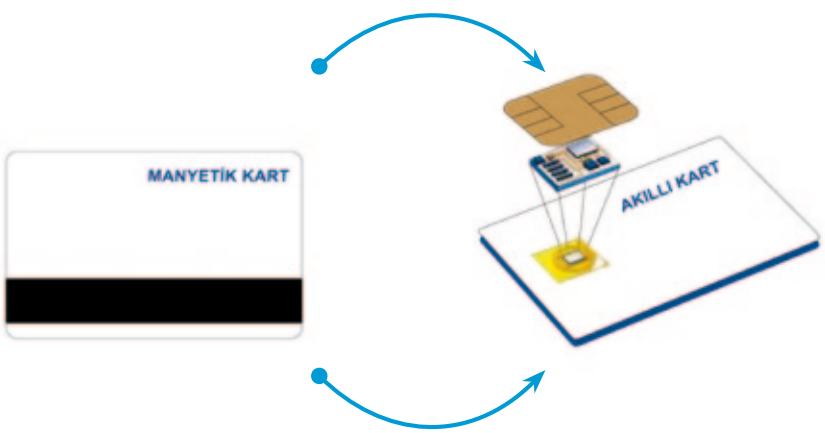
Akıllı Kartlar ve Türkiye'deki e-kimlik Uygulaması

Akıllı Kartlara Uzanan Yol Haritası

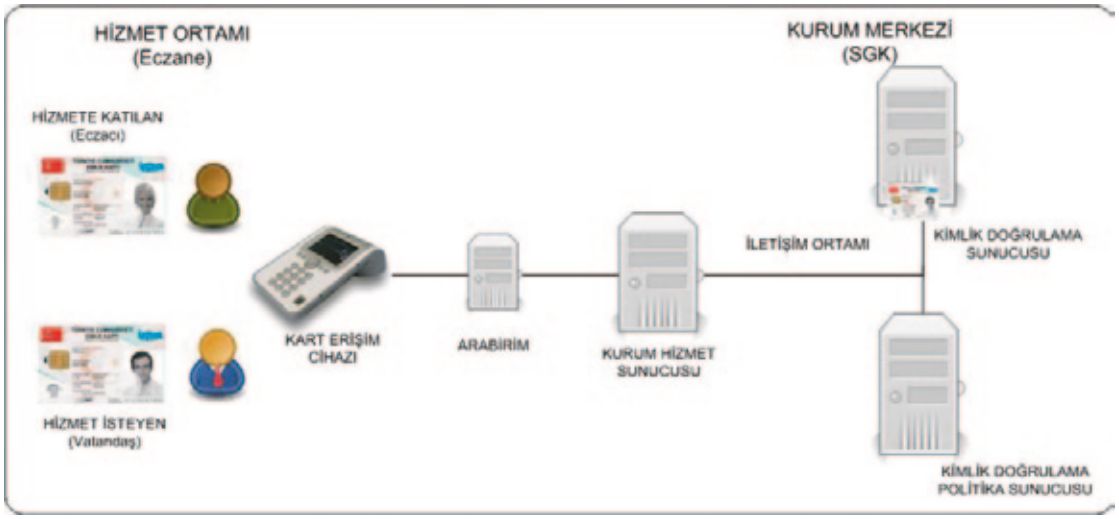
1950'li yıllarda ABD'de kâğıt ve karton kartların yerine dayanıklı ve biraz da güvenlik sağlayan plastik kartlar (PVC) kullanılmaya başlandı. Plastik kartların işlevselliğinin artması ile yetersiz kalan güvenlik, 1960'lı yıllarda arka yüzlerine manyetik şerit yerleştirilerek sağlandı. Her eline geçirenin kullandığı bu kartlara, Kişisel Tanımlama Numarası (PIN, Personal Identification Number) yani şifre konulmasıyla güvenlik üst seviyeye çıkartıldı. PIN konulmasıyla kişiye özgü hale gelen bu kartlar bankacılıktan kapı kilitlerine kadar pek çok değişik uygulamada kullanılmaya başlandı. Fakat biraz da varlıklarıyla körükledikleri tüketim artışı manyetik bantlı kartların sonunu getirecekti. 1970'li yıllarda elektronik sektöründeki gelişmelerle birlikte bilgi depolayan ve işleyebilen, birkaç milimetrekarelik yongaların yapılabilmesi olanaklı hale gelince, akıllı kartların ilk temelleri atıldı.



