E-imza Donanımları

Elektronik imza ile ilgili donanımlar aşağıdaki şekilde sınıflandırılabilir:

- Akıllı kartlar
- Akıllı çubuklar
- Akıllı kart okuyucular
- Donanım Güvenlik Modülleri (Hardware Security Module : HSM)

Bu donanımlarla ilgili detaylı bilgi takip eden bölümlerde verilmiştir.

Akıllı Kartlar

Üstte kredi kartı boyutunda bir akıllı kart görülmektedir.

Üstte sim kart boyutunda bir akıllı kart görülmektedir.

X.509 Sertifikalarını ve bunlarla bağlı olan anahtarları taşımak için kullanılan en yaygın ve güvenli cihazlar akıllı kartlardır (smartcard). Akıllı kartların genel sınıflandırması aşağıdaki gibidir:

Elektronik Devre Yapısına Göre

- Bellek Kartları
  - Güvenlik Donanımlı
  - Güvenlik Donanımı Olmayan
- İşlemcili Kartlar
  - Kripto İşlemcili
  - Kripto İşlemcisi Olmayan

Veri Aktarım Tipine Göre

- Temaslı
- Temassız
- İki Arayüzlü (Temaslı+temassız)

Boyutuna Göre

- Kredi Kartı Boyutunda (ID-1)
- SIM Kart Boyutunda (ID-000)

Açık anahtar altyapısı ve e-imza sistemlerinde kullanılabilecek akıllı kartlar kripto işlemcili sınıfta yer alırlar. Bu akıllı kartlar, programlanabilir alanları olan, dayanıklı, taşınabilir bilgisayarlar olarak tanımlanabilir. Akıllı kartlar veri güvenliği, kimlik gizliliği ve mobil kullanıcı ihtiyaçlarına sahip sistemlerde faydalıdır. Bu kartların başlıca teknik özellikleri şöyle sıralanabilir:

- Mikroişlemci olarak gerçeklenmiştir (8, 16 ve 32 bit modeller vardır)
- Bir işletim sistemine sahiptir (AKIS, CardOS, Multos vb)
- RSA, DSA, ECDSA gibi asimetrik algoritmaları çalıştırabilen yardımcı kripto işlemcisine sahiptir
- İşletim sistemi ve kripto kütüphanesi mikroişlemcinin ROM belleğinde saklanır
- Kripto anahtarlarını ve sertifikaları saklamak için yeterli büyüklükte EEPROM belleğe sahiptir (Tercihen 8Kb ve üstü)
- Özel anahtarlar kart içine yerleştirildikten sonra asla kart dışına çıkarılamaz.
- Kart içindeki özel anahtarla işlem yapmak için (örneğin e-imza oluşturmak) karta PIN kodu girilmesi zorunludur

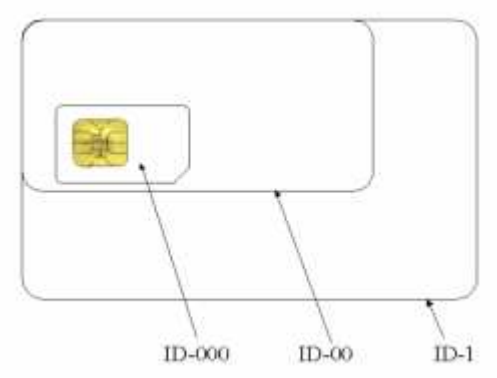
Bu tip akıllı kartlar aşağıdaki hizmetleri sunar:

- Kart üzerinde şifreleme ve şifre çözme
- Kart üzerinde imzalama ve imza onaylama
- Kart üzerinde özel ve açık anahtarların tutulması
- Kart içine bilgi yazabilme
- Kartın şifre ile korunması

Akıllı kartların özel (private) ve açık (public) alanları vardır. Özel alanda anahtar üretimi, imzalama, şifre çözme gibi işlemler yapılır, bu alana dışarıdan erişim yasaklanmıştır. Bu alanda yapılan işlemler Açık alana genel bilgiler yazılır. Akıllı kart yönetim yazılımı yardımıyla buradaki bilgiler görülebilir.

