E-DÖNÜŞÜM TÜRKİYE PROJESİ 2005 EYLEM PLANI

6. EYLEM MADDESİ

“AKILLI KARTLARIN KAMUDA KULLANIMI“ KONUSUNDA ÖN ÇALIŞMA RAPORU

TÜBİTAK-UEKAE

OCAK / 2006

ÇALIŞMAYI YAPAN İLGİLİ KURUM VE KURULUŞLAR

TÜBİTAK UEKAE

Adalet Bakanlığı

İçişleri Bakanlığı

Maliye Bakanlığı Sağlık Bakanlığı

Çalışma ve Sosyal Güvenlik Bakanlığı

DPT

NVİ Gn. Md.

Emniyet Gn Md.

Türk Telekom

İlgili Kamu Kurum ve Kuruluşları

Sivil Toplum Kuruluşları

İçindekiler

ÖZET

Akıllı kart tabanlı kimlik kartı uygulaması, kamu kurum ve kuruluşların vatandaşın kimliğinden emin olarak doğru kişiye hak edilen hizmetin verilmesini sağlar.

Elektronik ortamda vatandaşlarına hızlı, kaliteli ve güvenli hizmet vermeyi hedefleyen bir ülkede akıllı kart tabanlı kimlik kartı uygulaması, kabul edilen en yaygın çözümdür.

Kimlik kartı uygulaması, kurum ve kuruluşların kimlik sahteciliğinden kaynaklanan yolsuzluklardan dolayı maddi ve manevi zararlara girmelerini engeller.

Akıllı kart tabanlı kimlik kartı uygulamasında vatandaşların mahremiyet haklarının ihlal edilmemesine dikkat edilmelidir.

Akıllı kart tabanlı kimlik kartı uygulamasında, kart sahibinin biyometrik bilgileri yardımıyla kimlik doğrulama yapılması yeterlidir.

Akıllı kart tabanlı kimlik kartı uygulamasında. bir güvenlik zinciri oluşturularak sistemdeki her bir modülün ve iletişimlerinin güvenli olması temin edilmelidir.

Akıllı kart tabanlı kimlik kartı uygulaması, görsel ve kartlı kimlik tanıma yöntemlerini desteklemeli, çevrim-içi ve çevrim-dışı biyometrik kontrol yapabilmeli ve birden fazla yöntemle kimlik doğrulama yapabilmelidir.

Akıllı kart tabanlı kimlik kartının yaygınlaştırılarak tüm ülke sathına dağıtılması uzun zaman, yüksek ekonomik maliyet ve iyi bir kurumsal organizasyon gerektirir.

Biyometrik bilgilerin belirli periyotlarla yenilenmesi gereksiniminden dolayı , 75 milyon gibi çok büyük bir nüfusa dağıtılan kartların işletilmesi, değiştirilmesi ve yenilenmesi için uygulamalar geliştirilmelidir.

Tüm ülke nüfusunun kullanacağı akıllı kart tabanlı kimlik kartı uygulaması, yüksek maliyetli bir uygulama olacağından ulusal olanaklar dahilinde kart ve okuyucu temini sağlanmalıdır. Diğer durumda teknolojik yatırım ülkemizde yapılmayacak ve yüksek meblağların periyodik olarak yurt dışına akması ile karşı-karşıya gelinecektir.

Akıllı kart tabanlı kimlik kartı uygulamasına geçilmeden önce, kamu kurum ve kuruluşlarında örnek bir pilot uygulama yapılmalıdır. Pilot uygulama sırasında somut veriler elde edilmeli sistemin çalıştığından emin olunmalı ve kazanılan tecrübeler doğrultusunda yaygınlaştırma yapılmalıdır. Bunun için ilgili kamu kurum ve kuruluşlarının katıldığı bir pilot uygulama projesi başlatılmalıdır.

1. Ulusal Kimlik Kartı

Kimlik Kartı, devletin yetkili organı tarafından vatandaşa kanun çerçevesinde verilen ve vatandaşın kamu kurum ve özel kuruluşlarla olan ilişkilerinde kimliğini tanımlayan bir karttır. Vatandaş söz konusu kartı kamu ile ilgili olan bir çok işlemde kullanabilir. Örneğin, vatandaş vergi numarası kartı, adli sicili ve acil sağlık bilgileri tek kartta taşınabilir. Ayrıca özel kurum ve kuruluşlar da devlet tarafından onaylı bir kimlik kartı sayesinde, kimlik denetleme mekanizmalarını daha rahat kurabilirler.

Özellikle devlet kurumlarıyla her vatandaşın er ya da geç bir ilişkisi olacağından Ulusal Kimlik Kartı sistemine her vatandaşın dahil edilmesi gerekmektedir. T.C. Vatandaşı olmayan kişilerin kamu kurum ve özel kuruluşlarla olan ilişkilerinde Ulusal Kimlik Kartından yararlanıp yararlanmayacağının, yararlanırsa ne şekilde yararlanacağı yapılacak pilot uygulama çalışmasında belirlenmelidir.

1.1. Ulusal Kimlik Kartının Yararları

Ulusal Kimlik Kartı kullanımının faydaları ise kısaca aşağıdaki gibi sıralanabilir:

- Kanun dışı göçlerin ve kaçak işçi çalıştırmanın önüne geçilecektir.
- Kamu hizmetleri, vatandaşlara daha verimli, hızlı ve kaliteli verilecektir.
- Güvenlik güçlerinin görevlerini yapmalarına olumlu katkısı olacaktır.
- Organize suçların takip edilmesinde önemli katkıları olacaktır.
- Özel kurumlar devlet tarafından onaylı, her yerde geçerli ve kolay taklit edilemez kimlik kartları sayesinde kimlik denetleme mekanizmalarını daha düşük maliyetle ve daha etkin gerçekleyebilecektir.
- Kimlik hırsızlıklarından dolayı ortaya çıkan usulsüzlük ve yolsuzlukların önüne büyük ölçüde geçilerek ekonomik kayıplar ve prestij kayıpları önlenecektir. (Kimlik hırsızlığından dolayı İngiltere'de yılda 1.2 milyar pound ekonomik kayıp olmaktadır[1].)
- Sosyal Güvenlik Kurumları doğru bir şekilde gerçeklenmiş bir akıllı kart ve biyometrik tabanlı güvenli kart okuyucular yardımı ile Sosyal Güvenlik sisteminde karşılaşılan usulsüzlüklerden kaynaklanan kayıplarını asgariye indirgeyebilirler.

1.2. Kimlik Kartının Yasal Boyutları ve Mahremiyet Konusu

Kimlik kartının yalnız vatandaşın kimliğinin doğrulanmasında kullanılması mahremiyet açısından herhangi bir problem oluşturmamaktadır. Kanunlar vatandaştan kimlerin kimlik ibrazı isteyebileceğini belirlemiştir. Bunlar başlıca güvenlik güçleri, kamu hizmeti veren yetkililer ve ticari işlemleri (kredi kartı kullanımı) yapmağa yetkili (satış elemanı) olan

sorumlulardır. Fakat kimlik denetimi yapan insanların çoğalması, yetkisiz kişilerin vatandaşlara ait kimlik kartlarının kullanımını takip edebilmeleri ve hatta ifşa edebilmeleri, kişi mahremiyetlerinin ihlal edilmesi ile sonuçlanabilir. İhlal durumlarında hukuki, etik ve kişisel itirazlar doğmaktadır.

Mahremiyet ihlalleri genelde Ulusal Kimlik kayıtlarına erişimden kaynaklanmaktadır. Ulusal Kimlik Kartı ile Ulusal Kimlik kayıtları (veritabanı) farklı kavramlardır. Ulusal Kimlik katı bireyin kendi kimliğini ispat etmek için kullandığı bir araçtır. Ulusal Kimlik kaydı ise bireyin kimlik bilgilerinin bir yerde, tek merkezde tutulması işlemidir. Bu kayıtların kimlik bilgilerinden fazlasını kapsaması kişinin özgürlük haklarının ihlalini gündeme getirmektedir. Ulusal Kimlik kayıtlarında bu konulara gereken hassasiyet gösterilmelidir.

İngiltere de yapılan bir araştırmaya göre toplumun %61'i Ulusal Kimlik kartına olumlu bakmaktadır. %38'i olumsuz bakmaktadır. %1' ise olaya çekimser yaklaşmaktadır. Yukarıda verilen istatistikler kimlik kartlarının kullanıcılara ücretsiz dağıtımı söz konusu olduğunda geçerlidir. Bir ücret karşılığında kart dağıtımına olumlu bakanların yarısı olumsuz düşünmeye başlamaktadır. Ayrıca, Ulusal Kimlik Kartı uygulama planı hakkında topluma bilgi verilmesi oranında toplumdaki kart hakkındaki olumsuz düşünceler arttığı gözlemlenmiştir.[1]

Ulusal Kimlik kartı kayıt sisteminin içeriği, vatandaşların mahremiyet konusunu etkilemektedir. Vatandaşların yalnız kimlik bilgilerinin tek merkezde ve tek elde tutulmasına genelde kimsenin itirazı bulunmamaktadır. Fakat vatandaşın çeşitli bilgilerinin (sağlık, mali, adli, v.b.) tek bir merkezde tutulması vatandaşların mahremiyetinin ihlalini gündeme getirmektedir. Bu durum toplumsal huzursuzluklara ve tepkilere neden olabilir. Sosyal gelişimini tamamlamış birçok batı ülkesi için de aynı durum söz konusudur. Sivil toplum örgütleri, bireylerin kayıtlarının Avrupa İnsan Hakları anlaşmasının 8. maddesi (özel hayatın mahremiyetinin korunması) ile 14. maddesi'ne (bireyler arasında ayırımcılık yapılmaması) uyumlu olmasını öngörmektedir.

Ulusal Kimlik kartı sisteminin işletimi, kartın içeriği, dağıtımı ve imhası TBMM'de kabul edilmesi beklenen "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı" maddelerine uygun olmalıdır.

Özellikle Sosyal Güvenlik Sistemi için hayati önem taşıyan ve vatandaşların biyometrik verilerinin kullanıldığı güçlü kimlik doğrulama mekanizmaları yürürlüğe girecek olan kanunun ilgili maddelerine dayandırılmalıdır. Örneğin SSK için TÜBİTAK-UEKAE tarafından yapılan Güvenlik Analizi [2] sonucunda Sosyal Güvenlik Sistemi için tehdit oluşturan unsurlardan korunmak için biyometrik verilere dayalı çift yönlü kimlik doğrulama yöntemlerinin kullanılması gerekmektedir.

Kimlik kartlarında biyometrik veri kullanımının olacağı kabulüyle en çok yapılan itirazları şu şekilde özetlenebilir:

Toplanan biyometrik verileri ile birlikte bazı kişilerin fişlenebileceği ve özellikle bazı azınlıklar aleyhine ileride haksız ithamların olabileceği,

Kimlik kartı muhasebelerinin kişilerin takibinde kullanılabileceği (örneğin bir vatandaşın düşmanı, elektronik kayıtlara ulaşarak kurbanını takip edebilir),

Vatandaşların konumları itibariyle bulunmasının uygun olmadığı yerlerin başkaları tarafından ifşa edilmesi ve mahremiyet ihlali yapılan kişinin inkar edememesi

Fakat yeni kanun tasarısında vatandaşın özel bilgilerinin (kimlik bilgileri, Acil Durumlar için Klinik bilgiler) biyometrik bilgileri (Parmak izi, Sayısal Yüz resmi, İris bilgileri gibi) ile birlikte kimlik doğrulama uygulamasında kullanılmasında sakınca olmadığı görülmektedir. Ancak söz konusu biyometrik bilgilerin bir merkezde değil, vatandaşın kartında tutulması koşulu ile kanuna uygunluk olabilmektedir. Bu durumda vatandaşın biyometrik bilgileri yine vatandaş tarafından şifrelenmiş olarak yanında taşınmış olacaktır.

Yeni kanun tasarısında bu durum ile ilgili maddeler aşağıda sıralanmaktadır. İlgili maddeler olduğu gibi buya alınmıştır.

"Kişisel verilerin işlenmesine ilişkin ilkeler

Özel niteliği olan kişisel veriler **Madde 6.2 g)** bendi gereği koruyucu hekimlik, tıbbi teşhis, tedavi, bakım veya sağlık hizmetlerinin yürütülmesi amacıyla kişisel verilerin;

- Sağlık kurumları,
- Sigorta Şirketleri,
- Sosyal Güvenlik kurumları

tarafından ilgili kanunlara uygun olarak, hukuken veya meslek kurallarına göre sır saklama yükümlülüğü altında bulunan sağlık personeli veya eşdeğer seviyede sır saklama yükümlülüğü altındaki bir başka kişinin gözetimi altında işlenmesi."

"**Madde 6.3** Özel hayatın ve aile hayatının gizliliğine dokunmamak şartıyla, temel kamu yararlarının gerektirmesi halinde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, kurul, özel niteliği olan kişisel verilerin işlenmesine karar verebilir."

"İstimrar ve Meslek kuralları ile ilgili **Madde 22**

b) Kamu düzeninin korunması,

c) **Suçun önlenmesi için gerekli olması, suç veya meslek ahlak kurallarını ihlal eden eylemlerin soruşturulması veya kovuşturulması,**

d) Bütçe, vergi ve mali konulara ilişkin olarak devletin önemli ekonomik veya mali çıkarlarının gerektirmesi,

e) (b), (c), (d) bentlerinde belirtilen konularda, resmi mercilerin izleme, denetleme veya düzenleme görevlerinin gerektirmesi."

1.3. Bazı Ülkelerin Ulusal Kimlik Kartı Konusunda Tutumları

Dünyanın bir çok ülkesinde kimlik kartı sistemi bulunmaktadır. Ülke sakinlerinin kimlik kartı kullanımıyla hiçbir problemleri bulunmamaktadır. Yalnız Anglosakson ülkelerinde kimlik kartı kullanımına karşı olumsuz bir yaklaşım bulunmaktadır. Özellikle Amerika ve İngiltere'de zorunlu kimlik kartı kullanımı konusunda ciddi tartışmalar yaşanmaktadır. Bazı insanlar bu uygulamayı kişilik haklarına tecavüz olarak algılamaktadırlar. Vatandaşların kimlik doğrulama sistemine itiraz etmeleri vatandaşlık bilgileri ile diğer mahrem bilgilerinin tek kaynakta toplanmasıdır. Dolayısıyla merkezde yalnız kimlik bilgilerinin tutulması kişilik hakları açısından önemlidir.

Bir ülkenin bölgelerine ve etnik yapısına göre ulusal kimlik kartı kullanımının destekçileri değişmektedir. Örneğin İngiltere'nin İskoçya bölgesinde yaşayan vatandaşlar kimlik kart kullanımına büyük ölçüde karşı çıkmaktadırlar.