Böylece daha fazla bilgi depolama ve güvenlik sağlama olanağı doğdu. Nitekim 1980'li yıllarda Fransa ve Almanya'da haberleşme alanında bu tür kartların ilk denemeleri yapıldı ve kullanımı başladı.

Yongaların işlem kapasitelerindeki artış kriptografideki gelişmelere denk düşünce, akıllı kartlar matematiksel güçleri sayesinde karmaşık güvenlik algoritmalarını kullanabilecek hale geldi. Böylece kullanım alanları daha da gelişti; mali işlemlerde ve haberleşmede vazgeçilmez oldular. İlk defa sosyal iletişim uygulamalarında kullanıma girdiler. Elektronik bilet buna çok çarpıcı bir örnektir. Kimlik uygulamalarında da akıllı karta geçilmesi hizmet anlayışının vatandaş odaklı olarak değişmesine neden oldu. Vatandaş odaklı hizmet anlayışının sağlanmasıyla hizmet alıp vermek çok kolaylaşmış aynı zamanda da güvenli hale gelmişti.

Akıllı kartın kimlik kartı olarak kullanıldığı ilk ülkelerden biri Malezya'dır (2001). Elde edilen başarının ardından diğer ülkeler de bu konuda çalışmalara başlamıştır. Avrupa'da İtalya, Almanya, Portekiz, İsveç, İspanya ve Estonya e-kimlik uygulamasına geçmiştir. Önümüzdeki on yılda -kullanım alanları ve şekilleri genişleyip göreceli olarak değişse de- akıllı uygulamaların etki alanlarını giderek artıracağını söylemek abartılı olmaz. İlk uygulamadan itibaren küçüldükçe güçleri artan yongaları, yeni nesil iletişim araçlarını ve giderek etkinleşen güvenlik kavramlarını dikkate alırsak, gelecekte yaşamımızı, hizmet alımı açısından kolaylaşacağını öngörebiliriz..



Türkiye Cumhuriyeti Kimlik Kartı

Yakın bir gelecekte Türkiye'de kullanılmaya başlanacak olan Türkiye Cumhuriyeti Kimlik Kartı (e-kimlik), halihazırdaki nüfus cüzdanlarının yerine geçecek, akıllı kart teknolojisine dayanacak ve güvenli (taklit ve tahrif edilemez) bir kimlik olacaktır.

Bu kartlar, 2006 yılı Nisan ayında Sosyal Güvenlik Kurumu ile TÜBİTAK UEKAE arasında imzalanan bir proje kapsamında geliştirilmiştir. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü ve Sağlık Bakanlığı projeye sonradan dahil olmuştur.

T.C. Kimlik Kartı, sağladığı yüksek güvenlikle kimlik hırsızlıklarına son verecek ve kişilerin kimliğini doğru beyan etmesi sağlanacaktır. Bu yeni uygulama hak edene hak ettiği hizmetin verilmesi açısından çok önemlidir. Böylece e-dönüşüme güç verilecektir.

TC. Kimlik kartının ön ve arka yüzü

E-kimlik, TÜBİTAK UEKAE tarafından geliştirilen Elektronik Kimlik Doğrulama Sistemi (EKDS) üzerinde çalışmaktadır. Diğer kurumlar da EKDS sistemini kullanarak vatandaşın kimliğini yüksek bir güvenlik seviyesinde doğrulayabilecektir.

Elektronik Kimlik Doğrulama Sistemi

Bu sistem tüm kamu ya da özel kurum ve kuruluşlar tarafından internet üzerinden hizmet verilirken kullanılır. Hizmeti gerçekleştiren görevlinin (örneğin eczacının) ve hizmet isteyen kişinin (örneğin vatandaşın) gerçekten gösterdikleri kimliğe sahip olup olmadıklarının denetlenmesine yarar. Talep edenlerin TÜBİTAK UEKAE tarafından geliştirilen elektronik kimlik kartına sahip olması beklenir. EKDS'de doğrulama sırasında ihtiyaca göre parmak/damar izi ve/veya PIN kullanılır.

Elektronik Kimlik Doğrulama Sistemi Nasıl Çalışır?