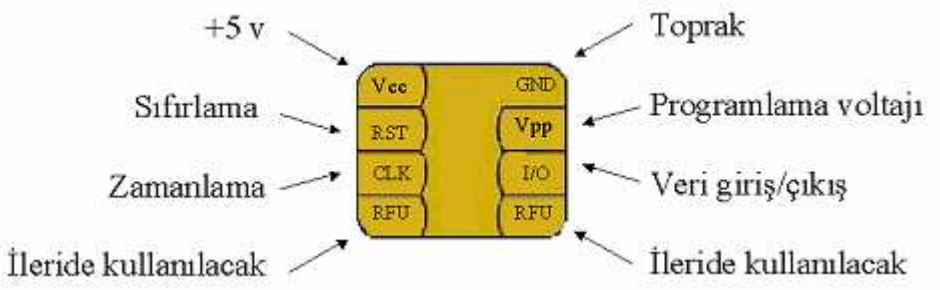
Kart Özellikleri

ISO 7816'da tanımlanan kart formatları aşağıdaki şekilde ve tabloda verilmiştir.



Format	Genişlik	Yükseklik	Kalınlık	Köşe Yarıçapı
ID-1	85,6 mm	54 mm	0,76 mm	3,18 mm
ID-00	66 mm	33 mm	0,76 mm	3,18 mm
ID-000	24 mm	15 mm	0,76 mm	1,00 mm

Kart üzerinde yer alan temas noktaları ve açıklamaları aşağıda verilmiştir.



Akıllı Çubuklar


Üstte çeşitli akıllı çubuklar görülmektedir.

Akıllı çubuklar, akıllı kartlarla aynı teknik özellikleri taşıyan fakat bilgisayarlara USB kapısından bağlanan cihazlardır. Yaygın olarak USB Token adıyla da anılırlar. Aslında akıllı çubuklar akıllı kart mikroişlemcisinin ve kart okuyucusunun bir araya getirildiği cihazlardır. Bu nedenle kullanılmaları için akıllı kart okuyucusuna gerek duyulmaz fakat maliyet olarak akıllı kartlardan 4-5 kat daha pahalıdırlar. Ayrıca bu tür cihazlarda kriptografik anahtarların ve sertifikaların saklanması için kullanılan EEPROM bellekler fiziksel olarak daha büyüktür. Bu nedenle akıllı çubukların içindeki kritik bilgilerin izinsiz olarak okunmasını hedefleyen saldırılar kolayca gerçekleştirilebilmektedir. Akıllı çubuklarla ilgili olarak yararlar ve sakıncalar aşağıda listelenmiştir.

Üstünlükleri

- Ayrı bir kart okuyucuya ihtiyaç duyulmaması
- Kolay taşınabilmesi
- Fiziki olarak dış etkilere daha dayanıklı olması

Zayıf Yanları

- Akıllı kartlara kıyasla 4-5 kat pahalı olması
- Güvenlik açısından akıllı kartlara göre çok daha zayıf olması (Kingpin tarafından yazılan "Attacks On and Countermeasures for USB Hardware Token Devices" makalesinde detaylı olarak bilgi verilmektedir)
- USB uçları çok fazla takma ve çıkarma işlemi sonucunda kısa sürede bozulabilmektedir
- Akıllı çubuk üzerine cihazın kime ait olduğunu gösterecek bir bilgi yazmak çok zordur (Farklı kişilerin akıllı çubuklarını ayırt etmek çok güçleşmektedir)

Yukarıda belirtilen sakıncalar nedeniyle akıllı çubukların kullanımı e-imza açısından çok faydalı görülmemektedir. Fakat yukarıda belirtilen yararları taşıyan akıllı çubuk şeklindeki kart okuyucuların kullanılması pratikte uygulanabilecek bir çözüm gibi gözükmektedir. Bu konuyla ilgili detaylı bilgi "Akıllı Kart Okuyucular" kısmında verilmektedir.

Akıllı Kart Okuyucular

Akıllı kartlar düşük kapasiteli birer bilgisayar olarak nitelendirilebilir. Bu kartların kendi enerji kaynakları olmadıkları için ancak bir okuyucu terminale bağlanarak kullanılabilirler. Bu terminallere akıllı kart okuyucu adı verilir. Akıllı kart okuyucuların bağlandıkları bilgisayarda kullanılabilmesi için sürücü yazılımlarının o bilgisayar yüklenmesi gerekir. Değişik akıllı kart okuyucu tipleri aşağıda anlatılmaktadır.