Günümüzde sosyal bir devlet olma sürecini tamamlamış ülkelerin Ulusal Kimlik Kartı konusu ile ilgili olarak birbirlerinden farklı tutum sergilemektedirler. Bazıları Ulusal Kimlik Kartı kullanımını zorunluluğunu öngörürken, diğer bir bölümü anlamsız bulmaktadır. Diğerleri de kart kullanımını isteğe bağlı olarak kullanmaktadır:

Ulusal Kimlik kartı kullanımını zorunlu koşan başlıca ülkeler Belçika, Estonya, Almanya, Hong Kong, Çin, İtalya, Polonya, Romanya, Singapur, İspanya, Mısır, Yunanistan, Malezya, Tayland, Lüksemburg ve Portekiz'dir.

Avustralya, Finlandiya, Fransa, Japonya, İsveç, İsviçre'de kimlik kartı kullanımı zorunlu değildir. İsteyen vatandaş kendisine kimlik kartı çıkartabilir.

Danimarka, Norveç, Amerika, İngiltere ve Grönland resmi ulusal kimlik kartına sahip değildir. Fakat bu ülkelerde vatandaşın kendini tanıtmada kullandığı kartlar bulunmaktadır. Örneğin ehliyet, öğrenci belgesi, meslek belgesi (doktor kartı) gibi.

1.4. Ulusal Kimlik Kartı Sistemine Uyum Sağlaması Zor Olan Kullanıcılar

Ulusal Kimlik Kartı kullanımında toplumun çok farklı kesimlerinden insanların durumları göz önünde bulundurulması gerekmektedir. Bu tür insanlara örnek olarak aşağıdakiler verilebilir;

- Eve bağımlı ve çeşitli sağlık sorunlarından dolayı dışarı çıkamayan insanlar,
- Yaşam alanlarının dışında yalnız yaşayan insanlar,
- Seyahat etmeye müsait olmayan (sağlık ya da maddi nedenlerle kayıt merkezine gelemeyecek durumda olan) insanlar,
- Adres bilgisinin kolay tespit edilemediği yerleşik hayatı olmayan göçebe hayatı yaşayan vatandaşlar,

- Evsiz ve kimsesiz vatandaşlar,

- Akıl sağlığı yerinde olmayan vatandaşlar

Bu ve benzeri nedenlerle biyometrik verisi alınamayan, kayıt merkezine gelemeyen vatandaşların sisteme kayıt edilmeleri için bazı özel uygulamalar düşünülmelidir. Diğer yandan bu vatandaşların mevcudiyeti biyometrik veri tabanlı ulusal kimlik kartına geçilmemesi için sebep teşkil edemez, çünkü kağıt tabanlı kimlik kartlarının verilmesinde de benzer sorunlar yaşanmaktadır.

2. Kimlik Hırsızlığı (Identity Fraud)

Kimlik hırsızlığı, gerçek bir kişinin kimliğine sürekli ya da uzun süreli bürünmektir. Kimlik hırsızlığı, zaman zaman sahte kimlikle karıştırılmaktadır. Sahte kimlik genellikle belli bir işi yapmaya yönelik olarak, örneğin ehliyet sınavını geçemediği halde araba sürebilmek ya da izni olmadığı halde yurtdışına çıkabilmek gibi, üretilir. Sahte kimlik üreten kişi ya gerekli yetkili mercilerden onay alınmasa da, kendi adına onaylı ve geçerli bir kimlik belgesi üretir ya da tam aksine kendi kimliğini gizleyebilmek amacıyla hayali bir kişinin kimliğini alır. Sahte kimlik düzenleme düşük seviyeli bir kimlik hırsızlığı gibi görülebilir.

Kimlik hırsızlığında kimliği "çalınan" kişi gerçek bir kişiye ait kimliktir. Bu gerçek kişi yalnızca hayatta olan biri olmayabilir. Ölen bir kişinin kimliğini de çalınabilir. Kimlik hırsızlığının sadece gerçek bir kimlik belgesinin çalınıp gerekli değişiklikten sonra hırsızın kimliği kullanımıyla sınırlı olduğu düşünülmemelidir. Örneğin, bir kimlik hırsızı gerçek bir ehliyeti değiştirip kullanmakla yetinmeyerek, hayatını o ehliyetin sahibi kişilik olarak sürdürebilir. Çıkardığı diğer kimlik belgeleri, yasal işlemleri hep bu kimlik üzerine düzenlenmiş olabilir. Gerçek kimlik adına banka hesabı açtırabilir, hatta gerçek kimlik sahibinin hesabı üzerinde işlem yapması dahi mümkün olabilir. Kimlik hırsızlarının sağlayabileceği bir diğer önemli menfaat de, (özellikle ölen bir vatandaşın kimliğini çalarak) sabıka kayıtlarının temiz görünmesini sağlamaktır.

Kimlik hırsızlığı özellikle ABD'de son yıllarda en yaygın suçlardan biri halini almıştır. Yakın bir gelecekte bu suçun ABD'de en ciddi suç olacağı tahmin edilmektedir. Bunun nedenleri arasında,

- kurbanların gelir seviyesinin yüksekliği (hırsızlık için gösterilen gayretin buna değmesi),
- ülke coğrafyasının ve nüfusun büyüklüğü,
- ABD vatandaşların yurt dışına ya da farklı ülke uyrukluların ABD içine giriş çıkış adedinin ve kalma toplam süresinin uzunluğu,
- iş, okul ya da komşu çevresinin "standart görünen" bireylerin gerçek kimliğine ilgisiz kalabilmesi,
- şahısların iş, şehir ya da konut değiştirmelerinin sıradan görülmesi,
- değişikliklerin merkezi kaydının alınmaması ya da alınan kayıtlar üzerinde mükerrer kayıt ve benzeri kontrollerin sıhhatli yapılmaması,
- kimlik belgelerinin federal yönetimlerce farklı standartlar üzerinden verilmesi,
- genellikle kimlik denetiminin merkezi yapılmaması,

- kimlik hırsızlarının kendilerinin ya da suç ortaklarının mali ve teknolojik olanaklarının yüksekliği,

- geliştirilen hırsızlık tekniklerinin federal yönetimlerce öğrenilmeden, suçlu şebekeleri tarafından çok çabuk bir şekilde yayılması,

- yapılan hırsızlıkların çoğunlukla çok geç fark edilmesi,

- ceset kimliklerinin her zaman sıhhatli tespit edilememesi,

- bazı hırsızlık tekniklerinin tedbirinin, yüksek maliyet nedeniyle alınamaması

gibi pek çok madde sıralanabilir. Üstelik sebeplerin kimlik hırsızlığına etkileri çoğunlukla kolayca ölçülebilir değildir. Bu sebeplerin bir kısmı başka ülkelerde örneğin ülkemizde çok geçerli olmasa da, gelişen kültürel ve ekonomik şartlar yakın veya orta vadede söz konusu sebebi geçerli kılabilir.

Biyometrik veri tabanlı kimlik belgelerinin bu hırsızlığı önleyeceği düşüncesi yaygındır. Ne var ki, bu çözümün getirebileceği bir takım sakıncalar da vardır:

- Kağıt tabanlı nüfus cüzdanını ya da kredi kartını çaldırdığını fark eden biri belgeyi iptal ettirebilir fakat biyometrik verisini örneğin iris taramasını çaldıran birinin bunu iptal ettirmesi zordur.

- Biyometrik veri ve diğer kimlik bilgileri kaydının saklanmasının getireceği maliyet nedeniyle, bir çok kimlik belgesinin tek bir kart üzerinde toplanması zorunlu olmaktadır. Bu durum kimlik hırsızının işini kolaylaştırabilir. Kimlik hırsızı tek bir kimlikle bir çok işi yapabilir.

- Tek bir kimlik kartı hırsızlar için cazip bir hedef teşkil etmektedir. Örneğin Avustralya'da, vergi numarası uygulamaya konulduktan sonra vergi kimlik hırsızlığı artmış bulunmaktadır.

- Bir çok biyometrik veri tabanlı kimlik denetimi çözümünde, biyometrik veriler veritabanlarında saklanmaktadır. Kimlik hırsızlığı gerçekleştirecek kişi, veritabanına erişerek daha kolay hedefleri, örneğin fiziki yapısını daha rahat taklit edebileceği kurbanları, seçebilir.

- Biyometrik veri tabanlı kimlik denetiminin daha güvenilir olacağı düşüncesiyle kontrol görevlileri bazı ek "sosyal" kontrolleri gevşetebilir ya da tamamen kaldırabilir. Örneğin, işyeri kapı girişlerinde güvenlik görevlilerinin giriş yapan kişilerin hal, hareket ve tavırlarından şüpheli şahısları seçebilme çabasının biyometrik okuyuculu sisteme geçilmeden önce ve sonra aynı olması beklenmez. Hatta bu tür bir çözümün varlığı nedeniyle güvenlik görevlisi kontrolleri hiç yapmayabilir.

- Biyometrik veriler sadece bir sistemde kullanılmıyor olabilir. Örneğin devlet kayıt altına aldığı biyometrik verileri çok iyi koruyor olabilir fakat vatandaşlar yurt içinde özel kurumlarda ya da yurtdışında biyometrik verilerini vermek zorunda kalabilirler. Diğer bir deyişle, biyometrik verilerin sadece o sistem içerisinde güvenli saklanması yeterli olmayabilir.

- Kullanılan biyometrik veri tabanlı sistemin zayıflığı farkedilse dahi, sistemin bu zayıflığı kapatabilmesi maliyet, kurulum, personel ihtiyacı ve tekrar kayıt zorluğu gibi nedenlerle mümkün olmayabilir.

- Hemen her biyometrik veri tabanlı sistemde "yanlış kabul", "yanlış alarm (reddetme)" ve "kayıt olamama" hatalarına maruz kalacak şahıslar bulunacaktır. Kimlik hırsızı, bu hatalardan birinden muzdaripmiş gibi davranarak, örneğin iris kaydı alınamayan biriymiş gibi yaparak, sistemi kendisinin başkasının verisini daha kolay taklit edebileceği bir kayıt almaya zorlayabilir.

- Aynı biyometrik veri kontrol tekniği farklı etnik gruplar üzerinde değişik hata oranları verebilmektedir. Bu durum kontrol edilenin mağduriyetine yol açabilir.

Diğer yandan biyometrik veri tabanlı sistemlerin **kimlik hırsızlığının önüne getireceği engeller**den de bahsetmek gerekmektedir.

- Bazı biyometrik verilerin örneğin retina kaydının kimlik doğrulama ya da kayıt işlemi dışında elde edilmesi çok zordur.

- Bazı biyometrik verilerin taklit edilebilmesi hırsızın eline geçse dahi çok zordur.

- Biyometrik veri okuma ve kaydetme teknik ve teknolojileri hızla gelişmektedir. Sistemler hem daha az hata paylı çalışmakta, hem daha az maliyetli olmaktadır.

- Tek bir biyometriğe bağlı kalınması şart değildir. Birden fazla biyometrik verinin kayıt ve kontrolü kimlik hırsızlarının işini imkansızlaştırabilir.

- Teknolojilerin ucuzlaması ile daha çok kurum ve kuruluş biyometrik veri kontrolü yapacak, hırsızların yakalanabileceği noktalar artacaktır.

- Biyometrik verilerin kayıt ve kontrol amaçlı kullanımlarına ilişkin yasal mevzuatlar birçok ülkede henüz yeni düzenlenmektedir. Birkaç sene içerisinde bu ülkelerde hukuki belirsizlik nedeniyle kimlik hırsızlarının kurtulma şansları kalmayacaktır.

- Yeni gelişen bazı tekniklerle okunan biyometrik verinin o anda hazır bulunan canlı bir kimseye ait olup olmadığı anlaşılabilmektedir. Örneğin parmak izi okuyucuları, eskiden başkasına ait parmak izini taşıyan bir şeritle ya da iris okuyucuları bir video kaydı görüntüsü ile atlatılabilirken, günümüzde vücut sıcaklığını ya da parmak izinin belirli bir derinlikte alındığını denetleyen parmak izi okuyucuları veya gözün o anda verilen ışık değişimlerine hassasiyetini ölçen

iris okuyucuları okunan biyometrik verinin canlı bir kişiye ait olup olmadığını ayırt edebilmektedir.

- Kimlik kontrolü yapılırken görevli memurun kimlik hırsızlığı yapan kişiyi yanlışlıkla başka birine benzetmiş olduğu mazeretinin geçerliliği kalmayabilir. Örneğin parmak izi ikizleri dahi birbirinden ayırabilmektedir.

3. Uygulanabilir Güvenlik Yöntemleri

Sistem kullanıcılarına verilecek karta konulacak ve kimlik doğrulama için kullanılabilecek yöntemler Tablo 3-1'de verilmiştir. Bununla ilgili olarak FMR (yetkili kimlik sahibinin yetkisizmiş gibi algılanması), FNMR (yetkisizmiş kimlik sahibinin yetkili gibi algılanması), maliyet, elektronik kartta ayrılması gereken veri alanı, kimliğin taklit edilebilirliği için her bir biyometrik yönteminin durumu incelenmiş ve son olarak da bir gerekçe ile uygulanabilir bir biyometrik tanıma öngörülmüştür.

	FMR	**FNMR**	**Maliyet**	**Kartta gerekli veri alanı (Byte)**	**Taklit edilebilirlik**
Parmak izi tarama	İyi	İyi	Ucuz	300-1200	Orta
El geometrisi tarama	Orta	Orta	Orta	9	Zor
Yüz tanıma	Orta	Orta	Ucuz	500-1000	Zor
İris tarama	Çok iyi	Çok iyi	Pahalı	512	Çok zor
Retina tarama	İyi	İyi	Pahalı	96	Çok zor
Konuşma ve konuşmacı tanıma	Orta	Orta	Ucuz	1500	Kolay
İmza doğrulama	Orta	Orta	Orta	500-1000	Kolay

Tablo 3-1Kartta kimlik doğrulamada kullanılabilecek biyometrik yöntemler ve kullanılabilirlik.

Tablo 3-1'de belirtilen yöntemlerden parmak izi ile kimlik doğrulama yapılması, sağlık sistemlerinde kullanım için, gerek kullanım kolaylığı ve maliyet gerekse FMR ve FNMR değerlerinin kabul edilebilir aralıkta olması sebebiyle tercih edilmiştir.