EKDS'nin çalışmasını yukarıdaki resim üzerinden incelemeden önce bileşenlerine bir göz atalım:

1. T.C. Kimlik Kartı: Vatandaşın Türk nüfus kütüklerine kayıtlı olduğunu kanıtlayan ve TÜBİTAK UEKAE tarafından geliştirilen akıllı işletim sistemi ve yongayı barındıran akıllı karttır.

2. Kart Erişim Cihazı: Kimlik doğrulamanın hizmetin sağlandığı yerde yapıldığını garanti eden ve TÜBİTAK UEKAE tarafından geliştirilen çok yuvalı güvenli kart okuma cihazıdır.

EKDS'de Kimlik Doğrulamalı Hizmet Senaryoları

Örneğin, sigorta hizmeti veren kurumun EKDS'yi kendi iş sürecine entegre ettiği düşünülürse:
Bireyin sahip olduğu kimlik kartı ile provizyon alma işleminde kimlik doğrulaması gerçekleştirilir.

Hizmet isteyen (vatandaş) kimlik kartıyla bir hastanenin kayıt masasına başvurur. Kimlik kartının görsel kontrolü görevli tarafından yapılır. Görevli tarafından vatandaşın kimlik kartı Kart Erişim Cihazı'nın (KEC) hizmet isteyen kısmına takılır. Kimlik doğrulama isteği karşısında merkezden kimlik doğrulamada kullanılacak politika çekilir. Örneğin vatandaştan parmak biyometrisi talep edilebilir ya da sadece PIN girişi yeterli görülebilir. Vatandaş tarafından T.C. Kimlik Kartı şifresi girilir.

Vatandaşın kimliği Sosyal Güvenlik Kurumu'nun (SGK) belirlediği güvenlik seviyesinden doğrulanır. Kimlik doğrulama sonucu olumlu ise, provizyon hizmeti alan vatandaşın gerçekten beyan ettiği kişi olduğunu tespit etmiş olur. Kimlik doğrulaması ve provizyon işlemi gerçekleştikten sonra T.C. Kimlik Kartı sahibine teslim edilir.

Vatandaş muayene için doktorun odasına gider.

3. Kimlik Doğrulama Sunucusu: Kart Erişim Cihazı tarafından oluşturulan kimlik doğrulama bilgilerinin doğruluğunun kontrol edildiği ve TÜBİTAK UEKAE tarafından geliştirilen sunucudur.

4. Kimlik Doğrulama Politika Sunucusu: Kuruma güvenlik politikalarını kendi gereksinmelerine göre seçme esnekliği tanıyan ve TÜBİTAK UEKAE tarafından geliştirilen sunucudur.

5. Arabirim uygulamaları: EKDS'nin kurumların kullandıkları elektronik uygulamalara entegrasyonunu sağlayan arabirim uygulamalarıdır.

EKDS'nin çalışmasındaki en önemli ayrıntı kimlik doğrulama güvenlik seviyesinin belirlenmesidir. Kurumlar gereksinimleri çerçevesinde, kendi politikalarına karar verir ve oluşturur. Örneğin sosyal sigorta hizmeti veren bir kurum için, eczaneden ilaç temininde kişisel kimlik numarası (PIN) ile kimlik doğrulanması istendiğini düşünelim. Bu durumda, vatandaş eczaneye ilaç almaya gittiğinde, kurumun merkezinde bulunan Kimlik Doğrulama Politika Sunucusu, istenen hizmet için PIN istemenin yeterli olacağını eczaneye iletir. Eğer vatandaş bu numarayı doğru girmişse, kimliği kurumun merkezinde bulunan Kimlik Doğrulama Sunucusu tarafından doğrulanır ve ilaç alma işlemi gerçekleşir.

Elektronik Kimlik Doğrulama Sistemindeki Yenilikler

Yeni sistemle birlikte yapılan en önemli tespit, devletin vatandaşı hizmet odağı yapacağı e-dönüşüm projesinin hız kazanacağıdır. Teknolojideki gelişmeler yardımı ile devletin sunduğu kamu hizmetlerini, e-devlet yapısı altında elektronik ortama alma çalışmaları sürdürülüyor. Böylece vatandaş devlet daireleri arasında dolaşmak zorunda kalmadan, gereksiz zaman ve iş gücü kaybı yaşamadan hizmet alabilecek. Bu esnada kişisel kimlik doğrulama işleminin güvenli bir şekilde yapılması ve doğru kişinin hizmet almasının önemi de ön plana çıkıyor.

