Akıllı Kartlar için Dinamik Güvenlik İşlevi
(Dynamic Security Function for Smart Cards)

Mustafa BAŞAK
ENTEK Elektronik ve Yazılım
mustafa@entekelektronik.com.tr

Prof. Dr. Eşref ADALI
İTÜ Bilgisayar Mühendisliği Bölümü
adali@itu.edu.tr

Özetçe

Günümüzde akıllı kartlar sıklıkla bilgi teknolojileri alanında kullanılmaya başladığından güvenlik önemli bir konu haline gelmiştir. Bu yazıda özellikle akıllı kartların güvenliğine yönelik saldırılar anlatılmıştır. Akıllı kart geliştirilmesi ile ilgili çalışmalar sırasında dikkat edilmesi gereken güvenlik konuları üzerinde durulmuştur. Bu makale güvenli akıllı kart işletim sistemi gereklerini ve akıllı kart donanım ve işletim sisteminin sağlaması gereken ortak ölçüt güvence seviyesini belirtir. Ayrıca bu makalede "dinamik güvenlik işlevi" olarak adlandırılan yeni güvenlik yaklaşımı ve kullanımı da anlatılmıştır.

Anahtar Sözcükler *:* Akıllı Kart, Güvenlik, APDU, DES, AES, RSA, PIN, PUK, SPA, CC EAL5+, CC

Abstract

Today, as the smart cards are frequently used in Information Technologies, smart card security has become an important issue. In this paper, security attacks that are specific to smart cards are described. Security considerations that need to be taken into account when developing a secure smart card are studied. The paper indicates that the requirements of the secure, robust smart card operating system and common criteria assurance level of the smart card hardware and operating system. Also, new security approach which is called "dynamic security function" is published. The usage of the dynamic security functions is described in this paper.

Key words: Smart Card, Security, APDU, DES, AES, RSA, PIN, PUK, SPA, CC EAL5+, CC

1. Giriş

Bugünün çok bilindik kartlarının geçmişi incelendiğinde, 19. Yüzyıla kadar inilebilir. Ancak bugünkü kartlara en yakın örnek olarak bilinen kartın Diners Club tarafından lokantalarda ödeme yapmak üzere uygulamaya konduğu bilinmektedir. Bu düşüncenin sahibinin Frank McNamara olduğu bilinmektedir. [1] İlk kredi kartlarının ise 1958 yılında American Express ve Bank of America tarafından üretilen BankAmericard (yeni adıyla Visa) olduğu bilinmektedir. İlk dönem kartlarında, kart sahibine ilişkin bilgiler, karbon kopyasının çıkarılabilmesi amacıyla kabartma yazı halinde basılmıştır. Bu bilgiler daha sonra kartın arka yüzüne yapıştırılmış olan manyetik şerit üzerine de kaydedilmiştir. Böylece bireysel bilgilerin elektronik aygıtlar tarafından kolayca okunabilmesi sağlanmıştır.

Ticari alanda kullanımı artan kartlar zaman içinde kimlik kartı gibi başka alanlarda da kullanılmaya başlanmış ve kullanım yaygınlığı giderek artmıştır. Kart kullanımının yaygınlaşması beraberinde önemli bir güvenlik sorununu getirmiştir. Kartların güvenlik sorununu gidermek amacıyla, üzerinde akıllı kart çözümleri üretilmeye başlanmıştır. Böylece 1950'lerde ortaya çıkan basit kartlar gerçek akıllı kartlara, yani üzerinde şifreleme işlemleri yapabilen bir mikrobilgisayar donanımı ve onun üzerinde çalışan bir işletim sistemine sahip olan akıllı kartlara dönüşmüştür. Akıllı kart konusundaki ilk çalışmaların 1968 yılında Helmut Gröttrup ve Jürgen Dethloff tarafından 1968 yılında başlatıldığı ve 1982 de patent alındığı bilinmektedir. Bu çalışmaya koşut olarak, mikroişlemci üreticisi firmaların çeşitli çalışmalar yaptıkları da bilinmektedir [2].