3.1. Uygulanabilir kart tipleri

Kart tipi	Güvenlik	Bellek büyüklüğü	Çoklu-uygulama desteği	Standartlar	Terfi ettirilebilme
Mikro işlemcili Akıllı Kart	Güçlü	Güçlü	Güçlü	Güçlü	Güçlü
Plastik	Zayıf	Zayıf	Hiçbiri	Güçlü	Hiçbiri
Manyetik şerit	Orta	Zayıf	Zayıf	Güçlü	Orta
2 boyutlu barkot	Orta	Orta	Zayıf	Güçlü	Orta
Optik Kart	Orta	Güçlü	Güçlü	Güçlü	Orta

Tablo 3-2 Elektronik kartların karşılaştırılması

Günümüzde hafıza kartları ve akıllı kartlar geniş bir pazar payını almaktadır. Ancak, limitli depolama kapasitesi ve düşük güvenlik seviyesi göz önüne alınarak, hafıza kartları çoklu-uygulama ve çok-amaçlı kartlar olarak günümüz gereksinimlerini karşılayamamaktadır Tablo 3-2.

Güvenli mikroişlemci çipi (akıllı kart) aşağıdaki maddeleri içermektedir :

- 8-bit – 32-bit işlemci (CPU)
- İşletim sistemini içerecek ROM veya flaş hafıza
- Veri için geçici kayıt olacak RAM
- Çevre sensörleri (voltaj, frekans, sıcaklık)
- En az bir seti iletişim portu

- Sayaçlar
- Seçmeli kriptografik motor (DES, 3DES, RSA)
- Kullanıcı verisini saklamak için kullanılan non-volatile bellek
- Güvenlik tehditlerini (Ortak Kriter, FIPS 140-2)karşılamak için kullanılan özellikler

Güvenlik, tipik bellek büyüklüğü, birçok uygulamayı birden desteklemesi, uluslararası standartlara uygunluk ve güncellenebilme yeteneği açısından güvenli mikroişlemcili akıllı kartlar (Secure Microcontroller Integrated Circuit Chip Cards) diğer birçok ortamın önündedir. Bu sebeple kullanılması muhtemel kartlar arasından akıllı kart özellikle güvenlik ve güncellenebilme seçenekleri sebebiyle ön görülmüştür .

3.2. Akıllı kartlar ve alternatif teknolojiler

Bu bölümde, mevcut ID teknolojileri ve özel-hassas ID sistemi uygulamasındaki avantajları ve dezavantajları incelenecektir.

Güven Belgesi dokümanı ve Kimlik Doğrulama tokenları: Güvenli standartları güvenlik belgesi olarak kimlik doğrulama token (akıllı kartlar ve biyometrik teknolojiler) olmasını gerektirir.

- Plastik kartlar veya Kağıt kartlar: Plastik kart veya kağıt kartlar üzerine basılan görsel kimlik bilgileri (ad, soyad, adres ve fotoğraf), farklı uygulamalar tarafından görsel olarak doğrulama amacıyla kullanılır. Görsel tanıma, güvenlik görevlisinin resimleri tanıma ve objektif değerlendirme yeteneğine bağlı olduğu için, bu yöntemi kullanan güvenlik yöntemleri oldukça zayıftır.

- Barkodlar: Barkot, değişik doğru genişliklerinde ve boşluklardan oluşan, içerisinde belirli bir ürün bilgisi, kişi veya konum bilgisi taşıyan bir görüntüdür. Kod, sayıları ve diğer sembolleri tanımlamak için bir dizi düşey bar ve boşluklardan oluşmuştur. Başlıca beş bölümden oluşmaktadır: Sade alan, başlangıç karakteri, veri karakterleri (opsiyonel olarak kontrol karakteri), bitiş karakteri ve sade alan. Barkodlar, kişisel bilgi barındırabilir ve plastik kartların üzerine basılabilir. Doğrusal barkodlar, alfa-sayısal verinin saklanmasında kullanılır. İki boyutlu barkotlar, daha az bir alanda daha çok bilgi saklar. (1108 byte) Basım aşamasında veri barkota iletilir. Kart, etkileşim noktasında, barkodu üzerinden taranır. Barkot okuyucu, doğru ve boşluk kalınlığı ve varyasyonu yansımalarına duyarlı bir laser ışık demeti kullanır. Barkotlar, standart fotokopi aletleri kullanılarak kopyalanabilir. Bu gerçek, güvenli uygulamalarda barkot kullanımını engellemektedir. Güvenliğ arttırmak için, bazı durumlarda barkot üzeri bir maske ile kapatılabilir. Yüksek karbon içerikli basıcı şeritle barkodu basmak ve daha sonra karbon olmayan siyah mürekkep ile maskelemek, barkodun çoğaltılmasını engeller ancak barkot kızılötesi bir okuyucu ile okunabilir.

- Manyetik şerit kartları: Kartlar üzerindeki manyetik şeritler 1970 den beri değişik alanlarda (kredi kartları, sürücü belgeleri, vb.) kullanılmaktadır. Id kartları arkasındaki manyetik şerit, plastik benzeri bir bant içerisinde bulunan demir bazlı manyetik parçalardan oluşmaktadır. Her bir manyetik parça, bir inçin 20 milyonda biri büyüklüğünde olan demir mıknatıstır. Demir mıknatıslar belirli bir yöne polarize olduklarında, manyetik şerit boştur. Şerit üzerine bilgi, küçük demir mıknatıslarını elektromanyetik bir yazıcı kullanılarak kuzey ya da güney kutup noktasına çekmesiyle yazılmaktadır. Standart bir manyetik okuyucu kullanılarak, şerit üzerindeki bilgiler kolaylıkla kopyalanabilir ve yorumlanabilir. Bilgiler, başka bir karta kolaylıkla aktarılabilir. Bu sebeple, bu kartlar düşük güvenli uygulamalarda kullanılabilir.

- Optik şerit kartları: Optik şerit kartları, tescilli dış bir cihazın compact disk benzeri bir medya üzerindeki veriyi okuma, yazma ve işleme özelliklerine dayanan, tescilli bir teknolojidir. Optik şerit kartları CD leri okuma ve yazmada kullanılan teknolojinin çok benzeridir. Optik şerit üzerindeki bilgileri sık sık okuma sonrasında, optik şeritler zarar görmektedir.

- Akıllı kartlar: Akıllı kartlar, kendi başına bir bellek çipi olan veya iç bellek ile mikrokontroller görevi gören, gömülü bir çip bulundurmaktadır. Kartlar, okuyucuya fiziksel temas ile veya uzaktan temassız elektromanyetik arayüz ile bağlanırlar. Gömülü mikrokontroller ile, akıllı kartlar büyük miktarlarda veri saklama kapasitesine sahiptir, kendi kart fonksiyonlarını (şifreleme ve dijital imza) gerçekleştirir ve akıllı kart okuyucusu ile iletişim sağlar. Akıllı kartlar, finans, iletişim, ulaşım, sağlık, vb. alanlarda kullanılmaktadır. Sağladığı kilitleme ve şifreleme yöntemleriyle, akıllı kartlar üzerinde saklanan bilgiler güvenli hale getirilmektedir. Akıllı kartlar, güvenli ortamıyla (kart üzerinde eşleştirme yeteneğiyle, vb) karmaşık işlemleri gerçekleştirmektedir.

- USB. Universal Serial Bus, bilgisayar ile add-on cihazlar arasında takılıp-çıakrtılabilen bir arayüzdür. USB ile, yeni bir adaptor kartı takmadan veya makinayı kapatmadan bilgisayar üzerinde yeni bir cihaz eklenebilir. USB, saniyede 12 megabit veri hızını destekler. Bu hız, bir çok cihazın (MPEG video cihazları, vb.) hızına bağdaşır. USB güvenlik tokenler, kullanıcıların değişik ağlara veya bilgisayarlara kimlik doğrulaması (kullanıcı adı, şifre, biyometrik veya kriptografik anahtar deposu olarak) işleminde kullanılmaktadır.

Tablo 3-3'da yukarıda değinilen ID teknolojileri ile ilgili karşılaştırma tablosu verilmiştir. Akıllı kartlar, barındırdığı çip tipine göre (kontak çip ve kontak olmayan çip) olarak ayrılmıştır. 'X' gereksinimin karşılandığı anlamındadır. (Y(Yüksek), O(Orta) ve D(Düşük)) ise karşılaştırma seviyeleridir.

İş gereksinimleri	Teknoloji								
	Barkot 1 boyutlu	Barkot 2D	Manyetik şerit	Optik şerit	Hafıza Çipi	Akıllı Kart – Contact Çipli	Akıllı Kart-Contact olmayan Çipli	İkili Arayüz Çipi	USB
Yeni hükümet kimlik (ID yayılmalarında kullanım)	**X**	**X**	**X**	**X**	**X**	**X**	**X**		
İmalatçı	Çok	Çok	Çok	Az	Çok	Çok	Çok	Az	Çok
Yayımlandıktan sonra güncelleme			**X**	**X**	**X**	**X**	**X**	**X**	**X**
Mantıksal (ME) ve Fiziksel (FE) erişim ile ilgili destek	Çok FE tercihen	Her ikisi FE tercihen	Her ikisi	Her ikisi FE tercihen	Her ikisi ME tercihen	Her ikisi ME tercihen	Her ikisi FE tercihen	Her ikisi FE tercihen	ME
ID cihazının maliyeti	D	D	D	O	D	O	O	Y	Y
Okuyucunun maliyeti	O	O	O	Y	D	D	O	Y	
Depolama kapasitesi	D	D	D	Y	O	O	O	O	Y
Güvenlik	D	D	D	O	O	Y	O	O-Y	O
Birden fazla uygulamayı desteklenmesi	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Finansal uygulamalar			**X**			**X**	**X**		
Standartların desteklenmesi	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**
Birden fazla işletim sistemini desteklemesi					**X**	**X**	**X**	**X**	
Kart üzerinde biyometrik bilgi saklama		**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Kart üzerinde biyometrik eşleştirme yapma						**X**		**X**	
Kart ile kart okuyucu arasında çift yönlü kimlik doğrulama yapma						**X**		**X**	
Kart üzerinde anahtar üretimi						**X**		**X**	

Tablo 3-3 İş Gereksinimi – Teknoloji karşılaştırması

3.3. Akıllı Kart Sisteminin Kazançları

Geniş bir altyapının henüz sağlanmamış olması ve akıllı kart sistemlerini işletme maliyeti sebebiyle, akıllı kart sistemlerine geçiş yavaş olmaktadır. Ancak, aşağıda belirtilecek değişiklikler ve gelişmeler, kurumların akıllı kart sistemlerini kullanma hızını arttırmaktadır:

- Çipli kart sayısının artması: Kullanımının yaygınlaşması, kart altyapısının gelişmesine katkıda bulunmaktadır.

- Kart ücretinin düşmesi: Kullanımda olan kart sayısı arttıkça, kart ücreti düşmektedir. Kart kabiliyetlerine bağlı olarak, kart kullanımının artmaya devam etmesi, kart fiyatlarını da düşürmeye devam edecektir.

- Yanıt verme zamanının düşmesi: Kartın üzerinde olacak gelişmiş işletim sistemlerinin ve daha hızlı işlemcilerin varlığı ile karttan veri okuma ve karta veri yazma süresi oldukça kısalmıştır.

- Bellek kapasitesinin artması: Bellek kapasitesi 1 Kbyte dan 64 Kbyte a kadar yükselmiştir. Ortalama 32 Kbyte olarak kullanılmaktadır. Farklı uygulamaları içinde barındıracak akıllı kart, bellek kapasitesindeki artış ile, farklı uygulamaların daha verimli bir şekilde çalışmasını sağlamaktadır.

- Çok-uygulamalı kartlara geçiş: Geliştirilmiş güvenlik, bellek ve kart yetenekleri ile, çok-uygulamalı kartlara geçiş hızlanmaktadır. Bu kartlar, sahiplerine sağladığı elverişlilik dışında, farklı uygulamaların kendi kaynaklarını ortak kullanımını da verimli hale getirmektedir.

- Standart geliştirme ve yasalara karşı ortak kullanılabilirlik: Ortak kullanılabilirlik, uzun vadede kalkınma planlarında yer alan ve hükümet tarafından desteklenen bir konudur. Farklı uygulamaların aynı kart üzerinde saklanan bilgileri kullanarak geliştirilmesi ve kullanılması planlanmaktadır.

Akıllı kart pazarındaki bu değişiklikler kapsamında, kurumlar akıllı kartlı çözümlere yönelmektedir. Bir sonraki bölümde, akıllı kartların iyi bir aday olup olmadığı değerlendirilecektir.

3.4. Neden Akıllı kart sistemi

Her ne kadar akıllı kartlar, düz plastik kartlara göre daha pahalı ise de, çok-uygulamalı bir ortam paylaşımı, akıllı kart çözümünün genel masraf toplamını düşürebilir. Kartı

dağıtacaklar ve uygulama sahiplerinin beklentisi, farklı uygulamaların aynı kart üzerinde olmasının sağlayacağı fiyat tasarrufudur. Bunlar,

- Birleşme. Kartın üzerine yüklenen uygulamalar, ana hizmetleri destekleyecek veri ve bilgi işlemlerini paylaşırlar. Bu paylaşım, uygulama sahiplerinin ve kart dağıtıcıların maliyet paylaşımına sebep olur.

- Veri Toplama. Uygulama sahipleri farklı uygulamaların kullanacağı ortak verileri toplayıp saklamak işini paylaşırlar.

- Kişiselleştirme. Her bir uygulama için ayrı ayrı olarak değil de, kartın kişiselleştirilip, kullanıcıya verilmesi işlemi bir kez yapılır.

- Altyapı paylaşımı. Altyapı paylaşımı farklı uygulama sahipleri arasında paylaşılır.

- Kart güvenilirliği. Akıllı kart performansı ve dayanıklılığı, fiyat performans gelişimine bağlı olarak artmaktadır.

Fiyat-fayda analizi yapılırken, akıllı kart ortamı ile kağıt kullanılarak yapılan işlemlerin bulunduğu ortamın karşılaştırmalı toplam maliyeti ele alınmalıdır.

Fiyat tasarrufunun dışında, asıl ele alınması gereken, kurumların, işlemlerini elektronik ortama taşımaları ile ilgili bütün sorumluluklarını çok iyi anlamaları gerektiğidir.Eğer kurumlar, kağıt işine devam ederlerse, akıllı karttan çok daha ucuz çözümler mevcuttur. Akıllı kartlı bir çözüm, kurum süreçlerini ve işlemlerini tekrardan planlama kapsamında düşünülmesi gereken bir çözümdür.

Akıllı kartlar aşağıdaki faydaları sağlamaktadır:

- Güvenliği arttırır: Dijital sertifika veya biyometrik model bulundurarak, kart kimliğini doğrulamayı kolaylaştırır.

- Binalara, toplantılara, bilgisayarlara, e-posta veya internete erişimi kolaylaştırır: PIN, biyometrik veya dijital sertifika bulundurarak, akıllı kart kullanıcılarının fiziksel ve elektronik sistemlere erişimini denetler. Kullanıcı, birden fazla şifre hatırlayıp, formlar doldurmak zorunda değildir.

