



TÜBİTAK

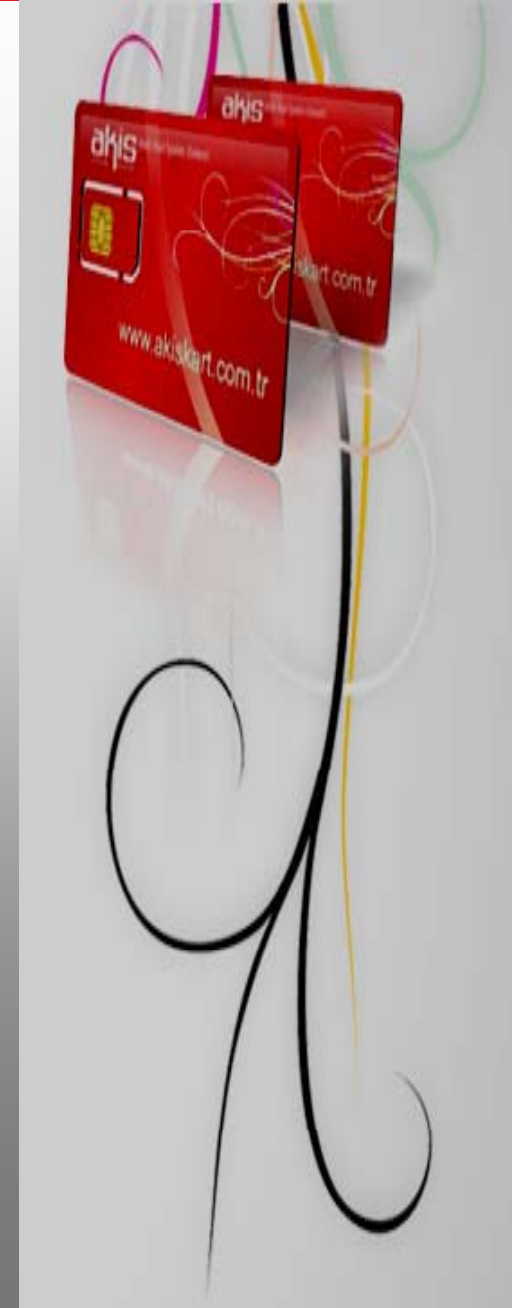
akış

Akıllı Kart İşletim Sistemi

Mustafa BAŞAK

9 Nisan 2009

- Akıllı Kart nedir?
- Akıllı Kart nasıl çalışır?
- Akıllı Kart Kullanım Alanları
- AKİS Uygulama Örnekleri
- Bilgi Güvenliğinde AKİS Kullanımı
- AKİS ve DONGLE Uygulamaları
- AKİS'in Güvenlik Önlemleri
- AKİS'li Yazılım Koruma Örnekleri



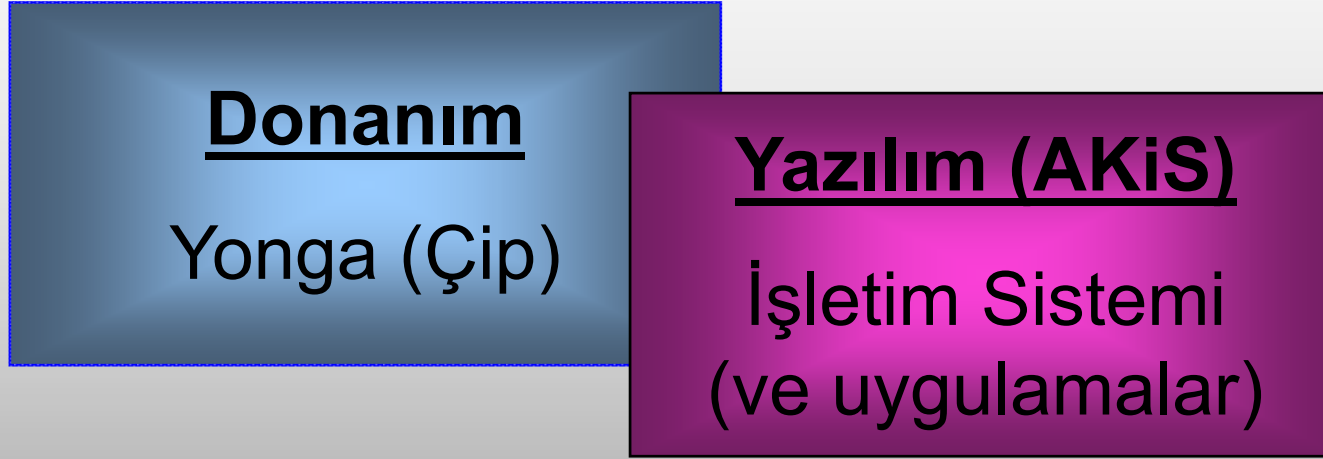
Akıllı Kart Nedir?

