Akıllı Kart Teknolojileri

Recep Selami Özbey
TÜBİTAK UEKAE Gebze, KOCAELİ,
Yazar Adresi : selami@ueake.tubitak.gov.tr

ÖZET : İşlemcili kartlara akıllı kart denir. Bu kartlar kimlik doğrulama işlemi yanında kart sahibine ek imkanlar sunar. Bunlardan birkaçı elektronik posta imzalama, şifreleme, elektronik cüzdan, kontrollü binalara fiziksel giriş, bilgisayar sistemlerine giriş, sağlık alanında kullanımıdır. Bu özellikler akıllı kartların geniş bir alanda kullanımını sağlamaktadır. Bu bildiride akıllı kartlar hakkında genel bir tanıtma yapılacaktır.

ANAHTAR KELİMELER: Akıllı K, HSM, Akıllı Kart Okuyucu, AAA

SUBJECT OF PAPER

ABSTRACT : Processor cards are smartcards that can functıon as an idendity authentication and may also provide the cardholder with additional capabilities, such as digital signatures for email, email encryption, payment using an electronic purse, physical access to controlled buildings, logical access to computer systems, and data storage for medical information for use by authorized personnel. These features enable a smartcard to be used widely. This paper gives an overview of general smartcard technologies.

KEYWORDS : SmartCard, HSM, Smartcard Reader, PKI

Giriş

Akıllı kartlar yeni bir teknoloji değildir. 1974'de Fransız gazeteci Roland Moréno'nun akıllı kartı bulduğu kabul edilir. Bununla beraber, Almanya'dan Jargen Dethloff ve Japonya'daki Arimura Technology Institute'den Kunitaka Arimura, sırasıyla Şubat 1969 ve Mart 1970'de ilk patentleri aldılar. Moreno'nun dünya çapındaki patentleri banka tipi bir plastik kart içine bir mikrokontrolör gömme kavramını kapsıyordu. Kart endüstrisindeki firmaların O'nun kavramlarını desteklemeleri sürpriz olmadı. Bu durum Fransa'da hükümet, mali çevreler, toplu taşım, tıp ve haberleşme sektörleri içinde tartışma başlattı ve böylece teknolojik deneyler başlamış oldu. Yapılan deneyler sonucunda akıllı kartların sahtekârlığı önleme potansiyeli de vardır hükmüne varıldı ve bu hüküm bu güne kadar doğrulanmıştır.[4]

Akıllı kartlar, kredi kartı boyutlarında içerisinde işlemci, RAM ve ROM belleği bulunan gömülü bir mikroçipe sahip donanımlardır. Üzerinde manyetik şerit, barkod, temassız radyo frekans vericileri gibi farklı teknolojilerini bulundurabilir. Günümüzde giriş kontrolü, elektronik ticaret, kimlik doğrulama, kişisel gizlilik gerektiren bir çok uygulamada çok yaygın olarak kullanılmaya başlanmıştır. Bununla birlikte X.509 sertifikalarını ve bunlarla bağlı olan anahtarları taşımak için kullanılan en yaygın ve güvenli cihazlar akıllı kartlardır. Bu yazıda, akıllı kartların sınıflandırılması, akıllı çubuklar, akıllı kart okuyucular, donanım güvenlik modülü (HSM), açık anahtar altyapısında akıllı kartın önemi, akıllı kartlara erişim yöntemleri hakkında bilgi verilecektir.

Akıllı Kartların Sınıflandırılması

Akıllı kartlar elektronik devre yapılarına, veri aktarım tipine ve boyutlarına göre sınıflandırılabilirler. Akıllı kartlar veri tipine göre aşağıdaki gibi sınıflandırılabilirler.[1]

- Bellek kartları
  - Güvenlik donanımlı
  - Güvenlik donanımı olmayan
- İşlemcili Kartlar
  - Kripto işlemcili
  - Kripto işlemcili olmayan

Akıllı kartlar üzerinde bulunan mikroçipe göre "temaslı" ve "temassız" olmak üzere iki ana sınıfa ayrılır. Bazı kartlar temaslı ve temassız ara yüzleri üzerinde iki ayrı mikroçip olarak sunabilir. Bu tür kartlara hibrid kart adı verilir. Bu özelliğin aynı mikroçip üzerinde birleştirildiği kart tipine ise dual kart adı verilir.