- Kişisel kimlik gereksinimlerini kolaylaştırır: Dijital kimlik sağladığı için, kullanıcının birden fazla kart taşıyıp, login bilgisi veya PIN bilgisi hatırlaması gerekliliğini ortadan kaldırır.

- Süreç yenilemeyi destekler: Akıllı kartlı çözümler kullanan kurumların, kağıt işinden elektronik ortama geçişte, kart üzerinde bulunan kaynakların verimli kullanımı ile uyguladıkları süreçleri yenilemeyi sağlar.

- Internet servisleri için gizli ve güvenilir erişim sağlar.

4. Biyometrik ve Akıllı Kartlar

Uzun yıllardır, güvenli erişim, "sahip olduğun" (kredi kartı,vb.) ve "bildiğin" (şifre, PIN, vb.) kavramları esas alınarak gerçekleştirilmektedir. Bu şekilde sağlanan güvenlik tipleri, PIN numarası kolaylıkla kayıp edildiği, unutulduğu veya çalınabildiği için, yüksek güvenlik gerektirecek sistemlerde yeterli olmamaktadır. Daha çok güvenlik gereksinimi olan sistemlerde, bahsi geçen iki unsurun yanında, biyometrik kullanımı gerektiren "ne olduğun" unsuru (değişik biyolojik özellikler) kullanılmaktadır.

Biyometrik, yaşayan bir insanın ölçülebilen ve özellikle ayırt edilebilen fiziksel veya davranışsal özellikleridir. Biyometrik, tekil olarak bir kişiye atanır ve kullanıcı kimlik doğrulaması esnasında kuvvetli bir faktör olarak kullanılır. Biyometrik, parola veya token ile birlikte kullanılarak kuvvetli ve iki-faktörlü (sahip olduğun ve bidiğin) kimlik doğrulama gerçekleştirilir.

Fiziksel (statik) biyometrik, insan anatomisinin bir parçasından ölçülen veriye dayanan bir biyometriktir. Biyometriklere örnek olarak parmak izi, el, yüz, iris ve retina verilebilir. **Davranışsal (dinamik) biyometri** ise, insan tarafından gerçekleştirilen bir davranıştan alınan ölçümlerden çıkartılan veriye dayanan bir biyometriktir. Davranışsal biyometriğin başlangıç ve bitiş zamanı vardır. Örnek olarak ses ve imza verilebilir. Fiziksel biyometrik, zorlama veya fiziksel engel haricinde değişmemektedir. Davranışsal biyometri ise, stress, hastalık, vb. durumlarda değişiklikler gösterir ve daha az güvenlidir.

Bu bölümde, akıllı kartlarla kullanılacak farklı fiziksel biyometrik tipleri anlatılacaktır.

Parmak İzi: En yaygın olarak kullanılan biyometriktir. Herhangi iki insanın aynı parmak izine sahip olması yüz milyarda bir olarak tahmin edilmektedir. Bir asırdır kullanılan parmak izlerinden, birbirinin aynısı parmak izine rastlanmamıştır. Bir insanın parmak izi, ölene kadar sabit kalmaktadır. Parmak izi görüntüsü dört değişik teknoloji ile elde edilir. Bunlar, optik, silikon, termal silikon ve ultrasoniktir. En yaygın olarak kullanılan optik teknolojilerdir. Uzun vadede silikon teknolojilerinin yaygınlaşması planlanmaktadır. Bununla beraber, parmak izi eşleştirme yöntemleri de geliştirilmiştir. Örnek olarak "Henry Classification System" verilebilir. Parmak izi üzerindeki **minutiae (olay (durum) noktaları)** alınarak, her bir detay sayı değişkenleri olarak ifade edilir. Tipik bir parmak izi 30 ila 40 durum noktası barındırır. Bir çok biyometrik sensör, durum noktaları karşılaştırarak eşleştirme yapar. Parmak izi, en büyük biyometrik kalıplardan birine sahiptir (250 bytes dan 1000 byte a kadar). Parmak izi kalıbı, parmak izinin görüntüsünü içermez, görüntüden elde edilen özellikleri içerir ve kalıptan parmak izi elde etmek mümkün değildir.

El Geometrisi: El geometrisi biyometrik tipini kullanan el geometri sistemleri optik teknoloji kullanarak, el topolojisinden elde edilen ana geometrik özellikleri, kişinin kimliğine eşleştirir. El geometri teknolojileri kalıpları hazırlamak için değişik ölçümler kullanırlar. Bu ölçümler, parmak uzunluğu, el kalınlığı, avuç içi şekli vb. 'dir. Değişik ölçüm alternatifleri kullanıldığı için, akıllı kartlarda kullanılabilecek standart bir kalıp mevcut değildir. Genel olarak, bir insanın eli insana özeldir ve zaman içerisinde değişebilecek bir tip değildir. Bu sebeple, kimlik doğrulamada kullanılabilir. El

geometrisi tarama cihazları, mekanik olarak veya görüntü işleme yaparak el geometrisinin görüntüsünü elde eder. Her iki durumda da elin üç boyutlu görüntüsü kullanılmaktadır. Uzunluk, genişlik, kalınlık ve alan ölçümleri, yaklaşık 90 defa yapılmaktadır. Bu ölçümler için, toplam kalıp büyüklüğü 10 ila 20 byte arasında değişmektedir.

Yüz tanıma: Sürücü ehliyet belgesinin yayımlanması esnasında kimlik doğrulaması için kullanılan bir biyometriktir.Yüz biyometriği, canlı olarak taranmış bir yüzün özellikleri ile daha önce kayıt edilmiş özelliklerin karşılaştırmasını yapar. Dijital kamera/video kullanılarak tüm yüz görüntüsüne göre yüz tanıma yapılabilir. Ayrıca, yüze ait bazı özelliklerin çıkartılması ve karşılaştırılması ile yüz tanıma yapılabilir. Örnek olarak, göz merkezinin kulak altına uzaklığı, göz merkezinin çene ortasına uzaklığı ve yanak noktasına uzaklığı, vb. Değişik yöntemler kullanıldığı için, yüz biyometriğinin belirli bir tanıma şablonu yoktur. Yüzün değişebilir özellikleri dikkate alınmadığı için (saç rengi, saç stili, vb.), bu yöntem birbirine çok benzeyen insanları (ikizler) ayırt edemeyebilir. Yüz tanıma sırasında kullanılan kalıplar: özyüz, dalgacık katsayıları, lokal özellik analizi ve termogramdır.

Iris: Bu biyometrik, optik parmak izi olarak kullanılabilecek bir tiptir. Kişiye özeldir ve değişmez. Kornea tabakasında meydana gelecek bir hasar dışında, iris değişmez ve korunaklı bir bölgede bulunan sağlam bir biyometridir. Parmak izine kıyasla 6 kat daha ayırtedici ve belirleyici özellikler barındırır. Iris görüntüsü elde etme cihazlarının hem kullanımı zordur (Kamera lensinden 15 ila 25 santimetre uzaklığında olunması gerekir, vb.) hem de maliyeti diğer biyometrik veri toplama cihazlarına göre oldukça yüksektir. Iris Şablonu (IrisCode), iris örüntüsünü demodüle ederek elde edilir. Matematiksel işlem, iris örüntüsünün büyüklüğüne göre değişmez.

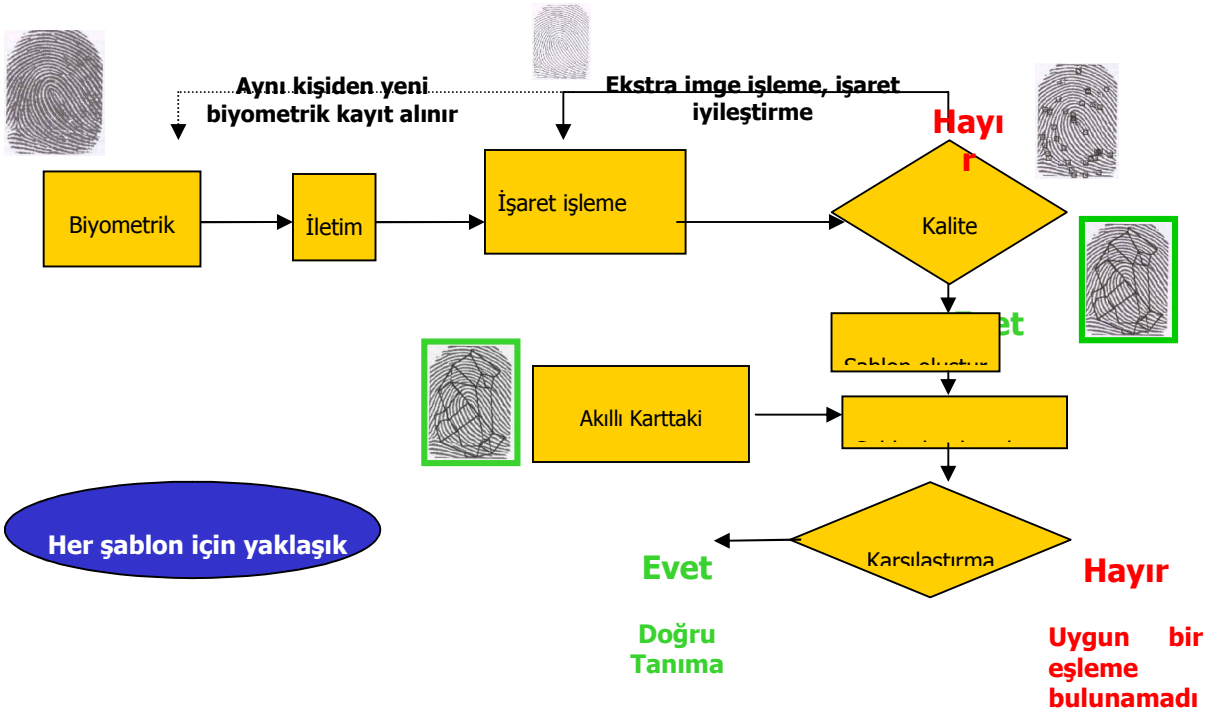
Retina: Retina üzerindeki kan damarlarının belirlediği örüntü kişiye özeldir. Iris teknolojisi ile birlikte, retina en doğru ve güvenilir biyometriktir. İkizler arasındaki retina kalıpları bile birbirinden farklıdır. Hastalıklar dışında (katarakt, vb.) retina bir ömür boyu kullanılabilir.

4.1. Biyometrik Sistemler

Biyometrik güvenlik sistemlerinde tanıma (Tanılama) ve doğrulama (Verification) kavramları öne çıkmaktadır. Tanıma (identification) kişiye ait bir delilin bir veri kümesinde (veritabanında) taranarak bulunması esasına dayanır. Tanıma da 1:N'lik bir tarama süreci söz konusudur Burada N, veritabanında karşılaştırma yapılacak örnek sayısı, genelde kişi sayısı olarak düşünülebilir. Doğrulamada ise kişi önce kendisinin kim olduğunu sisteme bir akıllı kart, kullanıcı adı veya kodu ile söyler. Sistem, bu kişinin ilgili biyometrik şablonunu veritabanından veya kişinin üzerinde bulunan karttan alır ve okuyucudan elde edilecek o anki test verisiyle karşılaştırır. Eğer kişi "iddia ettiği kişi" ise tanıma başarılı olur ve giriş yetkisi verilir.

Proje kapsamında değerlendirilecek kavram, 1:1'lik bir tarama süreci olan doğrulama (Verification)'dır. Şekil 4-1 'de doğrulama aşamasında uygulanan süreçler verilmiştir. Farklı biyometrikler kullanılmasına rağmen, tüm biyometrik sistemlerde ortak olan,

kullanıcıdan elde edilen örnek ile ayırt edici özelliklerin ortaya çıkmasını sağlayacak "doğrulama şablonu" oluşturulmasıdır. Şablonlar genel olarak büyük sayı dizileri oldukları için, şablondan örnek elde edilmesi mümkün değildir. "doğrulama şablonu" kişinin parolası yerine geçmektedir.



Şekil 4-1 Biyometrik Kişi Tanıma (Doğrulama) aşaması

Tek zamanlı bir parolanın veya ezberde olan bir parolanın doğrulanması evet/hayır kararının alınmasından ibarettir. Ancak, "doğrulama şablonu" nun doğrulanmasının sonucu evet/hayır değildir. Biyometrik sistemlerde, "doğrulama şablonu" , kişinin birçok ölçümler sonrası elde edilen ve kendisine eşleştirilen "referans şablonu" ile karşılaştırılması sonucunda, en yakın eşleşene göre (belirli bir eşikten sonrası için) eşleştirme sonucu belirlenir. Bu yüzden, biyometrik sistemler hata payı içerirler. "doğrulama şablonu" yanlış olarak başka bir kişinin "referans şablonu" ile eşleşebilir veya "doğrulama şablonu" kişinin kendi "referans şablonu" ile eşleşmeyebilir. Biyometrik sistemlerde doğruluk aşağıdaki yöntemlerle ölçülmektedir:

Yanlış eşleme (kabul etme) oranı (FMR): Buna FAR(False Aceptance Rate) de denir.

Yanlış eşleşmeme (reddetme) oranı (FNMR): Buna FRR(False Rejection Rate) de denir.

Eşit Hata Oranı (EHO): FMR ile FNMR'ın eşit olduğu durum

Her üç yöntem, sistemin yetkili kişilerin girişini engelleme yeteneğine odaklanmıştır. FMR düşük oldukça, sistem güvenliği daha iyi olacaktır. FNMR düşük oldukça, kullanım daha kolay olacaktır. Genel olarak verilen eşik değerine bağlı olarak FMR düşük oldukça, FNMR yüksek olmaktadır. Bu yüzden, biyometrik sistemlerin kullanımında güvenlik ile kolay kullanım arasında her zaman bir eşik noktası bulunmaktadır.Bu biyometrik güvenlik sisteminin genel başarımı için en iyi ölçüt EHO'dur. EHO maksimum %5 olmalıdır. EHO ölçülürken, genelde ilk tanıma girişiminin sonucuna bakılır. Yanlış tanıma durumunda sistem kullanıcıdan bir kere daha biyometriğini ister. Bu durumda ikinci tanıma başarımı, ilk tanıma başarımına göre artar.

4.2. Biyometrik Teknoloji Faydaları

- Güvenliği arttırır.
- Biyometrik bilgi kayıp edilemez, çalınamaz veya unutulamaz.
- Akıllı kartlar ile birlikte biyometrik sistemler, PKI servislerine (özellikle dijital imza) güvenli bir ortam sağlar.
- Kullanıcı herhangi bir PIN veya parola hatırlamak zorunda değildir. Biyometrik veriler, kullanıcılarda sürekli mevcuttur.
- Kurumlar, parola yönetimi işlemlerinden kurtulurlar ve müşteri servislerini geliştirirler.