Bu yazının giriş bölümünde akıllı kart tarihçesi, akıllı kart mimarisi başlığı altında akıllı kart kavramı

anlatılmıştır. Akıllı kartlarda güvenlik başlığı altında akıllı kartlara saldırı yöntemleri, daha sonraki bölümlerde güvenli bir akıllı kartın desteklemesi gereken güvenlik yöntemleri son bölümde ise güvenlik için yeni bir yaklaşım olan güvenlik işlevi ve bütün bunların uygulama alanları açıklanacaktır.

2. Akıllı Kart Mimarisi

Akıllı kartlar günümüzde Bilgi Teknolojileri alanında çok önemli bir rol oynamaktadırlar. Akıllı kartlar temel olarak iki sınıfa ayrılırlar: akıllı kartlar (mikrobilgisayarlı kartlar) ve akılsız kartlar (bellek kartları). Bellek kartları, telefon kartı veya ön ödemeli kart olarak adlandırılan kartlardır ve sadece basit bilgileri belleme yetenekleri vardır. Bu kartlar içerisinde basit bir seri numarası ve şifreli olarak sayaç barındırırlar. Bellek kartları akıllı kartlara göre daha az güvenlidir ve büyük miktarda bilgi saklaması da olanaklı değildir. Akıllı kartlar, yüksek seviyede güvenlik gerektiren alanlarda kullanılan kartlardır. Bu tip kartlar, yetenekli bir mikroişlemci, gelişmiş bir şifreleme birimi ve verilerin saklandığı bellekten oluşur. Akıllı kartların en belirgin özelliği içerisindeki bir işletim sisteminin bulunması ve işletim sistemi tarafından verilerin güvenli ve düzenli bir şekilde tutulabilmesidir. Bu tip akıllı kartlar özellikle cep telefonları için SIM kartı, bankacılıkta kredi kartı, ülkelerin ulusal kimlik kartları, pasaport, sağlık kartı veya geçiş denetimi kartı olarak kullanılmaktadırlar. Akıllı kartlar veri iletişimi yöntemine göre de iki sınıfa ayrılırlar: temaslı kartlar ve temassız kartlar. Temaslı kartların çalışması için gerekli olan enerji temas noktaları üzerinden iletilir. Temassız kartlarda ise herhangi bir elektriksel bağlantı olmaksızın kart için gerekli enerji belli bir mesafede elektromanyetik dalgalar ile iletilir. Temassız kartlar genellikle kuyrukların olduğu ve hızlı işlem gerektiren pasaport, geçiş denetimi, ulaşım, uçak bileti gibi uygulamalarda kullanılmaktadır. Değişik uygulamalar için hem temaslı hem de temassız arabirim özelliklerini tek kartta taşıyan kartlar çift arabirim kartlar olarak tanımlanmaktadır.

3. Akıllı Kartlarda Güvenlik Mimarisi

Akıllı kartların manyetik kart ya da disk gibi diğer veri saklama araçlarına göre üstünlüğü, herhangi bir akıllı dış birime ihtiyaç duymadan verileri şifreleyerek güvenli olarak saklayabilmesidir. Akıllı kartı oluşturan donanım ve işletim sistemi bir bütün olarak ve belli bir düzende verileri yönetmektedir. Akıllı kartlar dış birimi doğrulamadan içerdiği gizli bilgilerin kullanılmasına kesinlikle izin vermez. Günümüzde bilişim alanındaki hırsızlıklarının yazılımlar üzerinden yapıldığı bilinen bir gerçektir. Bu nedenle, bilişim sisteminin güvenliğini ana bilgisayar etrafında çözmek etkin ve yetkin bir çözüm yöntemi değildir. Buna karşılık güvenliğin kişinin sahip olduğu bir araçta bulunması, içerdiği özel ve gizli bilgilere erişilmesinin olanaksız oluşu hırsızlıklara karşı önemli bir güvenlik getirir. Bu görüşten yola çıkarak kişiye ilişkin özel bilgilerin, kişinin taşıdığı akıllı kartların içerisinde olması, bu kartların güvenlik konusunu gündeme getirmektedir.