Temaslı akıllı kart kullanımı sırasında kartın kart okuyucuya takılması gerekmektedir. Böylece kart yüzeyi üzerindeki iletken bölge ile doğrudan bağlantı kurulabilir.

Temassız akıllı kartlar bir işlem gerçekleştirebilmeleri için bir anten yanından geçirilirler. Bunlarda plastik kredi kartı görünümündedirler. Onlardan tek farkı içlerinde bir mikroçip ve bir de anten gömülü olmasıdır. Bu bileşenler fiziksel bir temas gerektirmeden, kartın anten ile bağlantı elemanı arasında iletişim kurmasını sağlar. İşlemlerin çok hızlı yapılmasının gerekli olduğu toplu taşımacılıkta ve jetonla çalışan sistemlerde temassız akıllı kartların kullanımı ideal bir çözümdür. Temassız akıllı kartlarda okuyucu ve kart arasındaki mesafe ise 10 cm'yi geçmemelidir.

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:[3]

- 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 dışarı çıkarılamaz.
- Kart içindeki özel anahtarla işlem yapmak için karta PIN kodu girilmesi zorunludur.

Yukarıdaki özelliklere sahip bir akıllı kart 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. Açık alana genel bilgiler yazılır. Akıllı kart yönetim yazılımı yardımıyla buradaki bilgiler görülebilir.

Akıllı kartın boyutları uluslararası ISO-7810 standardına göre belirlenir. ISO-7816 standardı ise ısı menzili, esneklik, elektriksel temasın pozisyonu ve mikroçipin dış dünya ile nasıl bağlantı kuracağı gibi özellikleri kapsayan, kartın fiziksel karakteristiğini de belirler.

Akıllı Çubuklar

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 tur cihazlarda kripto anahtarlarının ve sertifikalarının saklanması için kullanılan EEPROM bellekler fiziksel olarak daha büyüktür. Bu nedenle akıllı çubukların içindeki kritik bilgilerin izinsiz olarak okunmasını hedefleyen saldırılar kolayca gerçekleştirilebilmektedir. Akıllı çubukların kullanım kolaylıkları ve zayıf tarafları aşağıda listelenmiştir.

Kullanım kolaylıkları:

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

Zayıf yönleri:

- Akıllı kartlara kıyasla 4-5 kat pahalı olması.
- Güvenlik acısından 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 surede 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 acısından çok faydalı görülmemektedir. Fakat yukarıda belirtilen yararları taşıyan akıllı çubuk şeklindeki kart okuyucuların kullanılması pratikte uygulanabilecek bir çözüm gibi gözükmektedir.

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 yüklenmiş olması 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 Akıllı 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 Kart Seklinde 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 (HSM)

HSM (Hardware Security Module) çok yüksek kapasiteli akıllı kartlar gibi is gören özel bir donanımdır. Bu tür cihazlar da akıllı kartlar gibi kripto anahtarlarının saklanması ve cihaz vasıtasıyla kullanılması isine 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 iki temel tipte yer alır:

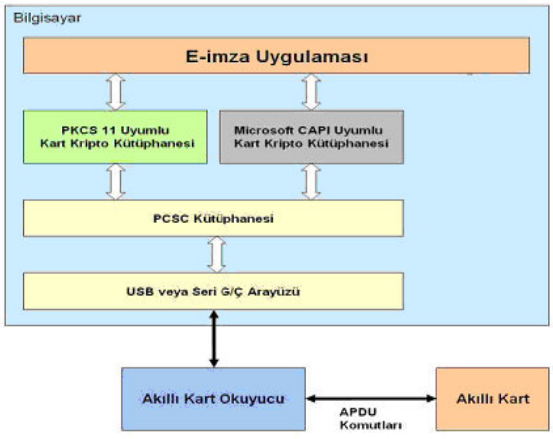
Adanmış modeller : Bu modeller sadece bir bilgisayara bağlı olarak çalışır. PCI kart seklinde veya bilgisayardaki bir SCSI kontrol kartına bağlana harici cihaz seklinde olan modeller vardır.
Ağ modelleri : Bu modeller kendi başlarına çalışırlar ama bir ağ ara yüzüne sahiptirler. Genellikle bir yerel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