Masaüstü Akıllı Kart Okuyucular

Bu kart okuyucular en yaygın kullanılan modellerdir. Kredi kartı boyutundaki akıllı kartlarla kullanılırlar. Bilgisayara USB veya seri bağlantı ile bağlanırlar. Üzerinde yer alan ışık sayesinde kart ile işlem yapılıp yapılmadığı gözlenebilir.

Tuş Takımlı Kart Okuyucular

Bu tip okuyucular akıllı kart parolasını kendi üzerlerindeki tuş takımı aracılığıyla alabilirler. Böylece kart parolası başka bir cihaza (örneğin bilgisayara) iletilmez. Bu yöntem diğer okuyuculara göre daha güvenli çalışmasını sağlar. Bazı modeller tuş takımının yanı sıra LCD ekran da barındırır. Bilgisayara USB veya seri bağlantı ile bağlanırlar.

Akıllı Çubuk Şeklinde Kart Okuyucular

Bu tür kart okuyucular USB kapısından bilgisayara bağlanır ve SIM Kart boyutundaki akıllı kartlarla çalışırlar. Taşıdıkları akıllı kart nedeniyle akıllı çubuklardan daha güvenlidirler. SIM kart üstündeki plastik alan sınırlı da olsa bu bölgeye kart sahibi ile ilgili bazı bilgiler sığdırılabilir. Sadece kart okuyucu olduğu için masaüstü kart okuyucularla aynı fiyat aralığında temin edilebilmektedir.

PC Card Şeklinde Kart Okuyucular

Genellikle bu okuyucular taşınabilir bilgisayarların (notebook, laptop vs) PCMCIA yuvalarına takılarak kullanılır. Taşınabilir bilgisayarlar ile kullanımı pratiktir.

Klavye ile Bütünleşik Kart Okuyucular

Bu tür okuyucular bilgisayarlar için üretilen klavyelere bütünleşiktir. Bu tip klavyeler normal klavyelerden daha pahalıdır. Eğer klavyedeki tuşlar bozulursa kart okuyucu kısmı sağlam bile olsa klavyenin değiştirilmesi gerekir; bu da maliyeti yükseltici bir faktördür.

Disket Sürücü Şeklinde Kart Okuyucular

Bu tür okuyucular bilgisayarları 3.5" veya 5.25" genişleme yuvasına monte edilir ve bilgisayarın ana kartına bağlanır. Mevcut bilgisayarlara takılması ayrı bir işgücü gerektirdiği için çoğu kişi tarafından kullanışlı bulunmamaktadır.