Akıllı kartların taklit edilmesi hemen hemen olanaksız olmakla birlikte kaybedilmesi en önemli sorundur. Kartın bu zayıflığı PIN (Personal Identifier Number) olarak adlandırılan ve sadece kart sahibinin bildiği bir bilginin sorgulanması ile ortadan kaldırılmıştır. Mikrobilgisayar barındıran kartlarda bu bilgi kart içerisinde şifreli olarak saklandığından bu bilgiyi doğrudan elde etmek olanaksızdır. Ayrıca PIN doğrulaması kartın içerisindeki işletim sisteminin işlevleri tarafından yapıldığından gerek duyulan güvenlik sağlanmış olur. Günümüzde akıllı kartların güvenliği yeterince arttırılmış olmasına karşın kullanımı yaygınlaştıkça saldırı teknikleri de geliştirilmektedir.

Gelişen saldırı tekniklerine karşın akıllı kartların güvenliğinin arttırılması düşüncesi arasında doğrudan bir ilinti vardır. Güvenlik önlemleri arttırıldıkça yeni saldırı teknikleri geliştirilecek yeni saldırı teknikleri geliştirildikçe de yeni güvenlik önlemleri alınacak ve bu ilişki sürüp gidecektir. Bu makalede, bu döngüyü kırmaya yönelik bir çalışma anlatılmaktadır. Konuyu daha anlaşılır kılmak için öncelikle akıllı kartların güvenliğine ilişkin, bilinen saldırı yöntemleri hakkında genel bir değerlendirmenin yapılması uygun olacaktır. Akıllı kartlara uygulanan temel saldırı yöntemleri aşağıda açıklanmıştır:

- **Veri iletişiminin dinlenmesi:** Kart okuyucu ve kart arasındaki hattın dinlenerek gelen/giden verinin ele geçirilmesi.

- **İletilen verinin değiştirilmesi:** Akıllı kart mikrobilgisayarının temas noktalarına tel iliştirilerek okuyucu ve kart arasındaki veri amaca uygun bir şekilde değiştirilebilir.

- **Alfa parçacığı ve UV ışığı kullanarak EEPROM'un silinmesi:** Alfa parçacığı veya UV ışık kaynğı ile EEPROM bellek değiştirilerek kartın güvenliği devre dışı bırakılabilir.

- **Gücün kesilmesi:** PIN denetimi sırasında güç kesilerek hata sayacının sıfırlanması önlenebilir.

- **Saat işaretinin kesilmesi:** Saat işareti kesilip elektron ışın sınayıcı ile O/Y bellek içeriği gözlenebilir.

- **Mikroişlemcinin lazerle kesilmesi:** Akıllı kart içerisindeki mikroişlemci biriminin üst tabakaları lazerle kesilerek içyapısı bozulabilir.

- **Zamanlama saldırısı:** Şifreleme algoritmalarında anahtara bağlı olarak işlem süresi değişebilmektedir. Bu değişimden yararlanarak anahtarlar ortaya çıkabilir.

- **DES anahtarı analizi:** Süper bilgisayarlar kullanılarak deneme yanılma yöntemiyle DES anahtarları ele geçirilebilir.

- **Yan kanal analizleri (SPA/DPA):** Kart çalışırken karttan sızan bilgileri inceleyerek yapılan işlemleri ve gizli verileri açığa çıkarmaya yönelik bir saldırıdır. Yan kanal analizlerinin zamanlama analizi, güç analizi, elektromanyetik analiz gibi türleri vardır [8].

- **Hata basmak:** Belli mekanizmalar kullanarak kart işlemcisine hata yaptırmayı amaçlar. Gerilimdeki değişimler işlemcinin sıralı komutları atlamasına ya da yanlış yorumlamasına sebep olabilir. Saat işaretindeki değişimler verinin yanlış okunmasına neden olabilir. Sıcaklıktaki değişimler işlemcide tutarsız davranışlara yol açabilir. İşlemciye yöneltilen lazer ışığı ya da beyaz ışık akıllı kart tümdevresinde hataya neden olabilir. Elektromanyetik değişimler Oku Yaz bellekteki (O/Y) verilerin değişmesine neden olabilir.