Çoklu Uygulamalı Akıllı Kartlar

Akıllı kart teknolojisi birden fazla uygulamanın aynı kart üzerinde bulunmasına imkan tanır. Çoklu uygulamalı akıllı kartlar kimlik doğrulama, elektronik imza, e-posta şifreleme, elektronik cüzdan, fiziksel ve mantıksal erişim uygulamaları, sağlık alanında tıbbi bilgilerin depolanması gibi uygulamalarda hizmet verebilir. Çoklu uygulama hem temaslı hem de temassız akıllı kartlarda uygulanabilir.

Akıllı Kartlara Erişim Yöntemleri

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



Şekil-1:Akıllı karta erişim yöntemleri

Bir akıllı kartın işletim sisteminde kullanılabilmesi için aşağıdaki yazılımların yüklenmiş olması gerekmektedir.

- 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.
- Akıllı kart kripto kütüphanesi: Programcının akıllı karta erişmesini sağlayıp imzalama, şifreleme gibi işlemleri yaptırabileceği fonksiyonların bulunduğu kütüphanelerdir. Bunun için iki kütüphane vardır. Bunlardan ilki olan PKCS#11 uyumlu kütüphane genellikle acık kaynak kodlu ürünlerin akıllı karta erişim için tercih ettikleri kütüphanedir. Bu kütüphane, platform bağımsız akıllı kart uygulaması geliştirmek için kullanılan kütüphane olduğu için Windows, Linux… gibi farklı ortamlarda kullanılabilir. Diğer kütüphane ise Microsoft CAPI uyumlu kütüphanedir. Bu tip kütüphane Microsoft Windows işletim sistemi üzerinde kullanılmak üzere tanımlanmış bir standarda uygun yazılmıştır. Uygulaması yapılmış çok fazla sayıda kripto algoritması bulunmaktadır. Bunun için CSP içinde farklı algoritmalar tanımlanabilir. Bu nedenle CSP'ler destekledikleri CryptoAPI metotlarına göre gruplandırılabilirler. Mesela PROV_DSS bize DSS, MD5, SHA gibi kripto algoritmalarını sunarken PROV_RSA_FULL ise RSA şifreleme, imzalama, RC2 ve RC4 şifreleme ile SHA ve MD5 özet algoritmalarını sunmaktadır.[2]

APDU Komut Seti

APDU (Application Protocol Data Unit) okuyucu ile akıllı kartın arasındaki haberleşmeyi sağlayan bir yapısıdır. APDU'nun yapısı ISO-7816 standartında tanımlanmıştır. APDU yapısı komut ve cevap APDU'su olmak üzere ikiye ayrılır. Komut APDU'su okuyucudan karta gönderilen 5 bytelık başlık bilgisi ve en fazla 255 bytelık veri bloğuna sahiptir. Cevap APDU'su ise katran okuyucuya gönderilen ve 2 bytelık durum bilgisi ile en fazla 255 bytlelik veri bloğu içeren bir yapıdır.

Sonuç

Akıllı kartlar, sağladığı kolaylıkların yanında her geçen gün üzerine eklenen yeni kabiliyetleri sayesinde hayatın her alanında kullanılmaya başlanmıştır. Özellikle çoklu uygulamayı destekleyen akıllı kartların, verimliliği artırdığı ve maliyetleri düşürdüğü için hem özel sektör hem de kamu projelerinde kullanılması bir zorunluluk haline gelmiştir.

Kaynaklar

[1] www.smartcardalliance.org/pdf/industry_info/smartcardhandbook.pdf

[2] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnscard/html/smartcardcspcook.asp

[3] http://www.smartcard.co.uk/tutorials/sct-itsc.pdf

[4] www.girisim.com.tr