Donanım Güvenlik Modülleri

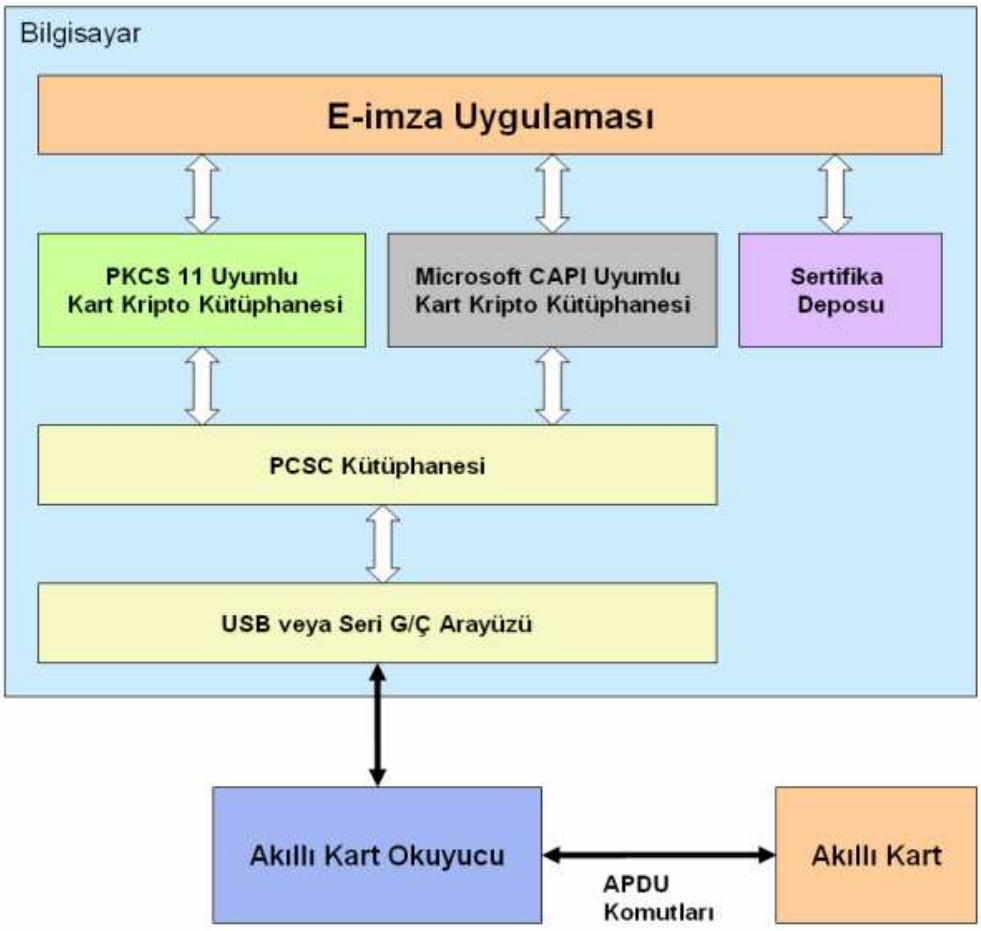
Donanım güvenlik modülleri çok yüksek kapasiteli akıllı kartlar gibi iş gören özel donanımlardır. Bu tür cihazlar da akıllı kartlar gibi kriptografik anahtarların saklanması ve cihaz vasıtasıyla kullanılması işine yararlar. Çok özel donanımlar oldukları için maliyetleri oldukça yüksektir. Bu cihazlar hem daha uzun anahtarlar kullanılmasına (4096 bit RSA gibi) yarar hem de çok yüksek performansla kripto işlemi yapabilirler (bazı modellerde saniyede 400 adet 1024 bit RSA işlemi gibi). Donanım güvenlik modülleri İngilizce HSM (Hardware veya Host Security Module) adıyla tanınır.

Donanım güvenlik modülleri iki temel tipte yer alır:

- **Adanmış modeller** : Bu modeller sadece bir bilgisayara bağlı olarak çalışır. PCI kart şeklinde veya bilgisayardaki bir SCSI kontrol kartına bağlana harici cihaz şeklinde olan modeller vardır.
- **Ağ modelleri** : Bu modeller kendi başlarına çalışırlar ama bir ağ arayüzüne sahiptirler. Genellikle bir yerel alan ağı (LAN) üzerinde çalışan birden fazla bilgisayara tarafından kullanılırlar.

İşletim Sistemleri ile Uyum

Akıllı kartların ve kart okuyucuların işletim sistemleri ile beraber çalışabilmesi için aşağıdaki çizimde gösterilen mimariye benzer bir yapı kullanılır.



Bir akıllı kartın işletim sisteminde kullanılabilmesi için aşağıdaki yazılımların yüklenmiş olması gereklidir:

- Akıllı kart kripto kütüphanesi
  - PKCS 11 Uyumlu Kütüphane: Bu kütüphane tipi genellikle açık kaynak kodlu ürünlerin akıllı karta erişim için tercih ettikleri kütüphanedir. Windows işletim sistemi dışındaki işletim sistemlerinde çok yaygın kullanılır.
  - Microsoft CAPI Uyumlu Kütüphane: Bu tip kütüphane Microsoft Windows işletim sistemi üzerinde kullanılmak üzere tanımlanmış bir standarda uygun yazılmıştır.
- Akıllı Kart Okuyucu Sürücüsü: Bilgisayara bağlanan tüm cihazlar gibi akıllı kart okuyucu için de bir sürücü yüklenmesi gereklidir.
- İşletim Sistemi Akıllı Kart Bileşenleri: Windows işletim sisteminde ve çoğu Linux dağıtımında hazır olarak gelen akıllı kart erişim altyapısı kullanılır. Yaygın olarak PCSC standardı kullanılır.