4. Güvenli Bir Akıllı Kart Nasıl Olmalıdır?

Akıllı kartlara yönelik geliştirilen saldırılara karşı akıllı kart tarafında hem donanımsal hem de yazılımsal önlemler alınmaktadır. Güvenli bir akıllı kart donanımında ve yazılımında bulunması gereken güvenlik önlemleri aşağıda sıralanmıştır:

Hata algılama duyargalarının yerleştirilmesi
Akıllı kartlarda anormal durumları sezmek için çok sayıda donanımsal hata algılama duyargası yer almaktadır. Bu duyargalar karta uygulanan gerilim, saat işareti, sıcaklık, ışık gibi etmenlerin tanımlı alt ve üst sınırlarının dışında olduğu anormal bir durumu sezdiğinde, kart tümdevresi bu durum ortadan kalkana kadar çalışmasını keserek kendini güvenli duruma alır (güvenli bekleme durumu). Bu duyargalar sayesinde UV ışığı kullanarak EEPROM belleğin silinmesi, saat işaretinin kesilmesi gibi saldırılara karşı koruma sağlanmış olur.

Akıllı kart tümdevresinde güvenlik önlemleri
Akıllı kart tümdevresinin yüzeyinin kazılarak analiz edilmesini önlemek için değişik yöntemler uygulanmaktadır. İlk olarak önemli bloklar tümdevreye rasgele yerleştirilirler. Bir başka yöntemde tümdevrenin lazerle kesilmesi saldırısına karşı tümdevre üzerine ikinci bir metal tabaka konarak kart içerisindeki yapıların ortaya çıkması engellenir. Güçlü akıllı kart mikrobilgisayarında, tümdevre yüzeyinden değerli verileri okumayı engellemek için etkin kalkan olarak adlandırılan özel bir yapı kullanılmaktadır. Bu yapıda tümdevre yüzeyinde gelişigüzel dizilmiş ve rasgele sayı üretecinden elde edilen verilerle beslenen çok ince veri yolları bulunmaktadır. Etkin kalkan yapısı bu veri yollarındaki değişken verilerin doğruluğunun denetlenmesi ilkesine göre çalışmaktadır. Eğer bu yüzey aşındırılacak olursa veri yollarındaki veriler hatalı olacağından mikrobilgisayar kendisini güvenli konuma sokacaktır (güvenli bekleme durumu).

Akıllı kart işletim sisteminin güvenlik önlemleri
Akıllı kartın işletim sistemi üzerinde yapılabilecek güvenlik artırıcı işlemler aşağıda açıklanmıştır:

- Algoritmaların işlem süreleri sabitlenerek yan kanal analizleri ve zamanlama analizleri ile gizli bilginin açığa çıkarılması önlenir. Eğer herhangi bir işlemin gerçekleşme süresi gizli bilginin içeriğine bağlı olarak değişiyorsa, bu

bilgi güç analizi ile ortaya çıkabilir. Bu nedenle giriş değerleri ne olursa olsun işlem süreleri sabit tutulmalıdır. Bunun için gerekiyorsa algoritmanın değişik noktalarına rasgele gecikmeler eklenebilir [6].

- Güvenlik açısından önemli olan verilere (anahtarlar, PIN, PUK, vs) toplama sınaması konularak verinin bütünlüğü denetlenir. Herhangi bir nedenle bütünlük bozulduğunda akıllı kart kendini korumaya alır.

- Algoritmalarda gerçeklenen işlemlerin işleyiş sırası değiştirilerek algoritmanın ne yaptığının saptanması güçleştirilir [6].

- Algoritmalarda gerçekleştirilen karşılaştırma işlemleri gibi kritik işlemlere çifte denetim konulup sonuçlar karşılaştırılarak hata üretilmesinin önüne geçilebilir.

- Güvenlik açısından önemli verilerin birden fazla kopyası birden fazla formda tutularak (verinin üssü, vs) verinin değiştirilmesi durumu sezilebilir.

- Yan kanal analizlerinde yanlış PIN girilmesi sonucu PIN hata sayacının azaltılma işlemi tespit edilip o sırada güç kesilerek hata sayacının azaltılması engellenebilmektedir. PIN doğrulaması yapılırken PIN'in doğruluğuna bakılmadan sayaç azaltılıp PIN doğru girilirse eski değerine çekilerek bu saldırı önlenebilir.