EKDS'deki en etkin yeniliklerden biri de TÜBİTAK UEKAE tarafından geliştirilen akıllı kimlik kartıdır. Görsel ve elektronik yolla içinde saklanacak bilgilerin güvenliği sağlanmıştır. Ayrıca parmak biyometrisi içerir. Böylece tüm doğrulama fonksiyonlarının kartta toplanması sağlanmış, hizmetlerin alımı ve sunumu kolaylaşmıştır.

Yeni kimlik kartında güvenlik parmağın ucundadır. Yüksek güvenlik gerektiren işlemlerde kişinin parmak veya damar izini kullanılmasına olanak sağlar. Böylece e-kimliğin sahibinden başka birisi tarafından kullanılmasını engeller.

Kimlik kartı ile sağlanan hizmetlerde, hizmetin özelliğine göre farklı güvenlik seviyelerinde kimlik doğrulama yöntemleri (şifre, fotoğraf, biyometrik veri) kullanılabilir. Kart üzerinde kişisel bilgiler (ad, soyadı, cinsiyet, doğum tarihi, geçerlilik tarihi, kart seri ve numarası, T.C. kimlik numarası, anne adı, baba adı, önceki soyadı-kadınlar için, doğum yeri, kan grubu, medeni hal, din), kayıt bilgileri (nüfusa kayıtlı olduğu il, ilçe, mahalle-köy) ve fotoğraf basılmıştır. Yonga içinde ise biyometrik (sağ ve sol elden alınan birer parmak biyometrisi) ve kriptografik veriler (kimlik doğrulama işlemi için gerekli sertifikalar ve anahtarlar) bulunur.

Sürdürülen çalışmalar ile kimlik kartına elektronik imza özelliği de kazandırılacaktır. Böylece ayrı bir e-imza kartına ihtiyaç duyulmadan, vatandaş elektronik imzasını da kimlik kartı vasıtayla atabilecektir.

Bolu İli Pilot Uygulaması

Bilindiği gibi Bolu ilinde e-kimlik'in gerçeklenmesi için tasarlanıp gerçekleştirilen yapılar nüfus, vatandaşlık, SGK ve Sağlık Bakanlığı uygulamaları üzerinden denenmektedir. Bu kuruluşlarca verilen hizmetler, yüksek bir güvenlik seviyesinde kimlik doğrulama yapılarak gerçekleştirilmektedir. Bu süreçte kurgulanan senaryolar ve sistemin hayata etkisi denenmektedir. Bu süreç kapsamında eczanelerde, aile hekimliği birimlerinde, otomasyon sistemli hastaneler ve bağlı polikliniklerde, nüfus ve vatandaşlık ofislerinde, e-devlet uygulamaları kapsamında 127 kamu uygulamasının tek çatı altında toplandığı e-devlet kapısında güvenli kimlik doğrulama başarıyla denemiştir.

Kimlik Kartında Kullanılan Teknolojiler

Günümüz ihtiyaçlarına bir yanıt olarak ortaya çıkan ve vatandaşa ait nüfus bilgilerinin yetkisiz kimseler tarafından yeniden üretilmesini ya da değiştirilmesini olanaksız hale getirecek şekilde tasarlanan kimlik kartı, hem görsel (gökkuşağı baskı gibi) hem de elektronik tedbirler (simetrik ve asimetrik asıllama yöntemlerini kullanan açık anahtar altyapısı-PKI) ile korunur.

Kimlik doğrulama işlemleri için açık anahtar altyapısı dahilinde her kimlik kartına özel bir anahtar çifti bulunur. Bu anahtardan gizli olanına, sahtesini oluşturmak amacıyla, denetimsiz ulaşmak mümkün değildir. Kimlik kartına yazılan verilerde kimlik yayıncısının da elektronik imzası bulunur. Bu sayede

e-Devlet Kapısı'na EKDS ile giriş ekranı

veri bütünlüğü sağlanır. Kimlik doğrulama ise kartın ve sahibinin doğrulanması anlamına gelir. Kimlik kartı sahibi için biriciktir; sadece onun için üretilmiştir. Kartın içindeki açık kimlik bilgisi dışındaki veriler şifrelenerek korunur.