Yıllara göre öngörülen toplam biyometrik pazar paylarına göre (IEEE Spectrum dergisinin Mart 2004 sayısında (sf. 9) yayınlanan bir araştırmaya göre biyometrik teknolojileri pazar büyüklüğü için 2008 yılına kadar öngörülen rakamlar), biyometrik teknolojiler önümüzdeki senelerde daha çok popülerlik kazanacaktır.

4.3. Biyometrik Teknoloji Riskleri

Gizlilik Sorunları: Biyometrik verinin saklanması ve dağıtılması kanuni açıdan sakınca oluşturabilir. Verinin farklı amaçlarla kullanılması ve veriyi toplayan kurum dışında farklı bir kurumda kullanılması riskleri mevcuttur. Biyometrik sistemler ile birlikte düşünülen akıllı kartlar, biyometrik verinin güvenli bir şekilde saklanmasını sağlayan ortamlar gibi düşünülmelidir.

Kişisel, Kültürel ve Dini Sorunlar: Biyometrik verinin sağlanması aşamasında, kişisel, kültürel ve dini sebeplerden dolayı, kişiler örnek vermeyi kabul etmeyebilirler. Parmak izinin polis kayıtlarında değerlendirilme ihtimaline karşı, kişilerde hassasiyet oluşabilir.

Tüm kullanıcılar için uygunluk: Bir toplumda yüzde 1 ila 3 arasında, herhangi bir biyometrik veri vermeye müsait olmayan kişi mevcuttur. Fiziksel olarak engelli olan kişiler biyometrik veri veremeyebilir. Bu durumda sistemin değişik senaryolar için alternatifler üretmesi gerekmektedir.

Tekrardan yayımlamak: Herhangi bir sebepten, biyometrik verisi ele geçirilen bir kişi için, aynı verinin kullanılması mümkün değildir. Kullanıcının sisteme tekrardan tanıtılması ve yayımlanması gerekmektedir. Bu duruma düşmemek için, biyometrik eşleştirme yapılan ortamlarda, alınan canlı örnek ile kalıp karşılaştırması akıllı kartta yapılmaktadır veya eşleştirme yapan cihaz kurcalayamaya karşı hassas olacak şekilde tasarlanmaktadır. Ağ üzerinden iletilen biyometrik veriler ise özel olarak şifrelenmektedir. 90 bit anahtarla yapılan simetrik şifreleme uzun bir süre veriyi koruyacaktır.

4.4. Biyometrik Seçim Rehberi

Kurumlar, uygulamaları için kullanılacak güvenlik seviyesini belirlemelidir. Uzun vadede düşünülmesi gerekenler:

- Kullanıcı kabulü,
- Kullanım kolaylığı,
- Güvenlik – doğruluk, sağlamlık ve tehditlere karşı direnç,
- Maliyet,
- Şablon depolama – konum ve kapasite planlama,
- Uygulanabilir standartlar: Uygulanan biyometrik çözüm standartlara uygun olmalıdır ve her durumda aynı şekilde çalışacağını belirtmelidir,
- Biyometrik veri işleme zamanı: Biyometrik eşleştirme yapıp, kimlik doğrulama sonucunun belirtilmesi en fazla 1 saniye sürmelidir,
- Biyometrik güncelleme.

Kurum, biyometrik kullanımın gerekliliğini belirledikten sonra, bir sonraki aşamada biyometrik tipi seçme ve bu seçim esnasında hangi kriterleri kullanma sorularını yanıtlamaktır. Aşağıdaki listede kriterler biyometriklere göre belirtilmiştir.

- Parmak izi: Maliyeti düşük, uygun ve müdahale edilemeyecek bir biyometriktir.
- El Geometrisi: Doğru ve müdahale edilemeyecek bir biyometrik tipidir. Ancak, akıllı kartlarda herhangi bir standart şablon mevcut değildir.
- Yüz tanıma: Video/dijital kamera kullanılarak temin edilir. Ancak, akıllı kartlarda herhangi bir standart şablon mevcut değildir.
- Iris: Çok güvenilir, sağlam ve müdahale edilemeyecek bir biyometrik tipidir ancak şablon oluşturma aşaması zahmetlidir.

- Retina: Çok güvenilir ve sağlam bir biyometriktir ancak görüntü alma esnasında müdahale edilebilir.

- Ses tanıma: Ses, telefonla yapılan işlemlerde doğrulama amacıyla kullanılabilen uygun bir biyometriktir. Ancak, ses tanıma sırasında ses taklit edilebilir veya değiştirilip kullanılabilir.

- İmza: Daha çok dokümantasyonda kullanılan ucuz bir biyometrik çözümdür.

Kullanıcı hususları aşağıda verilmiştir:

- Genel kabullenme: Kültürel ve dinsel faktörler göz önüne alınmalıdır.

- Kullanıcı kabullenmesi: Biyometrik verinin sağlanması aşamasında, doğruluğu daha fazla olsa da, sağlanma sırasındaki zorluklar kullanıcının kabullenmesini engelleyebilir.

- Kullanıcı zorlukları: Biyometrik verinin sağlanması aşaması mümkün olduğunca kolay olmalıdır.

- Kullanım kolaylığı: Tarama yöntemi, FMR, FNMR ve EHO ve hız kullanım kolaylığını etkileyen faktörlerdir.

5. Güvenli Kimlik Doğrulama ve Erişim Denetim Sistemi

Kimlik belirleme, kimliği bilinmeyen bir şahsın kimliğinin tespit edilmesi demektir. Kimlik doğrulama sistemi, kendisinin "(belli bir işi yapmaya yetkili) o kişi" olduğunu iddia eden bireyin kimliğinin denetlenmesi hedefine cevap vermeye çalışır. Erişim denetimi ise belli kaynaklara yalnızca o kaynaklara erişim hakkı olduğunu ispatlayan şahsa izin verilmesini sağlamaya çalışır.

Yukarıdaki üç kavram da kişilerin kimlikleri ya da yetkileri üzerinden denetleme yapılmasını gerektirir. Bu denetlemeler sırasında şahsın kimliğini ve yetkilerini ispatlamak için kullandığı malumat ve yöntemlere delil diyelim. Kullanıldıkları yere, istenilen güvenlik seviyesine, kimlik belirleme imkanları gibi birçok parametreye bağlı olarak deliller de çok muhtelif olabilir. Nüfus cüzdanı, parmak izi, parola, konser bileti, sertifika, matbu onay belgesi gibi örnekleri çoğaltmak mümkündür.

Şahsın belli bir işi yapmaya yetkili olduğu bilgisi her zaman delilin yanı başında durmayabilir. Kimliği belirlenmiş şahsın ne yapabileceği, ya da belirli bir işe yetkisi olup olmadığı erişim denetimi olmasına rağmen delillerin yetkilerle ilişkilendirilmesini gerektirdiğinden üç kavramın iç-içe geçtiği görülecektir. Örneğin, SSK çözümünde hastanın tedavi bilgilerine ulaşabilecek doktorların kimliklerinin önceden belirlenmesi, uygun delillerin verilmesi ve hasta bilgilerine ulaşma anında kimliklerinin doğrulanması ve verilen deliller ile hasta bilgilerine erişim hakkının olup olmadığının kontrol edilmesi gerekmektedir.

Kimlik belirleme, kimlik doğrulama ve erişim denetimi kavramlarının bu sıkı ilişkisinden dolayı üç kavramı kimlik belirleme çatısı altında toplanabilir.

Güvenli bir kimlik belirleme sisteminin sağlaması beklenen bazı özellikler vardır:

- Delil verilecek kişilerin kimliği doğru belirlenmelidir.
- Kimliğini doğrulatacak kişi, gösterdiği deliller ile ilişkilendirilebilmelidir.
- Gösterdiği delillerin geçerliliği kolayca kontrol edilebilmelidir.
- Deliller, farklı kişileri birbirinden kolayca ayırt edebilmelidir.
- Deliller kolayca taklit edilememelidir.
- Deliller vasıtasıyla kişinin gerekli yetki ve erişimi doğrulanabilmelidir.

Güvenlik ihtiyaçlarının yanında uygulanabilirlik de kimlik belirleme için çok önemlidir. Delillerin kolayca taşınabilmesi, deliller arasında güvenli üst merkezden alınan bir onay varsa bu onay alma yordamının kolaylığı gibi konular da kimlik belirleme sisteminin tasarım ve uygulamasında mutlaka göz önüne alınması gereken hususlardır. Bir diğer

dikkate alınması gereken husus ise bazı delillerin örneğin biyometrik verilerin merkezi bir yerde saklanmasına yönelik tek bir saldırı noktası olması, mahremiyet ihlali gibi çekincelerle sıcak bakılmamasıdır.

Delillerin kağıt tabanlı ortamda taşınması, birçok durumda sahte delil hazırlanmasını kolaylaştırmaktadır. Bununla beraber, belli bir kimlik belirleme için kullanılan delil başka amaçlarla da kullanılabildiğinden kağıt tabanlı sistemlerle kişilerin mahremiyetini sağlamak kolay değildir. Bir üçüncü sebep de, kimlik kontrolü yapanların, bireyler arası farkı kendi duyuları ile değil de otomasyona bağlı olarak yapmak istemeleridir. Bu nedenlerden dolayı, delillerin ilk kayıt ve/veya kontrol sırasında elektronik ortama aktarılmasını zorunlu kılmaktadır.

Delillerin hepsinin merkezi bir yerde saklanmaması, kişi tarafından kolayca taşınabilmesi, sistem tarafından kolayca kullanılabilmesi ve elektronik veri taşımaya uygun olması nedeniyle delillerin taşındığı ortamın bir kart olduğu kabul edilecektir. Buna kısaca kimlik kartı diyelim. Kimlik kartı, kişinin kimlik belirleme sisteminde kullanacağı verilerin taşınabilir, güvenilir ve kolayca kontrol edilebilir gösterimini içeren bir karttır. Tercihen içindeki veriler, kişinin kimliğini ispat ettiği sistem için haklarını ve imtiyazlarını da belirtmelidir.

Kimlik belirleme sistemleri temelde bir güvenlik sistemidir. Delilleri toplayana, varsa deliller toplandıktan sonra verilen üst makam onayına, delillerin geçerliliğini kontrol eden mekanizmaya (kart okuyucu, gözümüz vs.) ne zaman ne kadar güvenileceğinin belirlenmesi gerekir. Güvenlik politikası aynı zamanda tutarlı olmalıdır. Aynı delillerin eş (birebir aynı olmayan ama temel prensibi aynı) kontrol mekanizmalarında aynı sonucu vermesi beklenir.

5.1. Bir Kimlik Belirleme Sistemini Güvenli Kılan Adımlar

Güvenli kimlik belirleme tasarımı en azından aşağıdaki adımları içermelidir:

- Her bir bireyin kesinlikle o kişi olduğuna ait delillerin (haklarla beraber) tespit edildiği **kayıt** evresi.
- Delillerin kimlik kartına doğru ve güvenli aktarımı, sadece yetkili kurum ve kuruluş tarafından doğru kişiye verildiği **yayın/dağıtım.**
- Kimlik kartının **kullanım politikalarının ve işlemlerinin belirlenmesi** .
- Kartın **kullanım hayatı** (Eskime, bozulma, geçersiz kılma işlemleri de dahil).
- Kullanıcı ve kart yayımlayanların **eğitimi.**
- Kart sahiplerinin sistem içerisinde tutulan bilgilerine (kart sahibi, kontrol eden ve merkez dışında) üçüncü kişilerin erişememelerini sağlayan politika, işlem ve teknolojinin belirlenmesi (**mahremiyetin sağlanması**).

- Karttaki bilgileri sadece yetkili kişilerin görebildiğine dair güvenlik kontrolleri (**karta erişim denetimi**).

- Tanımlanmış güvenlik zincirini gerçekleyen kart sahiplerinin kimliklerini belirleyen ve karttaki delillerin geçerliliğini kontrol eden **kimlik doğrulama işlemi.**

Kartlı bir güvenli kimlik belirleme sisteminde güven zincirinin sağlanması için aşağıdaki koşullar mümkün olduğunca sağlanmalıdır:

- Kartın sahibi olduğunu iddia eden kişi doğru kimliğe sahip olmalıdır.

- Kartın sahibi olduğunu iddia eden kişi geçerli kimliğe sahip olmalıdır.

- Kart sahibi kimlik doğrulamada kullanılmak üzere kimlik delilleri göstermeli veya delillerin kontrol amaçlı kullanımına izin vermiş olmalıdır.

- Verilen delil yetkili bir merci tarafından onaylı olmalıdır.

- Verilen delil tahrif edilmiş olmamalıdır.

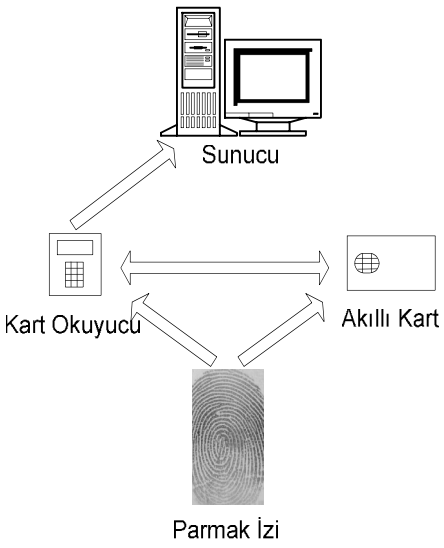
- Verilen kimlik kartı yapılan iş veya alınan hizmet için uygun kimlik kartı olmalıdır. (doğru yetkilendirmeli).

- Kontrol mekanizması sıhhatli (doğru ve tutarlı) çalışmalıdır.

- Kimlik kontrol mekanizması güvenilir olmalıdır. (Dışarıya bilgi sızdırmamalı).

6. Güvenlik Mekanizmaları

Ulusal Kimlik Kartının görevi vatandaşın kimliğinden emin olunmasını sağlamaktır. Şekil 6-1'de kart tabanlı kimlik doğrulamada görev alan elemanlar gösterilmektedir. Söz konusu sistemde kullanılan her eleman birbirinden emin olmak zorundadır. Kart, kart okuyucudan, kart okuyucu karttan, sunucu kart okuyucudan, kart okuyucu sunucudan emin olmak durumundadır. Bu sağlanmadığı takdirde, kimlik bilgileri üçüncü şahıslarca ele geçirilebilir, değiştirebilir ya da kişi, sahte kimlikle kimlik denetimini geçme imkanı bulabilir.



Şekil 6-1 Ulusal Kimlik Kartında kimlik doğrulamada görev alan elemanlar.

Kimlik doğrulamada amaç, kamu hizmeti veren kurum yetkilisinin veya kurum bilgisayar sisteminin hizmet vereceği vatandaştan emin olmasını sağlamaktır. Kamu kurumlarının amacı, hizmet almayı hak eden vatandaşın hizmet almasını sağlamaktır. Diğer bir ifade ile doğru vatandaşa doğru hizmet verilmesi ilkesi söz konusudur.

