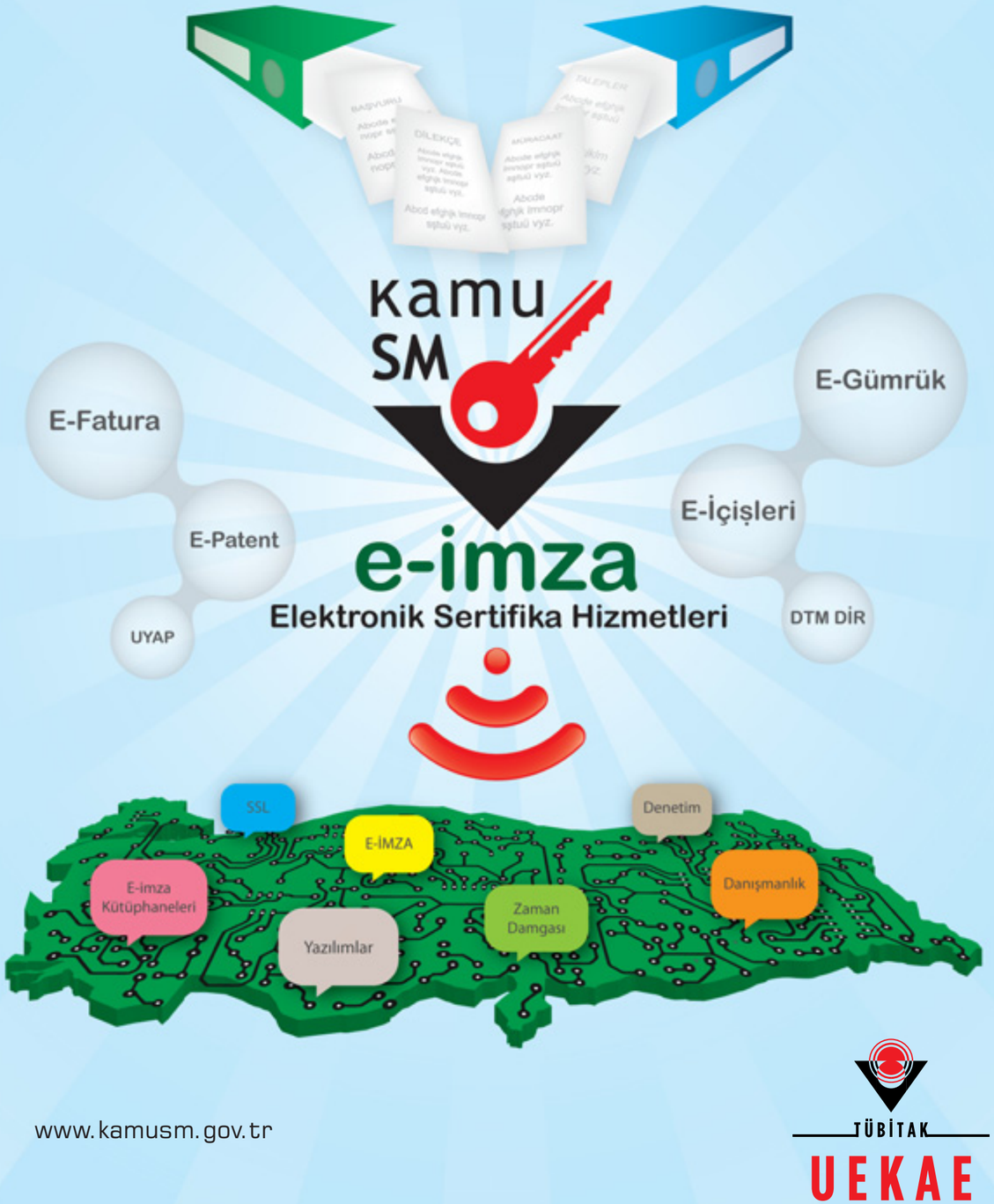
TÜBİTAK
UEKAE
Cilt 2 Sayı 4
Eylül-Aralık 2010

UEKAE dergisi



UEKAE dergisi
Cilt:2 Sayı:4 Eylül-Aralık 2010
ULUSAL ELEKTRONİK ve KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

Özgürlük ve bağımsızlık benim karakterimdir.

Mustafa Kemal Atatürk

Değerli Okurlar,

Yeni ve dolu dolu bir sayıyla karşınıza çıkmanın mutluluğunu yaşıyoruz. Bu sayımızda yazı dizilerine kısa bir ara verdik, sonraki sayılarımızda kaldığımız yerden devam edeceğiz. Kapak konusu olarak, devlet-vatandaş ilişkisini sanal ortama taşıyan ve bir hayli yeniliği beraberinde getiren "e-Kimlik Projesi"ni mercek altına aldık. Aynı çatı altında birçok kurumun altyapısını birleştiren bu proje, vatandaşlık işlemlerimizi güvenli, hızlı ve düşük maliyetli olarak yapabilmemizi sağlayacak. UEKAE tarafından başlatılan e-Kimlik Projesi'nde tamamlanma aşamasına gelindi. Çok yakın bir gelecekte kullanmaya başlayacağımız kimlik kartları sayesinde e-Devlet erişiminin yanısıra sağlık hizmetlerinden daha verimli bir biçimde faydalanabileceğiz. Aynı zamanda kimlik kartlarının ehliyet ve pasaport olarak kullanılması da gündemde. Bir sonraki genel seçimlerde oylarımızı tatil yaptığımız yerden veya internet üzerinden elektronik kimlik kartlarıyla kullanmamız hayal değil! Bu saydığımız yeniliklerin hepsinin önü e-Kimlik Projesi ile açılıyor.

Enstitü müdürümüz Sayın Önder Yetiş'in bu sayıda kaleme aldığı yazısı "Zamanı Yönetmek". Başarı öyküsü köşemizde İTÜ'de, TÜBİTAK'ta ve Türkiye'deki elektronik sanayiinde önemli katkıları olan Prof. Dr. Sayın Duran Leblebici'yi konuk ettik. Serbest kürsü bölümünde ise "Bilimsel Düşünceyi Hayata Geçirmek" başlıklı yazıyla devam ettik.

Derginin sonunda göreceğiniz "Şifresayar" yeni eklediğimiz bir bölüm. İlginizi çekeceğini umduğumuz bu bölümde ödüllü sorulara yer verdik. Cevaplarını sonraki sayıda sizlerle paylaşacağız.

Gelecek sayıda görüşmek üzere, şimdilik hoşçakalın.

Dergi Yayın Kurulu

İletişim Adresi
UEKAE Dergisi
P.K. 74, 41470 Gebze KOCAELİ

Telefon
(262) 648 1000

Faks
(262) 648 1100

Internet
www.uekae.tubitak.gov.tr/dergi

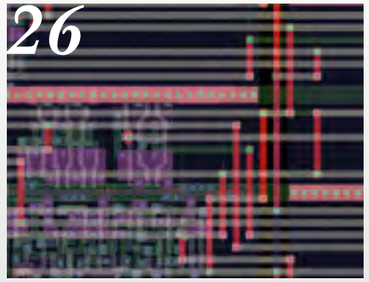
E-posta
dergi@uekae.tubitak.gov.tr

Baskı
Şan Ofset
Cendere Yolu 23 Ayazağa İSTANBUL
(212) 289 2424

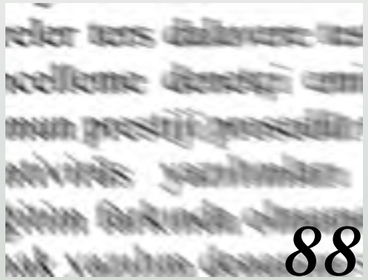
Baskı Tarihi
Eylül 2010

ISSN 1309-3444

içindekiler



içindekiler



Zamanı Yönetmek

"Çevremizdeki dostlarımızdan; 'Okumaya, yazmaya zamanım yok', 'Gelmeye zaman bulamadım', 'Çalışmayı bitirecektim ancak zamanım yetmedi' gibi bahaneleri sıkça duyarız. Her gün bize 24 saat sunar ve zaman kimseye farklı davranmaz. Zamanı olan insanların, zamanlarını etkin ve verimli kullandıkları için zamanları vardır. Zamanı olmayanlar genellikle boş insanlardır ve zamanları olmadığından şikayet ederler."

Zaman yönetimi; geri döndürülemeyen kaynak olan zamanı etkin şekilde kullanmamızı sağlayan planlama ve kendimizi zamana uydurma becerisidir. Diğer bir deyişle, günümüzü nasıl geçireceğimizin bizim tarafımızdan belirlenmesidir.

Zamanı yönetmek, çok iş yapmak demek değil; iş planlarını yapıp en etkin şekilde uygulamak demektir. İşlerimizi sıraya sokmak, hedefler oluşturmak ve hedeflerimiz doğrultusunda kendimizi zamana uydurmaktır.

Etkin bir zaman yönetimi planlamasına sahipseniz daha çok iş ve ürün çıkarmak şansına sahip olur, özel hayatınıza daha çok zaman ayırabilir, hayatınıza renk katan, yapmaktan keyif aldığınız bazı şeyleri de programınıza katabilirsiniz.

Zaman herkes için günde 24 saattir. Bireysel yeteneklerden kaynaklanan farklılıkları bir yana koyarsak, çalışanların performansları neden farklıdır? Bu fark zamanın nasıl kullanıldığı ile ilgili midir? Zamanımızı daha iyi yöneterek daha verimli sonuçlar elde etmek mümkün müdür? Zamanınızı kötü kullandığımız için ne gibi fırsatlar kaçırırız?

Fark yaratan etkenlerden en önemlisi zamanın nasıl kullanıldığıdır. Zaman yönetimi, zamanı akılcı kullanarak daha verimli sonuçlar elde edilmesini sağlar. Yaşamımızın gereklerini yerine getirmek günümüzde zamana karşı gerçekleştirilen bir uğraş halini almıştır. Faaliyetlerimizin önem derecesini, amaçlarımız açısından değerlendirip, yapılmaması ve yapılması gereken işleri bulmak, hangilerine ayrılan zamanın azaltılabileceğine ve hangilerinin arttırılabileceğine karar vermek, faaliyetlerimiz ile amaçlarımızın tutarlılık içinde olması gereği ortaya çıkmıştır. Kendimize her zaman, 'Daha önemli olan nedir?' sorusunu sormalıyız. Unutmamalıyız ki önem daima erişmek istediğimiz amaçlara göre oluşur.

İşlerimizin bütününü görmeye çalışmalı, ne yapmak istediğimizi ve amaçlarımızı düşünmeliyiz. Her bir faaliyetimizin önemini ve önceliklerini tespit etmeliyiz. Amaçlarımızın gerçekleştirilmesi açısından bazı şeylerin diğerlerinden çok daha değerli olduğunu kabul etmeliyiz. Önce, ne yapmamız gerektiğini daha sonra o şeyi en verimli nasıl yapacağımızı düşünmeliyiz. Zaman kullanım planımızı, yüksek öncelikli işlere daha çok zaman ayırabilecek şekilde yaptığımızdan ve gerçekten önemli işler için yeterli zamanı ayırdığımızdan emin olmalıyız. Başkalarının yapabileceği faaliyetleri onları yapabileceklere ve yardımcılarımıza bırakmalıyız.

Başarılarımızın çalışanlarımızın performansı ile sıkı sıkı ilintili olduğunu, başarının sadece kendimizden değil çalışanlarımızla gerçekleştirebildiğimiz takım çalışmasının sonucu olabileceğini bilmeliyiz. Eğer çalışanlarımızı yetiştiremezsek veya daha az önemli şeylere gereğinden fazla zaman ayırmaya başlarsak, sadece kendimizin yapmamız gerekli işler için yeterli zaman bulamayacak ve gelecekte zamanımız daha da sınırlı hale gelecektir.

Çalışanlarımıza güvenmeliyiz. Kendimizin yapması gerekli faaliyetleri belirlemeli ve diğerlerini yardımcılarımıza bırakmalıyız. Çalışanlarımızın gelişmesinden hem kendimiz hem de çalışanlarımız fayda görecektir. Çalışanlarımızı yetkilendirdiğimizde en iyi zaman yatırımını yapmış oluruz.

Çalışanlarınıza güvenmeli, az önemli olan kararlardan başlayarak zaman içinde daha önemli olan kararları yardımcılarımıza bırakarak çok sayıda karar vermekten kurtulabiliriz. Karar verme süresini en uygun düzeyde tutmalıyız. Acele karar vermemek, kararlarımızı sürüncemede bırakmamak kadar önemlidir.

Günün en uygun zamanında kendimize yaptığımız ve yapamadığımız hakkında düşünmek için zaman ayırmalıyız. Ne yaptığımızı ve yapmayı düşündüklerimizi, sık sık çalışanlarımızla tartışmalıyız. Faaliyete geçmeden önce düşünmek genellikle daha iyi sonuçlara götürür.

Zamanı nasıl tasarruf edebileceğimizi değil, zamanı nasıl harcamamız gerektiğini düşünmeliyiz. Zaman hiçbir şekilde yönetilemez ancak zaman içinde tutum ve davranışlarımızı yönetebiliriz. Zamanımız hayatımızdır. Onu iyi planlamalıyız. Eğer iyi planlayamazsak onu, yani hayatımızı israf ederiz.

Bu sayıdaki yazımı sonlandırırken tüm mesai arkadaşlarım adına siz değerli okurlarımıza saygılar sunar, keyifli okumalar dilerim.

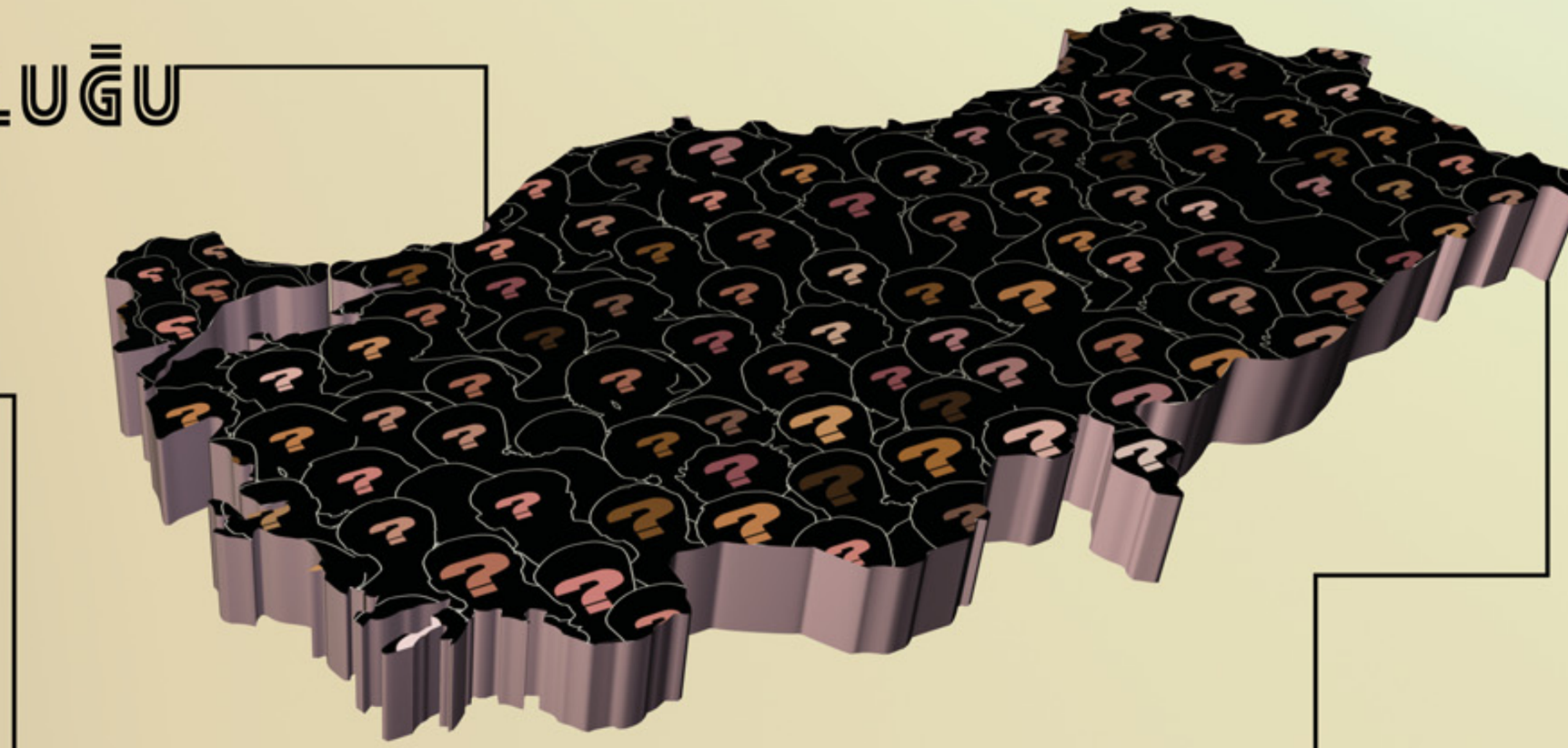
Mehmet Önder YETİŞ
Enstitü Müdürü

TÜRKİYE'NİN E-KİMLİK YOLCULUĞU

M. Aydın KUBİLAY
Oktay ADALIER
Apti KARADEMİR

Bu yazıda Türkiyenin e-Kimlik çalışmaları anlatılacak, geliştirme aşamalarına, çözümlere ve Bolu'daki ilk denemeye muhatap olan vatandaşların eğilimlerine değinilecektir. Bu arada proje kapsamında tasarlanan kimlik kartları, güvenli erişim modülleri, sunucu sistemleri ve açık anahtar altyapısı hakkında bilgi verilecektir.

Detaylı incelememize başlamadan önce bazı önemli noktaların altını çizmekte yarar vardır. TUBİTAK-UEKAE'nin gerçekleştirdiği bu proje birçok ilki başarmaktadır. Yongasından elektronik kimlik kartı yönetim sistemine, çeşitli senaryolar için gerekenlerin temininden saha uygulamalarına kadar Türk mühendis ve teknisyenlerinin emeğiyle oraya çıkarılmıştır. Avrupa birliğinde pek çok ülke de kimlik kartı projelerinde kendi özgün çözümlerini kullanmaktadır. TUBİTAK-UEAKE, Türkiyede yaşayan tüm insanları doğrudan ilgilendiren böyle bir projede ülkemizin özgün tasarımını ortaya koyduğu için gururludur. Bu çalışmalarda paydaş olarak daima yanımızda olan kullanıcı kamu kuruluşlarına da teşekkürü borç biliriz. Gerekli yerlerde yapıcı katkılarıyla projenin başarılı olmasına destek çıkmışlardır.



1. Giriş

Günümüzde bilişim teknolojilerindeki gelişmeler, birçok alanda olduğu gibi kamu uygulamalarında da yeni bir anlayışı ortaya çıkarmıştır. Elektronik devlet (e-devlet) diye adlandırılan bu oluşum kapsamında, kamunun elindeki bilgiler elektronik ortamda, çevrimiçi olarak vatandaş ve kurumlarla paylaşılmaktadır. Bu yaklaşım, bir taraftan kurumların hizmet sunumunda ihtiyaç duyduğu bilgileri diğer kurumlardan anında alabilmesini, diğer yandan da vatandaşın kamu kurumlarındaki işlerini elektronik ortamda yapabilmesini sağlamaktadır. Ayrıca vatandaşı hizmetin odağına koyarak, vatandaş ağırlıklı bir sistemin giriş kapısı olmaktadır.

28 Temmuz 2006 tarih ve 26242 sayılı Resmi Gazete'de yayımlanan Yüksek Planlama Kurulu'nun 11.07.2006 tarih ve 2006/38 karar nolu kararı ile Bilgi Toplumu Stratejisi Eylem Planı kabul edilmiştir.

Planın 46 nolu eyleminde "Vatandaşlık Kartı; Pilot Uygulaması ve Yaygınlaştırılması ile biyometrik unsurlar da içeren elektronik vatandaşlık kartının kimlik doğrulama için kullanımının sağlanması ve tüm kimlik doğrulama fonksiyonlarının tek bir elektronik kartta toplanması" öngörülmüştür.

TÜM KURUMLAR KENDİ UYGULAMALARI İÇİN GEREKEN KİMLİK DOĞRULAMA İŞLEMLERİNDE BU SİSTEMİ KULLANABİLECEKTİR.

Vatandaşlık Kartı projesinin pilot uygulamasının yürütüldüğü, TÜBİTAK destekli "Akıllı Kart Tabanlı Güvenli Sosyal Güvenlik Sistemi Geliştirimi" adlı projeye Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (NVİ), Sağlık Bakanlığı (SB) ve Sosyal Güvenlik Kurumu'nun (SGK) taraf olarak katılımı sağlanmıştır. Böylece kartın dağıtımı, sosyal güvenlik ve sağlık hizmetlerinde kullanımına yönelik süreçlerin de test edilmesi sağlanmıştır.

Vatandaşlık kartlarına e-imza sertifikalarının da eklenmesi söz konusudur. Böylece kamu hizmetlerinin hızlanması sağlanacaktır.

Pilot proje Bolu'da 250.000 kişiye kart dağıtılarak başarıyla sürdürülmektedir. Maliyet ve sürdürülebilirlik yönünden herhangi bir probleme rastlanmamıştır. Bundan sonraki aşama yaygınlaştırmadır. TÜBİTAK UEKAE'den sağlanacak teknoloji transferi ve destekle bu kartın tüm vatandaşlar için üretilmesi ve dağıtılması sağlanacaktır. Bu durumda vatandaşlık kartı, eyleminin hayata geçirilmesindeki diğer süreçler TÜBİTAK UEKAE'den tam destek almaktadır. Yonga tasarımı başarılmış, kart basımı tanımlanmış ve kullanıma hazır hale getirilmiştir. Bu çalışmalardan sonra kurumlar kendi uygulamalarının, vatandaşlık kartına entegrasyonu için TÜBİTAK UEKAE ile birlikte projeler üretebilecektir.

Yeni kimlik kartının, pilot uygulama için, şeklini ve kapsamını belirlemek amacıyla İçişleri Bakanlığı, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, TÜBİTAK UEKAE ve Plaskart ile birlikte çalışmalar yapılmış, son hali Bolu uygulamasında kullanılmıştır. Bu çerçevede AB ve üye ülkeler başta olmak üzere, diğer ülkelerin kimlik kartlarına ilişkin çalışma ve uygulamalar da (İtalya, Belçika, İsveç, Estonya, Finlandiya, Avusturya, İspanya, Portekiz, Birleşik Krallık, Almanya, Fransa, Hollanda, Danimarka, İrlanda, ABD, Japonya, Avustralya, Kanada ve Pakistan) incelenerek onlardan yararlanılmıştır. Yapılan araştırmada, Avrupa Birliği (AB) düzeyinde ortak karara varılmış kimlik kartı standartları (ISO 7816, 14443) kullanılacaktır.

Çağdaş kimlik kartı, MERNİS[1] Projesini tamamlayan bir uygulama olacaktır. Vergi toplanmasından sahteciliğin önlenmesine, kimlik taşıma kolaylığından, devlete başvuruların hızlanmasına kadar birçok amaca hizmet edecek olan bu projenin, hedeflendiği gibi 2011-2014 yılları arasında yaygınlaştırılması halinde e-devlet sürecini kolaylaşacaktır.

Kimlik kartının kişiselleştirmesi ve dağıtımı ile ilgili mevcut süreçlerinin iyileştirilmesi ve çağa uyum sağlayacak şekilde düzenlenmesi de önem arz etmektedir.

2. Kimliğin Türkiye'deki Tarihçesi

Nüfus devletin bir bakıma sosyo-ekonomik potansiyelinin ve yapısının temelini teşkil etmektedir. Nüfus araştırmalarında ayrıntılara girilerek yapılan sağlam tasnifler ve tahliller, devletin gelecek hakkında planlar yapmasına de önemli katkılar sağlamaktadır. Bu açıdan nüfus dağılımının bilinmesi çok önemlidir. Nüfusun demografik yapısıyla ilgili elde edilen bilgiler ışığında toplumsal hayatı tanımlama çalışmaları 15. yüzyıla kadar dayanmaktadır. Bunlar 15. ve 16. yüzyıllar arasında periyodik olarak sürdürülen ancak 16. yüzyılın sonlarından itibaren içeriği değişen ve "arazi ve nüfus tahrirleri" olarak adlandırılan sayımlardır. Bunların yer aldığı defterlerin başında Tapu tahrirleri vardır. Fakat 16. yüzyıldan itibaren tımar sisteminin çözülmeye başlaması ile beraber önemini yitirmiştir.

19. yüzyılın sonlarına kadar gerçek anlamda, erkek ve kadınların bir arada sayıldığı nüfus sayımı yapılmamıştır. Dünyada özellikle 18. yüzyılda başlayan modern nüfus sayımları Osmanlı İmparatorluğunu da etkilemiştir. Böylece insan kaynakları ve meslek erbabının sayısının ortaya çıkarılmasına yönelik "esnaf tezkire defterleri" ve "nüfus tahrir defterleri" gibi çeşitli defterler tutulmaya başlanmıştır.

[1] MERNİS (Merkezi Nüfus İradesi Sistemi): Mernis Projesi tüm Ahvali Şahsiye bilgilerini elektronik ortama aktaran ve Ahval-i Şahsiye bilgilerinde meydana gelen her tür değişikliğin ülkenin her tarafına dağılmış 957 merkezden anlık güncellenmesini ve bir ağ üzerinden güvenle paylaşımını sağlayan bir projedir.

Nüfus hizmetlerini yürütmek üzere Ekim 1884 yılında "Nüfusu Umumiye Müdüriyeti" kurulmuştur. Genel Müdürlüğe 1889 yılında "Sicilli Nüfus Ahali İdare-i Umumiyesi" adı verilmiş ve asıl hizmetin yanında Pasaport Kalemi, Murur Kalemi, Vilayet Kalemi, Dersaadet Kalemi gibi alt kademelere ayrılarak yapılanmıştır. Bu yapı gereğince Osmanlı halkının ilk nüfus tezkeresi dağıtılmaya başlanmıştır.

Şekil 1. *İlk nüfus kağıdı örneklerinden.*

Ancak bu nüfus teskerelerinin herhangi bir nüfus kaydına dayanmaması ve tezkereyi taşıyan kişinin nüfus kütüğüne kayıtlı olmaması nedeniyle özel ve resmi işlemlerde pek yararlı olamamıştır.

Zamanla nüfus tezkireleri yerini defterlere bırakmıştır. Defterler Cumhuriyet döneminde de kullanılmıştır ve kayıtlar harf inkılâbına kadar Osmanlıca tutulmuştur. 1928'den itibaren, dönemin imkânları ölçüsünde, cüzdanlarda yer yer fotoğraf da konulmuştur.

Şekil 2. *Eski Türkçe nüfus defteri.*

01 Kasım 1928 tarihinde harf inkılabı ile kayıtlar Türkçe tutulmaya başlanmıştır. Cumhuriyet dönemi defterlerin ön kapağında "Türkiye Cumhuriyeti" alt kısımda "Hüviyet Cüzdanı" ibaresi yer almıştır.

Şekil 3. *Yeni Türkçe nüfus defteri.*

Farklı tip uygulamalar ve sistemler denenerek süreç günümüz kimlik cüzdanları uygulamasına kadar gelmiştir. Kapsamlı yapılan nüfus sayımından sonra tezkirelerin yerine nüfus kütükleri oluşturulmuştur. Nüfus cüzdanları kütüklerde yer alan bilgilere göre düzenlenmiş ve 1963 yılında değerli kağıt niteliğine kavuşturulmuştur. böylece nüfus cüzdanı bireyin Türkiye Cumhuriyeti vatandaşı olduğunu ve bu nedenle Türk nüfus kütüklerine kayıtlı olduğunu kanıtlayan resmi bir belge olma özelliğini kazanmıştır. Bu işlevi nedeniyle kimlik kartı "devletle fert arasındaki vatandaşlık bağını somut hale getiren ilk ve temel belge" olarak kabul edilmektedir.

1972 yılında çıkartılan 1587 sayılı Nüfus Kanunu ile nüfus hizmetlerinin merkezi bir yapı içerisinde yürütülmesine ilişkin MERNİS projesinin temelleri atılmıştır.

01.06.1976 tarihinden itibaren çok yapraklı cüzdanlar kalkmış ve kart şeklindeki haliyle kullanılmaya başlamıştır [1].

Şekil 4. *Cinsiyete dayalı düzenlenen kimlik kartları (son hal).*

Bu yeni kartlarla beraber bir Türk vatandaşı için nüfus kağıdının önemini bir kere daha vurgulamakta yarar vardır.

• Bireyin Türk vatandaşı olduğunu ve bu nedenle Türk nüfus kütüklerine kayıtlı olduğunu kanıtlayan resmi bir belgedir. Önemi ise günlük hayattaki yoğun kullanımıyla ilgilidir.

• Şekil ve içeriği İçişleri Bakanlığı'nca tespit edilir ve Maliye Bakanlığı, Darphane ve Damga Matbaası'nda bastırılır. Burada depolanan nüfus cüzdanları ihtiyaç miktarları göz önünde tutularak il defterdarlıklarına, buradan da mal saymanlıklarına gönderilir.

• Nüfus aile kütüğüne kayıt edilen her Türk vatandaşına bir nüfus cüzdanı verilir. Nüfus cüzdanı; doğum, kayıp, yeniden kayıt, yenileme veya değiştirme nedeniyle düzenlenir. Düzenlenen nüfus cüzdanının veriliş nedeni alanına verilme nedeni yazılır.

• Nüfus cüzdanınında aşağıdaki bilgileri kapsar:

a) Devletimizin adını, Belgenin adını, Bayrağımızın renklerini ve ay-yıldızını, Belgenin seri ve numarasını,

b) Özlük bilgileri: Türkiye Cumhuriyeti kimlik numarasını, Soyadını, Adını, Baba adını, Ana adını, Doğum yerini, Doğum tarihini, Medeni halini, Dinini, Kan grubunu, Bekarlık / Önceki soyadını, Özür durumu (talep edilmesi halinde)

c) Kişinin kaydına ulaşmayı sağlayan bilgileri; Kayıtlı olduğu: İli, İlçeyi, Mahalle/Köyü, Cilt numarasını, Aile sıra numarasını, Sıra numarasını,

d) İşlemle ilgili bilgileri; Verildiği yeri, Veriliş nedenini, Kayıt numarasını, Veriliş tarihini,

• 15 yaşını doldurmuş olanların nüfus cüzdanlarına fotoğraf yapıştırılması zorunludur.

Yurdumuzda 2002-2006 yılları arasında 50.309.160 adet nüfus cüzdanı verilmiş, 5 yılda ortalama olarak;

Yılda	10.061.832 adet
Ayda	838.486 adet
Günde	38.113 adet (22 iş günü)

nüfus cüzdanı düzenlenmiştir.

2003 yılında MERNİS uygulamaya geçirilerek nüfus müdürlüklerinin çevrim içi çalışması başlatılmıştır [2]. Böylece uç noktalardan merkezdeki bilgi bankasına ulaşım sağlanmıştır. Nüfus kağıdında bulunması gereken bilgiler MERNİS veri tabanından çevirim içi otomatik olarak aktarılmakta ve çıktısı alınmaktadır. Bu kapsamda, nüfus cüzdanı 4-5 dakikalık bir süre içerisinde düzenlenerek ilgilisine imza karşılığı teslim edilmektedir.

Ayrıca MERNİS, Türkiye'de yer alan kamu kurumlarının vatandaşı tanımlamakta ve kimliğini teyit etmekte yaşadığı sıkıntıyı "***T.C. Kimlik Numarası***"nın üretilmesi ile büyük ölçüde çözmüştür. Her vatandaşa tekil T.C. Kimlik Numarası verilmiştir. [3] Bu uygulama, kamu/özel kurumlarda yapılan işlemlerde kolaylığın yanında bir takım güvenlik zaafiyetlerini de beraberinde getirmektedir. Örneğin birinin T.C. Kimlik Numarası'na ulaşan biri, onun birçok mahrem bilgisine hakkı olamadığı halde erişebilmektedir.

Hızla gelişen teknoloji günümüzde kimlik kartının nüfus cüzdanından farklı, diğer bir deyişle "akıllı" olmasını zorunlu hale getirmiştir. Kimlik için akıllı kart kullanımıyla devlet tarafından verilen hizmetlerin alımı ve sunumu kolaylaşacaktır. Bu yönüyle kimlik kartı bir hizmet kartı olarak elektronik devlet (e-devlet) yapısının vazgeçilmez bir bileşenidir.

Şekil 5. *Bolu pilot uygulaması için geliştirilen tek düzen kimlik kartı.*

Bu çerçevede, TÜBİTAK UEKAE tarafından başlatılan T.C. Kimlik Kartı projesi, 2010 yılı içinde tamamlanacak ve yaygınlaştırma evresine geçilecektir.

3. Dünyada e-Kimlik

Akıllı kartların kimlik kartı olarak kullanıldığı ilk ülke Malezya'dır (2001). Aynı şekilde İsveç, Almanya, Portekiz, İspanya ve Estonya akıllı kart özelliklerine sahip kimlik kartı uygulamasına geçen Avrupa ülkeleridir. Bunları sırasıyla inceleyelim:

Estonya

Kimlik kartı dağıtımına 28.01.2002 tarihinde başlanmıştır. 15 yaş üzerindeki tüm vatandaşların ve sürekli oturma izni alanların kimlik kart almasını zorunlu hale getirmiştir. 1.4 milyon nüfusu sahip Estonya'da yaklaşık olarak 1.000.000 kişiye kart dağıtılmıştır.

Kimlik kartları kamu kuruluşlarında ve bankalarda kullanıldığı gibi, çevrimiçi işlemlerde de kimlik doğrulama amaçlı olarak kullanılmaktadır. e-Kimlik'e herhangi bir sınır getirilmemiş tüm uygulamarda kullanılması hedeflenmiştir. Nitelikli imza kartı yerine de geçecektir. 10 yıllık geçerliliği olan kimlik kartının vatandaşa maliyeti 10 avrodur.

Portekiz

Kimlik kartları 2007 yılından itibaren yaygınlaştırılmaya başlanmıştır. 5 yıllık süre içerisinde yaklaşık 10 milyon kart dağıtımını hedefleyen Portekiz'de 2007 yılından bu yana 200.000 kişiye kart dağıtılmıştır.

Portekiz kimlik kartlarının elektronik ortamda kimlik doğrulama, tanıma ve imza atma fonksiyonlarına sahip olması hedeflenmiştir.

Belçika

2002 ile 2003 yılları arasında 11 ayrı ilde pilot çalışmaları başarı ile gerçekleştirilmiş ve yaygınlaştırma başlatılmıştır. 2009 yılına kadar 12 yaş üzeri tüm vatandaşlara dağıtımının sağlanacağı ve 5 yıl kullanım ömrünün olduğu bilinmektedir.

Birçok banka ve kamu uygulamalarında kullanılmaktadır. Ayrıca kart Avrupa Birliği ülkelerinde seyahat belgesi niteliği de taşımaktadır. Vatandaşa maliyeti 10 avrodur.

İsveç

İlk akıllı kart tabanlı kimlik kartı çalışmaları 1998 yılında SIS (*Swedish Standarts Institude*) ve SEIS (*Secured Electronic Information in Society*) tarafından oluşturulmuştur. Kartlar, İsveç bankaları ve ulusal sertifika otoritesi olarak rol alan posta kurumları tarafından dağıtılmıştır.