KİOSK tipi Kart Erişim Cihazı

Kurumsal tip Kart Erişim Cihazı

Bireysel tip Kart Erişim Cihazı

Kimlik kartı, güvenli fiziksel tasarım, çeşitli sertifikalar ve kart sahibine ait biyometrik veriler gibi taklit edilemeyecek özelliklere sahiptir. Bu yapısıyla kamu ve özel kurum/kuruluşların çevrimiçi ve çevrimdışı uygulamalarda kimlik doğrulama ihtiyaçlarını karşılayacak niteliktedir.

Kimlik kartının üzerinde bulunan yonganın tasarımı TÜBİTAK UEKAE'de gerçekleştirilmiştir. Bu yonga üzerinde çalışan akıllı kart işletim sistemi UKİS de yine bir TÜBİTAK UEKAE ürünüdür.

İnternet üzerinde elektronik hizmet veren kamu/özel kurum ve/veya kuruluşların uygulamalarında, e-kimlik kartıyla EKDS arasında güvenli uç birim cihazları kullanılır. Bunlar kullanım amaçlarına göre farklılık arz eder: Kurumsal tip Kart Erişim Cihazı (KEC), Bireysel, Gezgin, KIOSK, Kart Yayıncı KEC gibi.

Kurumsal Tip Kart Erişim Cihazı, hizmet isteyenin (vatandaş) ve hizmete katılanın (görevli) kimlik doğrulama işleminde kullanacağı kimlik kartları ile hizmete katılanın yapılan işleme elektronik imzasını atmak üzere kullanacağı cihazdır.

Bireysel Tip Kart Erişim Cihazı, hizmet alan ve veren arasında yürütülen işlemlerin güvenliğini ev ve ofis kullanıcıları için sağlar. Ayrıca cihaz masaüstü veya taşınabilir bilgisayarlardaki internet ve masaüstü uygulamaları ile USB arabirimi üzerinden haberleşip kimlik doğrulama işlemini yerine getirir.

KIOSK Tipi Kart Erişim Cihazı kart verme noktalarında vatandaşın PIN değiştirme, PIN bloke kaldırma ve kartını test edip içeriğini görüntüleme gibi işleri kendi başına yapabilmesi için geliştirilmiştir.

T.C. Kimlik Kartının Faydaları

- Her çeşit taklit, tahrif ve sahteciliği ortadan kaldıracaktır
- Kolay taşınabilir (kredi kartı ebatlarında)
- Biriciktir; yalnız kart sahibi tarafından kullanılabilir
- Kamu hizmetlerine güvenli erişim sağlar
- Yapılan işlemlerde kimliğin gizli tutulmasını sağlar
- İşlemlerin hızla gerçekleştirilmesine katkıda bulunur
- İnternet ortamında sunulan hizmetlerin güvenliğini artırır
- Elektronik imza özelliğine sahiptir

T.C. Kimlik Kartının Gelecekteki Uygulamaları

Gelecekte gerçekleştirilmesi planlanan uygulamalar:

Kaynaklar
Mutlugün, M., Adalıer, O., "Turkish National Electronic Identity Card", ACM Press, SINCONF, 2009.
Başak, M., "Akıllı Kart Nedir?", UEKAE Dergisi, Sayı 1, Eylül-Aralık 2009.

Oktay Adalıer, 1992'de ODTÜ Matematik bölümünden mezun oldu. Yine aynı üniversitede 1995'te Bilgisayar Mühendisliği bölümünde yüksel lisans programını tamamladı. Ayrıca, Ege Üniversitesi Bilgisayar Mühendisliği bölümünde doktora programını tamamladı. Halen TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde (UEAKAE), Tasarım & Gelişim bölümünde başuzman araştırmacı olarak çalışmakta ve "Yeni Nesil Türkiye Cumhuriyeti Kimlik Kartı" projesini yürütmektedir. Proje yönetimi ve kontrolü, proje risk yönetimi, kamu ve halk kullanımı için geliştirilen e- uygulamaları üzerine dayanan akıllı kart doğrulamaları alanlarında çalışmaktadır.