Kimlik tanıma işlemi, görsel ve/veya kart yardımı ile yapılabilir. Görsel tanıma, kart üstünde vatandaşın fotoğrafına ve kimlik bilgilerine bakılarak tanıma yapılmasıdır. Kart tabanlı tanımada genellikle iki yöntem kullanılmaktadır:

Şifre kullanılarak kartın sahibinin şifreyi bilen olduğu varsayılmaktadır.

Kart sahibinin biyometrik bilgileri yardımıyla kimlik doğrulama yapılabilir. Bu tür tanımada, kart sahibinin biyometrik verileri bir donanım yardımı ile kartta saklanan veri ile karşılaştırılır. Biyometrik veri olarak parmak izi, yüz bilgileri ve iris bilgileri sayılabilir.

Kimlik denetleme mekanizmalarında genellikle görsel ve kartlı tanıma yöntemi birlikte uygulanmaktadır.

6.1. Kart Okuyucu Ulusal Kimlik Kartından Nasıl Emin Olabilir?

Bir kimlik doğrulama sisteminde, kimlik doğrulamanın doğru bir şekilde yapılabilmesi için, öncelikle kimlik doğrulama araçlarının birbirlerinden emin olmaları gerekmektedir. Bunun için, kart okuyucu ile akıllı kart birbirlerinin kimliklerini bazı güvenlik mekanizmalarını kullanarak doğrulayacaktır.

Kart Okuyucu Ulusal Kimlik Kartından aşağıdaki adımları izleyerek emin olabilir:

- Ulusal Kimlik Kartı, kart okuyucuya takılır.
- Kart okuyucuya Ulusal Kimlik Kartının kimliği (ID) verilir.
- Kart okuyucu, nüfus idaresindeki sunucudan kartın açık anahtarını alır.
- Kart okuyucu, rasgele bir değer üretir, belirli bir örüntüyü de ekler.
- Kart, imza özel anahtarı ile kart okuyucunun yolladığı değeri imzalar ve kart okuyucuya gönderir.
- Kart okuyucu, (sunucudan alınan açık anahtar yardımıyla) kartın attığı imzayı kontrol eder.
- İmza doğru ise kart okuyucu için kart güvenilirdir.

6.2. Kart, Kart Okuyucudan Nasıl Emin Olabilir

Ulusal Kimlik Kartı kart okuyucudan aşağıdaki adımları izleyerek emin olabilir:

- Kart Okuyucu, Ulusal Kimlik Kartına kendi sayısal sertifikasını gönderir.
- Ulusak Kimlik Kartı, elindeki KSYM sertifikası yardımıyla kart okuyucunun sertifikasının doğruluğunu kontrol eder.
- Ulusal Kimlik Kartı, kart okuyucuya rasgele değer gönderir.
- Kart okuyucu rasgele değeri imzalar.
- Kart önceden almış olduğu kart okuyucunun sertifikasının yardımı ile, gönderilen rasgele değerin imzasını kontrol eder.
- İmza doğru ise kart için kart okuyucu güvenilirdir.

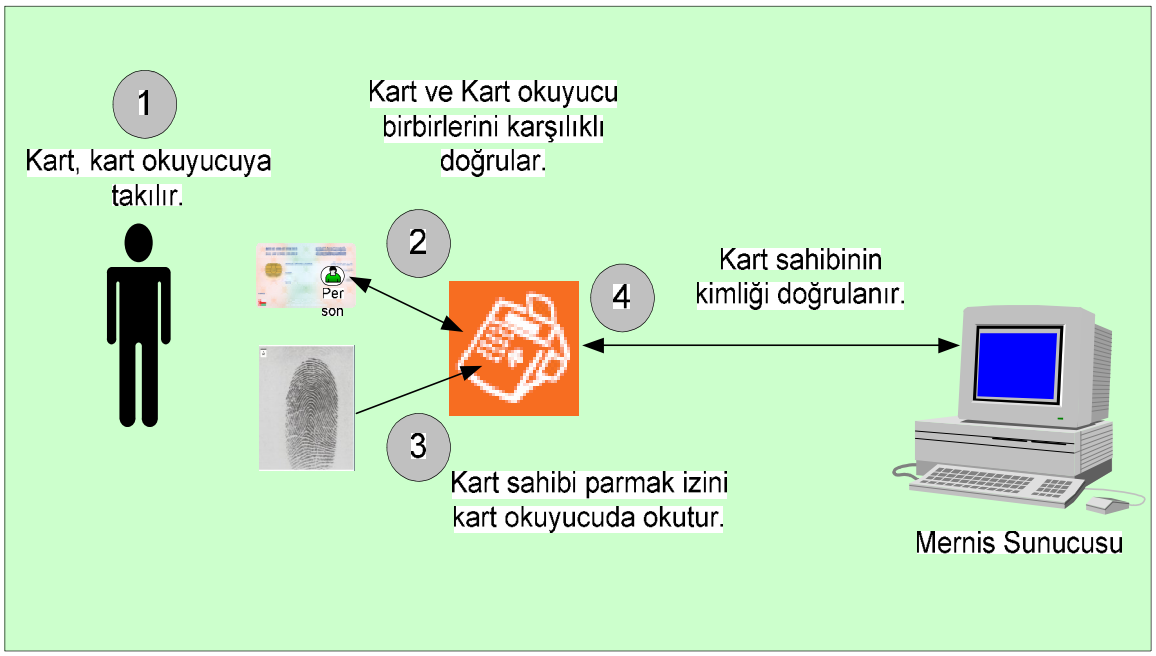
6.3. Ulusal Kimlik Kartın Görsel Kontrolü ile Kimlik Doğrulama

Şekil 6-2 Kart ile görsel kimlik kontrolü yapılması.

Kart sahibinin kimlik kontrolü görsel olarak yapılır. Bunun için Şekil 6-2 de gösterildiği gibi, kimlik doğrulama işlemini gerçekleştiren kamu görevlisi ilk kartın üzerinde bulunan resim ile vatandaşın dış görünüşünü karşılaştırır. Kart üzerindeki resim ile kart sahibinin görünümleri aynı ise, Ulusal Kimlik Kartının özel kaplaması ultraviole ışığı altında incelenir. Kartın doğruluğundan emin olunduktan sonra, operatör Internet üzerinden kart sahibinin bilgilerini Mernis sunucusundan kontrol eder.

6.4. Kart Sahibinin çevrim-içi doğrulanması

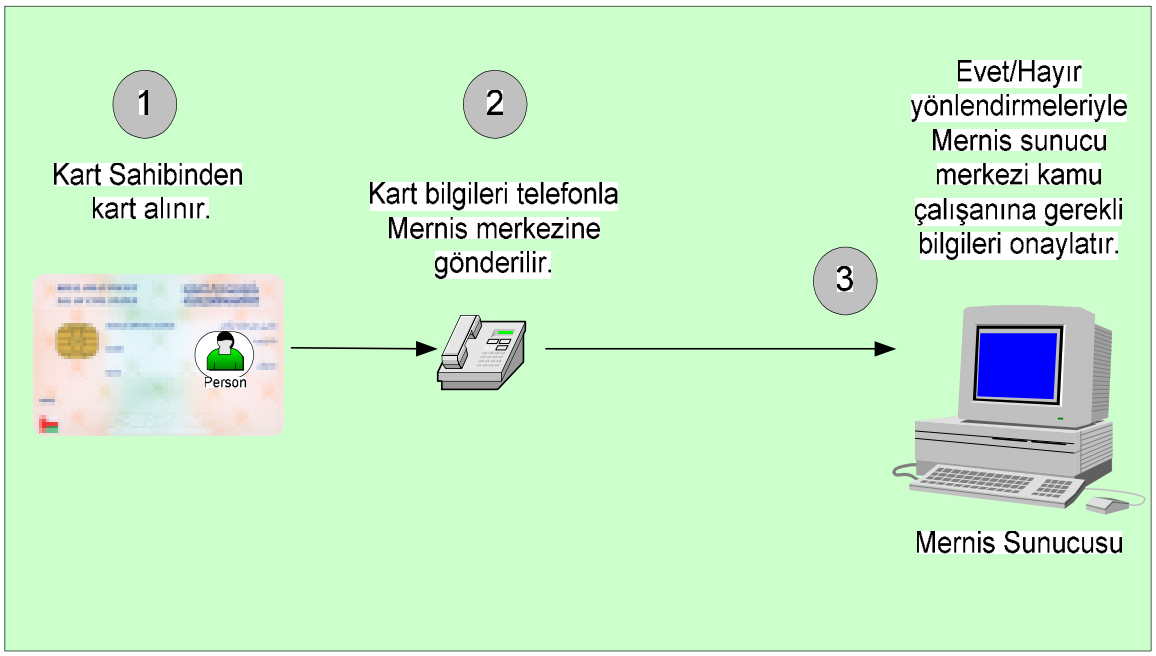
Görsel kimlik doğrulamadan sonra, kart sahibinin kimliği Şekil 6-3 de görüldüğü üzere çevrim-içi olarak doğrulanır. Bu işlemde, kart sahibi kartını kart okuyucuya takar. Kart ile kart okuyucu birbirlerinin sahte olmadıklarından karşılıklı kimlik doğrulama (mutual authentication) yöntemi (bölüm 1.6.1 ve 1.6.2 de kısaca tarif edildiği gibi) ile emin olurlar. Bir sonraki adımda, kart sahibinin parmak izi kart okuyucu tarafından okunur. Kontrol sonucu olumlu ise, kart sahibinin kimlik bilgileri Mernis'teki sunucudan sorgulanır. Sonuç başarılı ise diğer işlemlere devam edilebilir.



Şekil 6-3 Kart Sahibinin Kimliğinin çevrim-içi doğrulanması.

6.5. Kart Sahibinin Kimliğinin Telefon Yardımıyla Kontrol Edilmesi

Kart sahibinin çevrim-kimlik doğrulamasında, gerekli ortam ve donanım her zaman müsait olmayabilir. Buna alternatif olarak, bugün bankalarda sıklıkla kullanılan telefon üzerinden kimlik doğrulama yapılabilir. Fakat bu tür kimlik doğrulama yönteminin seviyesi güçlü kimlik doğrulama sınıfına girmemektedir. Kritik işlemler bu tür kimlik doğrulama sonucunda yapılmamalıdır. Mümkün olduğunca kart sahibinin kimliği çevrim-içi olarak doğrulanmalıdır. Kart sahibini kimliğinin telefonda doğrulanması Şekil 6-4 de gösterilmektedir. Bu yöntemde, yetkili kamu görevlisi tarafından kart sahibinden Ulusal Kimlik Kartı alınarak, Mernis çağrı merkezi (böyle bir merkezin mevcut olduğu varsayılmaktadır) aranır. Telefonda evet / hayır yönlendirmeleri ve telefon tuşları kullanılarak gerekli bilgiler girildikten sonra, işlem sonuçları olumlu ise kart sahibinin kimliği doğrulanmış sayılarak diğer işlemlere geçilir.



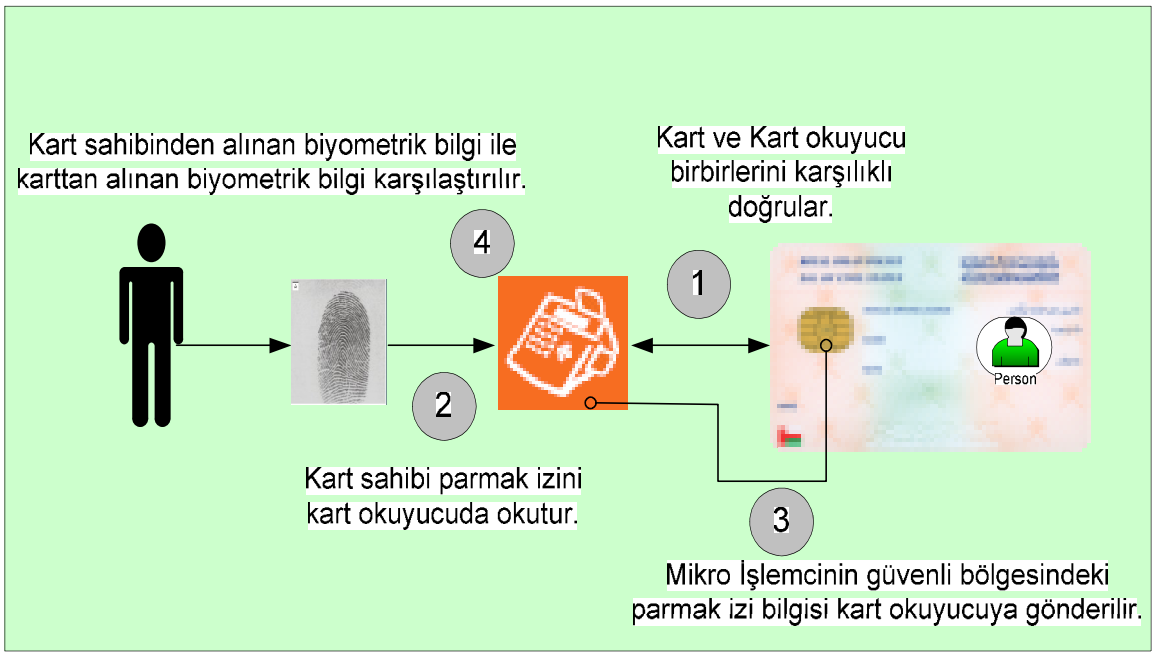
Şekil 6-4 Kart Sahibinin Kimliğinin Telefon Yardımıyla doğrulanması

6.6. Çevrim-dışı Biyometrik Kontrol

Çevrim dışı kimlik doğrulama, merkeze kimlik sorgulaması yapılmasının gerekmediği durumlarda kullanılabilir. İşlem yükü akıllı kart okuyucuda yoğunlaşmaktadır ve Mernis kimlik doğrulama sunucusuna herhangi bir yük getirmemektedir, diğer yandan karttaki kimlik bilgilerinin güncel olup olmadığı ya da sonradan kartın iptalinin istendiği anlaşılamaz. Bu mahzur, karta çevrimiçi kontrol yapılan son yerde tarih bilgisi düşülmesi ile kısmen çözülebilir.

Bu yöntem, Şekil 6-5 de gösterildiği üzere akıllı kart okuyucu ile Ulusal Kimlik Kartının birbirlerinin kimliğini doğrulaması ile başlamaktadır. İki araç arasında kimlik doğrulama başarılı ise, kart sahibinin parmak izi kart okuyucu tarafından okunur. Ulusal Kimlik Kartının güvenlir alanında kapalı olarak duran kart sahibinin biyometrik bilgileri, karttan okunarak kart okuyucuya güvenli bir şekilde gönderilir. Parmak izi okuyucusundan alınan biyometrik veri ile karttan okunan veri karşılaştırılır.