- Bilgiyi **güvenli** olarak kaydedebilen,
- Bilgiyi **saklayan**,
- Bilgiyi **paylaşan**,
- **İşlem yapan**,
- Cüzdanımıza girebilecek kadar **küçük**,
bir bilgisayardır.



Akıllı Kart Nasıl Çalışır?

Akıllı kart Mimarisi Bilgisayar Mimarisine benzer



İşletim sistemi üzerindeki yazılım parçacıkları

tüm işlemlerin

↓
güvenli ve **hızlı** şekilde gerçekleşmesini
↑
sağlar.

Akıllı Kart Kullanım Alanları

e-Kimlik, Akıllı kart tabanlı Ulusal Kimlik Kartı,
Nüfus sayımı, seçimler, askerlik belgeleri, evlilik
cüzdanı v.b.

e-Ehliyet, Akıllı kart tabanlı sürücü belgesi (Ehliyet).

e-Pasaport, Elektronik pasaport uygulaması.

Akıllı Kart Gerekliliđi (Güvenlik)

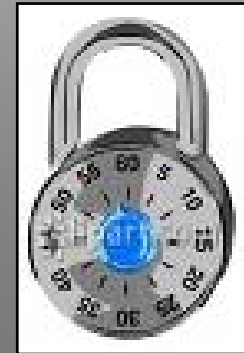
TEHDİT

- Veriye ulaşılması
- Verinin deđiştirilmesi



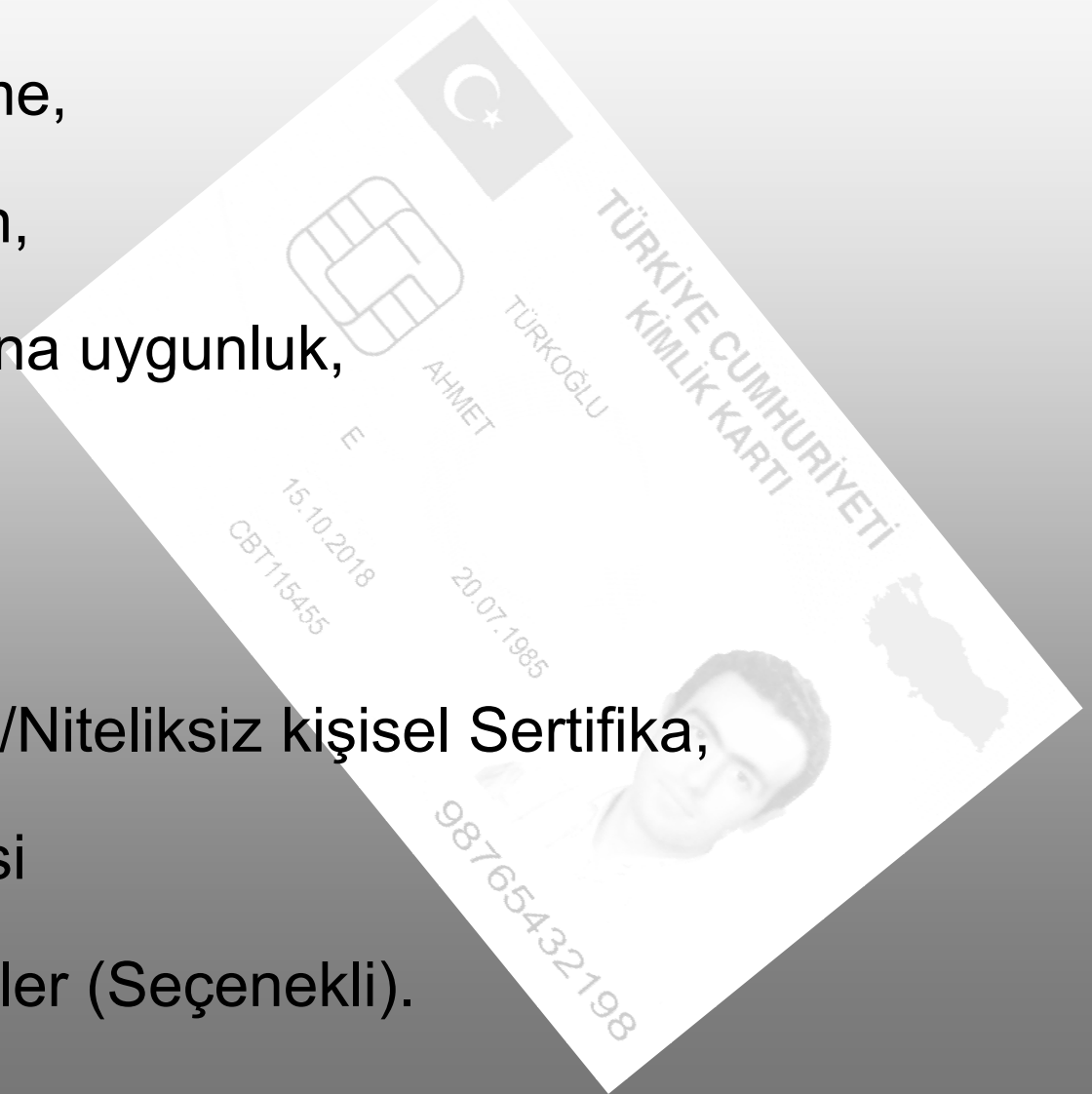
ÖNLEM

- Özel Güvenlik Algoritmaları
- Anahtarlar



- **Elektronik Kimlik Kartı Uygulaması (e-Kimlik)**

- Taklit edilememe,
- Kişiyeye özel alan,
- AB standartlarına uygunluk,
- Görsel bilgi,
- Elektronik bilgi,
- e-imza: Nitelikli/Niteliksiz kişisel Sertifika,
- Yeşil Kart Bilgisi
- Biyometrik Veriler (Seçenekli).



Güvenlik ögesi olarak kullanımı

- Yazılımın Güvenlik yardımcı işlemcisi,