Kart özel ve kamu kurumlarının verdikleri hizmetlere erişimde kullanılmıştır. 5 yıllık geçerliliği olan kimlik kartının vatandaşa kart maliyeti 40 avrodur.

Almanya

Almanya'da parmak biyometrisini destekleyen kimlik kartı çalışmaları proje aşamasındadır. 2010 yılında kimlik kartı dağıtımına başlanması öngörülmüş olmasına rağmen henüz başlatılmamıştır. Projede 16 yaşından büyük vatandaşlar için 6 yıl geçerli, 24 yaşından büyük vatandaşlar için ise 10 yıl geçerli temassız yongalı kimlik kartı verilmesi öngörülmüştür. Kimlik kartının vatandaşa kart maliyeti 28 avrodur.

Gönüllülük esasına göre vatandaşın biyometrik verisinin alınmasına karar verilmiştir. Yeni kimlik kartının üç temel fonksiyona sahip olması hedeflenmiştir:

• Elektronik ortamda kimlik doğrulama,

• Elektronik imza atma,

• Seyahatlerde kimlik doğrulama amaçlı seyahat dokümanı olarak kullanımı.

İspanya

Kimlik kart projesi 2002 yılında başlamış olup ilk kart dağıtımı 2006 Nisan ayında başlamıştır. 2008 yılının Haziran ayına kadar 6 Milyon kart dağıtılmıştır. Policarbon (PC) materyale sahip kimlik kartı çeşitli güvenlik öğelerini içermektedir. Vatandaşa kart maliyeti 13 avrodur.

4. Elektronik Kimlik Doğrulama Sistemi (EKDS) Projesi Amaç ve Hedefleri

EKDS, TÜBİTAK UEKAE'nin geliştiricisi olduğu e-kimlik süreçleri ve buna uygun bileşenlerin tasarlandığı bir projedir. Bolu ilinde, kimlik, sağlık ve sosyal güvenlik uygulamalarının yapılacağı bir pilot çalışmayı da kapsamaktadır.

4.1. EKDS Projesinin Amaçları

Bu proje aşağıda belirtilen amaçlar doğrultusunda gerçekleştirilecektir.

Vatandaş Yönünden

- Nüfus işlemlerini hızlandırmak,
- Kamu hizmetlerinin tek bir noktadan ve güvenli alınabilmesini sağlamak (e-Devlet dönüşümüyle kamu kurum ve kuruluşlarının T.C. kimlik kartı vasıtasıyla tam entegrasyonu sonucu vatandaşın, askerlik, pasaport ve iş başvurusu işlemleri, noterlik işlemleri gibi birçok hizmeti alırken kamu kurumlarını dolaşmak zorunda kalmaması),
- Hizmet alımı giderlerini azaltmak.

Devlet Yönünden

- Vergi tahsilatı ve denetimini kolaylaştırmak,
- Kayıt dışı ekonomiyi kontrol altına alabilmek.

Güvenlik Yönünden

- Suçlu takibi ve yakalanmasında kolaylık,
- Hızlı kimlik tespit imkanı sağlamak ve sahteciliği engellemek.

Askerlik Yönünden

- Askere alma işlemlerinde asker kaçaklarının takibini kolaylaştırmak.

Sağlık Yönünden

- T.C. Kimlik Numarası sayesinde kişinin birden fazla sağlık dosyası olmasını engellemek,
- sağlık bilgilerinin birleştirilmesini kolaylaştırmak ve doğru kişinin hizmetlerden yararlanmasını sağlamak.

Eğitim Yönünden

- Eğitimle ilgi kayıt ve sınav gibi işlemlerde doğru kişinin hizmetlerden yararlanmasını sağlamak.

Sosyal Güvenlik Yönünden

- Tek numara ve güvenli kimlik kartı ile sosyal güvenlik kurumları arası bilgi takibi ve hizmet birleştirilmesini kolaylaştırmak.

Adalet Yönünden

- Davalarda kimlik tespitlerinin daha hızlı ve doğru bir şekilde yapılmasını sağlamak.

4.2. EKDS Projesinin Hedefleri

- Türk vatandaşlarının sahip oldukları nüfus cüzdanlarını Avrupa ve dünya standartlarına uygun, her çeşit taklit, tahrif ve sahteciliği ortadan kaldıracak özelliklerde yeni ve güvenli kimlik kartlarıyla değiştirmek,
- Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün yükümlülüğünde olan kimlik kartı düzenleme süreçlerinin yeni teknolojik altyapıya uyumunu sağlamak,
- Uluslararası standartlara uyum sağlamak,
- İhtiyaç duyulan verilere elektronik ortamda ulaşılmasını kolaylaştırmak,
- Kamu kurum ve kuruluşları arasındaki bilgi akışını hızlandırmak,
- İşlem zorluklarının yarattığı savurganlık, zaman ve işgücü kaybını önlemek, vatandaşlara kaliteli ve hızlı hizmet vermek,
- Kimlik kartı işlemlerini, hukuki ve teknik olarak merkezden denetlenebilir hale getirmek,
- Özel ve resmi işlemlerde sahteciliği en aza indirerek "mal güvenliği" ve "kişi haklarını" sağlamak,
- Kart materyalinin isterler çervesinde gerçekleştirmek,
- Milli bir kart ve yonga işletim sistemi kullanmak,
- Yeni teknolojilere uyum sağlayabilen kart üretim ve kişiselleştirme sistemi oluşturmak.

5. EKDS projesi İş Süreçleri

- 2010 yılına kadar Bolu'daki bütün vatandaşlarımıza yeni bir kimlik kartı vermek üzere gerekli altyapı kurulmuştur.
- Kurulan sistem ile kimlik kartı düzenlenmiştir.
- 2011 yılında yaygınlaştırmanın başlayabilmesi için TÜBİTAK UEKAE tarafından bir yaygınlaştırma planı hazırlanmaktadır.

6. EKDS Projesinin Bileşenleri

6.1. Akıllı Kartlar:

Bu projede kullanılacak akıllı kart üzerine güvenli kimlik doğrulama uygulamalarında kullanılmak üzere milli olarak geliştirilmiş kontaklı tümdevre konulacaktır. Ayrıca sınır geçiş uygulamaları (*e-pass*) için de bir temassız yonga bulunur. Bu tu tip akıllı kartlara melez (*hybrid*) denmektedir.

Akıllı kimlik kartı, geleneksel nüfus cüzdanlarından farklı olarak, bünyesinde biri görsel diğeri elektronik olmak üzere iki farklı bilgi tutma ortamı barındırmaktadır. Bu ortamlardan birincisi, kart sahibine ait fotoğrafın ve nüfus bilgilerinin (T.C. Kimlik Numarası, adı, soyadı, doğum yeri vb.) üzerinde basılı bulunduğu ve en az 10 yıl dayanıklılığa sahip malzemeden üretilmiş olan kart gövdesidir. Kartın kopyalanmasını ya da üzerinde değişiklik yapılmasını engelleyecek şekilde üretilmektedir.

Kimlik kartının diğer bilgi saklama ortamı ise kartla bütünleşik olarak üretilen ve içinde kart sahibine ait nüfus bilgilerinin tutulduğu yongadır. Bunun yanı sıra içinde tuttuğu özel kriptografik anahtarları ve bu anahtarlarla ilişkili olan sayısal sertifikaları sayesinde ataklara karşı dirençli bir belleği de içermektedir.

6.1.1. Kimlik Kartının Özellikleri:

Türkiye'de e-devlet anlayışının yerleşmesinde temel rol oynayacak olan Elektronik Kimlik Doğrulama Sistemi (EKDS) projesi kapsamında vatandaşlara dağıtılacak kartlar fiziksel ve işlevsel güvenlik özelliklerine sahiptir. Bunlar aşağıda özetlenmiştir:

- Kimlik kartı ID-1 ve ISO 7810 standartlarına uygundur.
- Kimlik kartının gövdesi aşınmaya ve kırılmaya dayanıklı malzemedendir.
- Kimlik kartı, üzerinde sahteciliği önlemek üzere güvenlik öğeleri içerir.
- Kimlik kartı, üzerinde taşıdığı görsel elemanlar ve kişisel bilgiler bakımından tamamen alenidir (açık, seçik ve net).
- Karttaki yonga içindeki bilgilere sadece yetkili kimseler erişilebilir.
- Kimlik kartında, üzerine güvenlik, bilgi saklama, her türlü sahteciliği önleme ve e-devlet anlayışı kapsamında elektronik sertifikalar gibi uygulamaları da içerebilecek kapasitede bir yonga vardır.
- Kimlik kartının her iki yüzeyine de bilgi yazılabilir.
- Kimlik kartı taklit, tahrifat ve sahteciliğe imkan vermeyecek niteliktedir.
- Kimlik kartının üzerine işlenen görsel öğeler, karta zarar vermeden hiçbir şekilde değiştirilemez.
- Kimlik kartının kişiselleştirilmesi için gerekli olan tüm grafik elemanları kolaylıkla programlanabilir. (Görüntüler, imzalar, kodlar, alfa nümerik veriler vs.)
- Kimlik kartının üzerinde vatandaşa ait siyah-beyaz bir fotoğraf vardır.
- Kimlik kartında fotoğraf, lazer baskı tekniğiyle basılır.
- Kartın üzerine T.C. kimlik nosu barkod olarak da yazılabilir.
- Kartın ön ve arka yüzüne vatandaşa ait bilgiler silinmez, bozulmaz, karta zarar vermeden değiştirilemez şekilde yazılarak kişiselleştirilir.
- Bilgiler yonga içine de güvenli bir şekilde yazılır.
- Kadın ve erkek tek tip kart kullanılıp kart üzerine cinsiyet alanı bulunmaz.

6.1.2. Kimlik Kartlarının Kullanım Amaçları

- Türk vatandaşlarının sahip oldukları nüfus cüzdanları; batı standartlarına uygun, her çeşit taklit, tahrif ve sahteciliği ortadan kaldıracak özelliklerde bir akıllı kimlik kartı ile değiştirilecektir.
- Vatandaşın kimliğinin elektronik ve biyometrik özellikler kullanılarak saptanabilmesine olanak tanınacaktır.
- Kimlik kartlarının özellikleri sayesinde ülkemizin e-devlet anlayışına uygun bir yapıya kavuşturulması sağlanacaktır.

6.1.3. Kimlik Kartının Dayanıklılığı

- Kart on yıl kullanıma olanak sağlayan Polikarbon (PC) malzemeden üretilmiş olacaktır.

6.1.4. Kimlik Kartının Boyutu

- Kartın boyutları için ISO IEC 7810 ve TSE 7246 ID-1 Akıllı Kart standartları geçerli olacaktır (Kart boyutları 85,6 x 53,98 x 0,76 mm ± 0,08 mm ve her köşe 3 mm'lik yarıçapla yuvarlanmış olacaktır).
- Kişiselleştirme sürecinde veriler, kartın kenarlarından itibaren, +/- 0,5 mm'lik bir alana kaydedilecektir.

6.1.5.Kimlik Kartı Malzeme ve Yapısı

- Kişiselleştirilmiş kimlik kartı kırık, kesik, kir, leke, kıvrık, kabarık ya da delaminasyon içermez.
- Çevresel değişikliklere (ısı, nem, UV ışık etkileri vb.) mekanik, kimyasal ve termal dayanıklılığa sahiptir.

KART MALZEMESİ KARŞILAŞTIRMA TABLOSU

Özellik	PVC	Polistiren (PS)	Polikarbon (PC)	PET-F	PET-G
Yoğunluk (g/cm^3)	1,3-1,4	1,05	1,2	1,33	1,27
Vicat A50 (1 kg, oil) (°C)	75-83	95	150-160	>180	76
Dayanabileceği en yüksek sıcaklık (°C)	65	70	100-115	130	55
Dayanabileceği en düşük sıcaklık (°C)	-20	-10	-100	-70	-15
Yanmazlık derecesi (UL 94)	V0	HB	V2-HB	V2	V2-HB
Işık dayanımı	iyi	iyi	çok iyi	çok iyi	iyi
Gerilme dayanımı	iyi	zayıf	çok yüksek	çok yüksek	çok yüksek
Aşınma dayanımı	oldukça iyi	zayıf	çok iyi	çok iyi	oldukça iyi
Laminasyon açılımı	kolay	kolay	imkansız	zor	zor
Diğer malzemelerle uyum	oldukça uyumlu	PVC ile lamine edilebilir	PVC ile lamine edilebilir	PVC ile lamine edilebilir	diğer malzemeler ile lamine edilemez
Basılabilme	oldukça iyi	oldukça iyi	özel boya ihtiyacı	özel boya ihtiyacı	iyi
Lazer uygulama	iyi	zayıf	en iyi	zayıf	zayıf
Kesilme	kolay	-	Zor	zor	kolay
Termotransfer baskı	kaliteli	zor	yüksek kalite	kaliteli	kolay
Büküm dayanımı (büküm sayısı)	3000-5000	-	> 20000	>30000	500-2000
Ana tedarikçi	-	-	Bayer	Dupont	
Fiyat Euro /kg	2-4	-	15-30	7-10	6-8

• Üstün bir mekanik esnek yapıya sahip, bükme yoluyla kırmaya dayanıklıdır. (ISO 7810, 7816).

• Gelişmiş sayısal kopyalama sistemleri ile kopyalanmasını engelleyecek yapıya sahiptir.

• Genel olarak PVC için 3 yıl, PC için 10 yıla yakın kullanım ömrü bulunmaktadır. Kimlik kartı projelerinde PC olacaktır. PC seçildiğinden lazer baskı uygulanacaktır.

6.1.6. Kimlik Kartı Yongasının Özellikleri

• Yonga özellikleri, ilgili kurumların gereksinmesi çerçevesinde TÜBİTAK UEKAE tarafından belirlenmiştir. e-Kimlik temasının içinde yer alan ayrı bir yazıda incelenecektir.

6.1.7. Kimlik Kartı İşletim Sistemi Özellikleri

• Kimlik Kartları ISO 7816-4'te standardında tanımlanan dosya ve güvenlik komutlarıyla uyumlu bir akıllı kart işletim sistemine sahiptir.

• Kart işletim sistemi TÜBİTAK (UEKAE) tarafından geliştirilmiştir.

• e-Kimlik temasının içinde yer alan ayrı bir yazıda incelenecektir.

6.1.8. Standartlar

Kimlik kartı ülke içi ihtiyaçları yanında, uzun dönemde, başta Avrupa Birliği olmak üzere, diğer ülkelerde de kullanılma ihtimali dikkate alınarak uluslararası standartlara uyumu sağlanmıştır. Bu kapsamda, Avrupa Birliği ve CEN (*Comité Européen de Normalisation*) bünyesinde çalışmalar dikkatle takip edilmiştir. Bu bağlamda oluşturulan ECC (Avrupa Vatandaşlık Kartı) standardına uyulmuştur.

• ISO/IEC 7810, Kart Fiziksel Karakteristik

• ISO/IEC 7816-1, Temaslı Yongalı kart Fiziksel Karakteristik

• ISO/IEC 7816-2, Temaslı Yongalı kart; boyutlar ve temas yerleri

• ISO/IEC 7816-3, Temaslı Yongalı kart: Electronik işaretler ve iletişim protokolleri

• ISO/IEC 7816-4, Temaslı Yongalı kart: bilgi paylaşımı için organizasyon, güvenlik ve komutlar

• ISO/IEC 7816-5, Temaslı Yongalı kart: Uygulama kaydı

• ISO/IEC 7816-6, Temaslı Yongalı kart: Bilgi paylaşımı veri elemanları

• ISO/IEC 7816-7, Identification cards — Temaslı Yongalı kart: SCQL (*Structured Card Query Language*) için komutlar

• ISO/IEC 7816-8, Temaslı Yongalı kart: Güvenlik işlemleri için komutlar

• ISO/IEC 7816-9, Temaslı Yongalı kart: Kart yönetim komutları

• ISO/IEC 7816-10, Temaslı Yongalı kart: Senkron kart için electronik işaretler ve reset'e yanıt

• ISO/IEC 7816-11, Temaslı Yongalı kart: biometrik metodla kişisel doğrulama

• ISO/IEC 7816-12, Temaslı Yongalı kart: USB arabağı ve işlem

• ISO/IEC 7816-15, Temaslı Yongalı kart: Kriptografik bilgi uygulaması

• ISO/IEC 14443-1, Temassız Yongalı kart: Fiziksel karakteristik

• ISO/IEC 14443-2, Temassız Yongalı kart:: Radio frekans güç ve işaret arabağı

• ISO/IEC 14443-3, Temassız Yongalı kart:: İlklendirme ve anticollision

• ISO/IEC 14443-4, Temassız Yongalı kart:: iletişim protokolü,

• ICAO 9303, Part 1, Makinaca okunabilen geçiş kartı

• ICAO 9303, Part 2, Makinaca okunabilen Visa

• ICAO 9303, Part 3, Makinaca okunabilen kimlik kartı

6.2. Açık Anahtar Altyapısı (PKI):

e-Kimlik ve e-Devlet uygulamalarında ana unsur bilgiye güvenli erişimdir. İnternet üzerinde hizmet veren kurumların uygulamalarında, hizmet gerçekleştirilirken hizmete katılan (görevli) ve hizmetten yararlanmak isteyen kişilerin (vatandaş) kimliğinin belirlenmesi, yasalar önünde delil niteliği taşır. Bu nedenle e-kimlik altyapısında sertifika sistemi oluşturulmuştur. EKDS projesinde milli olarak geliştirilen Açık Anahtar Altyapısı (PKI[2], '*Public Key Infrastructure*') kullanılmıştır. Bu yapıda sertifika tanzim eden ve sertifika dağıtımı konusunda yetkili kurumlar ile kullanıcıların/kişilerin bulunduğu güvene dayalı bir düzen mevcuttur. Sertifikalar amacına göre istenilen bir yaşam süresi için üretilerek kullanımı sağlanmaktadır.

Sertifika (Elektronik), bir varlığa ait kimlik bilgisi ile bu varlığın kullanımı için atanan açık anahtar bilgisini bir arada tutan belgedir.

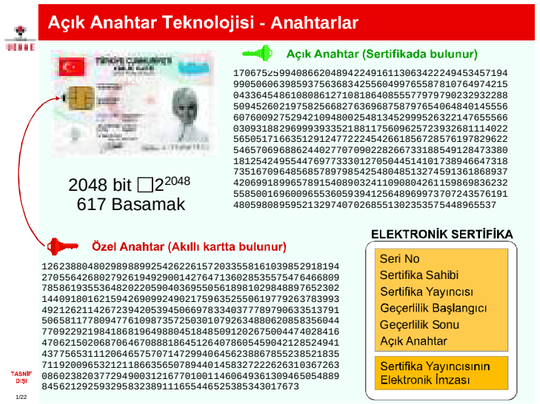
Açık Anahtar Altyapısı, veri (bilgi) iletişiminde açık anahtarlı kriptografinin yaygın ve güvenli olarak kullanılabilmesini sağlayan ve birbirleriyle eşgüdüm içinde çalışan anahtar üretimi, anahtar yönetimi, onay kurumu, sayısal noterlik, zaman damgası gibi hizmetlerin tümünü kapsamaktadır.

Açık Anahtar Altyapısı modellerine göre;

• Simetrik (Tek anahtarlı) şifreleme sistemlerinde, veriyi şifrelemek için ve şifrelenmiş veriyi okuyabilmek için aynı anahtar kullanılır. Karşılıklı olarak şifreli haberleşebilmek için her iki taraf simetrik anahtarları başka birinin eline geçmeden birbirleriyle paylaşmak zorundadırlar.

• Asimetrik (açık anahtarlı) şifreleme sistemlerinde, açık anahtar ve özel anahtar bulunmaktadır. Bu anahtarlar tek yönlü çalışmakta ve birbirlerini tamamlamaktadırlar. Açık anahtar veriyi şifrelemek özel anahtar ise açık anahtar tarafından şifrelenmiş veriyi deşifre etmek rollerini üstlenmişlerdir. Özel anahtarlar sadece ait oldukları kişide bulunurlar. Fakat açık anahtarlar bilinir ve dağıtımları açık olarak yapılır.

[2] PKI (*Public Key Infrastructure*): Sertifikaların, anahtar ikililerinin yönetimini sağlayan yazılımsal ve yordamsal bütünlüğe Açık Anahtar Altyapısı denmektedir.



Şekil 6. *Açık anahtar ve özel anahtar örneği.*

Açık Anahtar Altyapısı; gizlilik, bütünlük ve kimlik kontrolü fonksiyonlarını kullanıcıların elektronik sertifika kullanması yolu ile sağlar. Sertifika elektronik bir kimlik olduğu gibi aynı zamanda sahibine ait bilgiler ile gerekli algoritma anahtarlarını üzerinde bulundurur. Sertifikalar kişiye özeldirler. Sertifikalar, akıllı kimlik kartları ile güvenli bir şekilde ve güvenli ortamlarda muhafaza edilmektedir. Akıllı kartlar sahip oldukları güvenlik mekanizmaları sayesinde içindeki bilgiyi çalma amaçlı yapılan tüm saldırılara karşı kendilerini korurlar. Kart üzerine gizli anahtarlar yüklendiğinde bu bilgiler kesinlikle karttan okunamaz ve kullanımları bir şifre ile (PIN kodu) korunur.

Açık Anahtar Sertifikalarının Ortak Özellikleri;

• Sayısaldır (X.509 standardı).

• Sahibi hakkında gerekli bilgileri içerir.

• Yayın ve son kullanma tarihini içerir.

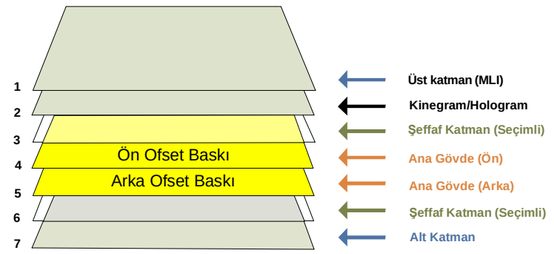
• Yayıncısının adını içerir ve onun sayısal imzasıyla doğrulanması yapılır.

• Yayıncı adı ve sertifika seri numarası sertifikanın tekil olmasını sağlar.

6.3. Kart Üretim ve Basım Teknolojileri:

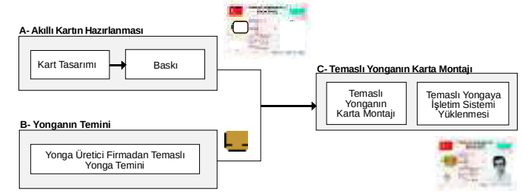
6.3.1. Akıllı Kart Üretimi

Akıllı kartı, en az 10 yıl dayanıklılığa sahip malzeme olan polikarbon kart levhasının kimlik kartı şekline getirilerek üretilmektedir. Kart materyali her çeşit taklit, tahrif ve sahteciliği ortadan kaldıracak nitelikte ve 7 katmanlı olacak şekilde uluslararası standart özelliklerine sahiptir.



Şekil 7. *Kimlik kartı katmanları.*

İlgili kurumlar tarafından belirlenen uluslararası standartlar (kart materyali, ebatları, yonganın kart üzerindeki yeri) dikkate alınarak oluşturulan akıllı kart, üretici tarafından da üretim standartlarına uygun işlem adımları ile üretilmektedir.

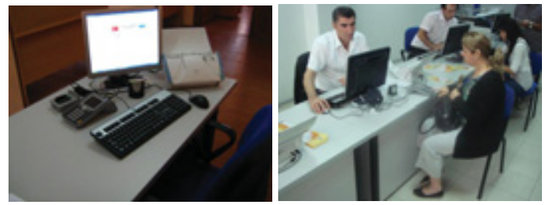


Şekil 8. *Kimlik kartı üretim iş adımları.*

6.3.2. Basım ve Dağıtım Teknolojileri

Kimlik kartı dağıtım teknolojisi olarak dağıtık ve merkezi model geliştirilmesinin yanı sıra gezici model geliştirilerek uygulanmıştır.

Dağıtık modelde vatandaş, ilçe nüfus müdürlüklerine bizzat başvuruda bulunmakta ve başvuru anında kimlik kartını almaktadır.



Şekil 9. *Dağıtık sistem ile kart dağıtımı yapılan ilçelerde her personel için kart dağıtım ortamı.*

Merkezi modelde ise vatandaş, ilçe nüfus müdürlüklerine kimlik kartı için başvuruda bulunmakta ve bilgilerini vermektedir. Kimlik kartları bir merkezde kurulu merkezi kart basma makinesinde basılmakta ve vatandaşa 15 gün sonra şahsen başvuru veya kargo ile teslim edilmektedir.

Şekil 10. *Kimlik kartı üretim iş adımları.*

Gezici modelde ise, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü memurları tarafından vatandaşın bulunduğu yere gidilmekte ve kimlik kartı başvurusu için vatandaştan gerekli bilgileri alınmaktadır. Kimlik kartları bir merkezde kurulu merkezi kart basma makinesinde basılmakta ve vatandaşa 15 gün sonra şahsen başvuru karşılığında veya kurumda görevli memur tarafından teslim edilmektedir.

Şekil 11. *Gezici Sistem Çantası ile şehir merkezinden uzak köylerde kimlik kartı başvurunun gerçekleştirilmesi.*

7. e-Kimlik'te Biyometri

Bir zamanlar bilim-kurgu filmlerinin vazgeçilmez öğelerinden biri olan biyometrik öğeler, gelişen teknoloji ile birlikte günlük yaşamımızın bir parçası haline gelmiştir. Birçok gelişmiş ülkede özellikle son 10 yılda biyometrik teknolojileri kullananların sayısı çığ gibi artmakta, gelişmekte olan başka toplumlarda ise biyometrik doğrulama ve tanıma teknikleri sıradan süreçler olma yolunda hızla ilerlemektedir. e-Devlet uygulamaları, bankacılık işlemleri, e-Ticaret, uluslararası dolaşım gibi çok kullanıcılı uygulamalar dışında kişisel bilgisayarlara ve hatta cep telefonlarına erişim gibi az kullanıcılı sistemler de bu teknolojinin artık vazgeçilmez olduğunun en büyük göstergesidir.

Kişiye özel tekil biyolojik karakteristikler olarak tanımlanabilecek olan biyometriklerin önemi özellikle 11 Eylül saldırılarından sonra artmış ve hem sivil hem de kriminal amaçlı birçok alanda biyometrik kimliklendirme yöntemleri popülerlik kazanmıştır. Bu konuda gelişmiş ülkeler milyonlarca dolarlık araştırma fonları kurmuş, ve biyometri konusu üniversiteler, araştırma kurumları ve özel şirketler için yepyeni bir yatırım alanına dönüşmüştür. Çok geniş bir yelpazeye sahip olan biyometrikler arasında özellikle parmak izi, yüz, konuşma biçimi ve ses, iris, retina, imza, vücut duruşu ve yürüyüşü gibi kişiye özel fizyolojik veya davranışsal özellikler güvenlik sistemlerinde gitgide daha sıklıkla kullanılmaktadır. İstihbarat ve adliye alanlarındaki kriminal uygulamaları yıllardır bilinen biyometrikler, artık pasaport kontrollerinde, vize kontrollerinde, vatandaşlık kimlik kartlarında (e-Kimlik), sürücü belgelerinde, kredi kartları ve bankacılık uygulamalarında da yaygınlaşmıştır. Özellikle parmak izi, yüz, iris, damar izi ve konuşma işareti Amerika Birleşik Devletleri'nden Malezya'ya, Japonya'dan Güney Afrika Cumhuriyeti'ne kadar birçok ülkede kullanım alanı bulmuştur.

Ulusal veya uluslararası ölçekte biyometriklerin e-Pasaport, e-Vize, e-Ehliyet ya da e-Kimlik alanlarında kullanımı hem bu süreçlerdeki güvenlik açığını hem de kaçakları azaltma yolunda müthiş bir etki yaratmıştır. Herşeyden önce, vatandaşlara dağıtılan akıllı kartların yongalarına kaydedilen biyometrik imzalar sayesinde bu kartların sadece sahipleri tarafından kullanılması garanti edilmektedir. Başka bir deyişle sadece yetkisi olanın kullanabileceği kartlar ilgili süreçlerin takibini de kolaylaştırmaktadır. Örneğin çoktan hayatını kaybetmiş bir sigortalının emekli maaşının kötü niyetli kişilerin eline geçtiğini düşünün. Ya da sizin yerinize tapu işlemi yaparak arazilerinizin satıldığını. Trafikte ehliyeti olmayan kişilerin sahte kimlikle dolaşabildiğini ya da sahte pasaportla dolaşan teröristleri hayal edin. Üstelik bu eylemlerin tozlu arşiv dosyalarında kaybolup gittiğini. Bunun yerine tüm bu işlemlerin elektronik olarak gerçekleştiğini, sadece yetkili kişilerin yetkileri dahilindeki işler yapabildiğini varsayın. Kişiler inkar etse bile elektronik kayıtların incelenmesiyle saniyeler içinde kaçakların tespit edilebildiğini düşünün. Biyometrik doğrulama yöntemleri ile bu ve buna benzer risklerin büyük ölçüde bertaraf edilebildiği, bilgi teknolojileri ile de tüm işlemlerin doğru biçimde kayıt edilebildiği ve gerektiğinde sorgulanabildiği teknolojiler artık mevcut ve kullanılmaktadır.

Kriminal ve istihbarat uygulamaları bir yana, sadece sivil biyometrik kimliklendirme teknolojileri bile devletler ve yasal organizasyonlar için milyar dolarlarla ifade edilen büyük ekonomik kazançlara dönüşmektedir. Son yıllarda yapılan eğilim araştırmalarında sadece biyometri endüstri pazarının yıllık ortalama %22.3 büyüme ile 2014 yılında 3.5 milyar doları bulması beklenmektedir (IBG, '*Biometrics Market and Industry Report*', 2014). Dolaylı kazançların ise ülkemiz için yıllık 2-3 milyar dolar,dünyada ise 400-500 milyar dolar düzeyinde

olması öngörülmektedir. Bu rakamlar gelişmiş ya da gelişmekte olan ülkelerin bu teknolojiye neden bu kadar önem verdiğinin en büyük göstergelerinden biridir.

Uluslararası ölçekte biyometrik teknolojilere verilen öneme bakılacak olursa özellikle, İngiltere, Fransa, Almanya, İtalya, İspanya gibi AB ülkeleri yanında ABD, Japonya, Çin, Brezilya, Hindistan, İsrail, Avustralya, Kanada gibi ülkelerin de bu konuda büyük yatırım yaptığı bilinmektedir. Örneğin AB, hem ulusal stratejilerde hem de Çerçeve Programı (*Framework Programme*), Rekabetçilik ve Yenilikçilik Programı (*Competitiveness and Innovation Programme*) gibi AB içindeki uluslararası bilim ve teknoloji stratejilerinde biyometrik teknolojilere ve akıllı kart temelli çözümlere öncelik vermektedir. Özellikle, biyometriklerin kullanıldığı ve başarısız olan birkaç akıllı kart tabanlı otomasyon sisteminin sahaya inmesinden (Hollanda'daki sistemin 3 saat içinde kırılması ile tartışmalar alevlenmiştir) sonra AB bu konudaki çalışmaları daha yoğun biçimde destekleme kararı almıştır. Bu desteğe ilgi gösteren birçok araştırma kurumu ve özel şirket, AB projeleri almak için ortak aramaya başlamışlardır. Bunun yanında ulusal kaynaklar da bu teknolojilerin geliştirilmesi ve daha sonrasında AB çapında bütünleştirilmesi için seferber edilmiştir. Örneğin sadece Almanya'nın biyometri için ayırdığı bütçe 2009 yılında yaklaşık 400 milyon € civarında idi (http://en.wikipedia.org/wiki/Biometrics). Biyometrikler, AB çapında pasaport ve vize gibi uygulamalar yanında, ulusal bazda kamusal işlemlerde yetkilendirme ya da yeni kimlik çıkartma gibi farklı süreçlerde de kullanımdadır. Bunun yanında AB, güvenlik çekincesi yanında kişisel hak ve özgürlükler bağlamında mahremiyeti de güvence altına alan çözümlerin geliştirilmesinde öncü rol oynamaktadır.

ABD ise FBI (*Federal Bureau of Investigation*) ve NIST (*National Institute of Standards and Technology*) önderliğinde yürütülen çalışmalarla özellikle parmak izi, yüz ve iris konusunda birçok uygulamayı hayata geçirmiştir. Vize uygulamalarında turistlerden dahi artık biyometrik veri toplayan ABD, 11 Eylül saldırılarının da saldığı korkuyla yoğurdu üfleyerek yemektedir. ABD, sadece FBI'a her sene biyometrik veritabanını genişletmesi için 1 milyar dolarlık bütçe ayırmıştır.

Biyometrikler Latin Amerika'da da gündemdedir. Örneğin Brezilya'da 2 boyutlu barkodların içine kimlik bilgileri yanında biyometrik imza da yerleştirilmiştir. Peru ve Şili'de ise parmak izi akıllı kartların içinde yer alma sürecindedir. Asya ise hem teknoloji üreten hem de bu teknolojiyi kullanan gelişmiş ülkelerin rekabetine sahne olmaktadır. Özellikle Japonya ve Kore sadece parmak izi değil, damar izi, iris, yüz tanıma gibi teknolojileri olgunlaştırmış ve ABD ve AB'ye rakip olabilecek düzeye gelmişlerdir. Hatta bazı teknolojilerde öncü konuma yükselmişlerdir. Sadece teknoloji üretimi değil, biyometriklerin kullanımı ile ilgili süreçlerin olgunlaşmasında da Asya öncü konumda sayılabilir. Örneğin Malezya ve Tayland eKimlikleri yıllardır başarıyla kullanan ve birikimlerini dünyanın dört bir yanına pazarlamayı başarmış ülkeler arasındadır. Çin ve Hindistan ise adeta gümbür gümbür pazara girmekte ve devasa nüfusları ile bu arenada kendilerine sarsılmaz kaleler inşa etmektedirler

Dünyada biyometrik teknolojiler adından bu kadar söz ettirirken Türkiye de bu duruma kayıtsız kalmamıştır. Emniyet ve istihbarat örgütlerimizin biyometriklere verdiği önem zaten bilinmektedir. Buna ek olarak ülkemiz, biyometri ile ilgili olarak, Devlet Planlama Teşkilatı'nın (DPT) hazırladığı Bilgi ve İletişim Toplumu (BİT) Stratejisi ve e-Dönüşüm politikaları sayesinde tüm ülkeye yaygınlaştırılmak üzere Vatandaşlık Kimlik Kartı Projesi'ni UEKAE'ye vermiş ve proje pilot aşamasına gelmiştir. Bu projenin en ilginç bileşenlerinden biri olan biyometrik doğrulama modülü ise özellikle kamu işlemlerinde ortaya çıkabilecek yolsuzluklarla mücadelede önemli bir güvenlik bileşeni olarak tasarlanmıştır. Proje kapsamında deneyleri yapılan süreçlerde, vatandaşlarımıza dağıtılan kimlik kartlarının içine parmak izi ve parmak damar izi biyometrikleri de saklanmakta ve kamu işlemlerinde kartı taşıyanın gerçekten o kartın sahibi olup olmadığı biyometrik doğrulama ile sorgulanmaktadır. Geliştirilen sistemde hem biyometrik doğrulama başarımının yüksek olması, başka bir deyişle biyometrik güvenliğin yüksek düzeyde garanti edilmesi, hem de biyometrik verinin kıyılarak ve şifrelenerek mahremiyetin korunması hedeflenmiştir. Biyometrik doğrulamanın sadece Kart erişim cihazı denilen terminallerde yapılıyor olması ve mahrem biyometrik verilerin hiçbir biçimde kart ve bu terminallerin dışına çıkarılmaması UEKAE'nin mahremiyete ve kişisel güvenliğe verdiği önemi göstermektedir. UEKAE araştırmacı ve mühendisleri, bu projede ileri düzeyde işaret ve imge işleme tekniklerini, kriptoloji, veri ve ağ güvenliği ve akıllı kart teknolojileri ile birleştirmiş ve geniş ölçekte bir ağ yapısı kurarak, ülke çapında çalışabilecek modüler bir çözümü ortaya koymayı başarmıştır.

