEKLENEN DONANIMLAR

- Infineon SLE78CLX1600P
- NXP P5CD081

KİŞİSELLEŞTİRME

- AKİS e-Pasaport uygulaması, ICAO LDS v1.7 ile uyumlu veri gruplarının kişiselleştirme sürecini standartlara uygun olarak yönetir.
- ISO/IEC 7816-9 uyumlu komut seti
- RSA 1848 (Active Authentication), SHA-1, SHA-256 desteği
- PKCS#11 ve PKCS#15'e göre anahtar ve sertifikaların yönetimi
- Esnek ve dinamik dosya yönetimi

DOĞRULAMA

- ICAO 9303 LDS veri grupları ve sayısal imzayı destekleyen e-Pasaport uygulaması
- ISO/IEC 7816-4 uyumlu komut seti
- Basic Access Contol
- Kopyalamaya karşı Active Authentication

BASIC ACCESS CONTROL (BAC)

Temassız yonga içerisindeki verilere yetkili bir terminal tarafından erişimi sağlayan ve terminal ile temassız yonga arasındaki mesajlaşmanın güvenli bir şekilde yapılmasını sağlayan mekanizmadır. e-Pasaport üzerinde basılı olan MRZ bilgisinin optik olarak okunması ile oturum anaharlarının oluşturulmasını, doğrulanmasını ve güvenli mesajlaşmanın başlatılmasını sağlar.

ACTIVE AUTHENTICATION (AA)

e-Pasaport yongasının birebir kopyasının yapılmasını engeller.

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

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