Cihazların birbirlerinin kimlik doğrulamaları için gerekli kriptografik işlemlerden geçildikten sonra, biyometrik veri karşılaştırması başarılı ise kart sahibinin kimliği doğrulanmış olur.

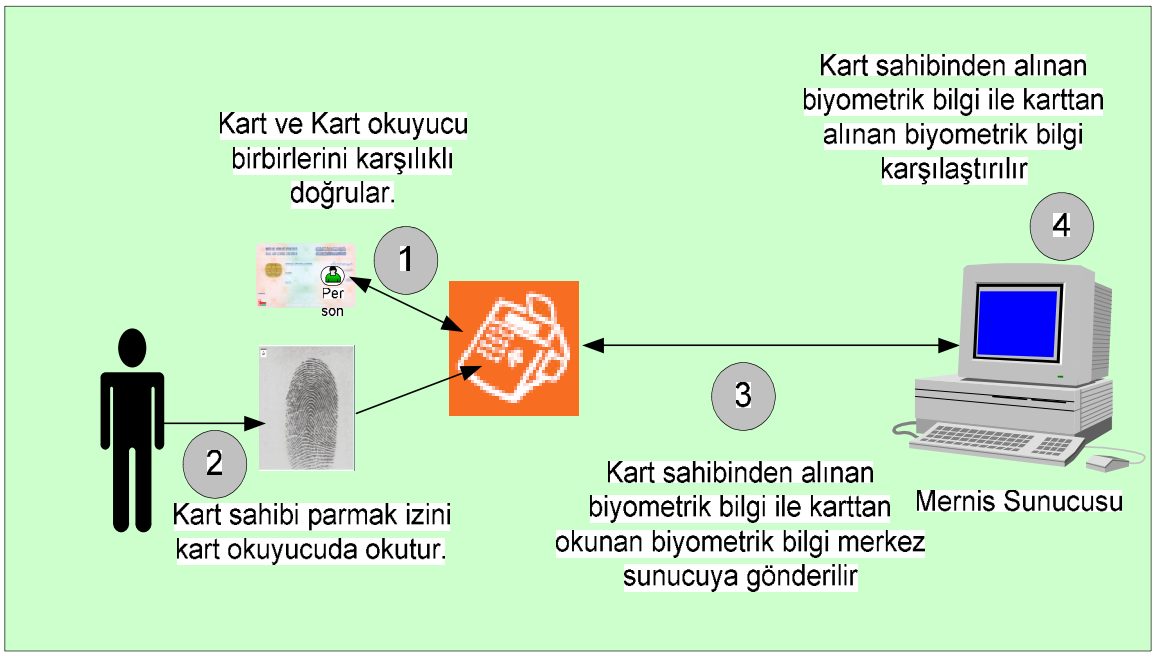


Şekil 6-5 Çevrim-dışı Biyometrik kontrol

6.7. Çevrim-içi Biyometrik Kontrol

Biyometrik tabanlı kimlik doğrulama yöntemlerinden ikincisi çevrim-içi biyometrik kontrol olarak adlandırılmaktadır. Bu yöntem, kart okuyucunun Mernis kimlik doğrulama sunucusu ile güvenli haberleşmesini zorunlu kılmaktadır. Kimlik doğrulama yönteminin işlem yükü, Mernis kimlik doğrulama sunucusu üzerinde yoğunlaşmaktadır. Bu yöntem, Şekil 6-6'da gösterildiği üzere, akıllı kart okuyucu ile Ulusal Kimlik Kartının birbirlerinin kimliğini doğrulaması ile başlamaktadır. İki araç arasında kimlik doğrulama başarılı ise, kart sahibinin parmak izi kart okuyucu tarafından okunur. Ulusal Kimlik Kartının güvenlir alanda kapalı olarak duran ve daha önce alınmış olan kart sahibini biyometrik bilgileri ilgili yerden okunarak kart okuyucuya güvenli bir şekilde gönderilir. Kart okuyucu, her iki bilgiyi güvenli haberleşme ortamında Mernis kimlik doğrulama sunucusuna gönderir.

Araçların birbirlerini doğrulaması için gerekli kriptografik işlemlerden geçirildikten sonra biyometrik veri karşılaştırması başarılı ise, kart sahibinin kimliği doğrulanmış olur.



Şekil 6-6 Çevrim-içi biyometrik kontrol

7. Ulusal Kimlik Kartının İşletilmesi

7.1. Ulusal Kimlik Kartı kimlik bilgileri kayıt İşlemleri

Kayıt kurumlarının maliyetini (kurulum maliyeti, çalışan sayısı, fiziki standartlar, gerekli cihazlar vs.) belirlemek için en azından aşağıdaki hususlar göz önüne alınmalıdır:

- Kimlik kartında kurumları ilgilendiren hangi verilerin konulacağı,
- Bu bilgilerin saklanma koşulları (bu bilgilerin alındığı kurumlarda saklanmaya devam edilecek mi yoksa kayıt merkezi de bu bilgileri saklayacak mı?),
- Verilerin güncellenme ihtiyacı,
- Alınacak biyometrik verilerin mahiyeti,
- Güvenlik için alınacak ek tedbirler (soğuk damga, fotoğraf vs.)
- Kayıt sırasında vatandaşların beyan ettiği kimlik bilgileri ile varolan kayıtlardaki bilgilerin denetlenmesi,
- Kayıt için alınan verilerin onay makamı,
- Yapılacak işlemlerin ne kadarının kayıt merkezinde gerçekleşeceğinin belirlenmesi,
- Kartın kimlik doğrulama sürecinde kullanacağı anahtarların üretim metodu,
- Kartlar adreslere dağıtılmayacaksa dağıtım noktaları,

Ulusal Kimlik Kartının insanın biyolojik özelliklerinin değişmesinden dolayı belirli aralıklarla biyometrik veri kaydının yenilenmesi gerekmektedir. Ayrıca bir çok vatandaşın kartında bulunan verilerin de güncel tutulması (evlilik durumu, askerlik, sabıka kaydı vs.) gerekmektedir. Dolayısıyla, her beş yılda bir vatandaşın kayıt yenilemesi gerekmektedir.

7.2. Ulusal Kimlik Kartı'nın Dağıtılması

SSK uygulamayı planladığı yeni sağlık kartı sisteminde, akıllı kart üzerinde, vatandaşların acil sağlık bilgileri ve kimlik doğrulamada kullanılacak diğer bilgiler bulunacaktır. SKK bu konuda öncü olabilir ve edinilecek tecrübelerle Ulusal Kimlik Kart seçimi ve dağıtım sürecinde daha isabetli tercihler yapılabilir.

Ulusal Kimlik Kartının vatandaşlara nasıl verileceği önemli bir konudur. Yaygınlaştırma evresinde kamu kurumları ile belirli bir işi olan vatandaşlara kart alınması zorunlu

koşulabilir. Örneğin, yeni ehliyet alma, askere gitme, doğum yapma, orta öğretimden mezun olunması ve benzeri durumlarda Ulusal Kimlik Kartının çıkarılması şart koşulabilir. Uzun vadede tüm ülke nüfusuna kartın yaygınlaştırılabilmesi için, ilköğretimden mezun olunurken, diploma almadan önce Ulusal Kimlik Kartının alınması zorunlu olabilir.

Yeni doğanlar için Ulusal Kimlik Kartı çıkartılabilir. Fakat bebeğin biyometrik bilgileri alınmaz. Onun yerine bebeğin kartına velilerinin kartlarına sanal bağlantılar kurulur. Dolayısıyla bebek ve çocuk için yapılacak işlemlerde ilk önce bebek veya çocuğun kartı doğrulanır. Arkasından velinin kartı takılarak, veli kimliği doğrulanır ve işlemler gerçekleştirilir. Bu sayede, vatandaşların erken yaşlardan itibaren kaydı alınmış olur. Diğer yandan, erken kart alımı, gelişim çağında kartın sürekli yenilenmesi ihtiyacı sebebiyle maliyet açısından etkin olmayabilir. İngiltere'de kart alma yaşı olarak vatandaşın 16 yaşına girmiş olması şart koşulmaktadır.

Ulusal Kimlik Kartı yaygınlaştırma çalışması uzun vadeli bir çalışmadır. Bir iki yıl gibi kısa bir sürede, 75 milyon insana kart dağıtımı (daha önce bahsi geçen kart dağıtımında sorun yaşanabilecek bazı durumlar da göz önüne alındığında) normal koşullarda olanaksızdır. İngiltere, 2008 yılında başlayacağı kimlik kartı dağıtımında 2013 yılına kadar nüfusunun %80'nine kart dağıtmış olmayı hedeflemektedir. Aynı durum Türkiye için de geçerlidir.

7.3. Ulusal Kimlik Kartı'nın İptali

Kartın iptal edilmesinin dört temel nedeni olabilir. Bunlar sırasıyla;

- Vatandaşlıktan çıkarılma,
- Kaybolma,
- Çalınma,
- Vefat.

Kart sahibinin vatandaşlıktan çıkarılması durumunda, mahkeme kararı ile kart sahibinin Ulusal Kimlik Kartını kayıt merkezlerine getirmesi gerekir ve bu merkezlerde kart imha edilir. Kart sahibinin herhangi bir kayıt merkezine uğramaması durumunda, nüfus müdürlüğü Mernis sunucusundan kartın geçerliliğini iptal eder.

Kaybolma durumunda, hâlihazırdaki yönetmelikler uygulanarak, kart sahibinin güncel bilgilerini içeren yeni bir kart çıkartılarak, vatandaşa teslim edilir. Mernis sunucusunda gerekli güncellemeler yapılır.

Çalınma durumunda, yine hâlihazırdaki yönetmelikler uygulanarak, kart sahibinin güncel bilgilerini içeren yeni bir kart çıkartılarak, vatandaşa teslim edilir. Mernis sunucusunda gerekli güncellemeler yapılır.

Vefat durumunda ise, müteveffanın yakınları ya da yetkililer tarafından gerekli belgeler temin edildikten sonra, kart iptal edilerek kart kayıt merkezi tarafından alınır. Mernis sunucusunda gerekli güncellemeler yapılır.

7.4. Ulusal Kimlik Kartı Yaşam Döngüsü Yönetim Sistemi

Kart kullanımında sistem güvenliğinin en önemli ayaklarından birisi, kart yönetimini otomatize edecek, kartların kişiselleştirilmesi, gerekli kart ve kullanıcı envanterlerinin tutulması ve kart değiştirilmesi ile ilgili görevleri üstlenecek bir kart yönetim sistemi kurulmasıdır. Kart yönetim sistemi, kart basım sistemi ve kurum veritabanı ile entegre çalışacaktır.

Herhangi bir kartlı sistemde kart edinilmesi, kart ilklendirilmesi, kart kişiselleştirmesi, kart dağıtımı, kart değiştirme, kart kilitleme ve çözme, PIN sıfırlama, sertifika yönetimi, anahtar yönetimi, kimlik veritabanı yönetimi, kart envanteri ve kart sahipleri ile ilgili hizmetlerin bulunması zorunludur. Tüm bu faaliyetleri kapsayan süreçlerin tümüne kart yaşam döngüsü yönetim sistemi adı verilmektedir. Bu süreçler yazılım, donanım, kullanım yönergeleri ve prensipleri unsurlarından oluşmaktadır.

Yazılım unsurları ise kart üzerinde gerçekleştirilen işlemleri, haberleşme ve veritabanı işlemlerini ve yönetim işlemlerini kapsamaktadır. Donanım unsurları kartın işletilmesinde kullanılan kart okuyucuları ve akıllı kartlar gibi donanım unsurlarını kapsamaktadır. Kullanım yönergeleri ve prensipleri unsurları, Ulusal Kimlik Kartı kullanımının kanuni, hukuki ve uygulama kurallarını tarif eden bir dizi yönergedir.

Bir Ulusal Kimlik Kartı uygulaması için tüm bu unsurlar bir proje dahilinde geliştirilmeli ve pilot uygulama yapılarak sistemin nasıl çalıştığı gösterilmelidir.

Kartın Üreticiden Temin Edinilmesi

Ulusal Kimlik Kartı uygulamasında, ekonomik açıdan büyük meblağlar tutacak olan unsurların başında akıllı kartların kendisi gelmektedir. 75 milyon vatandaşa kart dağıtmak oldukça maliyetli bir iştir. Akıllı kartların tanesinin asgari $3'dan temin edileceği düşünülürse, 75 milyon akıllı kart için $225 milyon dolar ödenek ayrılması gerekmektedir.

Ayrıca, kartların işletileceği ortamlarda kullanılacak kart okuyucular, uygulama yazılımları ve kart kayıt merkezlerinde kullanılacak cihazlar da büyük bir uygulama bütçesini gerektirmektedir.

Sonuç olarak kartların üreticilerden temin edilmesi kritik bir süreçtir. Bu konu ile ilgili olarak Türkiye'de neler yapılabileceği araştırılmalıdır. Yoksa her beş yılda bir $225 milyon gibi bir meblağın yurtdışına çıkması gibi bir durum söz konusudur.

Kartın İlklendirilmesi

Kart ilklendirme, kartların mikroçiplerinin yığınlar halinde, uygun veriler ile programlanmasıdır. İlklendirme logo gibi bazı bilgilerin kart üzerine yazılmasını da

içerebilir. Kart ilklendirmesi genelde kart üreticiler tarafından gerçekleştirilir. Fakat bu iş kart kişiselleştirmesi ve dağıtımı esnasında da olabilir. Kart ilklendirme sürecinde aşağıdaki işlemler gerçekleştirilebilir:

- ROM'a işletim sistemi yüklenmesi
- Hafıza alanlarının tahsis edilmesi
- Güvenlik anahtarlarının üretilmesi
- Diğer kart ilklendirme işlemleri.

Kart Kişiselleştirmesi

Kişiselleştirme, kart sahibine ait verilerin kart yüzeyine mikroçip üzerine yüklenmesidir. Gereksinimlere göre kişiselleştirme süreci farklı şekiller alabilmektedir. Bu işin ortak yönü, kart sahibinden onu tek olarak ifade edecek gerekli verilerin toplanması (kimlik bilgileri, biyometri vs.) ve bunların karta ve veritabanına uygun şekillerde yazılmasıdır. Bu işlemler için, otomatik bir arayüz hataları azaltmada önem kazanmaktadır. Uygulamaya has olarak aşağıdakilerden bazıları kişiselleştirme sürecinde yer almaktadır:

- Uygulama yazılımı, kimlik bilgileri ve anahtarların mikroçip üzerine yüklenmesi
- Karta resim ve kimlik bilgilerinin yazılması
- Karta kuruma ait bilgilerin yazılması

Kayıt ve kart kişiselleştirme sürecinin bir parçası olarak, kurum veya atanmış kart verici, belirli kabiliyetlere ve gerçekleme stratejilerine göre, aşağıdaki fonksiyonların birleşimini gerçekleştirecektir:

- Bir dijital fotoğraf sistemi kullanarak, kişilerin dijital fotoğraflarının çekilmesi,
- Bir biyometrik cihaz kullanarak, kişilerin biyometrik verilerinin alınması,
- Kişilerin kişisel bilgilerinin bir veritabanından veya kişiden alınıp, gerekli verilerin mikroçipe yazılması,
- Karta dijital ve biyometrik sertifikaların yazılması.