Kuşkusuz, biyometrik teknolojiler işaret işlemenin diğer alanları gibi hataya açık teknolojilerdir. Biyometrik işaretler çevresel koşullara, gürültüye, sensör farklılıklarına, veri toplama sırasında oluşabilecek dönme, öteleme, kayma, basınç gibi mekanik yan etkilere oldukça duyarlıdır. Bunun yanında bu tip teknolojilere aşina olmayan insanlardan kaynaklanabilecek sorunlar, kimi zaman yıkanmamış bir parmak, kimi zaman kremli bir el veya çalışma ortamında yıpranmış biyometrikler sorun çıkarabilmektedir. En gelişmiş sistemlerde bile başarımın %90-95 aralığında olması da benzer problemlerden kaynaklanmaktadır. T.C. Vatandaşlık Kimlik Kartı Projesi de bu sorunların görülmesine katkı sağlamıştır. UEKAE'de bu sorunlara çözüm bulabilmek için çok önemli bilimsel çalışmalar yapılmıştır. Bu çalışmalar sayesinde, pilot uygulamada, %60'larda seyreden başarımlar %90'lara kadar çıkarılmıştır. Alınan derslerle UEKAE, projenin ikinci safhası olan tüm ülkeye yaygınlaştırmada daha güçlü algoritmalar ve daha güçlü sensörlerle hazırdır. UEKAE, diğer alanlarda da olduğu gibi

biyometri konusunda da, ulusal çıkarlarımızı gözeten ve yurt dışına bağımlılığı giderecek bilimsel ve teknolojik çalışmalarına son hızla devam etmektedir.

8. EKDS (eKimlik) Projesinde Geliştirilen Ürünler

Bu proje kapsamında, aşağıda sıralanan, tüm ürünler milli olarak geliştirilerek pilot uygulamada kullanılmıştır:

- Milli Yonga,
- Ulusal İşletim Sistemi,
- Elektronik Kimlik Doğrulama Sistemi,
- Milli Açık Anahtar Altyapısı,
- Kart Yönetim Sistemi,
- Güvenli Kart Erişim Cihazları.

Milli Yonga: UEKAE YİTAL[3] Tümdevre Tasarım grubu tarafından UKTÜM[4] adıyla tasarlanmıştır. İçine yerleştirilen, vatandaşa ait nüfus bilgilerinin güvenli bir şekilde kaydedilmesini sağlar. Ayrıca bu işlemden sonra yetkisiz kimseler taradından yeniden üretilmesini ya da bilgilerin değiştirilmesini olanaksız hale getirecek tüm önlemler alınmıştır. Milli yonga CC EAL 5+ güvenlik sertifikası değerlendirmesindedir. Bu konu, e-Kimlik teması içinde ayrı bir yazıyla incelenecektir.

Milli İşletim Sistemi; UKiS[5], T.C. Kimlik Kartı uygulamaları için TUBİTAK UEKAE tarafından geliştirilmiş bir işletim sistemidir. UKTÜM yongası üzerinde çalışmaktadır. UKTÜM'ün sağladığı donanımsal simetrik (AES ve DES/3DES) ve asimetrik (RSA1024/2048) algoritmalar ile şifreleme/deşifreleme yapar. UKIS, CC EAL 4+ güvenlik sertifikası değerlendirilmesindedir. Bu konu, e-Kimlik teması içinde ayrı bir yazıyla incelenecektir.

[3] YİTAL: Yarı İletken Teknolojileri Araştırma Laboratuarı (TÜBİTAK Gebze Yerleşkesi).
[4] UKTÜM: Ulusal Akıllı Kart Tümdevresi.
[5] UKiS: Ulusal Kart İşletim Sistemi.

Elektronik Kimlik Doğrulama Sistemi (EKDS): Türkiyenin e-Kimlik projesinin alt yapısıdır. Tamamen TUBİTAK UEKAE tarafından gerçeklenmiş ulusal bir yapıdır. e-Devlet kapısında vatandaşı hizmetin odağına koyan e-Dönüşümü gerçekleştirecek düzenin kurulmasında baş rolü oynayacak kimlik doğrulama mekanızmasını oluşturmaktadır.

e-Devlet kapısına başvurularda hizmetin hak edene verilmesi çok önemlidir. Hizmet gerçekleştirilirken hizmete katılan ve hizmetten yararlanmak isteyen kişilerin gerçekten öne sürdükleri kişi olduklarının (kimliği çalan veya taklit eden başka bir kişi olmadığının) doğrulamasını EKDS gerçekleştirmektedir. EKDS içinde, doğrulama işlemini gerçekleştiren temel bileşenler ve işlemin işlevselliğini ve güvenirliğini arttıran yardımcı bileşenler vardır. Bu konu e-Kimlik teması içinde ayrı bir yazıyla incelenecektir.

Şekil 12. *EKDS amblemi.*

EKDS Temel Bileşenleri; Elektronik Kimlik Kartı, Kart Erişim Cihazı (KEC), Kimlik Doğrulama Sunucusu (KDS) Kimlik Doğrulama Politika Sununcu ve Arabirim Yazılımları'ndan (Güvenlik Servisleri Platformu ve Otomasyon Yazımı Arabirimi) oluşmaktadır.

EKDS Yardımcı Bileşenini ise Açık Anahtar Altyapısı üzerinden Sayısal İmza oluşturmaktadır.

Güvenli Kart Erişim Cihazları (KEC): İnternet üzerinde hizmet veren kurumların uygulamalarında, elektronik kimlik doğrulama gerçekleştirilmesi amacıyla tasarlanan Elektronik Kimlik Doğrulama Sistemi'nin uç birimidir. Kullanım yerlerine göre Bireysel, Gezgin, Acil Hizmet, Kiosk, Turnike, Kart Yayın KEC'leri isimlerini alır KEC'de gerçekleştirilrn işlem sırasında hizmet alanın kimlik doğrulamasının güvenirliliğini arttırmak için parola uygulamasının yanısıra biyometrik yöntemler de kullanılmaktadır. Ayrıca hizmet alanın parmak izini ve/veya damar izini okumak amacıyla, cihazın üzerinde parmak izi ve harici olarak bağlanan damarizi sensörü bulunmaktadır. Cihazın yaptığı işlemlerin güvenliğini, cihazın içinde kendisine ait sertifikaların yer aldığı güvenlik erişim modulü (GEM) ile sağlamaktadır. Cihazlar CC EAL 4+ güvenlik sertifikası değerlendirilmesindedir. Bu konu e-Kimlik teması içinde ayrı bir yazıyla incelenecektir.

Kurumsal Tip KEC hizmet isteyen (vatandaş) ve hizmete katılanın (görevli) kimlik doğrulama işleminde kullanılacağı kimlik kartları ile hizmete katılanın yapılan işleme elektronik imzasını atmak üzere kullanacağı cihazdır. Kurumların uç hizmet noktalarında kullanım için tasarlanmıştır. Örneğin; hastane poliklinikleri, eczaneler, banka şubeleri, vergi daireleri, adliyeler.

Şekil 13. *Kurumsal tip kart erişim cihazı.*

Bireysel Tip KEC EKDS'te hizmet alan ve veren arasında yürütülen işlemlerin güvenliğini ev ve ofis kullanıcıları için sağlar. Ayrıca cihaz masaüstü veya taşınabilir bilgisayarlardaki internet ve masaüstü uygulamaları için USB üzerinden kimlik doğrulama işlemini yerine getirir. Böylece kullanıcı, kurumların hizmet veren uç noktalarına gitmeden ev veya ofisinden işlemlerini gerçekleştirebilme imkanına sahip olur.

Şekil 14. *Bireysel tip kart erişim cihazı.*

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

Şekil 15. *KİOSK tipi kart erişim cihazı.*

Milli Açık Anahtar Altyapısı: EKDS'in internet üzerinden elektronik hizmet veren kurumların gereksinim duyduğu kişisel kimlik doğrulama işlevini T.C. Kimlik Kartı kullanarak sağladığı anlatılmıştı. Bu sistemde birbiriyle muhatap olan tüm uç unsurlar (kart-KEC) açık anaktar yapısı üzerinden aidiyetlerini karşılıklı doğrular. Aksi takdirde hizmet verilmez. Bu amaçla, kartlarda, sunucularda ve kart erişim cihazlarında asimetrik anahtar çiftleri kullanılmaktadır. Sertifikalar, çift anahtarlı kriptografi teknolojisine dayanır.

Sistemde üç tip sertifika kullanılmaktadır.

1. **Kart Doğrulama Sertifikası**, kimlik kartını üreten makamın doğrulamasında kullanılır. Kartın yetkili bir kurum tarafından üretildiğinin ispatı olarak da değerlendirilmektedir.

2. **Kimlik Doğrulama Sertifikası**, kart sahibinin kişisel bilgilerini doğrulamada kullanılmaktadır.

3. **GEM Sertifikası** ise kimlik kartını doğrulayan nitelikli okuyucuların onaylı ve geçerli olduğunu ispat etmek için kullanılmaktadır.

Bu anahtar çiftlerinin yönetimi için TÜBİTAK UEKAE tarafından geliştirilmiş Milli Açık Anahtar Altyapısı altındaki yazılımlar ve donanımlar kullanılmaktadır.

Kart Yönetim Sistemi: Kimlik kartlarının Kişiselleştirilmesi, kişiye teslimi ve kartın kullanımına ilişkin desteklerin yönetildiği sistemdir. Kimlik kartı yönetim sistemi; kart yönetim merkezi, kişiselleştirme ve kart yönetim birimlerinden oluşmaktadır.

Kart Yönetim Merkezi: Kimlik kartı yönetim sisteminin merkezidir. Veritabanı ve uygulama sunucularından oluşur. Uygulama sunucusu kendisine atanan hizmetleri web servisleri aracılığıyla vermekte ve veritabanı yönetimini sağlamaktadır. Kart Yönetim Merkezi (KYM); KYB (Kart Yönetim Birimi), NEKSIS (Nüfus envanter kayıt sitemi), Mobides (Mobil bilgi derleme sistemi), KRS (Kart raporlama sistemi), KAPSİS (Kart bilgisi paylaşım sistemi) alt sistemlerine hizmet vermektedir.

Kişiselleştirme Birimi (Toplu Kart Basım Birimi):

Kişiselleştirme, başvuran kişi adına kimlik kartının düzenlenmesi ve baskı işlemlerinin yapılmasıdır.

Dağıtık modelde kişiselleştirme; Kart yönetim birimlerindeki KYB terminallerinde masaüstü kart yazıcılar vasıtası ile yapılmaktadır.

Merkezi modelde kişiselleştirme: Kartların tümü bir merkezde kurulu endüstriyel kart yazıcılarda yapılmaktadır.

Kart yönetim birimleri: Kimlik kartı talep, düzenleme ve destek işlemlerinin yapıldığı birimdir. Kart Yönetim Birimi kısaca KYB adı ile adlandırılmaktadır.

9. Pilot Uygulama

"Elektronik Kimlik Doğrulama Sistemi Geliştirimi ve T.C. Kimlik Kartı Tasarımı" isimli proje ile ilgili olarak Yüksek Planlama Kurulunun 11.07.2006 tarih ve 2006/38 nolu kararı ile Bilgi Toplumu Stratejisi ve eki Eylem Planı kabul edilmiştir.

Planın 46 nolu eyleminde "*Vatandaşlık Kartı; Pilot Uygulaması ve Yaygınlaştırılması ile biyometrik unsurlar da içeren elektronik vatandaşlık kartının kimlik doğrulama için kullanımının sağlanması ve tüm kimlik doğrulama fonksiyonlarının tek bir elektronik kartta toplanması*" ile 04 Temmuz 2007 tarih ve 26572 sayılı Resmi Gazetede yayımlanan 2007/16 No'lu Başbakanlık genelgesinde "*Vatandaşlık kartının hayata geçirilmesi öncelikle sağlık ve sosyal güvenlik alanında olacaktır. Eylem kapsamındaki pilot çalışma, TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ve Sosyal Güvenlik Kurumu (SGK) arasında imzalanan protokolle başlatılmıştır. Pilot proje 3 aşamadan oluşacaktır. Birinci aşamada, vatandaşlık kartı, kart okuyucular, TÜBİTAK UEKAE tarafından geliştirilecek işletim sistemi ve uygulamaların testi Kurum (UEKAE) içerisinde yapılacaktır. İkinci aşamada, ilgili tarafların kararıyla belirlenecek bir ilçede 10.000 vatandaşı kapsayan bir pilot uygulama gerçekleştirilecektir. Üçüncü aşamada ise uygulama 300.000 vatandaşı kapsayacak şekilde, ikinci aşamanın uygulandığı ilçenin bağlı bulunduğu ilde denenecektir.*" denilmektedir.

Pilot uygulama birinci aşaması, TÜBİTAK UEKAE tarafından geliştirilen farklı tip kart malzemesine sahip (PVC[6], PC ve PET[7]) kimlik kartları, Kart Erişim Cihazları, işletim sistemi ve uygulamaların testi Kurum kapsamında yapılarak denenmiştir. Proje paydaşları tarafından pilot uygulama birinci aşamasının değerlendirilmesi ile Temmuz 2008 tarihinde ikinci aşamaya geçilmesine karar verilmiştir.

Elektronik Kimlik Doğrulama Sistemi ve T.C. Kimlik Kartı'nın ilk olarak sosyal güvenlik alanında denenecek olmasından dolayı ikinci aşamada kart dağıtımı yapılacak 10.000 vatandaş Sosyal Güvenlik Kurumu (SGK) tarafından belirlenmiştir.

İkinci Aşama Kart Dağıtım Süreci (01 Eylül 2008–05 Aralık 2008): Eylemin sorumlu kuruluşu olarak İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü belirlenmiştir. Bolu İli Merkez İlçe Nüfus Müdürlüğünce davetiye ve randevu sistemi kullanılarak SGK tarafından belirlenen 13.453 vatandaşa parmak izi alınmadan (Kanun tasarısı çalışmaları henüz tamamlanmamıştı) dağıtık model ile T.C. Kimlik Kartı dağıtılmıştır.

Bu süreçte, **PC, PET, PVC tipi** kart malzemeleri kimlik kartı olarak dağıtılmıştır. Ayrıca farklı baskı teknolojilerini (lazer ve termal) kullanılmıştır.

Baskı denemeleri aşağıdaki gibidir:

- PVC kart tipindeki kimlik kartlarına termal yazıcı teknolojisi ile renkli baskı,
- PC kart tipindeki kimlik kartlarına lazer yazıcı teknolojisi ile siyah-beyaz baskı,
- PET kart tipindeki kimlik kartlarına termal yazıcı retransfer teknolojisi ile renkli baskı uygulanmıştır.

Pilot uygulama 3. aşamada (ve yaygınlaştırmada) dağıtılacak kimlik kart malzemesini belirlemek için 2. aşamada dağıtılan üç tip kart (PVC, PC ve PET), TÜBİTAK UEKAE tarafından Amerikadaki "*Eclipse Laboratories*" adlı laboratuara test için gönderilmiştir.

İlgili laboratuardan gelen rapora göre iyi puanı PC kart tipi almıştır; çevresel şartlardan kaynaklanan fiziksel bozulmalara karşı CEN/TS 15480-1 standartlarını karşılamaktadır.

Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü ile yapılan gözden geçirme toplantılarında, laboratuardan gelen test sonuçları değerlendirilmiştir. Pilot uygulamanın 3. aşamasında PC kart malzemesinin kullanılması kararlaştırılmıştır.

Dağıtımı yapılan kimlik kartlarının sağlık ve sosyal güvenlik uygulamalarında kullanılacağı aşağıda adı geçen sağlık tesisleri ve birimlerinde 2008 yılı Ekim ayının sonuna kadar EKDS bileşenleri (kart erişim cihazı ve yazılım uygulamaları) kurulmuş ve eğitimleri gerçekleştirilmiştir.

- **Eczane:** Bolu ili Merkez ilçesinde SGK anlaşması olan 67 birim,
- **İzzet Baysal Devlet Hastanesi Köroğlu Ünitesi:**
  - **Kayıt Kabul:** Kart Erişim Cihazı (KEC) 1 adet,
  - **Poliklinikler:**
    - Beyin cerrahi (1 adet KEC),
    - Dermatoloji (1 adet KEC),
    - İntaniye (1 adet KEC),
    - Üroloji (1 adet KEC),
- **Aile Hekimliği Birimi:**
  - **Tevfik Atay A.S.M:** 5 aile hekimi birimine birer adet kart erişim cihazı ve uygulama yazılımları,
  - **12 Kasım A.S.M:** 4 aile hekimi birimine birer adet kart erişim cihazı ve uygulama yazılımları.

Sosyal güvenlik alanında yapılan denemelerde T.C. Kimlik Kartı'yla vatandaşın kimliğinin doğrulanması elektronik ortamda gerçekleştirilerek vatandaş adına provizyon alma işlemi gerçekleştirilmiştir.

01 Eylül 2008'de kurulumların başladığı ve 30 Ekim 2008 tarihinde tamamlandığı süreçte testler ve geliştirmeler sürdürülmüştür. Kimlik kartlarında parmak izi alınabilmesi için gerekli kanun 26.06.2009 tarihinde kabul edilmiştir.

10 Temmuz 2009 tarihinde DPT Müsteşarlığında yapılan toplantıda pilot uygulama 3. aşamaya geçiş konusunda,, paydaş kurumlar (NVİ, SB ve SGK) ve yürütücü kuruluş TÜBİTAK UEKAE yetkilileri tarafından herhangi bir engel olmadığı ifade edilmiştir.

Üçüncü Aşama Kart Dağıtım Süreci (31 Ağustos 2009-): Bolu ilçelerinde farklı dağıtım senaryoları ile biyometrik unsur (parmak izi) içeren kimlik kartı dağıtımı devam etmektedir. Dağıtım senaryolarında kullanılan kimlik kartları PC kart malzemesinden oluşmaktadır. Bu aşamada ilçelerde uygulanan dağıtım senaryoları ile genel uygulama öncesi en uygun dağıtım yöntemi belirlenmesi amaçlanmaktadır. Bolu il genelinde 31 Ağustos 2009 tarihinden 02 Ağustos 2010 tarihine kadar yaklaşık 212.000 vatandaşa kart dağıtılmıştır.

Üçüncü aşama sırasında dağıtık, merkezi ve gezici kart dağıtım modelleri denenmektedir. **Dağıtık modelde** kimlik kartı basımı için Ixla, Muhlbauer, DIS-LES marka lazer yazıcılar kullanılmaktadır.

Merkezi modelde ise kimlik kartı basımı için farklı merkezi kart basma makineleri denenmiştir. Saatte 260 adet kimlik kartı basabilen Mühlbauer Scope 5400 merkezi makinesi Ekim 2009-Ocak 2010, DataCard firmasına ait saatte 250 adet kimlik kartı basabilen merkezi makinesi ise Ocak 2010-Nisan 2010 tarihleri arasında kullanılmıştır.

Denemelerde, hız, kullanılabilirlik, bakım, arıza, sarf malzeme ihtiyacı bakımından karşılaştırmalar yapılmıştır.

6 PVC (Polivinil Klorür): geniş kullanım alanı olan bir plastik türüdür.

7 PET (Polietilen Tereftalat): Polyester ailesine ait termo-plastik bir malzemedir.

DIS- LES 9000 (Almanya) | **IXLA 100 PLUS (İtalya)** | **Muhlbauer CLP 54 (Almanya)** | **Mühlbauer Scope 5400 merkezi makinesi (Almanya)** | **DataCard MPR 5800 merkezi makinesi (Amerika)**

Şekil 16. *Pilot uygulamada kullanılan bazı kart kişileştirme makineleri.*

Gezici modelde Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü memurları tarafından vatandaşın bulunduğu toplam 5 ilçede şehir merkezinden uzak 490 köyden 282 köye gidilerek kimlik kartı başvurusu için vatandaştan gerekli bilgileri alınmıştır. Vatandaştan alınan kayıtlar, merkeze kurulan merkezi yazıcılarda kimlik kartı olarak basılmakta ve kimlik kartları, vatandaşa 15 gün sonra teslim edilmektedir.

05-06 Ocak 2010 tarihlerinde Sosyal Güvenlik Kurumu ile TÜBİTAK UEKAE yetkilileri arasında e-reçete ve provizyon gözden geçirme toplantıları gerçekleştirilmiştir. Bu toplantılar sonucunda alınan kararlar doğrultusunda; kimlik kartının 07 Ocak 2010 tarihinden itibaren Bolu ilinde bulunan Bolu İzzet Baysal, Gerede, Mudurnu ve Göynük Devlet Hastaneleri, Ağız ve Diş Sağlığı Merkezi, Fizik Tedavi ve Rehabilitasyon Hastanesi ile İzzet Baysal Kadın Doğum ve Uygulama Hastanesinde provizyon alma işlemlerinde kullanılmasına karar verilmiştir.

Şekil 17. *Gezici Sistem Çantası ile şehir merkezinden uzak köylerde kimlik kartı başvurunun gerçekleştirilmesi.*

İkinci ve üçüncü aşama kapsamında dağıtımı yapılan kimlik kartlarının kullanılacağı aşağıda adı geçen sağlık tesisleri ve birimlerine Ocak ayının sonuna kadar EKDS bileşenleri (kart erişim cihazı ve yazılım uygulamaları) kurulmuş ve eğitimleri gerçekleştirilmiştir.

- **Gerede Devlet Hastanesi:**
  - Kayıt kabul ve poliklinik: 12 adet KEC,
- **Mudurnu Devlet Hastanesi:**
  - Kayıt kabul ve poliklinik: 1 adet KEC,
- **Göynük Devlet Hastanesi:**
  - Kayıt kabul ve poliklinik: 1 adet KEC,
- **İzzet Baysal Kadın Doğum ve Uygulama Hastanesi:**
  - Kayıt kabul ve poliklinik: 6 adet KEC,
- **Ağız ve Diş Sağlığı Merkezi:**
  - Kayıt kabul ve poliklinik: 3 adet KEC,
- **Fizik Tedavi ve Rehabilitasyon Hastanesi:**
  - Kayıt kabul ve poliklinik: 3 adet KEC.

26 Ocak 2010 tarihinde T.C. Kimlik Kartı ile sağlık tesislerinde provizyon ve e-reçetenin gerçekleştirilebilmesi amacıyla Sosyal Güvenlik Kurumu Başkanlığı Ankara yerleşkesinde Sosyal Güvenlik Kurumu, TÜBİTAK UEKAE yetkilileri ve hastane otomasyon sistemi geliştiricileri ile çalıştay gerçekleştirilmiştir. SGK ve hastane otomasyon sistemi geliştiricilerinin MEDULA e-reçetenin uygulanmasına ilişkin bazı çalışmaları yaparak tamamlanmasına ilişkin karar alınmıştır. Tüm gereken değişikliklerin Mayıs 2010'da tamamlandığı bildirilmesine rağmen T.C. Kimlik Kartı ile e-reçete uygulaması henüz gerçekleşmemiştir.

25 Şubat 2010 tarihinde projenin Bolu ilinde VII. Dönem Gelişme Raporu değerlendirme toplantısı gerçekleştirilmiştir. Toplantıda, kimlik doğrulamada kullanılan parmak izi teknolojisinin yanında damar izinin de de kullanılması önerilmiştir.

Buna göre, Gerede Devlet Hastanesinin 12 polikliniğinde kurulan EKDS altyapısı, 05 Mart 2010'de yeniden düzenlenerek kimlik doğrulamasında hem parmak izi hem de damar izi kullanılabilir hale getirilmiştir.

07 Ocak – 02 Ağustos 2010 tarihleri arasında kurulum yapılan tüm sağlık birimlerinden toplam 4.719 adet civarında provizyon işlemi gerçekleştirilmiştir.

10. Yaygınlaştırma

Türkiye'nin e-Kimlik aşamasına geçmesi için TÜBİTAK UEKAE tarafından yürütülen projenin pilot uygulamasında geliştirilen tüm ürün ve alt bileşenler denenmiştir. 01 Kasım 2010 tarihinde tamamlanacak olan bu projenin ülke geneline yaygınlaştırılmasının başlaması için 2012 yılı hedeflenmektedir.

Pilot uygulama kapsamında kullanılan farklı dağıtım modellerinin (dağıtık, merkezi) arasında İçişleri Bakanlığı, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü tarafından 2010 yılı içinde bir seçim yapılarak dağıtım modeline karar verilecektir.

Dağıtım modelinin belirlenmesi ile birlikte sürdürülen diğer paralel çalışma ise yaygınlaştırmada rol tanımları belirlenen kamu kurumlarının, gerekli yatırım çalışmalarını başlatabilmeleridir. Bunun için Devlet Planlama Teşkilatı Müsteşarlığı'na ilgili kurumlar tarafından Fizibilite Raporu hazırlanmaktadır. Bu rapor doğrultusunda, yatırımlarının 2011 yılı Kamu Yatırımları Programı kapsamına alınması hedeflenmektedir.

10.1. Yaygınlaştırma Yönetimi

Projenin etkin bir şekilde yönetilebilmesi, ürün ve hizmetlerin vatandaşa tam ve zamanında ulaşmasını sağlamak için etkin, sonuç alıcı ve hızlı bir yöntem izlenmelidir. Bu işlem TÜBİTAK UEKAE'de hazırlanan yaygınlaştırma raporuna göre 3 yıl içinde tamamlanabilmekted Bu süreçte TÜBİTAK UEKAE'nin pilot uygulama sonuçları kullanılacaktır.

Dağıtım ve yaygınlaştırma süreci AB uygulamalarının da işaret ettiği üzere tüm kurumsal etkinliklerde olduğu gibi "takip edilmesi, değerlendirilmesi ve yönetilmesi" gereken bir etkinliktir. Bütün bunlardan bağımsız olarak sistem canlı kullanıma geçtiğinde "çok iyi donatılmış", "çok iyi yönetilen" ve "rolleri oturmuş" paydaşlarla "mükemmel bir orkestrasyon" içerisinde çalışmalıdır. Bu organizasyonunun özenle yapılması, ihtiyaçların öngörülerek temini ve buna ek olarak yaygınlaştırma destek yönetiminin başarılı olarak yürütülmesi çok önemlidir. Bu sebeple dağıtım ve yaygınlaştırma sürecinin kendisi bir proje gibi değerlendirilerek yönetilmelidir. "Yaygınlaştırma Projesi Yönetim Modeli" olarak adlandırılan yönetim yaklaşımının aşağıda önce gerekçeleri bir sonraki bölümde de içeriği tanımlanmıştır. Öncelikle gerekçelerine kısaca göz atalım:

• Dağıtım ve yaygınlaştırma sürecinde birden fazla kurum, kuruluş ve farklı roller mevcut olacaktır. Her bir paydaşın güvencesi ve ortak paydası olacak, dağıtım ve yaygınlaşmanın hedef ve kısıtlar içinde planlandığı şekilde ilerlemesini güvence altına alacak bir üst çatı yapının, bir birimin varlığı bu orkestrasyon için zaruridir.

• Dağıtım ve yaygınlaştırma sürecinde performans baskısı beklenmelidir. Ciddi bir kaynak ve zaman baskısı taraflarca hissedilecektir. Dolayısıyla "Proje Yönetimi" mantığı ile kaynak tahsisi ve zaman yönetimi bu sürecin etkin yönetiminde hayati derecede önemlidir. Otoritelerin zaman yönetimi baskısı konusundaki sıralamaları da bu sürecin neden bütünleşik yönetilmesi gerektiğini vurgulamaktadır.

• Tüm diğer Kamu kurumlarında bu uygulamanın yansımaları olacaktır. Dolayısıyla mesele sadece T.C. Vatandaşlık Kartının öngörülen süre ve maliyet çerçevesinde tüm vatandaşlara dağıtımı ile bitmeyecek, vatandaş nezdinde;

- vatandaş odaklı hizmet dönüşümü ve

- kamu yönetiminde modernizasyon

beklentilerini de şiddetlendirecektir. Kısaca sadece dağıtım ve yaygınlaştırma sürecinin kendisi değil, paralelinde "domino taşı" misali diğer kurumlara da yansımasının entegre-bütünleşik bir anlayışla yönetilmesi elzemdir. Kamu kurumlarının kendi içlerindeki uygulamalarda, vatandaşlık kartının iş süreçlerine entegrasyonu konusunda TÜBİTAK UEKAE ile birlikte paralel projeler yürütmesinin gerekliliği genelgede de dile getirilmektedir.

• e-Vatandaşlık Kartı bir bilişim teknolojisi (BT) ürünüdür. Bu alanda hızlı teknolojik gelişimler ve baş döndüren adaptasyonların varlığı kuşkusuz ürün gibi dağıtım ve yaygınlaştırma sürecinin zaman içerisinde güncellenmesi, iyileştirilip, geliştirilmesi ihtiyacını da beraberinde getirecektir. Yaygınlaştırma süreci ile birlikte özel sektör uygulamaları bu alanda farklı talepleri de gündeme getirecektir. Ürün ve hizmet çeşitlenmesi, türev ürünlerin ortaya çıkması, yaygınlaşma sürecinin tetiklediği yeni bir sektörel açılımı da ivmelendirecektir.

• Dokuzuncu Kalkınma Planı, "İstikrar içinde büyüyen, gelirini daha adil paylaşan, küresel ölçekte rekabet gücüne sahip, bilgi toplumuna dönüşen, AB'ye üyelik için uyum sürecini tamamlamış bir Türkiye" vizyonu ve Uzun Vadeli Strateji (2001-2023) çerçevesinde hazırlanmıştır. Bu çerçevede "İdarelerin yönetim sorumluluğunun güçlendirilmesi için gerekli olan iç kontrol ve iç denetim sistemleri, bu sistemlere rehberlik ve gözetiminden sorumlu Merkezi Uyumlaştırma Birimleriyle birlikte uluslararası standartlar ve AB uygulamalarıyla uyumlu olarak uluslararası geçerlilikte kaliteye sahip olabilecek şekilde tüm unsurlarıyla birlikte uygulamaya konulacaktır". e-Kimlik Kartının AB uygulamalarıyla uyumluluğunun sevk ve idaresi dinamik, kapsamlı bir çalışmadır. AB tecrübelerinden çıkartılan dersler doğrultusunda bir Üst Kurulun varlığı ve yaygınlaştırma sürecinin "proje" yaklaşımıyla yönetilmesi önemlidir.

İçerik 10 ana başlık altında toplanmıştır:

Bütünleşik Proje Yönetimi: Daha önce de gerekçeleriyle vurgulandığı üzere dağıtım ve yaygınlaştırma sürecinin bir proje yaklaşımıyla yönetilmesi gerekmektedir. Birkaç ortağı-paydaşı olan büyük projelerde ortak bir iş programı hazırlanır. Tüm ortaklarca kabul görmüş bu iş programının kaynaklarının yönetimi, kontrolü ve raporlanması bütünleşik proje yönetiminin işlevlerindendir. Üst kurul doğrudan bu birim ile irtibat halinde olacaktır. Yaygınlaştırma Yönetim Modelinin kalbi de denilebilir.

İletişim Yönetimi: Yaygınlaştırma bünyesindeki paydaşların tespit edilerek, bunlar arasındaki iletişim modellerinin çıkartılması, bilginin paylaşımı, paylaşım kayıtlarının ve performansların raporlanmasını içerir.

Risk Yönetimi: Yaygınlaştırma sürecinde potansiyel risklerin belirlenerek, yönetim planının yapılması, önlem paketlerinin alternatifleriyle birlikte hazırlanmasını ve denetimini içerir.

Zaman Yönetimi: Dağıtım ve yaygınlaştırma sürecinde belirlenen zaman planına uymasının sağlanması yönetimi olarak özetlenebilir. Etkinliklerin belirlenmesinden, sıralanmasına, kaynakların planlanması, sürelerinin programlanması, iş programlarının geliştirilip, kontrolü bu alt ekibin iş içeriğini oluşturur.

Tedarik Yönetimi: Dağıtım ve yaygınlaştırma sürecinde dışarıdan iş yapan birçok paydaş olacaktır. Bunlar ürün veya hizmet tedariki yapabilir. Bu tedarikçilerin sözleşmeleri, ihale şartnameleri, denetim ve raporlamalarıyla tedarik yönetimi ilgilenir.

Maliyet Yönetimi: Dağıtım ve yaygınlaştırmanın mali resmini çıkartarak, bu bütçe dahilinde kontrolü ve gerçek/bütçe tablolarının çıkartılarak raporlanmasıyla ilgilenir.

Kalite Yönetimi: Dağıtım ve yaygınlaştırma sürecinin uyduğu kalite standartlarını ele alarak, bir program hazırlanması, uygulanması ve kontrol edilmesi aktivitelerini içerir. Bilindiği üzere üretim modellerine göre dünyaca kabul edilmiş kalite ölçümü standartları vardır. CMMI günümüzde BT projelerini geliştirmede kullanılan kalite değerlendirme standardıdır. Diğer iş geliştirme modellerinde olduğu gibi BT projelerinde de kalite çok önemlidir. CMMI gibi tanınmış bir standarda göre üretildiği takdirde;

• ürünün beklendiği gibi çalışacağı, vatandaş memnuniyetinin yüksek,

• performansının da taahhüt edildiği şekilde güvence altında olacağı

konusunda kuvvetli bir görüş hakim olacaktır. Üretici açısından faydası ise spesifikasyon ve toleranslar dahilinde tanımlanmış bir yöntem sayesinde daha kısa sürede, daha az maliyetle daha iyi ürün/hizmet sunmak ve geliştirebilmektir.

İnsan Kaynakları Yönetimi: Yaygınlaştırma sürecinin operasyonel ve idari iş gücü kaynak gereksiniminin planlanması, tedariği, istihdamı, eğitimi, kadrolanması ve performans yönetimi gibi temel başlıkları içerir.

Kapsam Yönetimi: Her projede olduğu gibi yaygınlaştırma sürecinde de hedef ve amaçlarının yanında tanımlı bir iş kapsamı bulunmaktadır. Bu kapsam, yaygınlaştırma tamamlanana kadar izlenir ve denetlenir. Kapsam dışı işler çıktığında, kapsam yönetimi ekibi tarafından değerlendirilir.