- Veri iletişiminin dinlenmesi ve iletilen verinin değiştirilmesi ile ilgili saldırılara karşı akıllı kartlar ve arabirim cihazı arasındaki veri iletişimi güvenli iletişim yöntemi kullanılarak korunabilir. Böylece giden gelen veri araya giren saldırganlar tarafından anlaşılamaz kılınır. Güvenli iletişim yönteminde kart ve arabirim cihazı karşılıklı olarak bir oturum boyunca anlaşabilecekleri ortak bir simetrik şifreleme anahtarı oluştururlar. Bu ortak anahtara *oturum anahtarı* denir ve bir oturum boyunca değişmez. Komut içerisinde yer alan veri oluşturulan oturum anahtarı ile şifrelenerek iletilir. Oturum anahtarı oluşturulmasında asimetrik yöntem kullanılması güvenlik açısından tercih edilen bir yöntemdir.

- DES algoritmasının zayıflığından dolayı veri şifreleme ve çözüm için DES yerine 3DES veya AES algoritmasının kullanılması önerilir.

- PIN ve PUK gibi yüksek güvenlik gerektiren verilere uzunluk sınırlaması getirilerek deneme yanılma yöntemiyle tahminleri güçleştirilir.

Yukarıdaki paragraflarda akıllı kartlarda güvenlik sağlanması için uyulması gereken genel kurallar üzerinde durulmuştur. Bu paragraflarda akıllı kartlardan en temel beklentinin güvenlik olduğu ve güvenliğin yanısıra dayanıklı bir sistem olması gerektiği ortaya çıkmaktadır. Akıllı kartların güvenliği için hem akıllı kart donanımının (mikrobilgisayarının) hem de onun üzerinde çalışan işletim sisteminin uyması gereken kuralların bulunduğu vurgulanmıştır. Bu bölümde akıllı kart güvenliğini belirleyen etkenlerin veya kıstasların neler olduğu, nasıl belirleneceği sorularına cevap vermeye çalışılacaktır. Akıllı kart benzeri şifreleme cihazlarının ne kadar güvenli olduğu üzerinde fikir birliği sağlamak için birçok çalışma yapılmış ve uyulması gereken bazı ölçütler oluşturulmuştur. Bu ölçütler zamanla Ortak Ölçütler (Common Criteria, CC) adı ile sınıflandırılmış ve yayınlanmıştır [3]. Bu ölçütleri sağlayan donanım ve yazılımlara bulunduğu sınıfa göre CC sertifikası verilerek gerçeklenen ürünün ne kadar güvenli olduğu ifade edilmiştir. Böylece kullanılan donanımın hangi güvenlik seviyesinde olduğu aldığı CC sertifikası ile ifade edilmeye başlanmıştır. Günümüzde akıllı kart donanım platformu olarak, CC EAL5+ onayı almış yüksek güvenliğe sahip mikrobilgisayarların (örneğin SLE78CLX1600P ve P5CD081 tümdevreleri) kullanılması güvenlik için zorunlu olmaya başlamıştır. Akıllı kart ürünlerinin CC seviyesi Ortak Ölçütler Test Merkezlerinde belirlenmektedir. Bu merkezlerde akıllı kart ürününe uygulanan testlerin sonucuna göre güvenlik seviyesini belirtir CC sertifikası verilmektedir.

CC sertifikası akıllı kart donanımına verilebildiği gibi akıllı kart donanımı üzerinde çalışan işletim sistemine de verilmektedir. Akıllı kart kullanarak geliştirilen uygulamalar için kart donanımı, işletim sistemi ve o işletim sistemi üzerinde çalışan uygulamalar ayrı ayrı sertifikalandırılabilirler. Bu sertifikalar değişik güvenlik seviyelerine de sahip olabilirler. Burada uygulamanın ve uygulamayı kullananların istediği güvenlik seviyesi önemlidir. Örneğin Türkiye Cumhuriyeti Ulusal Kimlik kartları

için bu seviyeler donanım için CC EAL5+, işletim sistemi ve kimlik uygulaması için CC EAL4+ olarak belirlenmiştir [4].