Ayrıca kart sahibinin verilerinden kamu kurum ve kuruluşlarını ilgilendiren kısımları (Vergi No, Sosyal Güvenlik No vb.) ilgili kurumlarla karşılaştırılıp doğruluğu teyit edildikten sonra kart kişiselleştirilmesinin yapılmasının uygun olacağı düşünülmektedir.

Kart Dağıtımı

Bu süreç kişiselleştirilmiş kartların kart sahiplerine dağıtılmasıdır. Bu süreç, kart kişiselleştirme ile iç içe olabileceği gibi ayrı da olabilir. Gerekli uygulamalara bağlı olarak, kartlar kart kişiselleştirilmesinden hemen sonra dağıtılabileceği gibi, belli onay prosedürlerinin tamamlanması da gerekebilir. Kart dağıtımı ve kişiselleştirmenin beraber olduğu durumda, kart alacak kişiler önce kendilerine ait kurum evrakı ile başvurmalı, başvuru değerlendirilip şahsın kart kişiselleştirme sürecinde anlatılan verileri alınmalı (resim, biyometri) ve kart hazırlanarak şahsa verilmelidir. Diğer durumda, kişiselleştirme sürecinde veriler hazırlanır. Daha sonra, toplu bir kart kişiselleştirmesi süreci sonunda, hazırlanan kartlar kişilere imza karşılığı kurye ile gönderilir veya belirlenen tarihler arasında dağıtım merkezlerine kendilerinin bizzat gelerek almasını içeren posta ile bildirilir.

Kart Değiştirme

Kart değiştirme süreci, kayıp, çalıntı ve arızalı kart bildirilmesi veya veri değişikliği sonucu eski kartın iptal edilip yeni kartın verilmesidir. Bir kart kayıp, çalıntı veya arızalı olarak bildirildiğinde, kart dağıtım merkezi tarafından ilgili sertifikaların iptal edilmesi ve kartın geçersiz kartlar listesine alınması gerekmektedir. Yeni bir kart verildiğinde, yeni kart eski kartın bulundurduğu verilerin hepsini içermeli ve yapabildiklerinin hepsini gerçekleştirebilmelidir. Ayrıca yeni kart, kendisinin değiştirilmiş bir kart olduğunu da belirten bir iz bulundurmalıdır. Kart değiştirme süreci şunları içerir:

- Tekrar kart verme yordamları,
- Geçersiz kartlar listesinin kontrol edilmesi,
- Sertifikaların iptal edilmesi,
- Kartları kilitleme ve çözmeye yetkili personel,
- Kartların geçersiz kart listesinden kaldırılma yordamları,
- Biyometrik verilerin ve güvenlik anahtarlarının oluşturulma yordamları,
- Kartların tekrar verilmesi ve tekrar aktive edilmesi süresi.

Ayrıca kart sahibinin bilgilerinin değişmesi durumunda kartın Kart Dağıtım Merkezi tarafından güncellenmesi ve kart sahibine tekrar ulaştırılması gerekmektedir. Bu süreç içerisinde vatandaş kamu kurum ve özel kuruluşlarla olan ilişkilerinde hak mahrumiyeti yaşayacağından, bu durumda getirilecek çözümlerin de raporda belirtilmesinin uygun olacağı düşünülmektedir.

Kart Kilitleme ve Çözme

Kartların kaybolması veya çalınmasının bildirilmesi durumunda, bu kartların geçersiz kart listesine alınması ve bu listedeki değişikliklerin ilgili kurumlara iletilmesi gerekmektedir. Ayrıca, yanlış PIN girme ile kartın bloke olması gibi durumlarda, kart sahibi tarafından bazı kodlar girilerek kartın çözülmesi ile ilgili yordamlar tanımlanmalıdır.

Anahtar Yönetimi

Anahtar yönetimi, kart yönetim sisteminin önemli bir parçasıdır. Kart sisteminde tanımlı anahtarların yönetiminin gerçekleştirilmesi gerekmektedir. Kriptografik sistemler anahtar yönetimi olmadan yeterli güvenlik sağlayamazlar.

Anahtar yönetimi, kriptografik anahtarların üretimi ve idamesinde kullanılan bir uygulamadır. Kart üretim sistemi ve kart yönetim sisteminin entegre olması (birbirlerine arayüzleri olmalı) gerekmektedir. Anahtar yönetiminde anahtar üretimi, saklanması, dağıtımı, kullanımı ve yok edilmesi yordamları tanımlanmalıdır.

Kart Sahipleri Veritabanı Yönetimi

Kart yönetim sisteminde verilen bütün kartların arşivinin idamesi gerekmektedir. Veritabanı içerisinde, kart seri numarası veya kart sahibine verilen tekil tanımlayıcı ile birlikte kart sahibinin dijital resmi, varsa dijital sertifikası ve diğer gerekli bilgileri saklanmalıdır. Bu veritabanı kart değiştirme ve yenileme durumlarında kullanılacaktır.

Kart Envanteri

Akıllı kart stoku güvenli bir ortamda idame ettirilmelidir. Kartı dağıtan kurum, depoya gelen kartların seri numarasını tutar. Kartlar güvenli bir ortamda saklanmalı ve sadece yetkili personel tarafından erişilebilmelidir.

Kart Sahipleri İle İlgili Servisler

Kart dağıtan kurum, akıllı kart platformu için müşteri destek servisi sağlamalıdır. Tipik olarak kart sahiplerinin sorularına cevap vermek için bir yardım masası kurulur. Ayrıca, kart veren kurum otomatik cevap birimi ve müşteri hizmet temsilcisi sağlamalıdır. Bu hizmetlerin sağlanmasında, bankaların ve KSM'nin kart servislerinin yaşadığı tecrübeler ışık tutacaktır.

Genelde müşteri hizmet temsilcisi ve otomatik cevap birimi ile aşağıdaki hizmetler sağlanır:

- Kayıp, çalıntı, hasar görmüş veya çalışmayan kart raporlama,
- Bozuk kart raporlama,
- Yetkisiz kart kullanımı veya başka bir güvenlik ihlali raporlama,

- Kimlik ve irtibat bilgileri yenileme,
- Kart uygulamaları ve hizmetler ile ilgili bilgi desteği,
- Kart yenileme siparişi.

8. Maliyet

Kart tabanlı uygulamalar maliyet açısından değerlendirildiğinde, her zaman yüksek meblağlar tutan uygulamalardır. Genellikle, kart uygulama süreci uzun zaman almaktadır. Büyük ölçekli bir kart uygulamasının maliyeti dört alt başlıkta toplanabilir. Bunlar aşağıda ele alınmaktadır:

8.1. Kart Tabanlı Sistemin Kurulum Maliyeti

Kart tabanlı uygulamanın kurulumu sırasında üç alanda geliştirme yapılması gerekmektedir. Bunlar sırasıyla;

- Kart kullanımı ile ilgili hukuki, kanuni mevzuatın düzenlenmesi ve uygulama yönergelerinin oluşturulması gerekmektedir. Bu çalışma, bürokratik bir çalışma gerektirdiği için, oldukça uzun soluklu bir çalışmadır ve zaman açısından maliyet yükü getirmektedir. Ayrıca, kurumların aralarında gerçekleştirecekleri işlemlerde ortak servis standardı, veri yapıları ve erişim denetim seviyelerinde karşılıklı anlaşmanın sağlanması gerekmektedir.

- Kart kullanımı ile ilgili donanımların geliştirilmesi gerekmektedir. Bunların başında kart okuyucular gelmektedir. Yüksek seviyeli kimlik doğrulama yapılması gereken durumlarda, kart okuyucular da güvenli olmak zorundadır. Kartlar ile kart okuyucular birbirlerinden emin olmak durumundadır. Bunun için, her oturumda birbirlerinin kimliklerini doğrulamaları gerekmektedir. Ayrıca kart okuyucular kolay taklit edilememelidirler. Kullanımları kolay olmalıdır.

- Kart kullanımı ile ilgili yazılımların geliştirilmesi gerekmektedir. Uygulama yazılımlarının başında kart yaşam döngüsü yönetim yazılımları gelmektedir. Ayrıca, kullanıcıların bilgisayarlarında herhangi bir güvenlik zafiyetine meydan vermemek için, güvenlik servisleri yazılımları çalışmalıdır.

Yukarıda birinci madde kamu kurumlarının kendi aralarında gerçekleştirmesi gereken bir çalışmadır. Çoğunlukla, insan gücüne dayalı bir çaba gerektirmektedir. Kamuda devlet memurları bu görev için atanabileceğinden, devlete mali açıdan ek bir yük getirmeyecektir. Fakat bunun için özel kurum ve kuruluşlardan danışmanlık alınabilir.

8.2. Kart Okuyucular ve Diğer Biyometrik Okuyucuların Maliyetleri

Akıllı kart okuyucular teknik özelliklerine göre çeşitlilik arz etmektedir. Kablolu masa üstü veya kablosuz elde çalışanlar bulunmaktadır. Çift kart okuyuculu tek kart okuyucuları bulunmaktadırlar. Sıkı kimlik doğrulama yapmaya uygun ve biyometrik işlemleri destekleyen kart okuyucuların fiyatı $250-$500 arasında değişmektedir. Kablosuz olanlarının fiyatı $500'a yaklaşmaktadır. Türkiye'de kamu kurumlarında söz konusu cihazlara olan gereksinim 400 bin civarında olabileceği kabul edilirse, $200.000.000'lık bir ekonomik Pazar söz konusudur.

Kart okuyucuların yerli üretimi için bir geliştirme sürecine gereksinim bulunmaktadır. Bu da iki yıl gibi bir zaman ve $2,2 milyon gibi bir AR-GE masrafı demektir.

8.3. Kart Üretim ve Dağıtım Maliyeti

Akıllı kart tabanlı bir Ulusal Kimlik kartının yaklaşık olarak 18K bilgi tutması söz konusudur. Dolayısıyla, 32K'lık akıllı kartların uygulamada kullanımı gerekmektedir. Böyle bir kartın 75 milyon için birim fiyatı 3-4 $ civarında olmaktadır. Tüm nüfusa dağıtımında $250 milyonluk bir kaynak ayrımı gerektirecektir. Ayrıca, insanların biyolojik bilgilerinin değişmesinden dolayı, her beş yılda bir yenilenmesi gerekmektedir ve her yenileme işleminde $250 milyonluk bir kaynak kullanılacaktır. Burada kritik nokta, akıllı kartın yurt içinden temin edilmesinin yollarının araştırılması gerekliliğidir. TÜBİTAK-UEKAE'de yapılan bazı çalışmalar, akıllı kart üretim tesisinin kurulumu ($250 milyon bir kaynak) ile söz konusu meblağların yurt dahilinde kalabileceğini belirtmektedir. Tesisin ülke içerisinde kurulumu, kart üretim ve dağıtım maliyeti açısından değerlendirildiğinde üretim tesisinin sadece işletim masraflarının karşılanmasını gerektirecektir. Diğer kart gereksinimleri için yapılacak üretimler işletmeyi kâr'a geçirecektir.

8.4. Kart İşletim Maliyeti

Kart işletim maliyetleri olarak, bozulan kartların yenilenmesi ve tüm kartların ömürlerinin dolması durumunda periyodik olarak 5 yılda bir yenilenmesi, arızalanan kart okuyucuların tamir edilmesi veya yenileri ile değiştirilmeleri verilebilir. Ayrıca, sistemde kullanılan yazılımların ve uygulamaların lisans maliyetleri kart uygulamasına ek maliyet olarak gelmektedir. Kart işletme maliyetinin diğer kalemlere göre yüksek meblağlar tutması beklenmemektedir.

8.5. Kart Kullanım Yaptırımları

Kimlik kartı uygulaması, ilk etapta gönüllülerin kayıt olmasını öngörmektedir. Fakat belirli bir zaman aşımı süresi sonunda zorunlu olmalıdır. İngiltere'de 2008 yılında kart dağıtımı başlayacaktır. Kimlik kartı dağıtımında 2013 yılında İngiltere nüfusunun %80 kapsanılması hedeflenmektedir.

Kimlik sistemine uymak istemeyen vatandaşlar için kanunlar dahilinde bazı yaptırımlar uygulanması kaçınılmazdır. Bunun için ilgili kanunların idari para cezaları maddeleri uygulamaya sokulmalıdır.

9. Olası Ulusal Kimlik Kart İçeriği

Kart içerisinde aşağıdaki bilgiler tutulabilir. Söz konusu bilgiler kartın güvenli bölgesinde tutularak kontrolsüz erişime karşı korunmuş olacaktır. Kart içerisinde Kamu Sertifika Makamının sertifikası bulunmalıdır. Kart, akıllı kart okuyucudan rasgele bir veri ve kart sahibinin parmak izi alınmadan herhangi bir bilgiyi dışarı çıkarmayacaktır. Kart içerisinde, akıllı kart mikroişlemcisi ve dahili kripto makinesi tarafından üretilecek asimetrik anahtar çifti bulunacaktır ve gerekli yerlerde kullanılacaktır.

Kimlik Bilgileri

Mernis Kimlik Bilgileri,

Birincil Türkiye İkametgâh Bilgileri,

Diğer Türkiye İkametgâh Bilgileri,

Varsa Yurt Dışı İkametgâh Bilgileri.

Tanıma Bilgileri

Renkli Vesikalık Fotoğraf ,

Yaş İmza,

Parmak İzi Bilgileri,

Diğer Biyometrik Bilgiler,

Kişisel Referans Numaraları

T.C. Kimlik No,

Sosyal Güvenlik No,

Vergi No,

Ehliyet No,

Pasaport No.

Vatandaşın Acil Klinik Bilgileri

ISO 21549-3 Health informatics — Patient healthcard data — Part 3: Limited clinical data standardının öngördüğü bilgiler kart içerisinde tutulacaktır.

Kart Güvenlik Bilgileri

Kart PIN Numarası,

Kart Şifresi,

Kart Değiştirme Nedeni ve Tarihi.

10. Referanslar

[1] The Identity Project, Interim Report, The London School of Economics & Political Science , March 2005, London.

[2] SSK TÜBİTAK-UEKAE 1007 Proje Teklif Dokümanı, 2005.