Kriz Yönetimi: Dağıtım ve yaygınlaştırma sürecini derinden etkileyebilecek ve üst yönetimin müdahalesini gerektirecek, plan dışı olarak gerçekleşen beklenmedik riskler, kriz yönetimi tanımı içine girmektedir. BT projeleri son derece dinamik bir ortamda geliştirildiği için çok fazla çeşitte riskler içerir. BT projelerinin insan ve teknoloji tarafı ağırlıkta olduğu için bunlar oldukça zor yönetilen karmaşık konulardır. İyi yönetilmediği takdirde proje her an başarısızlığa doğru gidebilir. Bu yüzden dağıtım ve yaygınlaştırma süreçine geçilmeden başlangıçta öngörülüp, risk önlem paketlerinin hazırlanması ve sık sık kontrol edilmesi büyük önem taşır. Burada uygun çeşitli risk ölçüm metotları kullanılır. UEKAE ve NVI kendilerine ve süreçe en uygun ölçüm metodunu belirleyerek her modül için olduğu gibi bu modüle de bir risk yöneticisi atamalıdır. Risk ölçümleri, özellikle Bütünleşik Proje Yönetimi Ekibine belirli aralıklarla raporlanarak uygun stratejilerin belirlenmesinde kullanılmalıdır.

13. e-Kimlik e-Dönüşüm Etkileşimi

Vatandaş Açısından e-Kimlik e-Dönüşüm Etkileşimi:

Elektronik devlete geçiş süreci hızlanacaktır. Vatandaşların devlet daireleri arasında dolaşmak zorunda kalmadan, gereksiz zaman ve iş gücü kaybına neden olmadan kamu hizmetlerinden yararlanmaları sağlanacaktır. Vatandaş açısından salacak faydalar aşağıda özetlenmiştir:

a. Uluslararası standartlara uygun, her çeşit taklit, tahrif ve sahteciliği ortadan kaldıracak özelliklerde kimlik kartına sahip olmak,

b. Kamu hizmetlerine hızlı ve güvenli bir şekilde erişmek,

c. Kamu hizmetlerinin tek bir noktadan alabilmek (e-Devlet dönüşümüyle kamu kurum ve kuruluşlarının T.C. Kimlik Numarası vasıtasıyla tam entegrasyonu sonucu vatandaşın, askerlik, pasaport, iş başvuru ve noterlik işlemleri vb.),

d. Hizmet alımı giderlerini azaltmak,

e. Vatandaşa ait bilgilerin mahremiyetini sağlamak,

f. Elektronik ortama alınan hizmetleri herhangi bir talep ettiği zaman aralığında gerçekleştirmek (7/24),

Kamu Kurumları Açısından e-Kimlik e-Dönüşüm Etkileşimi:

Kamu teşebbüslerin sundukları hizmetlerin elektronik devlet yapısı altına alınması artan kalite e-Kimlik ile sürdürülecektir. Kamu kurumlarına sağlanacak getiriler şöyledir:

a. Kurumlar tarafından sunulan hizmetin özelliğine göre farklı güvenlik seviyelerinde kimlik doğrulama yöntemleri (şifre, fotoğraf, biyometrik veri) kullanılarak doğru kişinin hizmet alınmasını sağlamak,

b. Hizmet sunumu sırasında hizmete katılan (görevli) ve hizmetten yararlanmak isteyen (vatandaş), birlikte orada olduğunu tespit edilmesini sağlamak,

c. Kurumlar arası iletişimde vatandaşın kimlik bilgilerinin çevrimiçi olarak hızlı bir şekilde paylaşılması ile zamandan tasarruf edilmesi,

d. Kimlik kartı ve elektronik kimlik doğrulama sisteminin sosyal güvenlik alanında başlatılması bu alandaki kaçakların önüne geçerek sosyal güvenlik açığının azaltmak,

e. İhtiyaç duyulan verilere elektronik ortamda ulaşılmasını kolaylaştırmak,

f. Kamu kurum ve kuruluşları arasındaki bilgi akışını hızlandırmak,

g. Kimlik kartı işlemlerini, hukuki ve teknik olarak bir merkezden denetlenebilir hale getirmek,

h. Özel ve resmi işlemlerde sahteciliği en aza indirerek "mal güvenliği" ve "kişi haklarını" sağlamak,

i. Suçlu takibi ve yakalanmasında kolaylık ve hızlı kimlik tespit imkanı sağlamak,

j. T.C. Kimlik Numarası sayesinde sağklanan tasarrufu güvene almak: Kişinin birden fazla sağlık dosyası olmasını engellemek, sağlık bilgilerinin birleştirilmesini kolaylaştırmak ve doğru kişinin hizmetlerden yararlanmasını sağlamak,

k. Eğitimle ilgi kayıt ve sınav gibi işlemlerde doğru kişinin hizmetlerden yararlanmasını sağlamak,

l. Davalarda kimlik tespitlerinin daha hızlı ve doğru bir şekilde yapılmasını sağlamak gibi birçok faydası olması hedeflenmektedir.

Özel Sektör Açısından e-Kimlik e-Dönüşüm Etkileşimi:

Elektronik devlet yapısı özel sektör için de pek çok fayda içermektedir. Bunlardan bazıları aşağıda verilmiştir:

a. Vatandaşın yaptığı işlemden sonra vatandaşın kimliğini doğrulamada kullanılan nüfus cüzdanı benzeri belge fotokopi ihtiyacı elektronik olarak gerçekleştirmek,

b. Ayrı personel kartı ihtiyacına gerek kalmaması,

c. Stadyum ve sinema salonlarında kimlik kontrolünün hızlı bir şekilde gerçekleştirilmesi,

d. Seyahat uygulamalarını desteklemesi,

e. Çevrimiçi bankacılık işlemlerinin gerçekleştirilmesi,

f. İnternet ortamındaki alışverişin güvenliğinin arttırılması,

İş Süreçleri Açısından e-Kimlik e-Dönüşüm Etkileşimi:

Nüfus müdürlüklerine yapılan başvuru ve bilgi toplama işlemleri elektronik ortamda yapılmaktadır. Oluşturulan veri tabanı ile tüm işlemler güvenilir ve güncel olarak çevrimiçi gerçekleşecektirilmektedir. Dış temsilciliklerce de Kimlik Paylaşımı Sistemi vasıtasıyla nüfus kayıtlarına erişilerek kimlik kartları düzenlenecektir.

Kimlik kartının kişiselleştirilme işlemleri nüfus müdürlüklerinden toplanan bilgiler ve yapılan taleplerle doğrudan bulunulan yer nüfus müdürlükleri ile dış temsilciliklerce yapılacaktır.

Kimlik kartının sahibine teslimi, kimlik doğrulaması yapılmak suretiyle yapılacaktır. Ayrıca parmak izi bilgisi de kontrol edilecektir.

Yeni sistemler tüm bu iş süreçlerinin güvenliği arttırılacak ve sahteciliğin önü alınacaktır.

Organizasyon Açısından e-Kimlik e-Dönüşüm Etkileşimi:

Kimlik kartı üretiminin, ilklendirilmesinin ve kişiselleştirilmesi elektronik ortamda olduğundan uygulamacıya yükü az olacaktır.

Yerleşim açısından da seçilecek yaygınlaştırma sistemine göre (dağıtık veya merkezi) ihtiyaç duyulan yerlerin yerleşim yapısında iyileştirmeler yapılacaktır.

Uygulama Açısından e-Kimlik e-Dönüşüm Etkileşimi:

- İşlemler elektronik ortamda yapılacak ve bu yeni süreç bugünkü mevcut uygulamadan iyileştirmeler getirecektir.
- Kimlik kartı ilklendirme kişiselleştirme işlemi yaygınlaştırma raporunda belirlenecek kurumlarca yapılacaktır.
- Yongalı kimlik kartı ilk uygulama olacaktır.
- Parmak/Damar izi bilgisinin kullanılması da yeni bir uygulama olacaktır.

Veri Açısından e-Kimlik e-Dönüşüm Etkileşimi:

- Fotoğraf ve biyometrik veriler, kişinin mahremiyeti dikkate alınarak, sadece kart yongasında tutulacağından MERNİS veri tabanında değişiklik gerekmeyecektir
- Fotoğrafların elektronik ortama aktarılması ile birlikte görsel kimlik doğrulaması daha kolay hale gelebilecektir.
- Kişilerin parmak izi bilgileri vektörel bilgi (minutae) olarak alınacaktır. Kimlik kartının tesliminde, bu veriler kullanılarak birebir kontrol yöntemi uygulamasıyla sahtecilik önlenecektir.
- Vatandaşlardan Adres Kayıt Sistemi ile bugüne kadar elde edilemeyen veya bildirilmeyen adres değişikliği bilgileri de bu proje kapsamında elde edebilecek veya bu konudaki muhtemel yanlışlıklar ile eksiklikler de düzeltilebilecektir.

Teknoloji Açısından e-Kimlik e-Dönüşüm Etkileşimi:

- Veri toplama sürecinde her türlü kişisel bilgiler elektronik olarak kartta depolanacaktır.
- Kullanılan nüfus cüzdanları yerine yeni elektronik kimlik kartları verilecektir.
- Kimlik kartı tesliminde ve gerçek sahibinin kontrolünde, parmak izi bilgisi kullanılacaktır.
- Kimlik kartları en son teknolojilerle üretilecektir.
- Başvurudan kimlik kartının vatandaşa teslimine kadar olan tüm süreçler elektronik olarak ve çevrimiçi kontrol edilecektir.

KAYNAKÇA

[1] Yüksel Arslan, Osmanlıdan Günümüze Çankırı Örneğinde Kimlik Belgeleri.
[2] Nüfus ve Vatandaşlık Hizmetlerinde e-dönüşüm (2003-2007).
[3] Dr. H. Tuğba Eroğlu, e-Devlet Uygulamaları Çerçevesinde MERNİS Projesi ve Beklentiler.

UYUSAL AKILLI KART TÜMDEVRESİ

Yaman ÖZELÇİ

Akıllı Kart Tabanlı Elektronik Kimlik Doğrulama Sistemi Geliştirimi ve Vatandaşlık Kartı Tasarımı projesinin temel adımlarından biri kimlik kartı olarak kullanılacak akıllı kartların ulusal olarak geliştirilmesidir. Proje çerçevesinde ulusal kimlik kartı olarak kullanılacak akıllı kart tümdevreleri tamamen özgün olarak UEKAE Yarıiletken Teknolojisi Araştırma Laboratuarı (YİTAL) Tümdevre Tasarım grubu tarafından tasarlanmış, yurtdışında ürettirilerek Bolu'daki pilot uygulamada denenmiştir.

Tüm vatandaşlarımıza kimlik kartı olarak dağıtılacak akıllı kartların;

- Yüksek güvenlikli,

- Düşük maliyetli,

- Zaman içinde gelişen yeni gereksinmeleri kolayca karşılayacak

şekilde geliştirilmesi gereklerinden dolayı, akıllı kart tümdevrelerinin tasarımının uygulamaya özgü olarak enstitümüz tarafından gerçekleştirilmesi bir zorunluluk olarak görülmüştür. Bilgi güvenliği konusunda benzer projeleri başarı ile tamamlayan enstitümüzün bünyesinde bulunan YİTAL'de bu tümdevre tasarlanmıştır. Tasarım çalışmalarına Mayıs 2006'da başlanmış, 2007-2009 arasında gerçekleştirilen dört deneme üretimi ile tasarım son halini almıştır. Kasım 2009'da başlanan pilot üretim sonucunda ürettirilen akıllı kartlar Şubat 2010'dan itibaren Bolu'da vatandaşlara dağıtılmaya başlanmıştır.

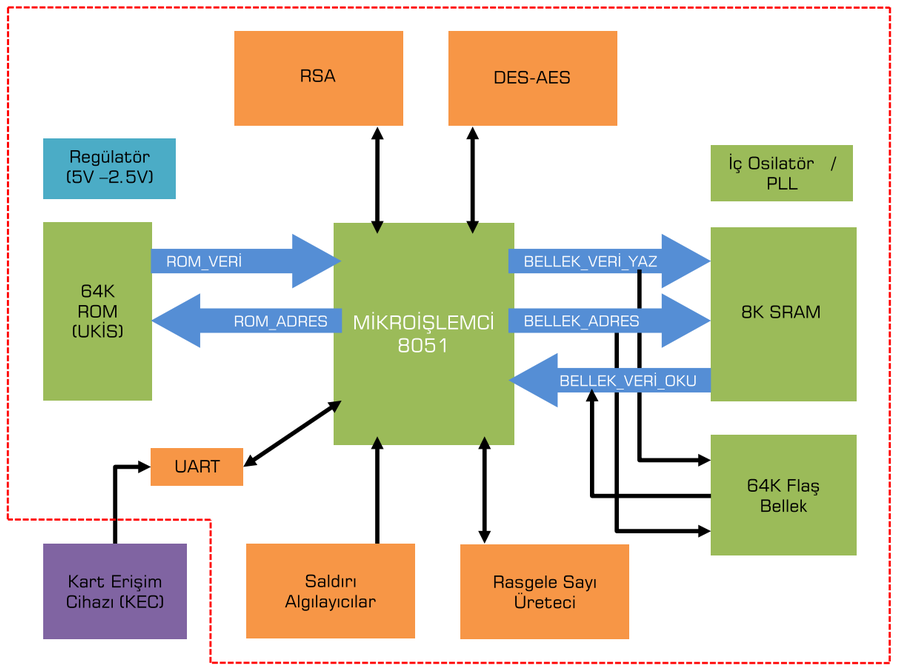
Kimlik kartı ya da sağlık kartı olarak kullanılabilecek bu kartlarda kişilere özel bilgiler saklanacağından, bu verilerin başka kişilerin eline geçmesine, kartların kopyalanmasına karşı tümdevre tasarımında gerekli önlemler alınmıştır. Bu amaçla geliştirilen kartların CC EAL 5+ güvenlik sertifikası alabilecek şekilde tasarlanması hedeflenmiştir.

Aşağıda teknik özellikleri ayrıntılı olarak tanıtılacak akıllı kart tümdevresinin, yeri geldikçe ticari ürünlerle performans kıyaslaması yapılacaktır. Tasarım, üretici bağımlılığını kaldırmak için birden fazla üretici firmanın teknolojisine ve tasarım kütüphanesine göre uyarlanarak ürettirilmiştir.

Genel Yapısı

Ulusal akıllı kart tümdevresinin blok yapısı Şekil 1'de verilmiştir.

Tümdevre, 8051 tabanlı bir mikroişlemci ile bu işlemcinin eriştiği farklı türde bellek yapıları (ROM, SRAM, Flaş Bellek), kripto algoritma blokları (RSA2048, DES-3DES,AES256), kart okuyucu arayüzü (UART), rasgele sayı üreteci ve dış saldırıları sezmeye/engellemeye yönelik güvenlik devrelerinden oluşmaktadır.



Şekil 1. *Geliştirilen akıllı kart tümdevresinin blok yapısı.*

8051 Mikroişlemci: Standart bir 8051 işlemcisinin tüm komutlarını gerçekleştiren mikroişlemci bloğu, tümdevrenin sağlaması gereken güvenlik koşullarına göre özel olarak tasarlanmıştır. Mikroişlemci ROM'dan okuduğu işletim sistemi komutlarını işlemekte, bu sırada gerek duyduğu bellek işlemleri için kendi 256 byte'lık iç belleği ile 8 KB'lık statik belleği kullanmaktadır.

ROM: Enstitümüz tarafından proje çerçevesinde geliştirilen Ulusal Akıllı Kart İşletim Sistemi (UKiS) 64 KB'lık ROM bloğuna üretim sırasında yerleştirilmektedir.

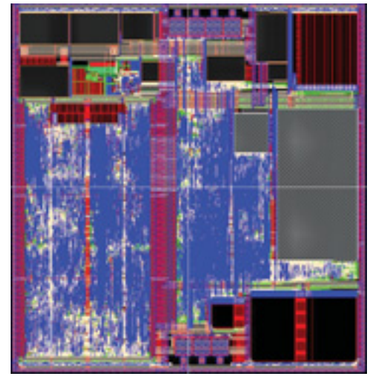
Flaş Bellek: Kişisel bilgiler, sertifikalar, anahtarlar gibi besleme gerilimi olmadığı durumda da sürekli saklanması gereken veriler 64 KB'lık flaş bellekte tutulmaktadırlar.

Kripto Algoritma Blokları: Tümdevre, işletim sistemine simetrik kripto algoritmaları DES-3DES ve AES 256 ile, asimetrik kripto algoritması RSA 2048 işlemlerini tam donanımsal olarak gerçekleştirme hizmeti vermektedir. Gerek kripto bloklarına gerek flaş belleğe UKiS'in erişebilmesi için gerekli erişim kütüphane yazılımları da tümdevre tasarımıyla beraber geliştirilmiştir.

Rasgele Sayı Üreteci: Rasgele sayı üretme bloğu, akıllı kart tümdevresinin çalışma sırasında gerek duyduğu FIBS-120 standartlarına uygun rasgele sayıları tam donanımsal olarak üretmektedir.

Saldırı Algılayıcılar: Saldırı algılayıcı bloğun işlevi, tümdevrede saklı gizli bilgileri ortaya çıkarmayı hedefleyen bir saldırganın müdahelesini sezdiği anda tümdevrenin çalışmasını durdurup saldırıyı engellemesidir.

UART Bloğu: UART bloğu, akıllı kart tümdevresi ile kart okuyucu arasındaki ISO/IEC 7816-3 standartlarına uygun haberleşmeyi sağlamaktadır.



Şekil 2. *Akıllı kart tümdevresi serim tasarımı.*

İç osilatör/ PLL Blokları: Tümdevrenin çalışması 5 MHz'lik iç saat osilatörü ile sağlanmaktadır. PLL bloğu ile bu saat işareti gerektiğinde hızlandırılarak işlem süreleri kısaltılmaktadır.

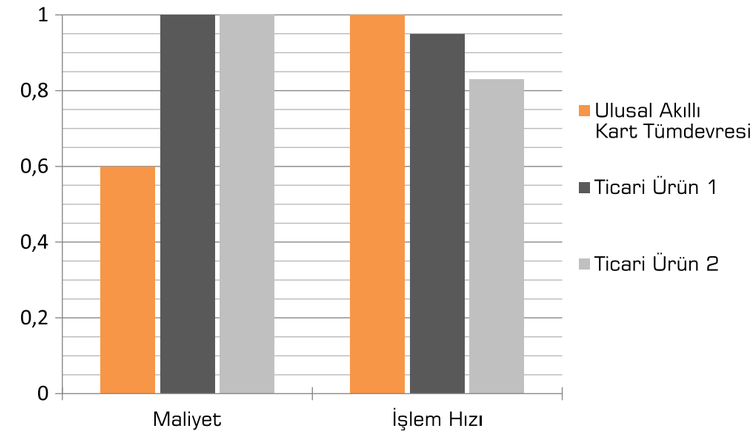
Gerilim Regülatörü: Gerilim regülatörü, devreye dışarıdan uygulanan 3.3V- 5V arasındaki besleme geriliminden yararlanarak , devre içinde kullanılan 2.5 V'luk iç besleme gerilimini üretmektedir.

0.25μm 5-metal CMOS e-Flaş teknolojisi kullanılarak tasarımı gerçekleştirilen ulusal akıllı kart tümdevrenin serimi Şekil 2'de verilmiştir. 8051 mikroişlemci, DES-3DES, AES ve RSA kripto blokları, rasgele sayı üreteci, saldırı algılayıcıları, UART bloğu proje gereklerine göre tamamen özgün olarak tasarlanmışlardır. Statik bellek, ROM, flaş bellek, iç osilatör ve gerilimregülatörleri üreticiden hazır olarak alınmışlardır. Tümdevre flaş bellek hariç 2.2 milyon tranzistör içermektedir.

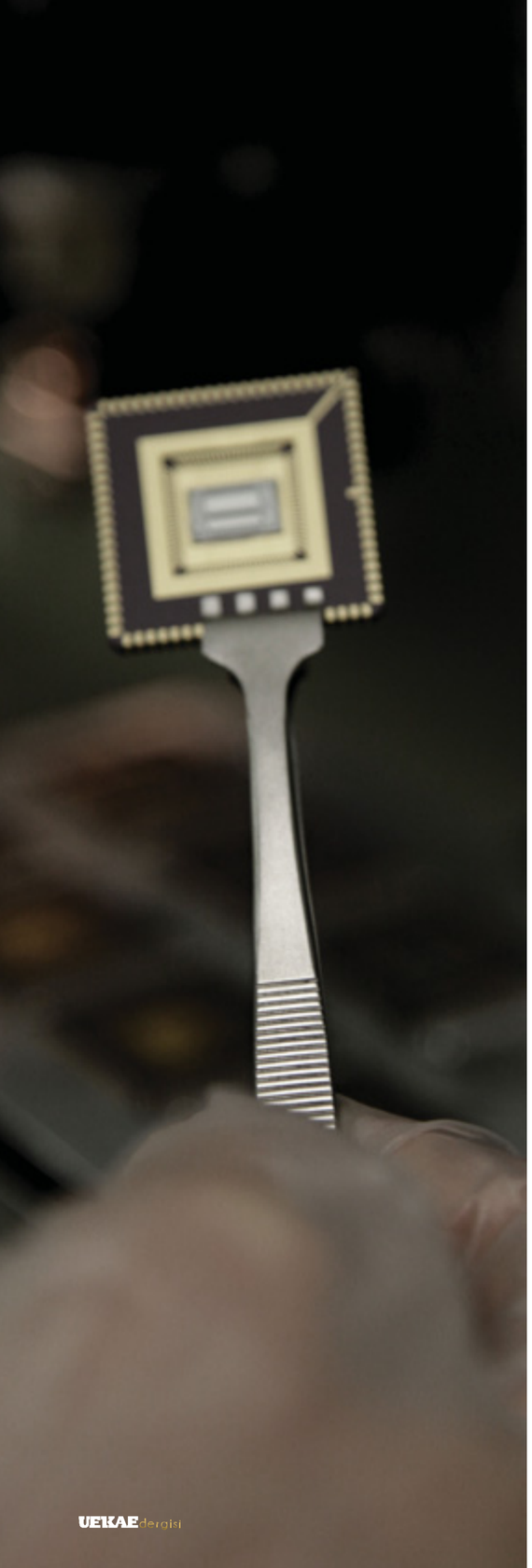
Şekil 3'te, geliştirilen ulusal akıllı kart tümdevresinin piyasada bulunan iki farklı ticari ürünle işlem hızı ve tümdevre maliyeti açısından karşılaştırılması verilmiştir. İşlem hızı, proje çerçevesinde geliştirilen Kart Erişim Cihazı (KEC) kullanılarak akıllı kartlara yaptırılan doğrulama işlemlerinin tamamlanma sürelerinden yararlanılarak belirlenmiştir. Ulusal akıllı kart tümdevresinin her iki ticari ürüne göre daha hızlı çalıştığı şekilden görülmektedir. Tümdevre maliyeti ise, bir tümdevrenin üretim ve akıllı kart modülüne kılıflanma maliyetini göstermektedir. Ulusal akıllı kart tümdevresinin maliyeti ticari ürünlerin maliyetinin yarısı mertebesindedir.

Güvenlik Önlemleri

Proje gereklerinden biri, üretilen akıllı kart tümdevresinin CC EAL 5+ sertifikası almasıdır. Bu sertifika tümdevrenin en yüksek profilli saldırganın dahi saldırılarına karşı dayanıklı olmasını gerekmektedir. Tümdevre tasarımında en fazla emek ve zaman güvenlik önlemlerinin geliştirilmesi için harcanmıştır.



Şekil 3. *Ulusal akıllı kart tümdevresinin maliyet ve işlem hızı açısından iki ticari ürünle normalize değerler bazında karşılaştırılması.*



Vatandaşların taşıyacağı akıllı kartlarda parmak izi gibi kişiye özel bilgiler saklanacaktır. Uygulamada kartlardaki bu bilgileri elde etmeye, kartları kopyalayarak sahtelerini üretmeye çalışacak kötü amaçlı kişilerle karşılaşılacaktır.

Tümdevrede saklı gizli bilgileri elde etmeyi hedefleyen bir saldırganın yapabileceği saldırılar ve tasarımda bunlara karşı alınan önlemler aşağıda özetlenmiştir:

1- Tümdevrenin çalıştığı dış ortam koşullarının izin verilen sınırların dışına çıkartılıp tümdevreye hata yaptırılmaya çalışılması:

Bir saldırgan tümdevrenin çalıştığı ortamın sıcaklığını, tümdevreye verilen besleme gerilimin değerini ya da dışarıdan uygulanan saat işaretinin frekansını izin verilen çalışma değerleri dışına çıkararak tümdevreye hata yaptırabilir. Tümdevre bu tür saldırıların sezilmesi halinde çalışmasını durduran algılayıcılara sahiptir.

Sıcaklık algılayıcısı, tümdevrenin çalıştığı ortamın sıcaklığını ölçerek, ortamın izin verilen sıcaklık aralığından yüksek ya da düşük olup olmadığını sezmektedir.

Besleme gerilimi algılayıcıları gerek dışarıdan uygulanan besleme geriliminin gerekse bu gerilimden yaralanılarak devre içinde regülatörler tarafından üretilen iç besleme geriliminin izin verilen sınır değerlerden yüksek ya da düşük olması durumunda devrenin çalışmasını durdurmaktadırlar. Saldırganın devreye hata yaptırmak üzere dış besleme gerilimi üzerine bindireceği çentik biçimdeki işaretlerin sezilmesi yine besleme gerilimi algılayıcıları tarafından gerçekleştirilmektedir.

Saldırganın tümdevreye dışarıdan uygulanan saat işaretinin frekansını sınırların üzerine yükselterek tümdevreyi hatalı çalıştırmasına, ya da düşürerek tümdevreyi adım adım çalıştırmasına engel olmak için farklı yöntemler uygulanmıştır. Tümdevre dış saat işareti ile değil, bu işaretten bağımsız olarak kendi içinde ürettiği, saldırganın dışarıdan müdahele edemeyeceği iç saat işareti ile çalışmaktadır. Dış saat işareti yalnızca kart okuyucu ile kart arasındaki haberleşmede kullanılmaktadır. Bununla birlikte, gerek dış saat işaretinin gerekse iç saat işaretinin frekanslarının izin verilen frekans aralığından yüksek ya da düşük olduğunda devrenin çalışmasını durduran frekans algılayıcıları da devrede bulunmaktadır.

2- Tersine mühendislik saldırıları:

Saldırgan tümdevreyi oluşturan tabakaları çeşitli kimyasal ya da fiziksel yöntemlerle adım adım kaldırarak, her tabaka kaldırıldıktan sonra tümdevreyi mikroskop altında inceleyerek tasarım ve güvenlik önlemleri konusunda bilgi edinmeye çalışabilir. Çok emek ve zaman gerektiren ve tümdevreleri tahrip eden bu tür saldırıların yanında, FIB (*Focused Ion Beam*) türü çok pahalı aygıtlar kullanılarak, tümdevre tahrip edilmeden üzerinde istenilen bölgeler aşındırılıp, istenilen bağlantılar yapılarak, kritik bilgi taşıdığından şüphelenilen hatlar tümdevre yüzeyinde oluşturulan adacıklara bağlanabilir ve bu adacıklara mikroskop altında iğnelerle dokunularak işaretler osiloskopla incelenebilir. Bu tür saldırılara karşı tümdevre tasarımında çeşitli önlemler alınmıştır:

a-) Tümdevre yüzeyi en üst düzey metal olan metal-5 seviyesinde paralel hatlarla kaplanmıştır. Tümdevre çalışırken aktif kalkan olarak adlandırılan bu hatlarda kısa devre ve açık devre denetimleri yapmaktadır. Saldırganın tümdevrenin alt düzeylerindeki bağlantılara ulaşmak için bu paralel hatlarda oluşturmak zorunda kalacağı kısa devre ya da açık devreleri tümdevre sezdiği anda çalışmasını durdurmaktadır.

b-) Saldırganın UKiS'in tutulduğu ROM bloğunu oluşturan tabakaları inceleyip işletim sistemi yazılımı hakkında bilgi edinmesini engellemek amacıyla, işletim sistemi şifrelenerek ROM'a yerleştirilmiştir. Mikroişlemci ROM'dan okuduğu şifreli verileri çözdükten sonra işlemektedir.

c-) Saldırganın tümdevre serimini incelediğinde blokların yerleri konusunda bilgi sahibi olmasını engellemek amacıyla, tüm sayısal blokların serimleri birbirinin içine geçmiş şekilde karmaşık yapılmıştır. Bloklar arasında veri ve adreslerin taşındığı yollar ayırt edilemez şekilde karışık durumdadır. Buna karşın, ROM, statik bellek, flaş bellek gibi bloklar ise yapıları gereği tümdevre serimi incelendiğinde kolayca ayırt edilebilirler. Dolayısı ile bu tür blokların adres girişleri ile veri giriş ve çıkış yollarının saldırgan tarafından incelenmesi tehlikesi bulunmaktadır. Bu tehlikeyi engellemek için, verilerin ROM'da olduğu gibi statik bellek ve flaş bellek yapılarında da şifreli olarak tutulması sağlanmıştır. Mikroişlemci statik bellek ve flaş belleğe verileri şifreleyerek yazmakta, buradan okuduğu verileri de şifrelerini çözdükten sonra işlemektedir. Mikroişlemci ile kripto blokları arasındaki veri ve adres yolları da, serimde ayırt edilememelerine rağmen yine de şifrelenmişlerdir. Saldırganın bu yollardaki işaretleri izleyebildiği durumda bile haberleşmeyi incelemesi şifreleme nedeniyle mümkün olmayacaktır.

3- Lazer saldırıları:

Saldırgan tümdevreye mikroskop altında lazer atışları yaparak, lazer ışınının üzerine düştüğü bir kütüğün değerini değiştirebilir. Değeri değişen kütüğün mikroişlemcinin ya da kripto bloğunun çalışmasını etkileyen kritik bir kütük olması ve lazer atışının doğru zamanda yapılması durumunda tümdevre gizli bir bilgiyi açığa çıkarabilecek şekilde hatalı çalışabilir.

Bu tehlikeyi gidermek amacıyla, mikroişlemcinin kritik kütükleri, birbirini denetleyecek şekilde çift gerçekleştirilmişlerdir. Lazer saldırıları her iki kütüğü aynı anda ve aynı şekilde bozamayacağı için, her zaman aynı değere sahip olması gereken kütüklerin değerleri arasında bir farklılık oluştuğunda bir saldırı olduğu anlaşılmakta ve tümdevre çalışmasını durdurmaktadır. Benzer yaklaşım kripto blokların tasarımında da kullanılmıştır.

Lazer saldırılarına karşı bir diğer önlem de gerek mikroişlemcinin gerekse kripto bloklarının işlemlerinin çalışma sırasında rasgele duraklatılmasıdır. Böylece saldırganın lazer atışlarının zamanlamasını istediği işlem adımına denk düşürecek şekilde ayarlaması zorlaştırılmaktadır.

4- Yan Kanal Analizi:

Yan kanal analizi çalışmaları, devrenin çalışması sırasında beslemeden çektiği akımın ya da dışarı yaydığı elektromanyetik yayınımın kayıt edilip istatistiksel yöntemlerle analiz edilmesi yoluyla devrede saklı gizli bilgilerin ortaya çıkarılması yaklaşımına dayanır. Bu tür analizlerin ve bunlara karşı önlemlerin geliştirilmesi günümüzde son derece güncel çalışmalardır. UEKAE YİTAL tümdevre tasarım grubu da 2002-2004 tarihleri arasında AB 6. Çerçeve programı çerçevesinde SCARD (*Side Channel Analysis Resistant Design Flow*, 'Yan kanal Analizine Dirençli Tasarım Akışı Geliştirilmesi') projesine bu alanda günümüzde öncü durumunda olan endüstriyel kuruluş ve üniversitelerle beraber katılmıştır. Bu proje sırasında kazanılan bilgi birikimi ve deneyim geliştirilerek akıllı kart tümdevresinde kripto blokları tasarımının yan kanal analizine karşı dirençli olarak gerçekleştirilmesinde kullanılmıştır.

Bir kripto algoritma bloğuna şifrelenecek ya da çözülecek veri ile, bu veriyi şifreleme ya da çözmede kullanılacak anahtar değeri giriş olarak verilmektedir. Bir saldırgan, kart okuyucu üzerinden algoritmaya girilecek veriyi kontrol edebilir. Ancak anahtar değeri akıllı kartın flaş belleğinde saklıdır ve saldırganın anahtara erişme olanağı yoktur. Saldırganın amacı yan kanal analizi yardımıyla anahtarı ortaya çıkarmaktır. Yan kanal analizi, kripto algoritma bloğunun çalışması sırasında tümdevrenin beslemeden çektiği akımın algoritmanın işlediği veri ve anahtar değerlerine bağlı olmasına dayanmaktadır. Saldırgan bilmediği anahtarla bildiği verilerin bildiği algoritma bloğu tarafından işlenmesi sırasında beslemeden çekilen akımları kaydeder. Farklı giriş verileri için topladığı akım eğrilerini istatistiksel yöntemler kullanarak analiz ederek gizli anahtarı bulmaya çalışır. Analizin başarılı olması için kaydedilmesi ve işlenmesi gereken farklı eğri miktarı kripto algoritma bloğunun yan kanal analizine karşı direnci arttıkça artmaktadır.

Geliştirilen akıllı kart tümdevresinin kripto bloklarının tasarımında yan kanal analizine karşı direnci arttıran çeşitli yöntemler uygulanmıştır. İşlenecek verilerin her seferinde ayrı bir rasgele sayı ile işleme sokulduktan sonra algoritmaya uygulanması, algoritma çıkışında bir ters işlemle gerçek sonucun elde edilmesine dayanan maskeleme yöntemi bunlardan biridir. Maskeleme yöntemi, her seferinde aynı veri işlense bile rasgele sayı ile işleme sokulma nedeniyle kripto bloğunun her seferinde beslemeden farklı akım çekmesini sağlamaktadır. Uygulanan diğer yöntemlerden biri de, kripto algoritma adımlarının arasına rasgele olarak sahte işlemler yerleştirilmesidir. Sahte işlemler saldırganın uyguladığı veriler yerine rasgele verilerin işlenmesine yol açtığı için kaydedilen güç eğrilerinin istatistiksel analizlerini zorlaştırmaktadır.

DES, AES ve RSA kripto algoritmalarının her birinin farklı yapılarına bağlı olarak farklı önlemler uygulanmış ve yukarıda sözü edilen tüm güvenlik önlemleri tümdevre alanının büyümesine yol açmıştır.

Projenin Gelişimi

Akıllı kart tümdevresi geliştirme çalışmalarına Mayıs 2006'da başlanmıştır ve Şekil 4'teki zaman planında gösterildiği gibi bugüne kadar dört deneme üretimi ve bir pilot üretim yaptırılmıştır.

Projenin ilk yılı üretici firma belirlenmesi, üretici firma tasarım kütüphanesinin kurularak eldeki tasarım yazılımları ile uyumlu çalıştırılması, temel akıllı kart bloklarının tasarlanması, tasarımların yine proje çerçevesinde tasarlanan FPGA tabanlı geliştirme kartları üzerinde sınanması çalışmaları ile geçmiş ve Haziran 2007'de ilk deneme tasarımı üretime gönderilmiştir. Akıllı kartı oluşturan tüm temel blokların işlevselliğini test etmeye amaçlayan bu tasarımda analog saldırı algılayıcıları dışında diğer güvenlik önlemleri yer almamıştır. Tümdevre, işletim sistemi geliştirilebilmesi için iç ROM yerine dışarıdan takılan bir EEPROM ile çalışacak şekilde tasarlanmıştır.