- Yazılımın kendisinin (emeğın) korunması,

Virüslere karşı Yazılım bütünlük denetimi



AKiS'in Güvenlik Önlemleri

- CC EAL5+ yongalı ürünler (INF ve NXP).
- CC EAL4+ Yazılım sertifikası.
- Güvenlik önlemi alınmış RSA1024/2048 asimetrik şifreleme/deşifreleme yöntemi.
- Güvenlik önlemi alınmış DES/3DES simetrik şifreleme/deşifreleme yöntemi.
- Yonga üzerinde MAC bütünlük denetimi ve SHA-1 özet alma algoritmaları.
- Yonga üzerinde Gerçek Rastgele Sayı üretici (TRNG).
- PKI uyumlu sayısal imza işlevleri (PKCS#11).
- Güçlü PIN/PUK yönetimi.
- Araya girme yöntemi ile verilerin ele geçmesini engelleyen güvenli iletişim yöntemi (secure messaging).

AKiS kullanılarak gerçekleştirilen Yazılım Koruma Örnekleri

- UEKAE “FORESC” projesi
- UEKAE “SIR” projesi
- UEKAE “Kalkan” projesi
- MAM BTE uygulaması “RKA yazgel”
- UEKAE Elektronik Kimlik Kartı Projesi GEM modülü (şifreleme/doğrulama işlevi)



- Bankacılık sektöründe (AKİS-PARA)
- Şehircilik uygulamalarında (belediyeler)
 - Bankalar ile tümleşik (EMV uyumlu)
 - Elektronik bilet (ulaşım).
 - Belediye Hizmetleri (halk ekmek v.b).
 - İnternet üzerinden belediye hizmetleri (kuyrukları azaltır).
 -

AKiS V1.2 ve AKiS V2.0