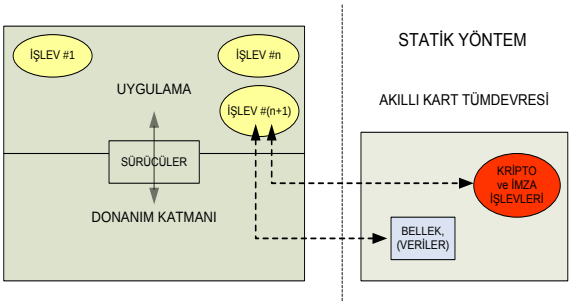
Güvenliğin yanısıra akıllı kartların sağlaması gereken bir diğer kısıtlama da standartlara uyumdur. Akıllı kartların iletişim arabirimi, protokol yapısı ve veri yapıları ile ilgili IEC/ISO 7816 ve ISO 14443 olarak tanımlanan standartlar bulunmaktadır. Bu standartlar bütün olarak, temaslı ve temassız donanımsal iletişim arabirim standartını (fiziksel katmanı), veri iletişim protokolleri standartını (veri katmanı), veri şifreleme standartlarını ve veri depolama standartlarını içermektedir. Örneğin ISO7816-2/3/4 standartları akıllı kartların fiziksel dünya ile iletişmini ve APDU olarak adlandırılan uygulama protokol veri paketlerini tanımlamaktadır. ISO7816-8, Açık Anahtar Altyapısında (AAA, PKI) kullanılan şifreleme/şifre çözme yöntemleri ile ilgili standartı, ISO7816-9 ise akıllı kart işletim sistemindeki dizin/dosya yapısına ilişkin standartları tanımlamaktadır [5].

Yukarıda anlatılanlardan anlaşılacağı gibi akıllı kart kullanımının yaygınlaşabilmesi güvenliğinin yeterli düzeye çıkması ile olanaklıdır. Bundan sonraki bölümde akıllı kartların güvenliğini artırmak üzere tarafımızca geliştirilmiş olan özgün yöntem anlatılacaktır.

5. Akıllı Kart Güvenliğinde Yeni Bir Yaklaşım, Güvenlik İşlevi

Akıllı kart kullanarak güvenlik sağlayan uygulamalar, Şekil–1'de gösterildiği gibi sabit (static) yöntem ile güvenlik sağlamaktadır. Sabit yöntemde güvenlik, akıllı kart içerisinde bulunan simetrik veya asimetrik anahtarlar ile verilen bir sertifikanın doğrulanması sonucu ile sağlanacağı düşünülmektedir. Şekil-1'de gösterildiği gibi bu yöntemin en belirgin özelliği değişmezliktir. Bu yöntemde özel verilere ulaşmak için bazı bilgilerin doğrulanması ve kişinin bildiği PIN ile geçerlenmesi esas alınmıştır. Bu yöntemde zaman içerisinde ne anahtar ne de bellek verileri değişmektedir. Kısaca bu yöntemde en önemli ayrıntı değişmezliktir (bu nedenle statik yöntem olarak adlandırılmıştır).

Ancak bütün bu önlemlere karşın bazı teknolojik olanakların (Bölüm-3'te açıklanan saldırı yöntemlerinin) kullanılması sonucu, akıllı kartlar üzerindeki gizli bilgilere ulaşmanın olanaklı olduğu ve akıllı kartlarda güvenlik açığı ortaya çıkardığı anlaşılmıştır.

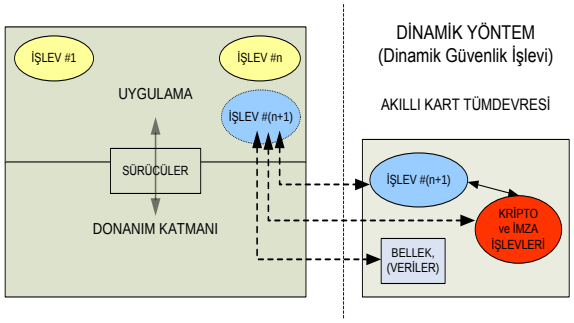


Şekil – 1 Statik yöntem ile akıllı kart güvenliği

Çünkü genele yayılmış, ancak her kart için özel bir yöntem bulunmamaktadır. Genele yayılan ancak kart için özel olan tek bilgi kart seri numarasıdır ve genel bir formülle veya asimetrik şifreleme ile sadece doğrulama yapmak için kullanılabilmektedir. Kartın içerisindeki bir nesne aracılığıyla etkin bir işlem yaparak bilgi üretmesi güvenliğe yeni bir boyut getirmektedir (gerçek anlamda kartın akıllı olması). Burada asimetrik algoritmanın kendisi değil ancak onun oluşturduğu bir güvenlik işleminden söz edilmektedir. Bu durumda akıllı kartlara saldırı gerçekleştirecek saldırgan için işlemin nasıl yapıldığının da bilinmesi gerekmektedir (daha önceki durumda uygulanan işlemin sadece asimetrik RSA algoritması veya bilinen bir başka şifreleme algoritması ile gerçeklendiği bilinmekteydi). İşlev içerisindeki şifreleme algoritmalarının kullanım şekli ve anahtarlarının gizliliği ile birlikte kart için üretilen işlevin gizliliği akıllı kartı kullanan uygulamayı kırılması olanaksız bir duruma getirmektedir. Gerçekte bu yöntemde akıllı kart, uygulamanın şifreleme işlemlerini de içeren güvenlik işlevi yardımcı işlemcisi gibi davranmaktadır.