İkinci yılki çalışmalarda yan kanal analizine karşı güvenlik önlemlerinin geliştirilmesi üzerine uğraşılmıştır. Akıllı kartın tüm sayısal blok tasarımları, güvenlik önlemleri göz önüne alınarak tekrar yapılmıştır. Nisan 2008'de üretime gönderilen ikinci sürüm tümdevrelere, ayrıca, işletim sisteminin dışarıdan yüklenebileceği ikinci bir 64 KB'lık flaş bellek eklenmiştir. Üzerine işletim sistemi yüklenme özelliğine sahip bu akıllı kartlar UKiS için bir geliştirme ortamı olarak kullanılmıştır.

Ekim 2008'de işletim sistemi UKiS'in ROM'a yerleştirildiği ilk tasarım olan üçüncü sürüm tümdevreler deneme üretimine gönderilmiştir.

Ürettirilen tümdevrelerin yan kanal analizi sonuçlarına dayanılarak güvenlik önlemlerinde yapılması gerekli görünen iyileştirmeler dördüncü sürüm tümdevrelerin tasarımında gerçekleştirilmiştir. Akıllı kart tasarımının son durumunu içeren dördüncü sürüm tümdevrelerin deneme üretimi Haziran 2009'da başlatılmıştır. Ağustos ayında teslim alınan sürüm 4 tümdevrelerin testleri sonucu, pilot üretime donanım tasarımını hiç değiştirmeden yalnızca işletim sistemini güncelleyerek gidilmesi kararlaştırılmıştır. Kasım 2009'da başlatılan pilot üretime ait akıllı kartlar Şubat 2010'dan itibaren Bolu'da dağıtılmaya başlanmıştır.

Neden Yurtdışında Üretim?

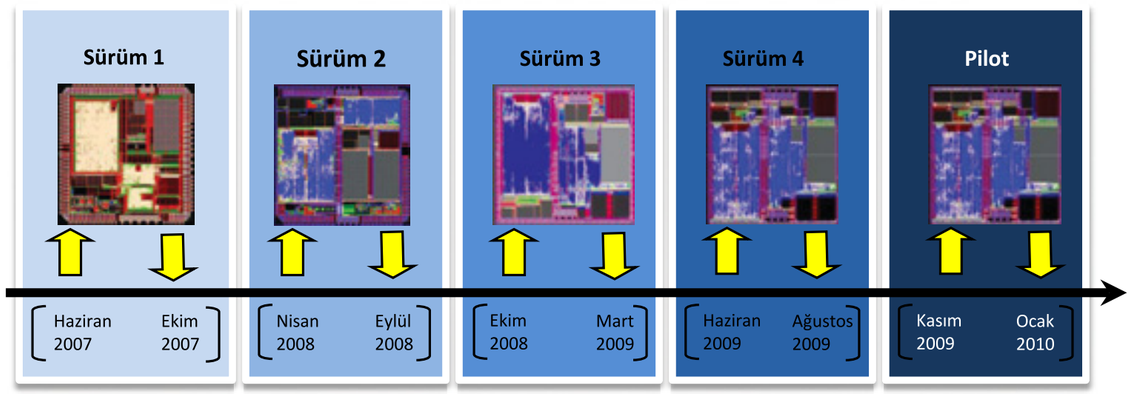
Kullanılacak akıllı kartların belirlenmesinde dört farklı yaklaşım değerlendirilmiştir.

1- Akıllı kartların yurtdışındaki bir firmadan işletim sistemiyle birlikte hazır alınıp kullanılması.

Bu yaklaşım, gerek işletim sistemi yazılımı gerekse akıllı kart donanımı tamamamen yabancı firmanın elinde olduğu için güvenlik açısından en zayıf yaklaşımdır. İşletim sistemi ve donanımın geliştirilmesine engel olan bu yaklaşım projenin ar-ge niteliğini ve kartların ulusal olma özelliğini ortadan kaldırdığı için gündeme alınmamıştır.

2- Akıllı kart işletim sisteminin yurtdışındaki bir firmanın akıllı kart donanımına uygun olarak geliştirilmesi.

Bu yaklaşım işletim sisteminin ulusal olarak geliştirilmesine olanak sağladığı için birinci yaklaşıma göre daha güvenli olsa dahi, akıllı kart donanımının içeriğinin bilinmemesi, yabancı firma denetiminde olması nedeniyle önemli güvenlik zayıflığı oluşmasını engellememektedir.



Şekil 4. *Proje süresinde gerçekleştirilen deneme ve pilot üretimlerin zaman planı.*

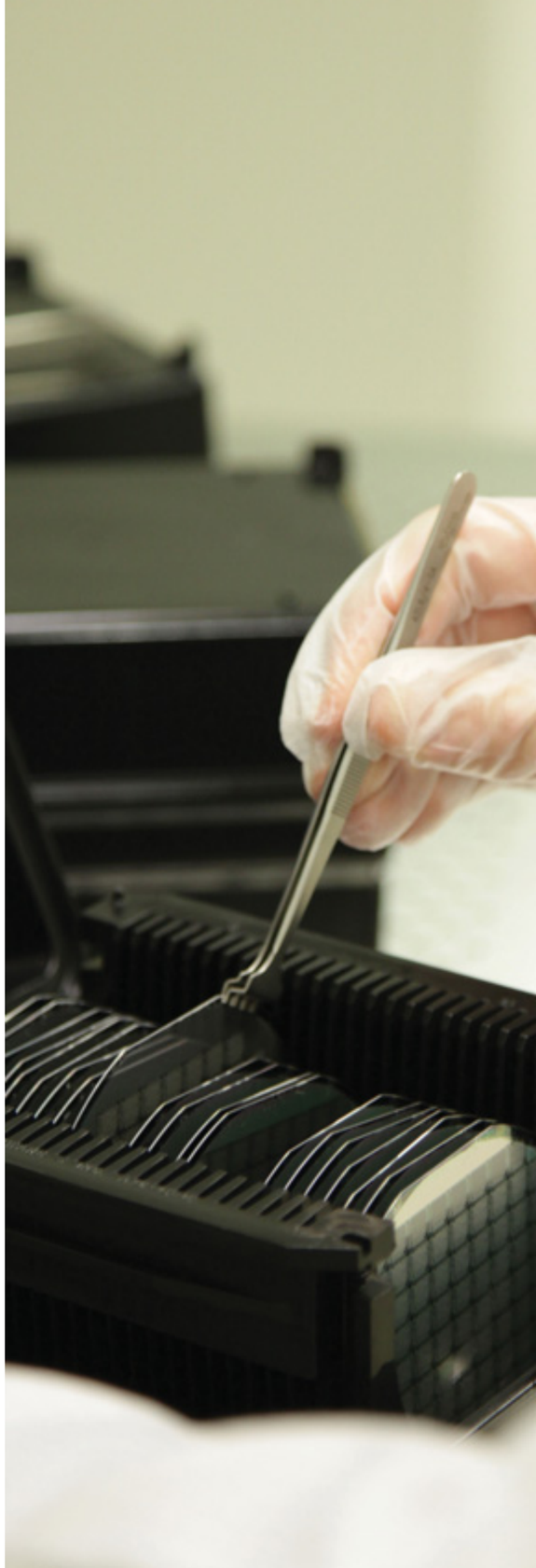
3- Gerek akıllı kart donanımının gerekse işletim sisteminin ulusal olarak geliştirilmesi, üretimin yurtdışında yaptırılması.

Donanım ve işletim sistemin ulusal olarak geliştirilmesi projenin AR-GE niteliğini tam olarak karşılamakta, bu alanda önemli bilgi birikimi elde edilmesini sağlamaktadır. Donanım ve işletim sisteminin denetiminin tamamen elimizde olması güvenlik zayıflığını önemli ölçüde gidermektedir. Olabilecek güvenlik açığı donanımı üreten firmanın tasarımı inceleyerek donanımın sahip olduğu güvenlik önlemleri konusunda bilgi sahibi olma olasılığıdır. Ancak bu işlem firmanın önemli bir emek harcamasını gerektirecektir.

4- Gerek akıllı kart donanımının gerekse işletim sisteminin ulusal olarak geliştirilmesi, üretimin Türkiye'de yapılması.

Her bakımdan en güvenli olan bu yaklaşım, Türkiye'de 100 milyon adet akıllı kart üretme teknolojisine sahip bir altyapı olmadığı için gerçekleştirilememiştir. Orijinal proje önerisinde varolan ve proje çerçevesinde enstitümüzün tümdevre üretim alt yapısını böyle bir ihtiyacı karşılayacak şekilde genişletilmesi savunan önerimiz projenin ilk değerlendirilmesi sırasında kabul edilmediği için, tasarımın ulusal, üretimin ise yurtdışında yapıldığı projenin üçüncü fazı ile sınırlı kalınmıştır. Bununla beraber ulusal kimlik kartımızı tamamen yurt içinde üretecek şekilde çalışmalarımız sürdürülmektedir.

Devletle vatandaş arasındaki işlemlerin kağıttan çıkıp tamamen sanal ortam üzerinde gerçeklenmesi ülkemiz için çok önemli bir gelişmedir. Bu projede üretilen akıllı kartların zaman içinde ortaya çıkacak yeni gereksinmelere cevap verebilmesi, güvenliğinin arttırılması, maliyetinin düşürülmesine yönelik geliştirme çalışmaları enstitümüz tarafından kesintisiz sürdürülecektir.



T.C. KİMLİK KARTI YÖNETİM VE DAĞITIM SİSTEMİ

Meral Yücel

Günlük hayatımızda önemli yer almaya başlayan yonga tabanlı kartlar banka uygulamalarından sonra artık kimlik doğrulama amaçlı da kullanılmaya başlandı. Üzerinde taklit edilmesi güç görsel güvenlik öğeleri barındıran ve elektronik bilgileri yonga içerisinde güvenli bir şekilde taşıyan kartlar; kimlik, seyahat, ehliyet, sağlık ve ruhsat gibi farklı alanlarda kullanılmaktadır.

Taşıdığı bilgiler kişiye özel olması sebebi ile elektronik kartların "yonga tabanlı değerli evrak" kapsamında yönetilmesi gerekmektedir: Elektronik Kart Yönetim Sistemleri (EKYS) kart yaşam dönemi içerisinde kart talebi, talebin kontrol edilmesi, güvenli olarak kişiselleştirilmesi, doğru kişiye kartın teslim edilmesi, kart yaşam dönemi boyunca üzerinde işlem yapılması ve kartı yok edilmesi aşamalarını gerçekleştirmek zorundadır. EKYS'ler, kart kişiselleştirme önce ve sonrasında hataları da kayıt altına alır. Ayrıca, vatandaşın kaydı, kartın teslimi, çevrimiçi (on-line) hizmetlere erişim konularında güvenli hizmet sunmak zorundadır.

EKYS'ler aslında birbirlerini tamamlayan 3 temel sistem ile iletişim halindedir. Bunlar; kart, kimlik kartı yönetimi (kayıt alma/dağıtım) ve kimlik doğrulama sistemidir.

Bu yazımızda elektronik kimlik kartını, içerdiği görsel ve elektriksel veriler açısından inceledikten sonra kimlik kartı yönetim sistemi konusu ele alınacaktır.

Geliştirilen kimlik kartı için belirlenen temel hedefler aşağıda belirtilmiştir:

- güvenli, taklit edilmesi güç kart tasarımı,
- vatandaşa tesliminin hızlı olduğu sorunsuz bir kart,
- e-Devlet ve diğer kimlik doğrulama gerektiren uygulamalara uygun kart tasarımı,
- işgücü ve ürün açısından ülke kaynaklarının maksimum kullanımı,
- dış dünyaya açılan farklı arayüzleri içeren bir kart,
- vizesiz geçişlerde kullanılmak üzere pasaport arayüzü olan bir kart
- iletişim ve erişim güvenlik özellikleri içeren bir sistem ve standartlarla uyumluluk.

Bu kapsamda ICAO 9303, ISO IEC 7816, CEN TS 15480 (ECC) standartları uygulanmıştır.

Kimlik kartları belirlenen kriterler kapsamında arayüzler, yonga özellikleri, işletim sistemi ve görsel özellikler ile yonga veri alanları açısından incelenecektir.

ELEKTRONİK KİMLİK KARTI ÖZELLİKLERİ

Kimlik Kartı Arayüzleri Kontaklı Yonga, Barkod (T.C. Kimlik Numarası), MRZ ve Kontaksız yongadan oluşmaktadır.

Kimlik kartı için kullanılan yonga çeşitleri CC EAL5+[1] onaylı NXP, INFINION[2] ve TÜBİTAK-UEKAE tasarımı olarak belirlenmiştir.

Kimlik kartı için yonga işletim sistemi EAL4+ sertifikasına sahip TÜBİTAK UEKAE ürünüdür(AKİS[3] 1.0, AKİS 1.2, UKİS[4]).

Kimlik kartı üzerindeki çeşitli görsel güvenlik öğeleri görsel doğrulamada yardımcı araçlar olarak kullanılır. 3 seviyede doğrulama yapılabilir:

1. Görsel güvenlik öğeleri çıplak gözle denetlenir. (meneviş baskı[5], gökkuşağı[6], OVI[7], MLI[8], İmza, DOVID[9], rölyef[10])

2. Görsel güvenlik öğeleri gözle net olarak görülemeyen ancak büyüteç gibi basit aletlerle ayırt edilerek denetlenir. (Örnek: raster baskı[11], mikro yazı[12], DOVID)

1 CC EAL onayı: *Common Criteria Evaluation Assurance Level*

2 NXP, INFINEON: yabancı yonga üretim fabrikaları. Ulusal işletim sisteminin bir sürümü de bu şirketlerin ürünlerinde çalışır haldedir.

3 AKİS: Akıllı kart işletim sistemi: NXP, INFINEON gibi şirketlerin yongalarında çalışır.

4 UKİS: Ulusal kart işletim sistemi: Sadece TÜBİTAK UEKAE'nin tasarladığı yongada çalışır.

5 Meneviş baskı: Guilloche, dairesel bir dizaynı tekrarlamak üzere çok karmaşık bir kombinasyon halinde karıştırılmış ve birbirine girmiş çok sayıda eğri çizgiden oluşan bir kümedir. Guilloche çizgileri, muhtemelen, banknot, hisse senedi ve pasaport gibi güvenli belgelerde kullanılan en eski güvenlik özelliklerinden biridir. Bu amaçla hazırlanmış Guilloche geliştirme yazılımı, çok karmaşık, kontrol edilebilir Guilloche çizgilerini oluşturmaya imkan sağlamaktadır.

6 Gökkuşağı: İki ayrı rengin aynı tankta karıştırılmasına olanak sağlayan, ofset baskı makinesine eklenmiş özel bir araçtır.

7 OVI (Optik Değişken Mürekkep): Görülebilirlik açısına bağlı olarak, farklı görülebilir (altın sarısından yeşile kadar) renkler sağlayan bir mürekkeptir. Optik değişken mürekkepler veya OVI, küçük özel film pulları içermekte olup, bu pullar görme açısı değişirken rengi değiştirmektedir. Sonuçta, görüş açısı değişirken rengi değiştiren aynı optik özelliğe sahip bir mürekkep ortaya çıkmaktadır. Çok pahalı mürekkepler bulunmakta olup, bunlar genellikle yalnızca küçük alanlarda kullanılmaktadır.

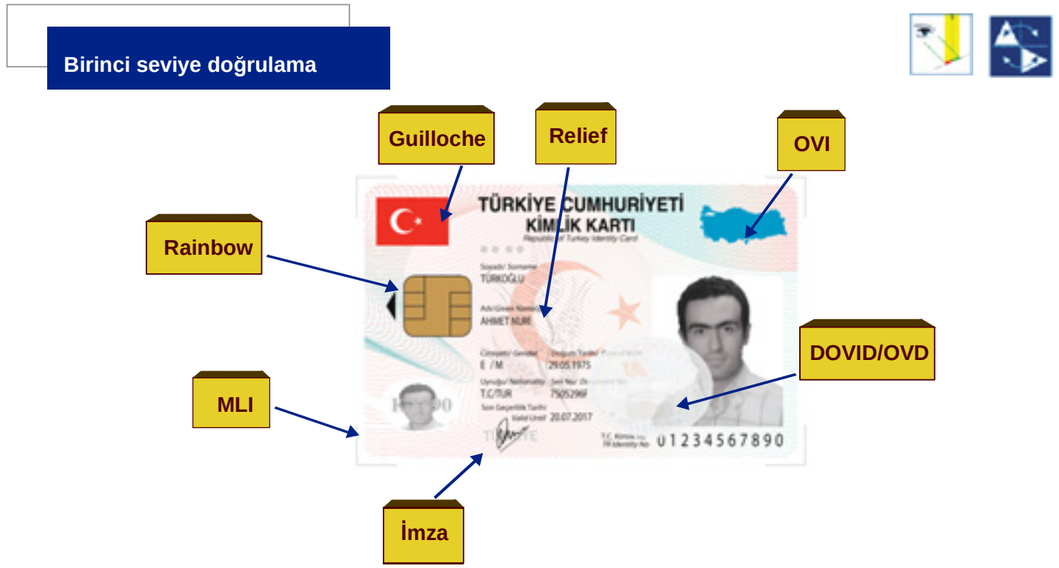
8 MLI: Kartlarda tahrifatı önlemek üzere kullanılan ve hayalet resim olarak adlandırılan nesnedir. Kişinin kartta bulunan fotoğrafının küçültülmüş niteliğinde olup kart açı aldığında resim netlik kazanmaktadır.

9 DOVID: Yansıtmalı Optik Değişken Görüntü Cihazlar ; Lazer ışınları ile elde edilen mikro yapılarla oluşturulan tasarımlardır. Bu tasarımlarla gelen ışığın yansıtma açısına göre taklit edilmesi zor olan iki veya üç boyutlu, kinematik ve renk değiştiren efektler elde edilmektedir.

10 Rolyef:Kart yüzeyinde olan ve desen niteliğini taşıyan kabartma nesnedir.

11 Raster baskı: Bu modül güvenli baskıda nadiren kullanılan geleneksel serigrafiye alternatif olarak kullanılmaktadır. Yansıtmalı ve dönmeli obje veya metinlerin tekrarlanmasıyla oluşturulan bir zeminin bir görüntü ile karıştırılmasından oluşmaktadır.

12 Mikro yazı: Küçük (<= 0,25mm) harf veya rakamlardan oluşan bir mesaj, kelime veya cümle olup, çıplak gözle okunamaz boyuttadır. Çoğu geleneksel sahtecilik tekniğinde, bu küçük mesajlar kaybolur, bu nedenle koruma açısından bu mikro yazılar ilave bir avantaj sağlar.



Şekil 1. *T.C. Kimlik Kartı görsel öğeleri 1. seviye.*

Şekil 2. *T.C. Kimlik Kartı görsel öğeleri 2. seviye.*

Şekil 3. *T.C. Kimlik Kartı görsel öğeleri 3. seviye.*

3. Görsel güvenlik öğeleri doğrulaması daha karmaşık cihazlar (mikroskop, UV ışık) kullanılarak denetlenir (DOVID, UV yazı gibi).

Kimlik kartındaki veri alanları içindeki bilgiye erişim açısından 3 kısımdan oluşur:

1. Açık veya doğrudan erişim (Fotoğraf, Sertifikalar)

2. PIN ile erişim (Elektronik İmza, Kimlik bilgileri)

3. PIN ve simetrik asıllama ile erişim: Koruma faktörü en yüksek alandır ve içinde parmak ve damar izini içeren biometrik veri bulunur. Bu alana erişebilmek için özel geliştirilen KEC[13] ve KEC'in simetrik anahtarının bulunduğu GEM (Güvenli Erişim Modülü) kartı gerekir.

Kimlik kartı yongasındaki veri alanları, kullanım sırasında oluşabilecek güvenlik açıkları analiz edilerek tasarlanmıştır.

ELEKTRONİK KİMLİK KARTI YAŞAM DÖNEMİ

Elektronik kimlik kartı yaşam dönemi, üretim, canlandırma, ilklendirme, özelleştirme, kayıt, kişiselleştirme, teslim, kullanım, imha ve iptal temel adımlarından oluşur. Özelleştirme ve kişiselleştirme işlemleri sırasında kartın üzerine ve yongasına kişisel bilgiler ile birlikte sertifika yazılır. Sistem PKI (Açık Anahtar Altyapısı) ile tümleşik çalışır ve karta gerekli sertifikalar yüklenir.

Kart yönetim sistemi mimarilerinde, kişiselleştirme açısından dağıtık ve merkezi olmak üzere iki temel yaklaşım vardır. Bunlar ülkenin coğrafi yapısı, nüfus dağılımı, dağıtım planının mali etkisi gibi sebepler dikkate alınarak seçilir. Aralarındaki temel fark kartın vatandaşa nasıl teslim edileceğidir; dağıtıkta anında, merkezide ise kişiselleştirme işlemi tek noktada yapılacağı için daha sonra teslim edilir.

Dağıtık mimari, sunucuda kart yönetim kısmı ve alt birimlerdeki kart kayıt alma, kişiselleştirme ve teslim aşamalarını gerçekleştiren öğelerden oluşur. Bu birimler kart basma makinaları ve kayıt alma sırasında kullanılan diğer araçlar ile entegredir (tarayıcı, yazıcı). Kart vatandaşa başvurusu ile birlikte 10 dakika içinde teslim edilir. Bu sürede kart yüzeyi kişiye göre düzenlenmiş ve yonga içine gerekli bilgiler yazılmış olur. Dağıtık mimaride, baskı makinaları her birimde yer aldığı için bakım hizmetleri önem kazanır.

Merkezi mimaride kişiselleştirme, yüksek baskı hızına sahip makinalar kullanarak yapılır. Merkezi baskıyı yöneten yazılım modülü, dağıtık olarak alınan kayıtların kontrollü bir şekilde basılmasını sağlar, paketler ve envanterini tutar. Bu mimaride kart sahipleri, kartını anında alamayacaktır, yapılan planlamaya göre posta ile gönderilir veya kişi kayıt verdiği birimden kartını alır.

Merkezi mimaride vatandaş kaydını ilgili birimden verirken kişisel bilgileri ve parmak izi alınır, merkeze gönderilir. Merkez sırası gelen peketleri basar ve kayıt alınan birimlere geri gönderir. Vatandaş kendisine bildirilen zamanda kayıt alma birimine giderek kartını teslim alır ya da posta ile gönderilir.

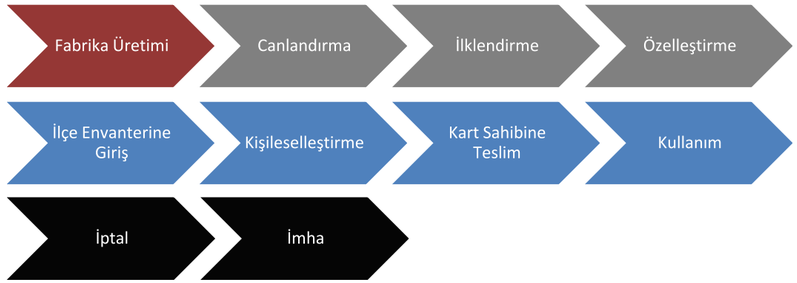
Bu süreçte vatandaş kartının durumunu (talep, basılma, dağıtılma, teslim gibi) internet üzerinden takip eder.

[13] KEC: Kart erişim cihazı, internet üzerinde elektronik hizmet veren kurumların uygulamalarında, elektronik kimlik doğrulama gerçekleştirilmesi amacıyla tasarlanan Elektronik Kimlik Doğrulama Sistemi'nin uç birim cihazlarından biridir.

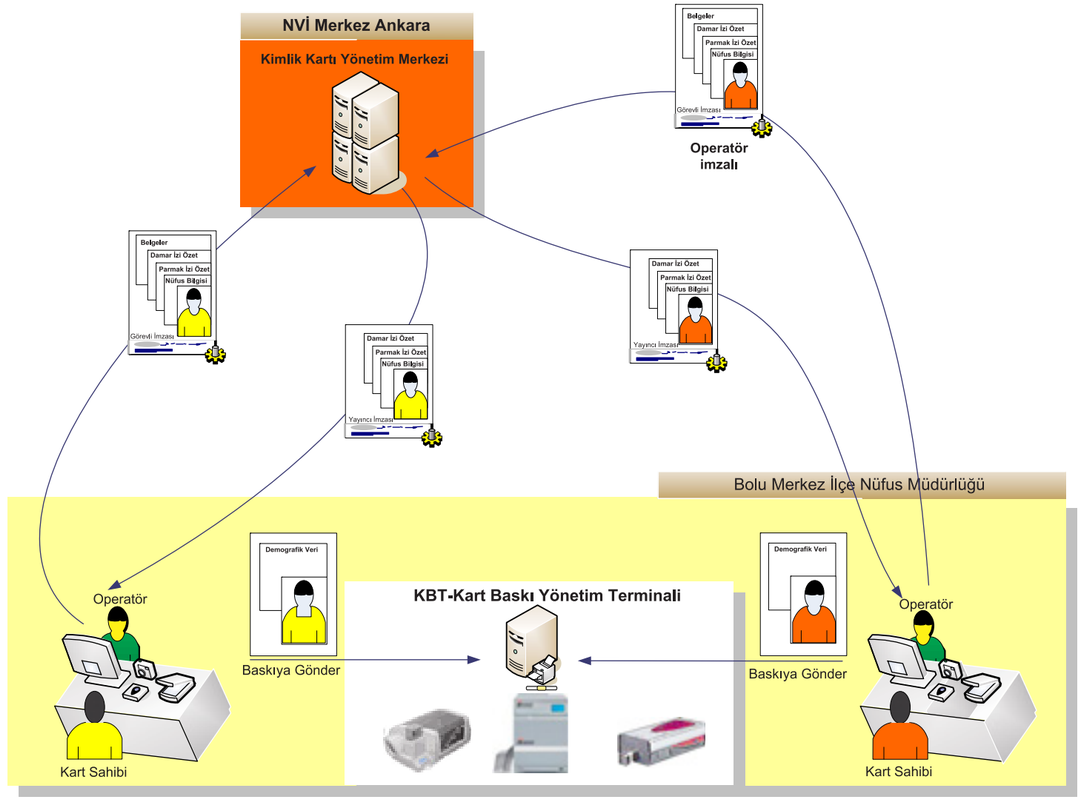
Bu sistemde kart sahibi, kimlik kartını müracaatından 1-2 hafta sonra teslim alabilecektir. Ayrıca kart kaydı (talep) ve teslim alma işlemleri için en az iki defa nüfus müdürlüğüne gidecektir. Ancak sistemde boş kartlar tek noktada depolandığı için sistemin daha güvenli olduğu söylenebilir. Merkezi sistemin yapısı şekilde verilmiştir:

ELEKTRONİK KİMLİK KARTI YÖNETİM SİSTEMİ YAZILIM MODÜLLERİ

Kart Yönetim Sistemi yazılımı modüler yapıda, java tabanlı ve J2EE teknolojisi kullanılarak hazırlanmıştır. Modüller masaüstü ve WEB hizmet uygulamalarından oluşmaktadır, sistemin yapısı gereği çok sayıda donanım ile entegrasyon gerçekleştirilmiştir.



Şekil 4. *T.C. Kimlik Kartı yaşam dönemi.*



Şekil 5. *T.C. Kimlik Kartı yönetim sistemi dağıtık mimari.*

Sistemi oluşturan modüller:

KEYS: Üretim ve özelleştirme aşamasında kullanılan Kart Envanter Yönetim Sistemi.

KYM : İmzalama, onaylama, MERNİS kontrolü gibi işlemlerin yapıldığı Kart Yönetim Merkezi.

KYB: Kayıt alma, kart teslim, bloke kaldırma, kart envanter, kart kişiselleştirme, kart iptal gibi işlemlerin yapıldığı Kart Yönetim Birimi.

KBT : İlçe Nüfus Müdürlüğündeki çoklu terminalin birden fazla kart basım makinasını kullanmasına olanak veren ortak Kart Baskı Terminali.

MATBAA : Merkezi kimlik kartı kişiselleştirme ve paket yönetim işlemini yerine getiren modül.

MOBİDES : Gezici Kimlik kartı kişiseleştirme talebi toplama birimi.

KRSWEB: Web tabanlı rapor izleme modülü.

KYS: Sistemi yöneten işlemlerin gerçekleştirildiği modül.

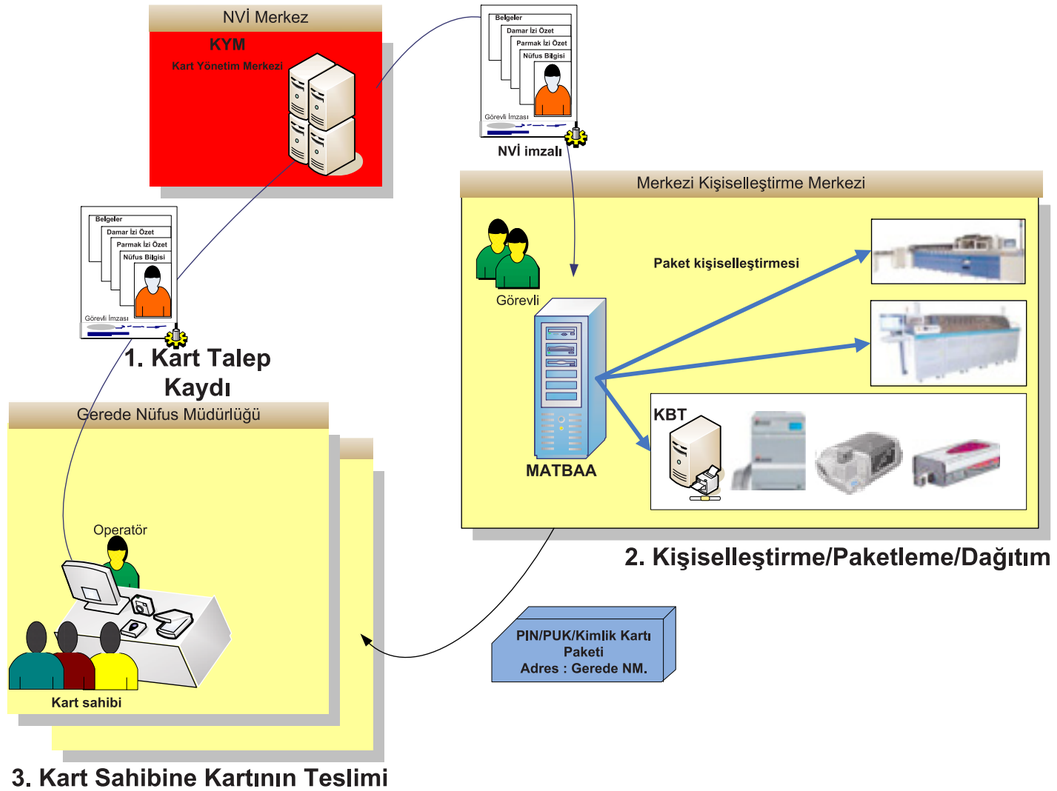
NEKSIS: KYB kart envanter yönetimi modülü.

KAPSİS: İnternet üzerinden kart durumların sorgulanmasını sağlayan sistem.

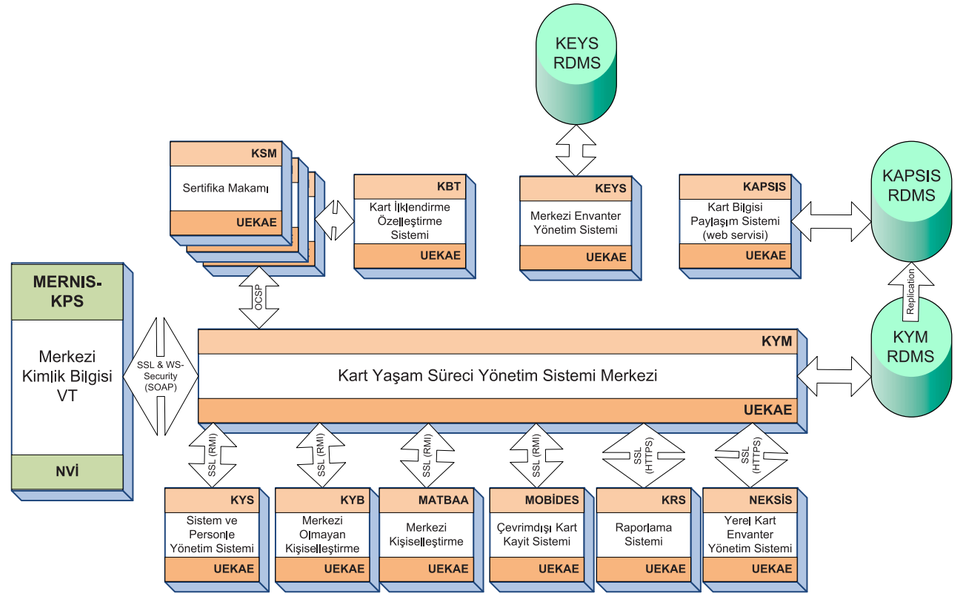
PİLOT UYGULAMA SONUÇLARI

Kart Yönetim Sistemi pilot çalışma olarak gerçekleştirilmiş ve aşağıdaki senaryoların sağlaması yapılmıştır:

- Kart kayıtları için vatandaş randevulu ve randevusuz olarak çağırılmıştır, merkezi ve dağıtık olarak kartlar basılmıştır.
- Vatandaşa gidilerek MOBİDES aracı ile mobil olarak kayıtlar alınmıştır.
- Merkezi basılan kartların kayıt alınan birimlerden, kurye ve MOBİDES Memuru İle teslimi gerçekleştirilmiştir.



Şekil 6. *T.C. Kimlik Kartı yönetim sistemi merkezi mimari.*



Şekil 7. *T.C. Kimlik Kartı yönetim sistemi yazılım modülleri.*

Bu çalışmayla projenin yaygınlaştırılmasına ışık tutacak aşağıdaki tecrübeler edinilmiştir:

- e-Kimlik kartlarının tasarımı ve dağıtımı konusunda amaç ve hedeflerin belirlenmesi önemlidir: Kullanımda güvenliği arttırmak, kısa sürede dağıtmak, temaslı/temassız yonga içermesi amaçlara örnek verilebilir (Kısa sürede dağıtılmak hedefleniyor ise bu doğrultuda yaygınlaştırma planlanır ya da kapı geçişlerinde kullanılması hedefleniyor ise temassız yonga kullanılması sağlanır).
- Kırsal kesimde yaşayan vatandaşlar için, *parmak izi ile kimlik doğrulamada* zorluklar yaşanabilir
- e-Kimlik kartlarının hızlı bir şekilde yaygınlaştırılması için uygulamaların sayısı arttırılmalıdır. Bu konuda bankalar, devlet daireleri (tapu, vergi dairesi gibi) gibi kurumların işlemlerinde güvenlik öğeleri taşıyan uygulamaları örnek verilebilir.
- Personelin kart dağıtım organizasyonuna etkisi büyüktür. Personelin başarısına bağlı olarak;
  - Parmakizi başarımı artmaktadır.
  - Hata/Arıza girişlerinin daha düzenli girilmekte hatalarda ve azalma görülmektedir.
  - Kart verme hızı artmaktadır.
- Kart kayıt ve teslim işlemleri sırasında banko sistemi yerine masa üzerinde işlemlerin yapılmasının daha verimli olduğu görülmüştür.
- Dağıtık mimaride kart basma makineleri için bakım/destek çalışmalarının planlanması gerekmektedir.
- Mobil kayıt sistemi ile vatandaşa giderek kayıt almak vatandaş için memnuniyet vericidir ve kendisinin ilçeye gelmeden kart almasını sağlar.
- Merkezi mimaride vatandaş kayıt verme ve kartını teslim alma için ilgili birime iki kez gelmesi gerekmektedir ki memnuniyetsizlik yaratabilir.
- Belli bir düzenleme yapılmadan (Davetiyesiz) kart verme/kayıt alma işlemi beklemelere sebep olmaktadır.

Pilot çalışma Bolu ilinde 10 ilçede, 52 personel, 10 mobil ünite ile gerçekleştirilmiştir. Bolu ilimizde yapılan pilot uygulama kapsamında yaklaşık 206.000 kart basılmıştır. Bu uygulamada dağıtık ve merkezi mimari başarı ile bir arada denenmiştir.

KAYNAKÇA

[1] NIST SP800-73 Interfaces for Personal Identity Verification, 2005.

[2] NIST SP800-63 Electronic Authentication Guideline, 2004.

[3] FIBS PUB 201 “Personal Identity Verification (PIV) of Federal Emloyees and Contractors”.

ELEKTRONİK KİMLİK DOĞRULAMA SİSTEMİ

Mücahit MUTLUGÜN

1. ELEKTRONİK KİMLİK DOĞRULAMA

Güvenliğin insanlara ve bilgisayar sistemlerine bakan pek çok yönü bulunmaktadır. Gizlilik, yetkilendirme, kimlik doğrulama, inkâr edememe, bütünlük, erişim denetimi ve kullanılabilirlik ilk başta sayılabilecek güvenlik kavramlarıdır. Bu kavramlardan bazıları birbirlerine bağımlıdır. Mesela bu yazımızda ele alacağımız kimlik doğrulama yapılmadan güvenli bir yetkilendirme ve erişim denetimi mümkün olamamaktadır. Diğerlerine temel teşkil etmesi açısından kimlik doğrulamanın sağlıklı yapılması çok önemlidir. Kimlik doğrulama kavramı bilgisayar ağlarının ortaya çıkışında ilk zamanlarda da ele alınan bir kavramdı. Fakat önemi zamanla daha da arttı ve bu konuda hem akademik alanda hem de ticari alanda ciddi şekilde çalışmalar yapıldı.

Kimlik Doğrulama birisinin veya bir şeyin kimliğinin doğru şekilde geçerlenmesi sürecidir. Günlük hayatta bunun pek çok örneği vardır. Mesela kapımız çalındığında kapının deliğinden bakıp kapıyı çalan kişinin yüzünü görür ve tanıdığımız kişi olup olmadığına karar veririz. Kapımızda delik yoksa "Kim o" der gelen cevabı söyleyen kişinin sesinden veya söylediği isimden kimliğini doğrularız. Bu noktada karşıdakinin iddia ettiği kişi olup olmadığını sesinden, yüzünden veya söylediği bir şeyden doğrulamış oluruz. Bu noktadan sonra kapıyı açıp açmama kararı veririz ki bu da yaptığımız kimlik doğrulamayı temel kabul eden bir süreçtir.

Elektronik Kimlik Doğrulama ise bir cihaz veya yazılımın bir kişiyi veya bir cihazı elektronik olarak doğrulamasıdır. Doğrulama işlemi yapılırken bilinen veriler, kriptografik yöntemler, matematiksel yöntemler vs. kullanılır. Doğrulama yapılırken iki taraf birbirlerine doğrudan erişiyor olabilecekleri gibi bir ağ üzerinden de erişiyor olabilir. Bundan sonraki bölümlerde bir elektronik kimlik doğrulama sisteminde olması gereken ana bileşenler açıklanacaktır.

1.1 Kayıt Otoritesi

Bir kimlik doğrulama sisteminin temel taşını kayıt otoritesi oluşturur. Kişi, elektronik sisteme kendisini tanıtabileceği yöntemleri ilk olarak bu otoriteye kayıt ettirmek ve kimlik doğrulama sırasında bu otoritenin sağlayacağı argümanları kullanmak durumundadır. Elektronik Kimlik Doğrulama Sistemi'nde (EKDS) bu kayıt otoritesi Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'dür. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (NVİ) tüm T.C. vatandaşlarının kimlik kayıtlarını bulundurmaktadır. Elektronik T.C. Kimlik Kartı'nın kullanıma geçişi ile herkes EKDS'yi kullanabilmek için NVİ'den kendisine verilen bir T.C. Kimlik Kartı'nı kullanmak durumundadır. NVİ kayıt sırasında vatandaşın resmini, ıslak imzasını ve parmak biyometrisini alıp vatandaş için bir kart üretir. Vatandaşa kartını ve PIN numarasını teslim eder.

1.2 Kimlik Doğrulama Yöntemleri

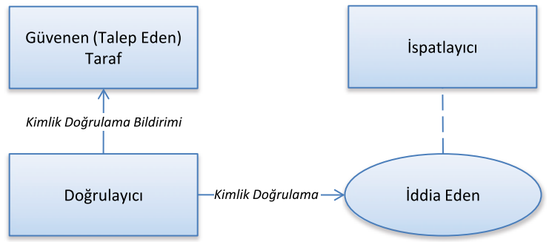
Elektronik sistemlerde yapılan kimlik doğrulama kişinin veya bir cihazın-yazılımın güvenilir olduğunu ve iddia ettiği kişi olduğunu karşı tarafa ispatlamasıdır. Kriptografi kimlik doğrulama ile ilgili problemleri çözmek için gerekli araçları sağlamaktadır. Kimlik doğrulamada çeşitli etmenler kullanılabilir. Bu etmenler "bilinen", "sahip olunan" ve "olunan" olarak sınıflandırılır.

Bilinen İle Kimlik Doğrulama: Bilinen ile kimlik doğrulama temel olarak, kimliğini ispatlamak durumunda olan tarafın kimliği doğrulayan taraf ile ortak bir bilgiye sahip olması ve bu ortak bilgiyi öne sürerek karşı tarafa kimliğini ispatlamasıdır. Buna en klasik örnek, parola tabanlı kimlik doğrulamadır. EKDS'de akıllı kart PIN'i bilineni karşılamaktadır.

Sahip Olunan İle Kimlik Doğrulama: Sahip olunan ile kimlik doğrulama esas olarak kimliği doğrulanan kişi veya cihazın içinde bazı kriptografik güvenekler (*credential*) bulunduran bazı cihazları kullanmasıdır. Akıllı kart bu konuda klasik bir örnektir. EKDS'de kullanılan T.C. Kimlik Kartı kişinin sahip olduğu ve sahipliğiyle de kimliğini ispatlayabildiği yöntemdir.

Olunan İle Kimlik Doğrulama: Olunan ile kimlik doğrulamada kişiye ait fizyolojik veya davranışsal özellikler, kişinin kimliğini doğrulamada kullanılır. Kimlik doğrulamada kullanılan fizyolojik özelliklere örnek yüz yıldan fazla süredir kullanılmakta olan parmak izi, yüz, el geometrisi, iris, retina, damar geometrisi, kulak geometrisi ve DNA sayılabilir. Kimlik doğrulamada kullanılan davranışsal özelliklere örnek olarak da tuş basım ritmi, ses ve imza sayılabilir. Kimlik doğrulamada kullanılan biyometriler evrensellik, tekillik, kalıcılık, toplanabilirlik, performans, kabul edilebilirlik ve önleme açılarından kıyaslanmaktadır. [1]

EKDS'de parmak biyometrileri kullanılmaktadır. Bu biyometriler parmak izi ve damar biyometrisidir.



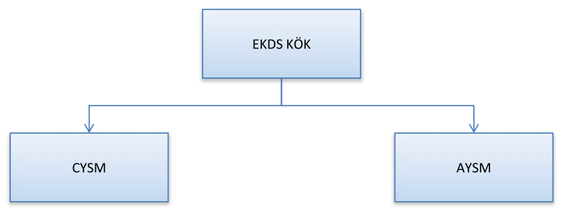
Şekil 1. *Elektronik kimlik doğrulama mimarisi.*

1.3 Elektronik İspatlayıcılar

Kâğıt tabanlı ispatlayıcılar (pasaport, nüfus cüzdanı gibi) genelde fiziksel güvenlik öğeleri içeren ve kişiye özel bilgilerin üzerine yazıldığı güvenilir kabul edilen dokümanlardır. Günümüz teknolojilerinde fiziksel güvenlik öğeleri tek başına yeterli olmamakta aynı zamanda elektronik sistemler tarafından tanınamamaktadır. Bu açıdan elektronik ispatlayıcı (*credential*) diyebileceğimiz argümanlara ihtiyaç vardır.

Elektronik sertifikalar bu ispatlayıcıların en yaygın olarak kullanılanıdır. EKDS'de de T.C. Kimlik Kartına yazılan bir elektronik kimlik doğrulama sertifikası bulunmaktadır. Sertifika mimarisinde bu sertifika EKDS Kök altındaki Anahtar Yönetimi Sertifika Makamı (AYSM) tarafından verilmektedir. Kayıt otoritesi AYSM'yi işletmek veya işlettirmek durumundadır. AYSM EKDS sistemine sertifika iptal sorgulama hizmeti verir.

Cihaz Yönetimi Sertifika Makamı (CYSM) ise EKDS kapsamında KEC'de kullanılan Güvenli Erişim Modulü (GEM) sertifikaları, GSP ve diğer sunuculardaki kullanılan SSL sertifikaları, KDPS imza sertifikaları gibi sertifikaların verildiği sertifika makamıdır.



Şekil 2. *Sertifika mimarisi.*

1.4 Doğrulayıcılar

Bir kimlik doğrulama işleminde doğrulayıcı iddia edenin kimliğini ispat edecek ispatlayıcılara (*credential*) sahip olduğunu doğrular. EKDS'de vatandaş kimliğini T.C. Kimlik Kartı, PIN, Sertifika ve biyometrik verisi ile ispatlayabilir. EKDS'de üzerinde GEM kartı taşıyan Kart Erişim Cihazı (KEC) vatandaşın kimliğini doğrulama işlevini gerçekleştiren bir doğrulayıcıdır.

1.5 Kimlik Doğrulama Bildirimi

Kimlik doğrulama gerçekleştikten sonra doğrulayıcı hizmet alınacak sisteme göndermek üzere gerçekleştirilen işlem hakkında güvenilir bir sonuç belgesi oluşturur. EKDS'de KEC gerçekleştirdiği kimlik doğrulama işleminin sonucu olarak bir Kimlik Doğrulama Bildirimi (KDB) üretir ve kimlik doğrulamayı talep eden hizmet uygulamasına gönderir. Kimlik doğrulamayı talep eden hizmet uygulaması (güvenen taraf) bu KDB'ye bakarak kimlik doğrulamanın gerçekleştiğini anlar.

1.6 Güvenen Taraf

Bir kimlik doğrulama işleminde bu kimlik doğrulamayı talep eden birisi veya bir kurum vardır. Bu doğrulama isteği bir kişinin bir yere veya bir şeye ulaşmak veya kullanmak istemesi üzerine talep edilebilir. Hizmeti veya veriyi sunacak tarafın kimlikten emin olması gerekmektedir. Bu yüzden doğrulayıcıya güvenmek durumundadır. Güvenen tarafın doğrulayıcı ile güvenli bir bağlantısı yoksa doğrulayıcı tarafından üretilen KDB'yi doğrulaması gerekir. EKDS kapsamında geliştirilen Kimlik Doğrulama Sunucusu güvenen taraf adına bu işi gerçekleştirmektedir.

Güvenen taraf birden fazla faktörün kullanılabildiği bir kimlik doğrulamayı isteğine göre esnek şekilde kullanabilmelidir. Kurum politikasına göre şekillenebilecek doğrulama şekli Güvenen Taraf tarafından doğrulayıcıya bildirilmek durumundadır. Doğrulayıcı böylece kimlik doğrulama talebine göre doğrulama işlemini gerçekleştirir ve iddia eden taraftan politikanın gerektirdiği ispatlayıcıları talep eder. EKDS'de Güvenen Taraf adına bu tanımlamalar Kimlik Doğrulama Politika Sunucusu'nda yapılmakta ve kimlik doğrulama esnasında KEC'ye bildirilmektedir.

2. Elektronik Kimlik Doğrulama Sistemi

Bir önceki bölümde elektronik kimlik doğrulamadan bahsedilmişti. Elektronik kimlik doğrulamadan bahsedilirken EKDS'de karşılık gelen ilgili bileşenler kısaca verilmişti. Şimdi T.C. Kimik Kartı ile birlikte geliştirilen EKDS'nin mimarisi ve bileşenlerinden daha detaylı şekilde bahsedeceğiz.

2.1 Genel Mimari

Elektronik Kimlik Doğrulama Sistemi'nin işleyişi Şekil 3'te verilmiştir. Bu mimaride daha önce sözü edildiği gibi:

Vatandaş ⟶ İddia eden

Parmak izi, PIN, kart, sertifika ⟶ İspatlayıcı

KEC ⟶ Doğrulayıcı

Kurum Hizmet Sistemi (İstemci/Sunucu) ⟶ Güvenen Taraf

olarak rol almaktadır. Bu mimari üzerinde bileşenlerin gerçekleştirdiği Kimlik Doğrulama şu adımlarla gerçekleşir:

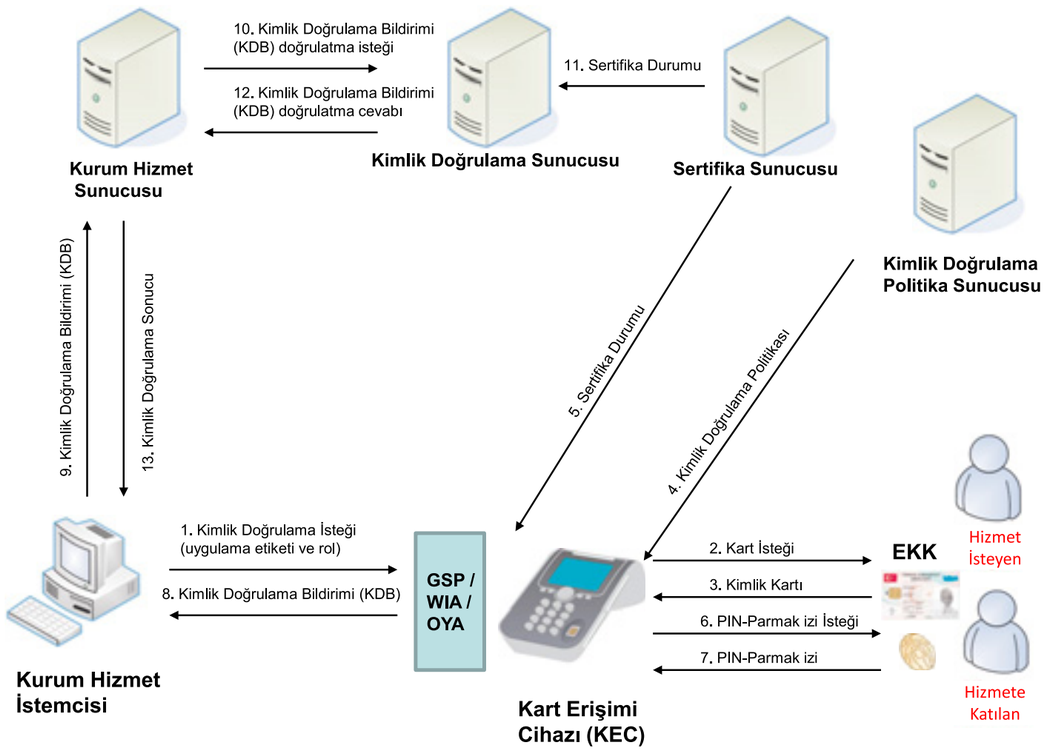
Bir vatandaşın hizmet alma/bir veriye erişme talebi vardır.

1. Kurum Hizmet İstemcisi bir Kimlik Doğrulama talebi başlatır. Kurum Hizmet İstemcisi bu talebi EKDS'nin doğrulayıcısı olan KEC'e arabirimler aracılığıyla gönderir. EKDS arabirimlerine genel olarak Güvenlik Servisleri Platformu (GSP) denmektedir. GSP ileride detaylı anlatılacaktır. İstemci GSP'ye talep gönderirken gerçekleştirilecek kimlik doğrulamanın ne için yapıldığını ve hangi rolle (hizmet isteyen/hizmete katılan) yapıldığını gösteren uygulama etiketi ve rol bilgisini de gönderir. GSP bu talebi ilgili KEC'e iletir.

2. KEC vatandaştan kartını talep eder.

3. Kart talebi doğrultusunda vatandaş kartını kimlik doğrulama rolüne göre ilgili kart girişine takar. KEC kartta KSTB doğrulaması gerçekleştirir. Bu işlem sırasında KSTB'nin imzası kontrol edilir.

4. GSP KEC tarafından oluşturulan Kimlik Belirtimi'ni kullanarak kendisinde tanımlı olan Kimlik Doğrulama Politika Sunucusu'na (KDPS) başvurur. Kimlik Belirtimi uygulama etiketi, rol ve kişinin T.C. Kimlik Numarası'nı içerir. KDPS kendi politika veritabanından ilgili uygulama ve kişi için geçerli



Şekil 3. *Elektronik Kimlik Doğrulama Sistemi mimarisi.*

politika verisini oluşturur, imzalar ve GSP'ye gönderir. Politika verisindeki en önemli parametre güvenlik seviyesidir. GSP politikaları önbelleğinde tutup geçerlilik süresi sonuna kadar tekrar kullanabilme yeteneğine sahiptir. GSP KDPS'ye ulaşamaz ise durumu KEC'e bildirir. Bu durumda kimlik doğrulama en üst seviyeden gerçekleşir.

5. GSP karttan okunan Kimlik Doğrulama Sertifikasının geçerlilik durumunu kontrol etmek üzere sertifika sunucusuna OCSP sorgusu gönderir. (OCSP sunucusuna gönderilecek talep verisini KEC oluşturur) GSP sunucudan gelen OCSP sonucunu KEC'e gönderir. KEC OCSP sorgusu sonucuna göre kart eğer iptal edilmiş ise işlemi sonlandırır. Diğer durumda işleme devam eder. GSP bir şekilde OCSP sunucusuna ulaşamaz ise KEC'i bilgilendirir. KEC işleme devam eder ve oluşan KDB'ye OCSP yapamadığı bilgisini koyar. GSP OCSP sorgularını önbelleğine alıp tekrar kullanabilme yeteneğine sahiptir.

6. KEC KDPS'den gelen politikadaki güvenlik seviyesine göre vatandaştan PIN/Parmak izi talep eder. Güvenlik seviyesinin sadece kart gerektiren 1 ve 2. seviyede olması durumunda vatandaştan bir şey talep edilmeden işleme devam edilir. Vatandaşın bunları kabul edilebilir süre içerisinde vermemesi durumunda işlem iptal edilir.

7. Vatandaş kendisinden talep edilen PIN/parmak izini KEC'e verir.

8. KEC güvenlik seviyesinin gerektirdiği doğrulama işlemlerini gerçekleştirdikten sonra doğrulama başarılı ise bir KDB oluşturarak GSP'ye döndürür. Güvenlik seviyelerinde KEC tarafından gerçekleştirilen doğrulama işlemlerinden daha sonra detaylıca bahsedilecektir. KDB PIN girilen güvenlik seviyelerinde GEM ve Kimlik Kartı tarafından, diğer seviyelerde ise sadece GEM tarafından imzalanır.

9. Kurum Hizmet İstemcisi KDB'yi kendi sunucusuna gönderir.

10. Kurum Hizmet Sunucusu KDB'yi doğrulatmak üzere güvenli bir kanaldan Kimlik Doğrulama Sunucusu'na (KDS) gönderir.

11. KDS kendisine gelen KDB'yi imzalayan GEM sertifikasının geçerliliğini kontrol eder. Bunun için Sertifika Sunucusu'ndan periyodik olarak indirdiği Sertifika İptal Listesini (SİL) kullanabileceği gibi direk OCSP sorgusu da yapabilir. KDS, KDB'de Kimlik Kartı'nın imzasının olduğu durumlarda KEC tarafından sertifika iptal kontrolü yapılmamış ise gerekli kontrolü SİL veya OCSP kullanarak yapar.

12. KDS KDB doğrulama işlemini gerçekleştirir, KDB'yi veritabanına kaydeder ve sonucu Kurum Hizmet Sunucusu'na döndürür.

13. Kurum Hizmet Sunucusu gerçekleşen doğrulama ile tanımlanan kişinin talep ettiği hizmete erişmesine yetkisi olup olmadığına karar verir ve sonucu Kurum Hizmet İstemcisine bildirir.

2.2 Elektronik Kimlik Kartı

T.C. Kimlik Kartı EKDS'nin en temel bileşenidir. Akıllı kart teknolojisi kullanılmaktadır. Kartın elektronik içeriği şunlardan oluşmaktadır:

- Kişinin T.C. Kimlik Numarası, ismi ve sertifika numarasının NVİ tarafından elektronik olarak imzalanmış hali: Kart Sahibinin Tekil Belirleyicisi-KSTB
- Kişinin dijital resmi (elektronik imzalı)
- Parmak Biyometrisi (elektronik imzalı)
- Kimlik Doğrulama Sertifikası
- Elektronik imzalanmış Nüfus bilgileri

T.C. Kimlik Kartı fiziksel olarak pek çok güvenlik öğe içerdiği gibi elektronik olarak da içermektedir. Kartın sahip olduğu akıllı kart işletim sistemi Common Criteria EAL4+ ve akıllı kart yongası Common Criteria EAL5+ güvenlik sertifikasına sahiptir. Akıllı kart üzerinde bulunan kimlik doğrulama sertifikası X.509 standardına uygundur.

2.3 Kart Erişim Cihazı

EKDS'de doğrulayıcı olarak rol alan KEC, üzerinde Güvenli Erişim Modülü (GEM) bulunan özel bir kart okuyucudur. Temel olarak gerçekleştirdiği işlev kimlik kartının doğrulanmasıdır. GEM, KEC'in kriptografik işlemlerden sorumlu birimidir. Farklı uygulamalar için KEC'in farklı modelleri bulunmaktadır. Kimlik kartını doğrulama için simetrik doğrulama, asimetrik doğrulama, imza kontrolü gibi farklı yöntemler kullanmaktadır. Kriptografik doğrulama protokollerini yürütürken üzerinde gömülü GEM'i kullanır.

2.4 Kimlik Doğrulama Sunucusu

Kimlik Doğrulama Sunucusu Güvenen Taraf'ın (Kurum Hizmet Sistemi) adına KDB doğrulaması gerçekleştirir. Ayrıca doğrulama yaptığı KDB'leri saklayıp sonradan sorgulama yapılmasına imkân sağlar. KDS üzerinde geçerli KEC seri numaraları, geçerli KDB sürümleri ve geçerli KEC versiyonları tanımlanıp KDB doğrulamasında bu parametrelerin de dikkate alınması sağlanabilmektedir.

Kimlik Doğrulama Sunucusu doğrulama yaptığı KDB'leri isteğe göre tek kullanımlık olarak değerlendirebilmektedir. Güvenen Taraf'tan gelen talebe göre bir KDB ikinci kez doğrulanmak istediğinde KDS hata döndürmektedir.

KDS'nin KDB üzerinde gerçekleştirdiği doğrulama işlemleri şunlardır:

- Kimlik Kartı Sertifikası doğrulanması (AYSM imza kontrolü, geçerlilik tarihi vb.),
- Kimlik Kartı Sertifikası iptal kontrolü,
- GEM Sertifikası doğrulanması (CYSM imza kontrolü, geçerlilik tarihi vb.),
- GEM Sertifikası iptal kontrolü,
- KDB içindeki KSTB'lerin kontrolü,
- Bildirim oluşturma tarihi kontrolü,
- Bildirim geçerlilik süresi kontrolü,
- KEC seri numarası kontrolü,
- KEC yazılım sürüm kontrolü,
- KDB sürüm kontrolü,
- KDB içindeki Uygulama Etiketi'nin KDS'ye gelen kimlik doğrulama talebi içerisinde gelen ile aynı olup olmadığı kontrolü,
- KDB işlem numarası tekillik kontrolü.

2.5 Kimlik Doğrulama Politika Sunucusu

Kimlik doğrulama sırasında KEC tarafından kullanılacak güvenlik seviyesi, geçerlilik süresi vb. parametrelerden oluşan kimlik doğrulama politikasını belirleyen merkezi sunucudur. Uygulama etiketi, rol ve kişiye göre politika belirleyebilmektedir. Ayrıca kişiden bağımsız jenerik politika tanımı da yapılabilmektedir. Her kurumun kendi uygulamalarını ve politikalarını belirleyebilmesi için kendi bünyesinde işletmesi gerekmektedir.

Uygulama etiketi {Uygulama İsmi}@{Kurum URL}'den oluşmaktadır. Örneğin Sosyal Güvenlik kurumunun provizyon web servis uygulamasının uygulama etiketi provizyon@sgk.gov.tr, e-reçete web servisinin uygulama etiketi erecete@sgk.gov.tr olabilir.

2.6 Kimlik Doğrulama Politikası

Kimlik Doğrulama Politikası KDPS tarafından üretilen dijital bir veridir. ASN.1 yapısında kodlanmıştır. İçeriği aşağıdaki gibidir:

- Kimlik Doğrulama Rolü,
- Güvence Seviyesi,
- Parmak izi güvenlik seviyesi,
- Politika geçerlilik süresi,
- KDB geçerlilik süresi,
- Kimlik Doğrulama Şartı,
- Jenerik Politika,
- Güvenlik Seviyesi tekrar kullanım izni,
- Aracı izni,
- Biyometrik katılan onayı izni,
- KDPS sertifika+imza.

2.7 Kimlik Doğrulama Arabirimleri

Kimlik doğrulama talep eden uygulamaların KEC'e erişebilmeleri için kimlik doğrulama arabirimlerini kullanmaları gerekmektedir. Bu arabirimleri iki tiptir. Ethernet arayüzlü KEC'ler için KEC'e GSP üzerinden, USB arabirimli KEC'ler için ise OYA üzerinden bağlanılması gerekmektedir.

Güvenlik Servisleri Platformu

Güvenlik Servisleri Platformu birden fazla KEC'in bir sunucu üzerinden kullanılmak istendiği ortamlarda KEC'lere arabirim vazifesini görmektedir. Örneğin bir hastanede her bir poliklinikte bulunan bilgisayarları doğrudan KEC'e bağlamak yerine KEC'ler Ethernet ağına bağlanır, hastaneye bir GSP kurulur ve Hastane Bilgi Yönetim Sistemi Sunucusu direk GSP ile muhatap olur. GSP politika önbelleği, OCSP önbelleği, KEC'lerin merkezi yönetimi ve yazılım terfisi yapabilme gibi özelliklere sahiptir.

Otomasyon Yazılımı Arabirimi

Otomasyon Yazılımı Arabirimi USB arayüzünden haberleşme yapan KEC'lerin PC üzerindeki uygulamalardan erişilip kimlik doğrulama yapabilmesini sağlamaktadır. Masaüstü ve Web uygulamalarından EKDS kullanarak kimlik doğrulama yapılabilmesine izin vermektedir.

2.8 Kimlik Doğrulama Bildirimi

Tablo 1. KDB İçeriği

KDB Verisi	Örnek
Id	72334
KDB Versiyon	1.00
Bildirim No	257
Kart Seri No	PL3072420
TC No	23722211539
Adı	MEHMET
Soyadı	ALTEKİN
Kart Geçerlilik Tarihi	19.11.2019
Aracı Kullanılmış mı?	Hayır
Aracı Kart Seri No	---
Aracı TC No	---
Aracı Adı	---
Aracı Soyadı	---
Aracı Kart Geçerlilik Tarihi	---
Hizmete Katılan Dogrulamış mı?	Hayır
Hizmete Katılan Kart Seri No	---
Hizmete Katılan TC No	---
Hizmete Katılan Adı	---
Hizmete Katılan Soyadı	---
Hizmete Katılan Kart Geçerlilik Tarihi	---
Uygulama Etiketi	hastakabul@sgk.gov.tr
Uygulama Etiketi Açıklaması	Hasta Kabul
Güvenlik Seviyesi	Seviye-3
Geçerlilik Süresi	86400
Rol	Hizmet İsteyen
Biyometrik Doğrulama Durumu	A/D
Cihaz Takip No	16777449
Hizmet Sağlayıcı Takip No	1,0203E+14
GEM Takip No	3366001c91ff274fda141c15
Oluşturma Tarihi	08.01.2010 13:38
KEC Yazılım Versiyonu	1.33.03
Kart İptal Kontrolü Yapılmış mı?	Evet
Tesis No	512344
GEM İmza	3bc90aba0d6789acc3bc3671
EKK İmza	c391cb4a23e00ccbf4d87e6a

Kimlik Doğrulama Bildirimi KEC tarafından gerçekleştirilen kimlik doğrulama sonucunda üretilen ve kimlik doğrulamanın sonucunu gösteren dijital bir veridir. ASN.1 yapısında kodlanmıştır. İçeriği Tablo 1'de örnek ile birlikte verilmiştir. Politika'ya göre kimlik doğrulama sırasında istenebilecek hizmete katılan kart bilgileri veya aracı kullanılması durumunda aracı'nın kimlik bilgileri de KDB içerisinde bulunmaktadır.

KDB mutlaka GEM tarafından imzalandığından KDB'nin bütünlüğü sağlanmaktadır. KDB KEC'den çıktıktan sonra herhangi bir noktada bozulsa veya değiştirilse KDS tarafından doğrulanamayacaktır. Kimlik Kartının KDB'yi imzaladığı durumlarda ise vatandaş için inkar edemezlik sağlamaktadır.

2.9 Güvenlik Seviyeleri

Kimlik doğrulama güvenlik seviyeleri Kimlik Doğrulama Politika Sunucusu'nda kurum tarafından belirlenir. Kart Erişim Cihazları kimlik doğrulama yaparken KDPS tarafından belirlenen politikaya göre işlem gerçekleştirir. Güvenlik Seviyeleri Tablo 2'de verilmiştir.

3. Örnek Uygulama

3.1 Örnek Uygulama 1

Bu bölümde EKDS pilot uygulaması kapsamında Bolu ilinde denemesi yapılan SGK MEDULA provizyon servisi uygulaması anlatılacaktır.

Şekil 4'te anlatılan EKDS mimarisi SGK provizyon uygulamasına göre revize edilip gösterilmiştir. Hastanelerdeki HBYS'ler'de halihazırda T.C. Kimlik Numarası ile alınan provizyon bu uygulama ile KDB ile alınır şekle çevrilmiştir. Hastane ortamında T.C. Kimlik Kartlı provizyon uygulaması aşağıdaki anlatıldığı şekilde cereyan eder:

1. Vatandaş muayene olmak için başvuru bankosuna gider.

2. Bankodaki memur HBYS ekranındaki düğmeye basarak kimlik doğrulamayı başlatır.

3. HBYS GSP'den Kimlik Doğrulaması talep eder. HBYS GSP'ye kimlik doğrulama isteğinde hastaKabul@sgk.gov.tr uygulama etiketini, rol olarak hizmet isteyen rolünü ve hangi KEC'in kullanılacağı bilgisini iletir.

4. GSP KEC ile Kimlik Doğrulama işlemini gerçekleştirir. Kimlik doğrulama sırasında GSP SGK'nın işlettiği KDPS'den hastaKabul uygulama etiketi için politika alır. Bu politikadaki güvenlik seviyesini (kimlik doğrulama sırasında PIN ve parmak izi talep edilip edilmeyeceği) SGK belirler.

5. GSP KEC'den aldığı KDB'yi HBYS'ye döndürür.

6. HBYS aldığı KDB'yi de kullanarak MEDULA'nın provizyon web servisini çağırır.

7. MEDULA kendisine gelen KDB'yi KDS'den doğrulatır.

8. MEDULA KDS'den gelen T.C. Kimlik Numarasını kullanarak veritabanından sorgulama yapar ve kişinin sağlık hizmeti almaya hak sahibi olup olmadığını sorgular ve HBYS'ye provizyon cevabını döndürür.

9. Provizyonun başarılı gelmesi durumunda memur vatandaşı ilgili polikliniğe gönderir.

3.2 Örnek Uygulama 2

Bu bölümde bir önceki bölümde anlatılan senaryonun aracı kullanılarak gerçekleştirilen hali anlatılacaktır. KDPS'de hastaKabul@sgk.gov.tr uygulama etiketi için aracı kullanım izni verilmiş olmalıdır.

1. Vatandaşın aracısı (akraba vs.) muayene provizyonu almak için başvuru bankosuna gider.

2. Bankodaki memur HBYS ekranındaki düğmeye basarak kimlik doğrulamayı başlatır.

3. HBYS GSP'den Kimlik Doğrulaması talep eder. HBYS GSP'ye kimlik doğrulama isteğinde hastaKabul@sgk.gov.tr uygulama etiketini, rol olarak hizmet isteyen rolünü ve hangi KEC'in kullanılacağı bilgisini iletir.

4. GSP KEC ile Kimlik Doğrulama işlemini gerçekleştirir. Kimlik doğrulama sırasında GSP SGK'nın işlettiği KDPS'den hastaKabul uygulama etiketi için politika alır. Bu politikadaki güvenlik seviyesini (kimlik doğrulama sırasında PIN ve parmak izi talep edilip edilmeyeceği) SGK belirler. Kimlik doğrulama başlangıcında kendisine provizyon alınacak kişinin kartı KEC'e takılır.

5. KEC aracı kullanılıp kullanılmayacağını sorar. Aracı kullanılacaksa aracı kartı talep edilir.

6. KEC kimlik doğrulamaya aracı kartı ile devam eder.

7. GSP KEC'den aldığı KDB'yi HBYS'ye döndürür.

8. HBYS aldığı KDB'yi de kullanarak MEDULA'nın provizyon web servisini çağırır.

9. MEDULA kendisine gelen KDB'yi KDS'den doğrulatır.

10. MEDULA KDS'den gelen T.C. Kimlik Numarası'nı kullanarak veritabanından sorgulama yapar ve kişinin sağlık hizmeti almaya hak sahibi olup olmadığını sorgular ve HBYS'ye provizyon cevabını döndürür. MEDULA aracı kullanıldığı bilgisini veritabanına kaydeder.

11. Provizyonun başarılı gelmesi durumunda memur vatandaşı ilgili polikliniğe gönderir.

3.3 Örnek Uygulama 3

Bu bölümde bir önceki bölümde anlatılan senaryonun hizmete katılanın zorunlu olduğu durumu içeren hali anlatılacaktır. KDPS'de hastaKabul@sgk.gov.tr uygulama etiketi için hizmete katılanın zorunlu tutulmuş olması gerekmektedir.