Güvenlik işlevi, tanım olarak güvenlik gereksinimi olan bir uygulamanın işlevlerinin bir kısmını akıllı kart içerisinde konuşlandırması ve uygulamanın doğru çalışması için sonucuna gereksinim duyduğu bu işleve verilen isimdir. Böylece işlevin farklı girdisine karşılık her defasında uygulamanın gereksinim duyacağı farklı çıkış üretmesi değişkenliğe neden olmakta ve bu nedenle bu yönteme ***dinamik yöntem*** adı verilmektedir. Dinamik güvenlik işlevinin girdisi kendisini kullanan uygulamanın vermiş olduğu bilgi, çıktısı

ise girdiyi veren uygulamanın içerideki işlemlerinde etkin olarak kullanacağı bir bilgidir. Bu nedenle işlevin çıktısı uygulama tarafından etkin olarak kullanılacağından dolayı işlev atlatılarak güvenlik açığı oluşturulamaz.



Şekil – 2 Dinamik yöntem (Dinamik Güvenlik İşlevi) ile akıllı kart güvenliği

Güvenlik işlevini üzerinde çalıştıran araç akıllı karttır. Güvenlik işlevi akıllı kart üzerinden doğrudan bir APDU komutu ile işletilebilir. Kartın üreteceği cevap ise güvenlik işlevinin çıktısı olacaktır.

Şekil-2'de gösterilen yöntemde uygulama işlevlerinden en basit ve matematiksel bir formül içeren işlevlerinden bir tanesi veya işlevin bir bölümü, uygulamanın bir parçası olarak akıllı kart içerisine yüklenir. Uygulama, gereksinim duyduğu işlevinin bir kısmının yüklendiği akıllı kart olmadan çalıştırılamaz. Uygulamanın doğru çalışması için mutlaka güvenlik işlevinin bulunduğu akıllı kart uygulama tarafından doğrulanmalıdır. Bunun için bilinen asıllamalar (sabit verilerin bütünlüğü, sertifikanın geçerliliği, ortak asıllama) tamamlandıktan sonra kart içerisinde yer alan güvenlik işlevinin çalıştırılıp verilen girdilere karşılık yazılımda kullanılacak çıktılar elde edilmesi ve elde edilen bu veriler doğrultusunda işlemlere devam edilebilmesi ile güvenlik sağlanmış olacaktır. Burada amaç sabit ve kart içerisinde tutulan bir kart sertifikası yerine, yine akıllı kart içerisinde bulunan dinamik bir kart sertifikası oluşturmaktır. Böylece değişik giriş parametrelerine karşın değişik sonuçlar üretilmesi ile güvenlik sağlanmış olur. Güvenlik işlevi, güvenliğinin sağlanması istenen yazılımın bir parçası olarak kopyalanamayan bir birim olarak akıllı kart içerisinde çalıştırılmaktadır.

Güvenlik işlevi olarak tanımlanan dinamik yöntem bu makalede tanıtılmış özgün bir yöntemdir.

6. Akıllı kart ve Güvenlik İşlevinin Kullanım Alanları

Akıllı artların kullanım alanları bu bölümde anlatılacaktır.

- **Elektronik Kimlik (eID) uygulaması**
  Elektronik kimlik uygulaması, akıllı kart tümdevresi içeren bir elektronik kimlik kartının kişinin ülke sertifikası ile doğrulanması ve uygulamaya özgü güvenlik işlevi ile bu kimlik kartının geçerlenmesi amacıyla tasarlanmış bir uygulamadır.