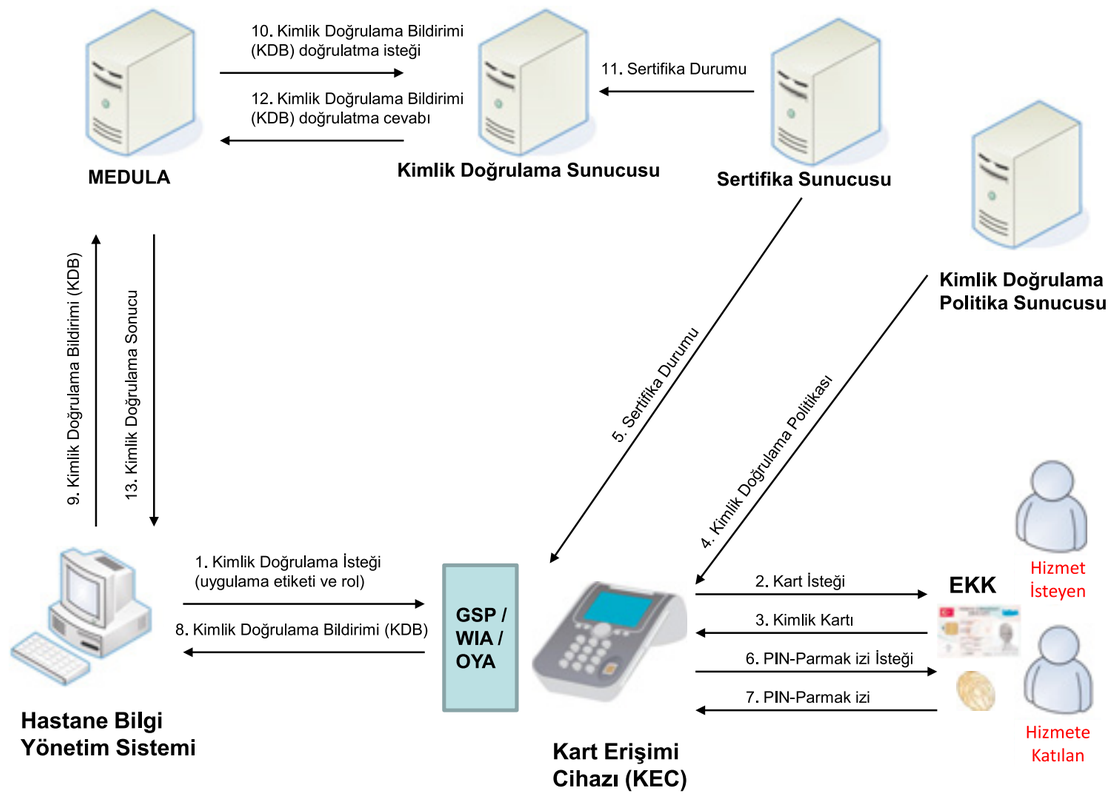
1. Vatandaş muayene olmak için başvuru bankosuna gider.

2. Bankodaki memur HBYS ekranındaki düğmeye basarak kimlik doğrulamayı başlatır.

3. HBYS GSP'den Kimlik Doğrulaması talep eder. HBYS GSP'ye kimlik doğrulama isteğinde hastaKabul@sgk.gov.tr uygulama etiketini, rol olarak hizmet isteyen rolünü ve hangi KEC'in kullanılacağı bilgisini iletir.

Tablo 2. Kimlik Doğrulama Güvenlik Seviyeleri

		KSTB Doğrulama	Sertifika Doğrulama	Sertifika İptal Kontrolü	PIN Kontrolü	Simetrik Doğrulama	Asimetrik Doğrulama	Biyometrik Doğrulama	KDB GEM İmzası	KDB EKK İmzası
Fiziksel Doğrulama	Seviye 0									
Kart	Seviye 1	X							X	
Kart	Seviye 2	X	X	X					X	
Kart + PIN	Seviye 3	X	X	X	X	X	X		X	X
Kart + PIN + BIO	Seviye 4	X	X	X	X	X	X	X	X	X



Şekil 4. *SGK provizyon uygulaması.*

4. GSP KEC ile Kimlik Doğrulama işlemini gerçekleştirir. Kimlik doğrulama sırasında GSP SGK'nın işlettiği KDPS'den hastaKabul uygulama etiketi için politika alır. Bu politikadaki güvenlik seviyesini (kimlik doğrulama sırasında PIN ve parmak izi talep edilip edilmeyeceği) SGK belirler. SGK'dan gelen politikada hizmete katılan zorunlu kılınır.

5. Hizmete katılanın kimlik kartı KEC'e takılıp doğrulatılmamışsa KEC hizmete katılan kartını alır ve hizmete katılanın kimlik doğrulaması yapılır. Hizmete katılan doğrulaması yapılmışsa direk hizmet isteyen için kimlik doğrulama devam eder.

6. Hizmete katılanın kimlik doğrulaması yapılmasını müteakip KEC hizmet isteyen için kimlik doğrulamayı tamamlar.

7. GSP KEC'den aldığı KDB'yi HBYS'ye döndürür.

8. HBYS aldığı KDB'yi de kullanarak MEDULA'nın provizyon web servisini çağırır.

9. MEDULA kendisine gelen KDB'yi KDS'den doğrulatır.

10. MEDULA KDS'den gelen T.C. Kimlik Numarasını kullanarak veritabanından sorgulama yapar ve kişinin sağlık hizmeti almaya hak sahibi olup olmadığını sorgular ve HBYS'ye provizyon cevabını döndürür. MEDULA hizmete katılan bilgisini kendi veritabanına kaydeder.

11. Provizyonun başarılı gelmesi durumunda memur vatandaşı ilgili polikliniğe gönderir.

4. Standart Kullanım

T.C. Kimlik Kartı'nın elektronik uygulamalarda standart kart okuyucu ile kullanılması mümkündür. Fakat bu kullanımda biyometri kullanımı mümkün değildir. Sadece PIN ve kartın içerisindeki sertifika ile kimlik doğrulama işlemi yapılabilmektedir. Bu kullanım www.turkiye.gov.tr'de sisteme girişte uygulanmıştır.

Bu mimaride akış şu şekilde gerçekleşmektedir:

1. İstemci bilgisayarın Web Tarayıcısına imzalı SWA yazılımı iner. (Giriş yapmak istediği sayfaya bağlanınca) Bu sayfa içerisinde Hizmet Sunucu KDS'den aldığı bazı kimlik doğrulama verilerini yerleştirir. Vatandaş sayfa üzerinden giriş düşmesine basar. SWA vatandaştan kartını takmasını ister.

2. Vatandaş kartını bilgisayarına bağlı standart bir kart okuyucuya takar.

3. SWA vatandaştan PIN'ini girmesini ister.

4. Vatandaş bilgisayarın kullanıcı arayüzünden PIN'ini girer.

5. SWA kartla kimlik doğrulama işlemi gerçekleştirir.

6. Kart SWA'ya gerekli bilgileri yollar.

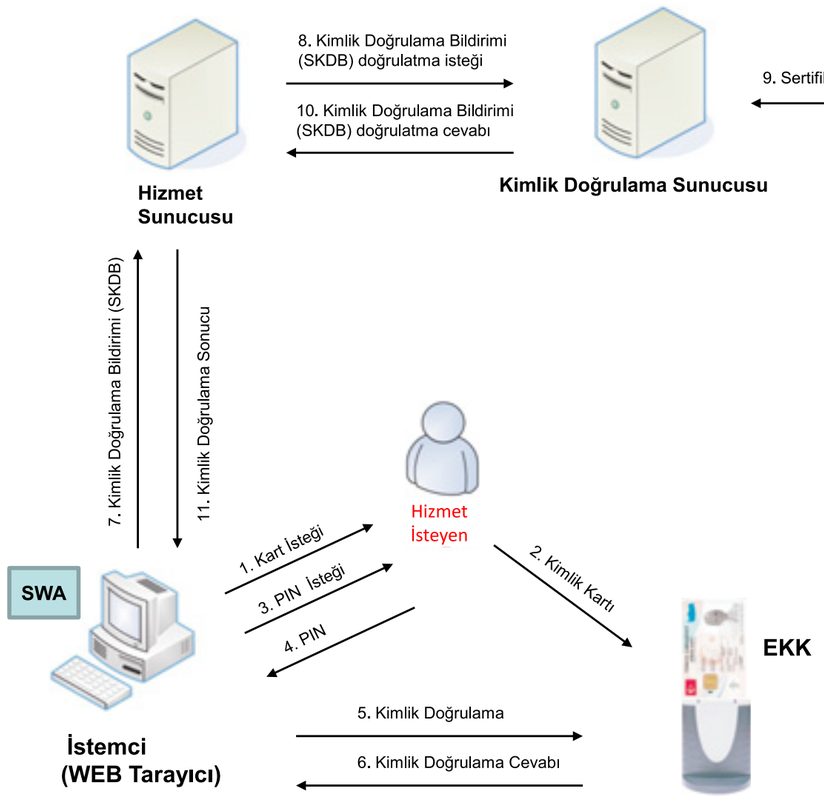
7. SWA SKDB (Standart Kimlik Doğrulama Bildirimi) oluşturur ve bunu Sunucu'ya yollar.

8. Sunucu SKDB'yi ve sayfaya koyduğu kimlik doğrulama verilerini doğrulatmak üzere KDS'ye yollar.

9. KDS vatandaşın kartının Sertifikasının geçerliliğini kontrol eder.

10. KDS Hizmet Sunucu'ya kimlik doğrulama sonucunu yollar.

Hizmet sunucu vatandaşın kimliğini tespit ettikten sonra erişmek istediği sayfaya erişme yetkisi olup olmadığına karar vererek web tarayıcıya gerekli sayfayı oluşturup yollar.



Şekil 5. *Standart okuyucu ile kimlik doğrulama.*

5. Sonuç

Her geçen gün sayıları artan elektronik uygulamalar kamu alanında olsun özel sektörde olsun hizmet alan kişinin kimliğini doğrulamaya ihtiyaç duymaktadır. T.C. Kimlik Kartı da bu temel ihtiyacı karşılayabilecek yegâne alternatif olarak görülmektedir. Elektronik Kimlik Doğrulama Sistemi ise kimlik kartının elektronik uygulamalarda kullanımını sağlayacak altyapı olarak geliştirilmiştir. Elektronik Kimlik Doğrulama sisteminin en temel özelliği kurumların farklı ihtiyaçlarına göre uyarlanabilir esnek bir yapıya sahip olmasıdır. Sistem tasarlanırken uygulamaların güvenlik seviyesinin ihtiyaca göre değiştirebilir olması ve ihtiyaç oranında uygun bileşenlerle çalışabilirliği esas alınmıştır. Ayrıca EKDS'nin elektronik uygulamalara kolay entegre edilebilir olmasını sağlayan arayüzler net bir şekilde tanımlanmıştır. EKDS'yi kullanacak kurumlar arayüz tanımlamalarına göre kolaylıkla entegrasyon işlemlerini gerçekleştirmektedir. Hedeflenen, işlemlerini elektronik ortamda takip eden tüm kamu kurumlarının kimlik doğrulama için bu altyapıyı kullanmasıdır. Bu hususta yaygınlaştırma çalışmaları da devam etmektedir.

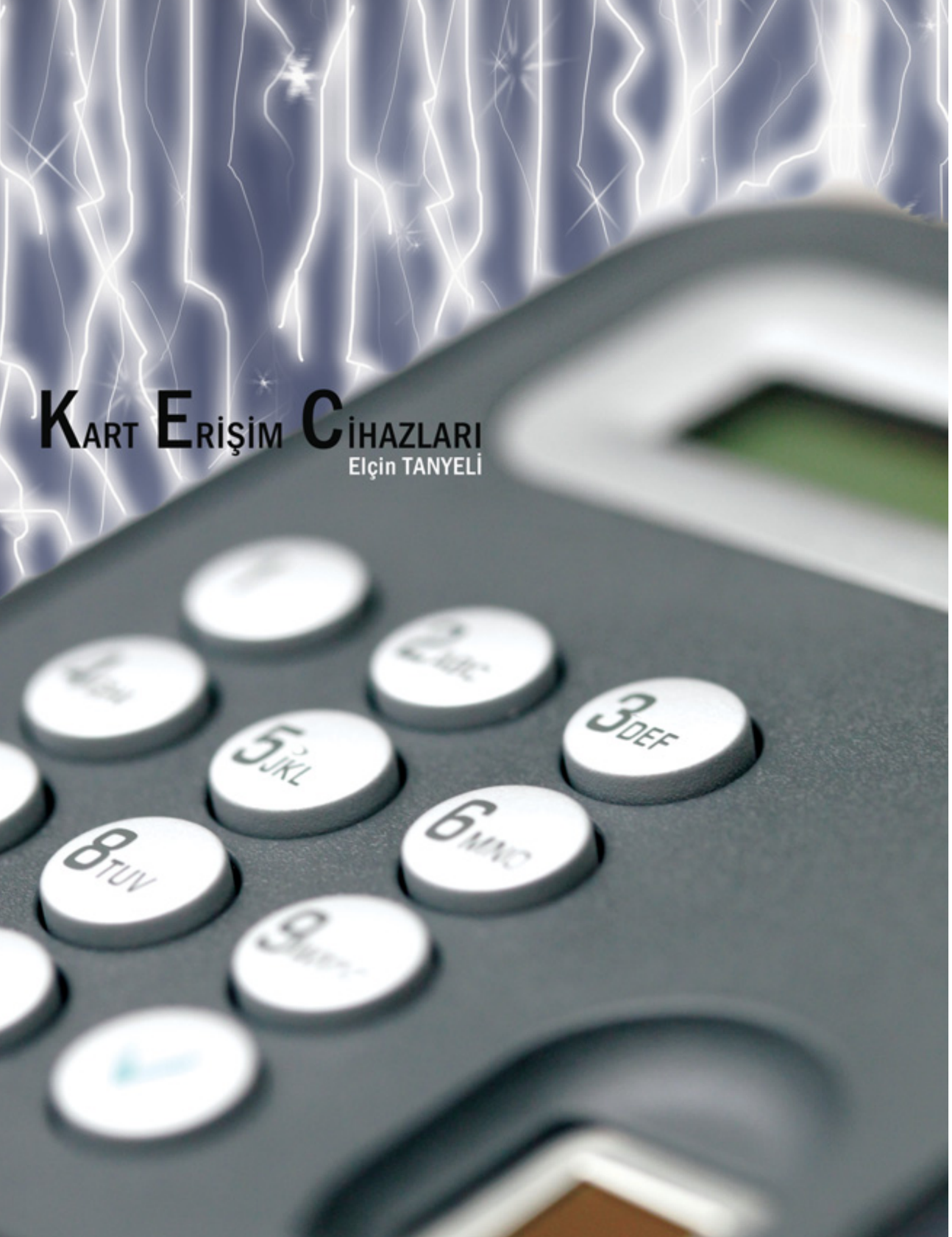
KAYNAKÇA

[1] Jain, A. K., "Biometric recognition: how do I know who you are?", *Signal Processing and Communications Applications Conference*, Proceedings of the IEEE 12th: 3 – 5, 2004.

[2] National Institute of Standards and Technology, *Electronic Authentication Guideline*, 800-63, September 2004.

[3] M. Mutlugün, O. Adalıer, "Turkish national electronic identity card", *International Conference on Security of Information Networks*, Turkish Republic of Northern Cyprus, 2009.

[4] Federal Information Processing Standard, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, PUB 201, 2006.



KART ERİŞİM CİHAZLARI

Elçin TANYELİ

2006 yılında başlayan Elektronik Kimlik Projesi kapsamında, TUBİTAK UEKAE tarafından geliştirilen kartların okutulması için güvenli uç birim cihazlarına gereksinim duyulmuştur. Projede yaygın bir şekilde kullanılan Elektronik Kimlik Doğrulama Sistemi'ninin (EKDS) en önemli bileşenlerinden birisi de bu kart erişim cihazlarıdır.

EKDS, Internet üzerinde elektronik "Hizmet Veren" kamu/özel kurum ve(ya) kuruluşların pek çok uygulamalarında, elektronik kimlik doğrulama amacıyla kullanılacaktır. EKDS, "Hizmet Alan" ve veren arasında yürütülen işlemlerin güvenliğini, kullanıcı tarafında kart erişim cihazları ile temin eder. Telli ve telsiz ortamlarda çalışan 6 çeşit Kart Erişim Cihazı (KEC) uçbirim cihazı kullanılmaktadır:

1. Kurumlar için Geliştirilen Kurumsal KEC/HUBC (Hareketli Uçbirim Cihazı),

2. Ev ve ofis kullanımları için geliştirilen Bireysel KEC,

3. Ortak alan kullanımları için geliştirilen Kiosk KEC,

4. Nüfus müdürlüklerinde kullanılmak üzere geliştirilen Kart Yayıncı KEC,

5. Gezici Nüfus müdürlüklerinde kullanılmak üzere geliştirilen Mobil Kart Yayıncı KEC,

6. Gezici birimler için geliştirilen Mobil KEC.

Kurumsal Tip Kart Erişim Cihazı (KKEC), kurum uygulamalarında hizmet isteyen (vatandaş) ve hizmete katılanın (görevli) kimliklerinin doğrulama işleminde kullanılır. Ayrıca hizmete katılanın yapılan işleme elektronik imzasını atmasını da sağlar.

Şekil 1. *Kurumsal tip kart erişim cihazı.*

Kullanım kolaylığı sağlamak amacıyla, 'Hizmet Alan'ın işlemleri için, KKEC ile beraber Hareketli Uçbirim Cihazları da (HUBC) kullanılabilir. Burada amaç hizmet alanın işleminin yapılmasını onun için kolaylaştırmaktır. Böylece 'Hizmet Alan'ın HUBC, ve "Hizmet Veren"in de KEC üzerinden işlem yapması sağlanarak uygulamada kolaylık sağlanmış olur. (Şekil 2)

HUBC, elektronik kimlik doğrulamada, kolaylık sağlamak amacıyla tasarlanmıştır. HUBC, ancak KEC ile birlikte çalışır. Tek başına, bağımsız bir cihaz değildir.

HUBC, KEC'e USB kapısından bağlanmaktadır. İletişiminin güvenliği şifreleme ile sağlanır. Uygulamalarda KEC cihazı hizmet verenin önünde sabit olarak dururken HUBC 'Hizmet Alan'a uzatılmaktadır.

Elektronik kimlik doğrulama sürecinde, "Hizmet Alan", HUBC üzerinden aşağıdaki güvenlik ve kullanıcı işlevlerini gerçekleştirebilir:

- PIN girişi/değiştirme (tuştakımı, ekran aracılığıyla),
- Parmakizi girişi/testi (parmakizi senörü aracılığıyla),
- Kart girişi/testi (kart arayüzü ile),
- Gelişmeleri görebilme (ekran arayüzü ile),
- Işıklı uyarı (LED ile),
- Sesli uyarı (BUZZER ile).

Şekil 2. *Hareketli uçbirim cihazı - HUBC.*

Bireysel Tip Kart Erişim Cihazı, ev ve ofis ortamlarında, EKDS'in 'Hizmet Alan' ve 'Hizmet Veren' rolleri arasında yürütülen işlemlerin güvenliğini sağlar (Şekil 3). Ayrıca cihaz masaüstü veya taşınabilir kişisel bilgisayarlardaki çeşitli uygulamalarla USB üzerinden haberleşip kimlik doğrulama işlemini yerine getirir. İlk kullanma alanı e-Devlet kapısı olacaktır. Ayrıca çeşitli uygulamalarla bankacılık alanında da kullanılabilir.

Şekil 3. *Bireysel tip kart erişim cihazı.*

Kiosk Tipi Kart Erişim Cihazı kart verme noktalarında bulunacaktır. Kolaylıkla ulaşılabilecek ortamlarda, ortak alanlarda işlemlerin yapılmasını sağlar. Operatör gerektirmediğinden hizmetlerin alınmasında kolaylık sunar. Aşağıda belirtilen amaçlarla kullanılır (Şekil 4):

- PIN'i değiştirme (Kart şifresinin unutulması durumunda parmak biyometrisi ile yeni şifre tanımlamayı sağlar),
- PUK ile bloke kaldırma,
- Nüfus bilgileri ve resim gösterme,
- Kartı test edip içeriğini görüntüleme,
- Başka ilave fonksiyonlar da tanımlanabilir.

Şekil 4. *Kiosk tipi kart erişim cihazı.*

Kart Yayıncı Kart Erişim Cihazı ise sabit kurulu kart üretim ve dağıtım birimlerinde kart içerisine bilginin yazılması ve üretilen kartları test edip içeriğini görüntüleme gibi işler için geliştirilmiştir. Cihazın görünümü Kurumsal KEC ile aynıdır. (Şekil 1).

Mobil Kart Yayıncı Kart Erişim Cihazı ise gezici mobil kart üretim ve dağıtım birimlerinde kart içerisine bilginin yazılması ve üretilen kartları test edip içeriğini görüntüleme gibi işler için geliştirilmiştir. Cihazın görünümü Kurumsal KEC ile aynıdır. (Şekil 1).

Mobil Kart Erişim Cihazı, el tipi bir cihazdır. Gezici kurum uygulamalarında hizmet isteyen (vatandaş) ve hizmete katılanın (görevli) elektronik kimlik kartları vasıtasıyla kimliklerini doğrular. Aynı zamanda hizmete katılanın işleme elektronik imzasını atmasını sağlar. Aşağıdaki özellikleri sayılabilir:

- Temaslı, temassız kartlara erişim sağlar,
- Haberleşeceği bilgisayara telli iletişim yanısıra telsiz iletişim olanağı sunar (bluetooth, wi-fi, gsm gibi).
- 6 saatlik çalışma olanağı veren lithium-ion bataryaya sahiptir.
- Çevrimiçi, çevrimdışı çalışma olanağı vardır.
- e-pasaport, e-ehliyet, e-ruhsat altyapısını tanır ve uygulamaya girer.
- Yürütülen işlemlerin güvenliğini sağlar.
- Cihaz masaüstü veya taşınabilir kişisel bilgisayarlardaki uygulamalarla USB üzerinden haberleşip kimlik doğrulama işlemini yerine getirir.

Kart Erişim Cihazları, her sektörün ihtiyacını (sağlık, adalet, maliye vb.) karşılayacak şekilde, genel amaçlı (sektörden bağımsız) tasarlanmıştır. Buna karşın, EKDS projesinde öncelikle Internet üzerinden "e-Sağlık" hizmeti verilmesinde kullanılacaktır. Bu süreçte elektronik yolla güvenliğinin sağlanması için kullanılan elektronik kimlik ve imza kartlarını okuyup içlerindeki kimlik bilgilerini doğrulayan kart okuyucuları olarak çalışacaktır. Güvenliğin sağlanmasında aşağıdaki adımlar atılacaktır:

1. e-sağlık web uygulamasında "Hizmet Alan" (sigortalı) ve "Hizmet Veren" (hekim, eczacı, sağlık personeli) kimliğinden emin olunması.

2. Web uygulamasına kullanıcılardan gönderilen verilerin gerçekten sahiplerine ait olduğunun güvence altına alınması.

3. Yapılan işlemlerde, kimin ne yaptığı ve ne zaman yaptığı bilgilerinin kaydedilmesi ve inkarı önlemek için sayısal imza kullanılması.

4. Kullanıcıların web uygulamasıyla iletişiminin güvenli hale

getirilmesi ve bu kapsamda internet üzerinde gönderilen verilerin gizliliğinin, bütünlüğünün ve tarafların kimlik doğruluğunun sağlanmasıdır.

EKDS ile telli /telsiz ortamlar üzerinden haberleşen kart erişim cihazları (Kurumsal KEC, Hareketli Uçbirim, Bireysel KEC, Kiosk KEC, Kart Yayıncı KEC, Mobil Kart Yayıncı KEC, Mobil KEC) sosyal güvenlik sistemindeki uygulamalarda hastane, eczane, aile hekimliği ortamlarında çalışmaktadır.

EKDS'nin halen NVİ (Nüfus ve Vatandaşlık İşleri) , Sağlık Bakanlığı, SGK (Sosyal Güvenlik Kurumu)'nın desteği ile, Bolu ilinde pilot deneme çalışmaları gerçekleştirilmektedir.

Hastane, eczane, aile hekimliği alanlarında, kullanıcıların Internet üzerinden erişerek aldığı "e-Sağlık" hizmetlerini güvenli hale getirmektedir.

Hastanelerde, yerel alan ağında çalışan uygulamalarda muayene açma, reçete yazılması gibi işlemlerde ethernet üzerinden EKDS'ye (Güvenlik Servisleri Platformu yazılımına-GSP) bağlanılarak doktor, sağlık memuru veya sağlık görevlisinin kimlik doğrulama ve imzalama işlemleri sağlanmaktadır.

Eczane ve aile hekimliği ortamlarında kişisel bilgisayarlardaki uygulama programşlarıyla birlikte çalışan bir uygulamacık (applet) geliştirilmiştir. Böylece KEC ile USB veya ethernet arabirimi üzerinden haberleşilmektedir. Bu yolla hasta ile eczacı veya aile hekimi elektronik kimlik kartlarının doğrulanması ve imzalama işlevleri sağlanmaktadır.

Kurumsal KEC cihazında 3 adet kart yuvası vardır:

1. "Hizmet Alan"ın elektronik kimlik kartını takacağı yuva,

2. "Hizmet Veren"in de elektronik kimlik kartını takacağı yuva,

3. "Hizmet Veren"in yapılan işleme elektronik imzasını atması için kullandığı e-imza kartı için bir yuva.

Diğer kart erişim cihazlarında, ihtiyaca ve uygulamaların niteliğine göre akıllı kart yuvaları 1 ila 2 arasında değişir. Tüm bu akıllı kart arabirimleri IEC/ISO 7816 standartlarına uyumludur.

KEC cihazlarında, "Hizmet Alan"ın kimlik doğrulamasının güvenirliliğini arttırmak için parola uygulamasının yanısıra bir çok biyometrik yöntem de kullanılmaktadır: "Hizmet Alan"ın parmak izini okumak amacıyla, cihazın üzerinde parmak izi sensörü vardır. Ayrıca dışardan (USB üzerinden) bağlanan damarizi sensörü canlılığın tespitinde yeni bir teknolojik yaklaşımdır. Her insanın kendine özel, biricik damarizini okuyarak hem kişinin doğrulanmasını hemde canlılığının tespitini yapmaktadır.

KEC cihazları tüm kimlik doğrulama işlemlerini genel ve lokal kimlik doğrulama işlemleri olarak yapar. Bunu politika seçimiyle beş ayrı güvenlik seviyesinde gerçekleştirir:

1. seviye: Kart doğrulama.

2. seviye: Sertifikalı kart doğrulama.

3. seviye: Sertifikalı kart doğrulama + biyometrik doğrulama.

4. seviye: Sertifikalı kart doğrulama + pin doğrulama.

5. seviye: Sertifikalı kart doğrulama +pin doğrulama+ biyometrik doğrulama.

Kendi güvenliğini sağlamak üzere, cihazın içinde sertifikalarının yer aldığı güvenlik erişim modulü (GEM) bulunmaktadır.

Tüm KEC cihazları AKiS kartları yanısıra tümüyle milli olarak tasarlanmış UKiS kartları ile de çalışabilirler.

Temel olarak, KEC cihazlarının güvenlik ve işlemsel özellikleri şunlardır:

- Ethernet üzerinden SSL bağlantısı kurulması (Hastanelerde),
- USB üzerinden Şifreli Haberleşme (Aile Hekimliği ve Eczanelerde),
- Eczane ve Hastane Otomasyon Yazılımları, Web Servisleri ile entegre olan güvenli haberleşme,
- EKDS'de güvenlik amaçlı kullanılan Güvenlik Servisleri Platformuna (GSP) bağlanabilme ve koordine edilebilme,
- Kimlik doğrulamasının güvenliğini arttırmak için pin uygulaması,
- KEC'in güvenliğini sağlamak üzere kendisine ait sertifikaların yer aldığı GEM,
- Ayarlar menüsüne erişim için kullanılan kullanıcı pin uygulaması,
- Elektronik kimlik kartların geçerli ve doğruluğunun karşılıklı olarak belirlenmesi için kullanılan simetrik ve asimetrik doğrulama,
- Elektronik kimlik kartlarının içinde yeralan verilere ait imza doğrulama,
- Politika paketi ve güncelleme işlemi için imza doğrulama,
- Güvenlik Erişim Modülü (GEM) kartının ve Elektronik Kimlik Kartlarının doğrulanması için sertifika doğrulama,
- Tüm sertifikaların geçerliliğinin sorgulanması için Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP) kullanımı ve bu şekilde tüm sistemde zaman senkronizasyonu,
- Uzaktan web servisi ile otomatik şifreli ve imzalı yeni yazılım sürümlerinin yüklenebilmesi,

• Günlük kayıtlar ve alarm kayıtları tutma, uzaktan kayıtlara erişebilme,

• Vekil kullanımına imkan sağlama,

• Farklı politika tanımlarıyla farklı senaryolarda kimlik doğrulama yapabilme,

• Elektronik kartlara ve imza kartlarına yeni pin tanımlama imkanı, Kiosk KEC'de parmak izi ile bloke olan kartlarda PIN tanımlayabilme imkanı, cihaz menüsünden PUK girerek PIN tanımlayabilme,

• İstatistiksel verilerin oluşturulması için sayaç toplama/gönderme imkanı,

• Cihazda oluşacak alarmların gönderilebilmesi

KEC cihazlarında çeşitli boyutlarda renkli TFT LCD ekranlar kullanılmakta olup, menüler kullanıcı dostu, simge (icon) gösterimli, sesli ikazlı ve dolayısıyla kullanıcıyı doğru işleme yönlendiren niteliktedir. KEC cihazı, EKDS tarafından gönderilen, UTC ('*Universal Time Coordinated*', Eşgüdümlü Evrensel Zaman) zamanı kaynaklı, periyodik sistem zaman mesajlarını değerlendirir ve kendi bünyesinde barındırdığı gerçek zamanlı saati (RTC) tetikler. Böylece yapılan işlemlerin doğru zamanlı kayıtlanmasını sağlar.

KEC Cihazlarının yazılımında dört ana bileşen bulunur:

1. Arayüz Protokolü:

a. USB arayüz protokol modülü,

b. Ethernet arayüz protokol modülü,

c. Hareketli uçbirim arayüz modülü,

d. Akıllı kart erişim ve parmakizi erişim modülü.

2. Güvenlik Katmanı: HUBC, OYA (Otomasyon Yazılım Arabirimi) ve GSP arasında protokollerin yürütüldüğü modülleri kapsar. Arayüzlerle yapılan haberleşmenin güvenli olmasını sağlar

3. Kimlik Doğrulama

4. Doküman İmzalama Katmanı: Kimlik Doğrulama ve Doküman İmzalama Katmanlarında, e-Kimlik ve GEM kartlarının okunması, aralarında güvenli erişimin sağlanması ve güvence seviyelerine gore yerel ve genel kimlik doğrulamasının sağlandığı modüller bulunur. Ayrıca XML olarak gönderilen dokümanların ekranda gösterimini ve hizmete katılanın imza veya nitelikli imza kartı ile imzalamasını sağlayan modülleri barındırır.

Telli ortamlarda kullanılan KEC'lerde bu katmanlarda kullanılan üç protokol bulunmaktadır. Bunlar şağıdaki protokollerdir:

1. SSL: '*Secure Sockets Layer*', Güvenli Yuva Katmanı,

2. KEC-GSP: Kart Erişim Cihazı-Güvenlik Servisleri Platformu,

3. PC/SC: '*Personal Computer/ Smart Card*'.

Büyük işletmelerin ihtiyacını sağlamak üzere bir çoğunun birarada, sunucu-istemci konfigürasyonunda, şebeke yapısı içinde çalışabilme yeteneği de, yakın gelecekte KEC cihazlarına kazandırılacaktır.

KEC cihazları ticari EMI/EMC, CE (*Electromagnetic Interference/ Electromagnetic Compability, Conformité Européenne*) gereklerine uygundur. Halen IEC/ISO 15408 Ortak Kriter (Common Criteria) EAL4 + düzeyinde CC güvenlik onayı alabilmesi için değerlendirme çalışmaları sürmektedir.

KEC Cihazlarının endüstriyelleşmesi kapsamında da aşağıdaki yol haritasının izlenmesine karar verilmiştir:

• Nitelikli kart erişim cihazlarının özellikleri TÜBİTAK UEKAE tarafından tanımlanacaktır.

• TSE söz konusu cihazlar için standart tanımlayacaktır.

• Sanayi Bakanlığı endüstrideki aday üreticileri yönlendirecektir.

• Üretilen ürünlerin testleri ve uyumluluğu TÜBİTAK UEKAE tarafından gerçekleştirilecektir.

• TSE üretilen cihazlara onay verecektir.

• Bayi ve teknik desteğe sahip dağıtım ağı ile son kullanıcıya ulaştırılacaktır.

KEC GENEL TEKNİK ÖZELLİKLER

Özellik	Açıklama
Güvenlik Seviyeleri	Politika ile belirlenebilen 5 güvenlik seviyesi (Kart(1), Kart(2), Kart+Biyometrik, Kart+PIN, Kart+PIN+Biyometrik)
Uygulamalar	Değişik güvenlik seviyeleri için kimlik doğrulama Her güvenlik seviyesi için yerel ve genel kimlik doğrulama XML tabanlı imza kartı kullanarak doküman imzalama Değişik kimlik doğrulama politikalarına uyumluluk (vekil kullanımı, kimlik doğrulama şartı, jenerik politika , biyometrik kimlik doğrulamanın geçmemesi durumunda hizmete katılanın onayının alınması vs.) Değişik güvenlik seviyelerine göre parmak izi onaylama
Dil Desteği	Türkçe, İngilizce (Değişiklik dillere genişletilebilir)
Erişim Güvenliği	Cihaz ayarları için kullanıcı şifresi, kimlik doğrulama işlemleri için AKiS işletim sistemine sahip Elektronik Kimlik Kartları
Algoritmalar	2048 bit RSA, SHA 256
Kullanıcı Arabirimi	3.5" 240x320 256K renk TFT-LCD Ekran, 20 Tuşlu Tuş Takımı
Kart Yuvaları	4 adet IEC/ISO 7816 uyumlu akıllı kart yuvası: 'Hizmet Veren' Elektronik İmza Kartı Yuvası, 'Hizmet Veren' Elektronik Kimlik Kartı Yuvası, 'Hizmet Alan' Elektronik Kimlik Kartı Yuvası, 1 adet IEC/ ISO 7816 uyumlu GEM yuvası
Biyometrik Sensörler	Parmak İzi Sensörü, Damar izi Sensörü
İkaz Mekanizmaları	Sesli, görüntülü ve ışıklı ikaz
Bilgisayar Arabirimi	1 adet USB 2.0 "Full Speed" host arayüzü (hareketli uç birimi cihazı veya parmak damar izi cihazı için bağlantı) 1 adet USB 2.0 "Full Speed" slave arayüzü 1 adet 10/100Mbit/s Ethernet Arayüzü 1 adet VGA monitor Arayüzü
Güç Sarfiyatı	<5W
Boyutlar	12cm / 21cm / 6,5 cm (G/B/Y)
Ağırlık	472 gr.
Çalışma Sıcaklığı	0ºC ... +45ºC
Depolama Sıcaklığı	-20ºC ... +65ºC
Bağıl Nem	+40ºC'de %90
Desteklenen Standartlar	IEC/ISO 15408 (Common Criteria) Ortak Kriteri- EAL4 EN 55022 EMI/EMC CE

e-kimlikte Açık Anahtar Altyapısı

Ersin GÜLAÇTI

1. GİRİŞ

e-kimlik projesi, uzun süredir kullanılmakta olan kağıda basılı nüfus cüzdanlarının yerini alacak, yeni teknolojileri kullanan bir kimlik kartını gerçekleme hedefiyle başlamıştı. Bugün bu hedefe ulaşıldığını rahatlıkla söyleyebiliriz. Bolu ilinde yapılan pilot çalışmalarla proje kapsamında tasarlanan kimlik kartı yüzbinlerce vatandaşımıza dağıtılmış ve çeşitli uygulamalarda başarıyla kullanılmıştır.