- **Sayısal İmza Açık Anahtar Altyapısı (AAA, Public Key Infrastructure PKI) uygulaması**
  Akıllı kart tabanlı sayısal imza uygulaması olarak kullanılan Açık Anahtar Altyapısı (AAA, PKI) uygulaması kişinin ıslak imzadan daha güvenli elektronik imza ile doküman imzalaması veya gelen dokümanın doğru kişiden ve güvenli olarak geldiğinden emin olunması amacıyla geliştirilmiş bir uygulamadır.

- **Elektronik Pasaport Uygulaması**
  Gümrüklerde ve ülke giriş/çıkışlarında uygulanan pasaport denetiminde kağıt pasaportlara ek olarak kullanılması planlanan mikrobilgisayar içeren elektronik pasaport uygulaması işlemlerinin daha güvenli, çok daha hızlı ve kolay yapılmasını sağlayacaktır. Elektronik pasaport uygulaması için ICAO kuruluşunun tanımladığı ICAO 9303 standardının sağlanması gerekmektedir [7]. Ancak ülkelerin birbirlerini ülke sertifikaları ile doğrulamalarının yanı sıra bir başka yöntem olarak elektronik pasaport uygulamasında her ülke başka bir ülkenin güvenlik işlevinden bağımsız kendi güvenlik işlevini kart üzerindeki mikrobilgisayara yükleyebilir. Uygulama, belirli zaman aralıklarında bu işleve değişik giriş bilgisine karşın değişik sonuçlar ürettirerek elektronik pasaportu geçerleyebilir.

7. Sonuçlar ve Öneriler

Bu makalede, öncelikle akıllı kartların donanımsal ve yazılımsal yapısı *akıllı kart mimarisi* başlığı

altında incelenmiştir. Güvenlik için yapılması gerekenler başlığında ele alınmıştır. Akıllı kartlarda güvenlik, *akıllı kartlarda güvenlik mimarisi ve güvenli bir akıllı kart nasıl olmalıdır?* başlıkları altında ele alınmıştır. Bu bölümlerde akıllı kartlarda güvenliğin önemi ve akıllı kartlar için geliştirilen saldırı yöntemleri ayrıntılı olarak incelenmiştir. Bu konu başlıkları altında, akıllı kartlara yapılan saldırılara karşı alınan donanım ve yazılım türü önlemler irdelenmiştir. Ayrıca ortak ölçüt sınamaları ile ilgili bilgiler verilmiştir. Akıllı kart güvenliğinde yeni bir yaklaşım ve güvenlik işlevi başlığı altında yeni bir güvenlik mekanizması olarak güvenlik işlevi açıklanmış ve son olarak Akıllı kart ve güvenlik işlevinin kullanım alanları anlatılmıştır. Elektronik pasaport uygulamasının anlatıldığı bölümde özgün bir yöntem olarak güvenlik işlevinin kullanımının nasıl uygulanacağı anlatılmıştır. Bu yöntemin ülkelerin elektronik pasaportlarında kullanılması ile ülkelerin kendilerine özgü bağımsız bir doğrulama yöntemine sahip olacağı ifade edilmiştir.

Güvenlik işlevi yöntemi, akıllı kart güvenlik önlemlerine bilimsel olarak yeni bir bakış açısı getirmesi bakımından önemlidir.

Bu makalede akıllı kartlar için çok önemli olan güvenlik konusuna özgün bir yaklaşımla katkı verilmiştir.

Kaynakça

[1] http://www.dinersclub.com Diner Club International'in resmi web sayfası

[2] **J. Ferrari, R.Mackinnon, S.Poh, L.Yatawara** *Smart Cards: A Case Study*, http://www.redbooks.ibm.com

[3] Common Criteria, http://www.commoncriteriaportal.org

[4] **M. Başak,** AKiS, Akıllı Kart İşletim Sistemi, TÜBİTAK-UEKAE Dergisi, 2009-2010

[5] ISO/IEC 7816-9:2004, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37990

[6] **W. Rankl, W. Effing**, *Smart Card Handbook*, Giesecke & Devrient Gmbh, Munich, Germany, 2003

[7] **K. E. Mayes, K. Markantonakis,** *Smart Cards, Tokens, and Applications*, University of London, UK, 2008

[8] **S. Mangard, E. Oswald, T. Popp,** *Power Analysis Attacks*, Graz University of Technology Graz, Austria, 2007