Bu yeni nesil kimlik kartı hem fiziksel güvenlik unsurlarıyla hem de elektronik özellikleriyle tam bir elektronik kimlik niteliğini taşımaktadır. Kısaca e-Kimlik olarak isimlendirdiğimiz bu yeni nesil kartın elektronik güvenlik özelliklerinden belki de en önemlisi olan elektronik sertifikaların nasıl kullanıldığı bu yazıda anlatılmaktadır.

2. AÇIK ANAHTAR ALTYAPISI İLE KİMLİK DOĞRULAMA

Kimlik doğrulamada güvenilir yöntemler kullanılması gerekir. Bir yöntemin güvenilir olması için matemaktiksel olarak güvenilirliğinin ispat edilmiş olması gereklidir. Bir karşılaştırma yapmak için günlük hayattaki yanlış bir uygulamayı – Türkiye Cumhuriyeti Kimlik Numarasının kimlik doğrulama için kullanımını – inceleyelim.

T.C. Kimlik Numarası (TCKNo) her vatandaşa İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (NVİ) tarafından verilen tekil bir numaradır. Bu numara bir vatandaşın diğer tüm vatandaşlardan ayırt edilebilmesini sağlar. TCKNo bir vatandaşın kim olduğunu belirler ancak bir kişinin iddia ettiği kimliğe sahip olduğunu ispatlamaz. Kimlik doğrulama için hala bazı kamu kurumlarında ve özel firmalarda sadece TCKNo bildirimi yapılması yeterli olabilmektedir. Oysa bir kişinin TCKNo bilgisi artık kişiye ait gizli bir bilgi olmaktan çıkmıştır. Çeşitli nedenlerle çok sayıda vatandaşın TKCNo'su internette yayınlanmış veya nüfus cüzdanı fotokopisini çeken banka, noter vb yerlerde TCKNo sahibinden farklı kişilerce görülmüştür. Bu nedenle sadece TCKNo'yu bilmek bu TCKNo'ya sahip kişi olunduğunu ispat etmek için yeterli olamaz.

Güvenli bir kimlik doğrulama yönteminin şu özelliklere sahip olması gerekir:

1. Kimlik bildirim bilgisi kopyalanamamalıdır. Bir işlemdeki kimlik bildirimi bilgisinin diğer bir işlemdekinden farklı olması gerekir.

2. Kimlik bildirim bilgisi taklit edilememelidir. Kimlik bildirim bilgisinin benzeri kolayca oluşturulamamalıdır. Kimlik bildirim bilgisi tahmin yoluyla oluşturulamayacak kadar zor olmalıdır.

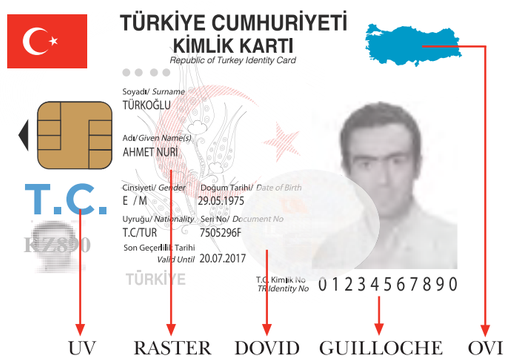
3. Kimlik bildirim bilgisi kimliğin gerçek sahibinin rızası dışında oluşturulamamalıdır.

4. Kimlik bildirim bilgisinin doğru veya yanlış olduğu kolayca ve kesin bir şekilde tespit edilebilmelidir.

Bu özelliklerden hiçbirisi TCKNo ile kimlik doğrulama yapılması yöntemi ile karşılanamamaktadır. Bu nedenle bu yöntemin terk edilmesi gerekmektedir.

Devletin vatandaşlara verdiği hizmetlerde, hizmetin gerçekten hak sahibine verildiğinden emin olunması gereklidir. Bunun için hizmet sunan kurumun kimlik doğrulamayı güvenli bir şekilde yapması zorunludur.

Yüz yüze hizmet noktalarında (hastahane, vergi dairesi vb.) kimlik doğrulama geçerli bir kimlik belgesine bakılarak yapılmaktadır. Ancak bu işlem kimlik doğrulamayı yapan memurun kişisel yorumu ve insiyatifine bağlı olarak gerçekleşmektedir. Bu tür doğrulama yöntemlerinin özellikle kayıt tutulması gereken işlemlerde terk edilmesi gereklidir. Ancak yine de bazı hizmetlerin verilişi sırasında kimlik belgesinin gözle denetimi yönteminden vazgeçilemez (Polis denetimi, kişinin yaşının kontrol edildiği mekanlar vb). Bunun için kimlik kartının fiziksel güvenlik öğeleri ile güçlendirilmesi gereklidir. Pilot projede kullanılan fiziksel güvenlik öğeleri Şekil 1'de görülmektedir.



Şekil 1. *Fiziksel güvenlik öğeleri.*

Uzaktan hizmet sunumu verilen veya yüz yüze hizmet sunumunun kayıt altına alınması gereken hallerde elektronik kimlik doğrulama yapılması gereklidir. Bunun için tüm vatandaşların e-Kimlik kartlarına sahip olması gerekir.

E-kimlik kartları akıllı kart teknolojisi ile üretilmiştir. e-Kimlik kartlarının üstünde yer alan mikroişlemci yongaları Ortak Kriterler Standartına göre test edilmiş ve CC EAL 5+ seviyesinde güvenliği belgelenmiş donanımlardır. Yine bu yongalar üstünde koşan işletim sistemi (AKİS) CC EAL 4+ seviyesinde belgelendirilmiştir. Bu yongalar kişilere ait özel sayıları saklamak için kullanılır. e-Kimlik kartı tasarımı kartın içine yüklenen özel sayıların dışarıya çıkarılmasına, okunmasına ve kopyalanmasına izin vermez. Kartın sahibi istese dahi bu sayıyı elde edemez ancak bu sayı ile matematiksel işlemler yapması için kartın yongasına komutlar gönderebilir. Kart özel anahtarla ilgili komutları işlemeden önce PIN adı verilen kişisel kart

parolasının girilmesini ister. Kart kendisine verilen parametrelere göre kendi içinde sakladığı özel sayı ile dışarından verilen sayılar üzerinde işlem yapar ve sonucu geri verir.

Bu yöntemde hangi özel sayının kime ait olduğu doğrudan bilinemez fakat kullanılan özel sayının matematiksel olarak ilintili olduğu başka bir sayı üretim anında hesaplanarak karta yüklenir. Bu sayının açık olarak yayınlanması bir sakınca taşımaz. Kullanılan algoritmalar özel sayı ile onun ilişkili olduğu açık sayının bu şekilde güvenli olarak kullanımını güvence altına alan ispatı yapılmış algoritmalardır.

Yukarıda bahsedilen algoritmalara açık anahtarlı algoritma adı verilmektedir. Bu algoritmalarda özel anahtar (özel sayı) ve açık anahtar (açık sayı) çifti aynı anda üretilir ve aralarında matematiksel bir bağlantı vardır ancak sadece açık anahtarı bilen bir kişinin özel anahtarı tahmin yoluyla veya başka bir şekilde bulması mevcut teknolojilerle imkansızdır.

Kullanıcıya ait açık anahtar ve kimlik bilgileri, varsa anahtarın kullanım koşulları bir elektronik belge haline getirilerek kullanılır. Bu elektronik belge yayınlayan tarafın elektronik imzası ile imzalanarak sertifika adı verilen bir belge oluşturulur.

Açık anahtar sertifikaları aşağıdaki özellikleri taşır:

- Sayısaldır.
- Sahibi hakkında gerekli olan tüm bilgileri içerir.
- Yayın tarihi ve son kullanma tarihi vardır.
- Yayıncısının adını barındırır ve onun elektronik imzasıyla doğrulanması yapılır.
- Yayıncı adı ve sertifika seri numarası sertifikanın tekil olmasını sağlar.
- Sertifikanın bütünlüğünün bozulması engellenemez ama böyle bir durum sertifika üstündeki elektronik imzanın kontrol edilmesiyle hemen anlaşılır.

2.1. Sertifika Tabanlı Kimlik Doğrulama

e-Kimlik kartının içinde kimlik doğrulamada kullanılabilecek bir anahtar çifti ve bu anahtarlardan açık olanın hangi kimlikle ilişkili olduğunu gösteren bir sertifika yer alır. Elektronik kimlik doğrulaması yapılacağı zaman, ilgili uygulama veya cihaz tarafından karta imzalanmak üzere bir bilgi gönderilir. Kart sahibinin karta ait PIN'i girmesinin ardından kart kendi içindeki özel anahtarla dışarından verilen bilgiyi beraber kullanarak bir değer hesaplar (Bu değere elektronik imza adı verilmektedir). Bu değer ve karta ait açık anahtar sertifikası uygulamaya cevap olarak verilir. Kimlik doğrulaması yapan uygulama gönderdiği bilginin gelen cevapla uyuşup uyuşmadığını denetler. Ayrıca karttan gelen cevabı oluşturan özel anahtara karşılık gelen açık anahtarı taşıyan sertifikanın doğruluğunu (uygulamanın güvendiği bir sertifika makamı tarafından yayınlandığını) ve geçerliliğini (yayıncısı tarafından iptal edilmediğini) denetler.

Sertifika tabanlı kimlik doğrulama düzgün bir şekilde gerçeklenirse güvenli kimlik doğrulamada ihtiyaç duyulan özellikleri sağlar. Tablo 1'de bunun nasıl yapılacağı görülmektedir.

Tablo 1. Sertifika Tabanlı Kimlik Doğrulama

No	Özellik	Sertifika Tabanlı Kimlik Doğrulama
1	Kimlik bildirim bilgisi kopyalanamamalıdır. Bir işlemdeki kimlik bildirimi bilgisinin diğer bir işlemdekinden farklı olması gerekir.	Kimlik bildirim bilgisi olarak kimlik doğrulama uygulaması tarafından gönderilen bilginin elektronik imzalı hali kullanılır. Her kimlik doğrulamada uygulamaların farklı bilgileri imzalanmak üzere e-kimlik kartına yollaması gerekir. Aksi takdirde kaydedilen bir kimlik doğrulaması sonraki işlemlerde de kullanılabilir.
2	Kimlik bildirim bilgisi taklit edilememelidir. Kimlik bildirim bilgisinin benzeri kolayca oluşturulamamalıdır. Kimlik bildirim bilgisi tahmin yoluyla oluşturulamayacak kadar zor olmalıdır.	Kimlik bildirim bilgisini hazırlayan özel anahtar e-kimlik kartının içinde çok yüksek güvenlik önlemleriyle saklanmakta ve kullanılmaktadır. Bu nedenle taklit edilmesi imkansız derecesinde zordur. Özel anahtarların boyutları tahmin yoluyla bulunamayacak kadar uzun seçilmelidir. Örneğin e-kimlik kartında kullanılan anahtar boyutu 2048 bittir ve onluk sistemde 617 basamaklı bir sayıya denk gelmektedir.
3	Kimlik bildirim bilgisi kimliğin gerçek sahibinin rızası dışında oluşturulamamalıdır.	E-kimlik kartının özel anahtarını kullanmak için gereken kartın PIN değeri sadece kart sahibi tarafından bilinmelidir.
4	Kimlik bildirim bilgisinin doğru veya yanlış olduğu kolayca ve kesin bir şekilde tespit edilebilmelidir.	Kimlik bildirimi elektronik sertifika ve elektronik imza kullanarak gerçekleştirildiği için kolayca ve matematiksel kesinlikle doğrulanabilmektedir.

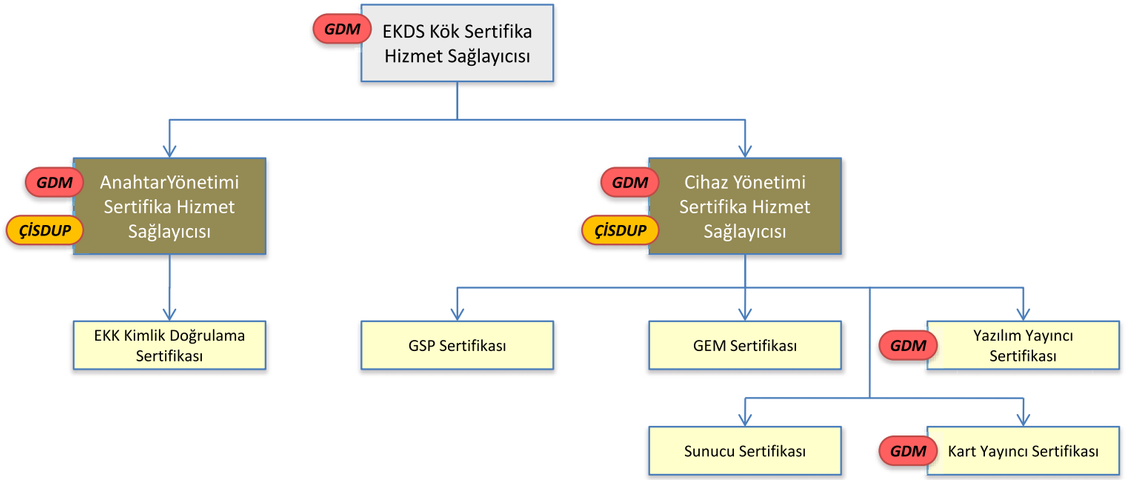
3. PİLOT PROJEDE UYGULANAN MİMARİ

EKDS (Elektronik kimlik Doğrulama Sistemi), internet üzerinden elektronik hizmet veren kurumların gereksinim duyduğu kişisel kimlik doğrulama işlevini e-Kimlik kartı kullanarak karşılamayı amaçlayan bir sistemdir. Bu sistemdeki kartlarda, sunuculara, kart erişim cihazlarında ve benzeri yerlerde asimetrik anahtar çiftleri kullanılmaktadır. Bu anahtar çiftlerinin yönetimi için TÜBİTAK UEKAE tarafından geliştirilmiş olan yazılımlar ve donanımlar kullanılmaktadır.

Pilot proje kapsamında Bolu ilindeki tüm vatandaşlara e-Kimlik kartı üretilmiş ve dağıtılmıştır. Pilot projede sertifika sisteminin ana mimarisi Şekil-2'de görüldüğü gibi kurulmuştur.

Bu mimaride görülen bileşenlerin açıklamaları aşağıda yer almaktadır:

- **EKDS Kök Sertifika Hizmet Sağlayıcısı (EKDS Kök):** Kendi açık anahtarını kendi özel anahtarı ile imzalamış olan makamdır. Bu makamın sertifikası tüm sistemin güvendiği kök sertifikadır. Bu nedenle sertifika kullanan yazılım ve donanımların içinde güvenli olarak saklanmaktadır.
- **Anahtar Yönetimi Sertifika Hizmet Sağlayıcısı (AYSM):** EKK (Elektronik Kimlik Kartı) kartlarının içine kimlik doğrulama sertifikası ve ilgili anahtar çiftini yazan makamdır.



Şekil 2. *Pilot projede AAA mimarisi.*

• **Cihaz Yönetimi Sertifika Hizmet Sağlayıcısı (CYSM):** GEM (Güvenli Erişim Modülü) kartlarının içine cihaz imza sertifikası ve ilgili anahtar çiftini yazan makamdır. GSP (Güvenlik Servisleri Platformu) ve sistemdeki diğer sunucular için ihtiyaç duyulabilecek sertifikaları ve anahtar çiftlerini üretir.

• **Kart Yayıncı Sertifikası:** NVİ tarafından kullanılan ve anahtar çifti bir GDM (Güvenli Donanım Modülü, '*Hardware Security Module*') içinde saklanan sertifikadır. Nüfus bilgilerini imzalamakta kullanılır.

• **Yazılım Yayıncı Sertifikası:** UEKAE tarafından yazılım terfi işlemlerinin güvenliği için kullanılan sertifika ve ilgili anahtar çiftidir (anahtar çifti bir GDM içinde saklanır).

• **EKK Kimlik Doğrulama Sertifikası:** Kartın üstüne basılan seri numaraya bağlı olarak üretilen sertifikadır. Asıl işlevi kartın güvenilen bir makam tarafından üretildiği göstermektir. Kartın içindeki elektronik nüfus bilgisi ile beraber kullanıldığında kimlik doğrulamaya yarar.

• **GEM Sertifikası:** Güvenli Erişim Modülü (GEM) adı verilen ve yüksek güvenlikte kimlik doğrulama yapmaya yarayan Kart Erişim Cihazına (KEC) takılan akıllı kartlara yüklenen sertifikadır. Bu sertifika KEC'in kimliğinin doğrulanması amacıyla kullanılır.

• **GSP Sertifikası:** E-kimliğin entegre edildiği sistemlerde güvenli kimlik doğrulama için kullanılan Güvenlik Servisleri Platformu sunucuları da yer alabilir. Bu sunucuların kimliklerinin doğrulanması için GSP sertifikaları kullanılır.

4. SERTİFİKA YAŞAM DÖNGÜSÜ HİZMETLERİ

e-Kimlik kartı pilot projesinde gerçekleştirilen sertifika yaşam döngüsü hizmetleri geleneksel bir açık anahtar altyapısı hizmetinden çok farklı değildir. ESYA Sertifikasyon Makamı yazılımları tarafından sunulan bu hizmetlerin içeriği kısaca aşağıda verilmiştir.

4.1. Sertifika Üretimi

Sertifika üretimi hizmeti bir sertifikaya yerleştirilecek kimlik bilgileri ile açık anahtar bilgisinin bir araya getirilmesi ve kullanılan sertifika formatı standardına (Ör. ITU X.509 standardı) uygun olarak kodlanmasıdır. Sertifika üretiminde kullanılacak sertifika şablonlarının titizlikle kurgulanması, test edilmesi ve üretim sürecine sokulması gereklidir.

Sertifika üretiminde, ESYA yazılımları TÜBİTAK UEKAE tarafından geliştirilmiş olan anahtar üretim kartlarını kullanarak yüksek kalitede ve çok miktarda anahtarı kısa sürede hazırlayabilmektedir. Anahtar üretim kartları özel olarak tasarlanmış ve istatistiki ve fiziksel testlerden geçirilmiş donanımlardır. Bu cihazların ürettiği anahtar çiftleri gerçek rastgele sayılardan türetilirler. Bu nedenle tahmin edilmeleri imkansızdır.

4.2. Sertifika Durum Değişikliği Yönetimi

Üretilen sertifikaların üç temel geçerlilik durumu bulunur. Bunlar

• Geçerli

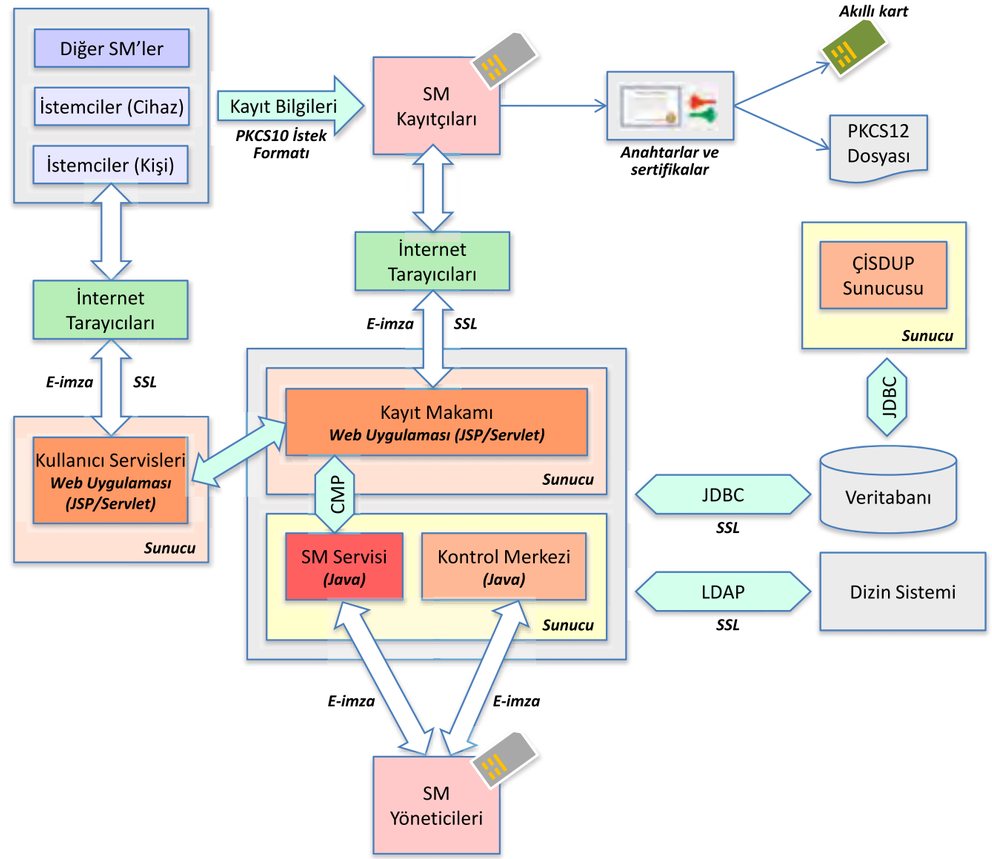
• İptal

• Askıda olarak listelenebilir. İptal edilen bir sertifika tekrar "Geçerli" duruma getirilemez. Askıya alınan bir sertifika sonradan" Geçerli" duruma getirilebilir. Bu işlem "askıdan indirme", "aktivasyon" vb. adlarla da bilinmektedir. Sertifikaların durum değişiklikleri, e-Kimlik projesi kapsamında geliştirilen ve NVİ tarafından kullanılan Kart Yönetim Merkezi (KYM) sunucuları tarafından ESYA Sertifika Makamına gönderilen komutlarla gerçekleştirilir.

4.3. Sertifika Durumu Sorgulama Hizmetleri

Üretim evresinden sonra bir sertifika e-Kimlik kartının kaybedilmesi, çalınması veya başka nedenlerle Askı veya İptal durumuna getirilmiş olabilir. Bu durumdaki sertifikalarla oluşturulan elektronik imza ve kimlik bildirim bilgileri güvenli kabul edilmez ve işleme sokulmaz. Bu nedenle e-Kimlik kartıyla yapılan hemen hemen tüm işlemlerde sertifika durumu sorgulanır. Günlük hayatta e-Kimlik kartının kullanımı yaygınlaştıkça sertifika durumu sorgu sayısı da artacaktır.

Sertifika durumu sorgulamak için iki temel yöntem vardır:



Şekil 3. *ESYA mimarisi*

Sertifika İptal Listesi (SİL)

SİL adı verilen liste, iptal veya askı durumundaki sertifikaların seri numaralarını, iptal gerekçelerini ve iptal tarihlerini tutan ve genelde sertifika yayıncısı tarafından üretilen bir elektronik belgedir. Her SİL'in bir geçerlilik başlangıç ve bir de geçerlilik bitiş tarihi vardır. Sertifika makamı yayımladığı SİL'in süresi bittiğinde yenisini yayınlar. SİL verileri genelde web sunucuları üstünden kullanıma sunulur.

Özellikle çok sayıda sertifika üretmiş sistemlerde SİL dosyasının boyutu çok artabilir. e-Kimlik projesinde SİL boyutunun artması ihtimali nedeniyle "Delta SİL" uygulaması yapılmaktadır. Delta SİL uygulamasında uzun aralıklarla "Temel SİL yayınlanır. Temel SİL yayın tarihinden sonra sık aralıklarla Delta SİL yayınlanır. Her Delta SİL, son Temel SİL'in yayınından sonra meydana gelen tüm sertifika durum değişikliklerini içerir.

e-Kimlik projesinde SİL kullanımının özellikle çok işlem yapan uygulama sunucularında yararlı olabileceği düşünülmektedir. Bu tür sunucular SİL içeriğini belleğe alarak her sertifika için Çevrimiçi Sertifika Durum Sorgusu Protokolü (ÇİSDUP) sorgusu yapmaktan zorunluluğundan kurtulabilirler.

Çevrimiçi Sertifika Durum Sorgusu Protokolü (ÇİSDUP)

İngilizce adıyla *Online Certificate Status Protocol (OCSP)* olarak bilinen ÇİSDUP, özellikle kısa mesaj yapısı ve sertifika durumlarının sunucuya tek tek sorulabilmesi nedeniyle tercih edilmektedir. Büyük ve hantal SIL dosyaları son kullanıcıların kişisel bilgisayarlarda kullanımına uygun değildir. Bu nedenle sadece işlem yapılan sertifikanın seri numarasının sorgu mesajı içinde gönderildiği ÇİSDUP sorgusu kullanılması pratik olmaktadır.

ÇİSDUP sunucusu kendisine sorulan sertifikanın seri numarasını kullanarak sertifikayı sertifika makamı veritabanından bulur. Sertifika eğer geçerli ise "GEÇERLİ" cevabı sorgu yapan tarafa gönderilir. Sertifika eğer veritabanında bulunmuyorsa "BİLİNMİYOR" cevabı sorgu yapan tarafa gönderilir. Eğer sertifika iptal veya askı durumundaysa iptal nedeni ve iptal tarihi sorgu yapan tarafa gönderilir.

5. AAA BİLEŞENLERİ

e-Kimlik projesindeki sertifika yönetimi işleri çok sayıda yazılım ve donanım gerekmektedir. Bunlara aşağıda kısaca değinilmektedir.

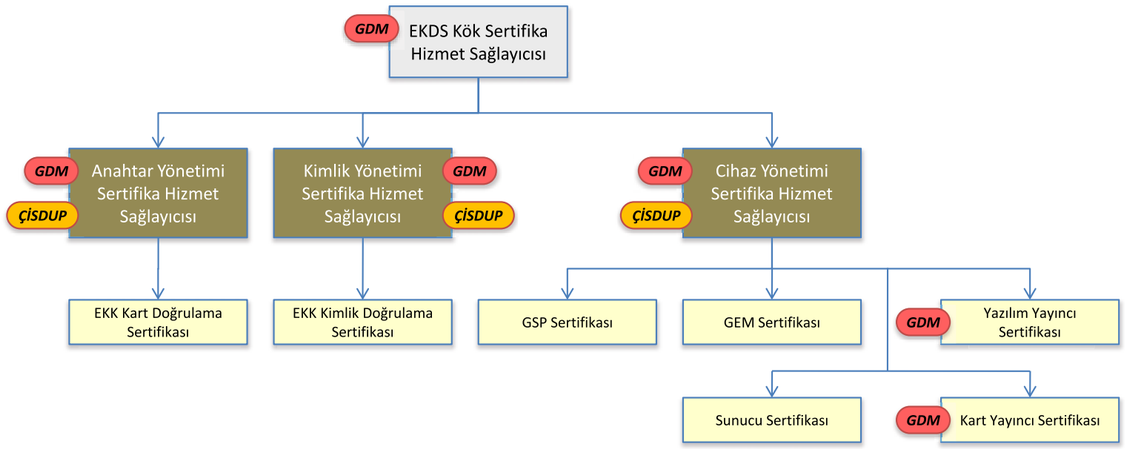
5.1. Yazılım Bileşenleri

Sistemdeki her bir sertifika sağlayıcısı ESYA yazılımı kurulu sunucu sistemleri çalıştırmaktadır. ESYA mimarisi Şekil-3'de görüldüğü gibidir.

ESYA Sertifikasyon Makamı yazılımları bugüne kadar 30'dan fazla kurumda 400,000'nin üzerinde elektronik sertifikanın üretiminde kullanılmıştır. ESYA 1.0 sürümü Türk Standartları Enstitüsü tarafından Ortak Kriterler Standardında göre test edilmiş ve 2 Mart 2010 tarihinde CC EAL4+ sertifikası almıştır. ESYA, dünyada benzer ürünler arasında CC EAL4+ sertifikası olan dördüncü ürün olmuştur.

5.2. AAA Donanım Bileşenleri

E-kimlik projesinde kullanılacak donanımların sertifika yaşam döngüsü ile ilgili ihtiyaçları karşılayacak kapasitede olması gerekmektedir. Pilot projede AAA sunucuları Kamu Sertifikasyon Merkezi'nde barındırılmış ve işletilmiştir. Seçilen donanımların özellikleri genel olarak şöyledir:



Şekil 4. *Yaygınlaştırma için Sertifika mimarisi*

Sunucu Özellikleri: 2 işlemcili (4 çekirdekli), en az 4 GB RAM'e sahip, tüm kritik bileşenleri (güç kaynağı vb) yedekli olan, hot swap disklere sahip.

Güvenli Donanım Modülü Özellikleri: Ağ tipi veya PCI yuvasına takılabilen, en az saniyede 100 adet RSA 2048 bit anahtar işlemi yapabilen, FIPS 140-2 Level 3 ve üstü sertifikaya sahip.

Anahtar Üretim Kartları: +5 C ile +55 C sıcaklıkları arasında aynı kalitede çalışabilen, PCI Express arayüzüne sahip, TÜBİTAK UEKAE Kripto Analiz Merkezi tarafından test edilmiş ve onaylanmış.

6. YAYGINLAŞTIRMADA UYGULANMASI DÜŞÜNÜLEN MİMARİ

Yaygınlaştırma aşamasında pilot projeden biraz daha farklı bir sertifika mimarisine geçilmesi planlanmaktadır. Söz konusu mimari Şekil 4'te gösterilmektedir.

Bu mimaride pilot projeden farklı olan bileşenler şöyledir:

• Anahtar Yönetimi Sertifika Hizmet Sağlayıcısı (AYSM): EKK (Elektronik Kimlik Kartı) kartlarının içine kart doğrulama sertifikası ve ilgili anahtar çiftini yazan makamdır.

• Kimlik Yönetimi Sertifika Hizmet Sağlayıcısı (KYSM): EKK (Elektronik Kimlik Kartı) kartlarının içine kimlik doğrulama sertifikası ve ilgili anahtar çiftini yazan makamdır.

• EKK Kart Doğrulama Sertifikası : Kartın üstüne basılan seri numaraya bağlı olarak üretilen sertifikadır. Asıl işlevi kartın güvenilen bir makam tarafından üretildiği göstermektir.

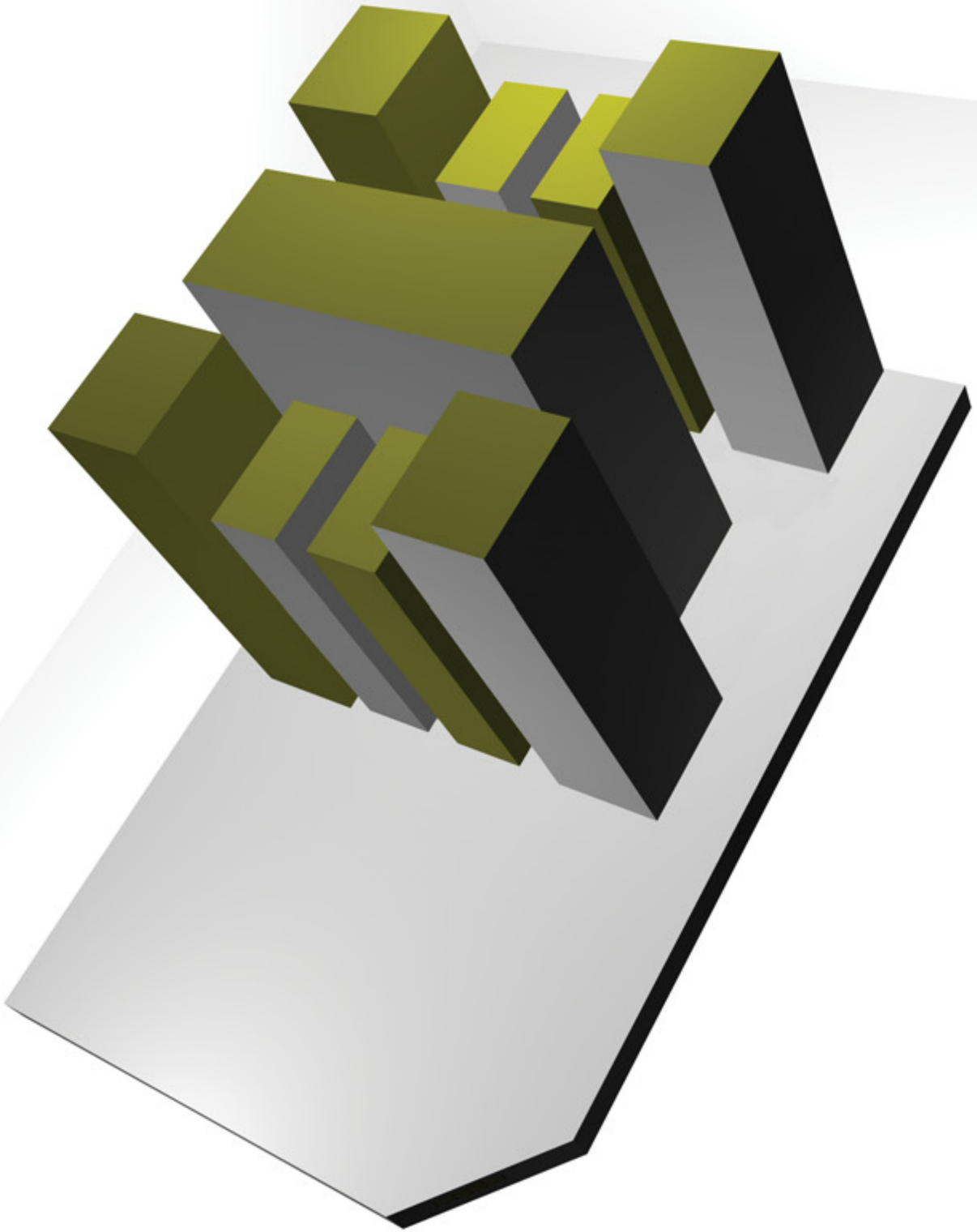
• EKK Kimlik Doğrulama Sertifikası : Kartın sahibi olan kişinin kimlik bilgilerini içeren ve kişiselleştirme sırasında üretilen sertifikadır. Tek başına kullanıldığında bile kimlik doğrulamaya yarar. Bu sertifika, e-Kimlikle çalışan ve internet üzerinden hizmet veren servislerin çok hızlı bir şekilde kurulması ve işletime alınması için yararlı olacaktır.

Yaygınlaştırma aşamasında tüm hizmetlerin ölçeklendirilmesi gerekmektedir. Yaygınlaştırma planı belirlendiğinde kesin rakamlar ortaya çıkacak olmakla beraber kurulacak sistemin her yıl en az 15 milyon yeni kimlik kartı üretmesi beklenmektedir. Toplamda 80-100 milyon arası kimlik kartının üretimi ve dağıtımı gerçekleşecektir. Her sene doğum, ölüm, kayıp, yenileme vb nedenlerle de 10 milyon üzerinde yeni kartın verilmesi gerekecektir. Bu bakımdan kurulacak sistemin dünyanın en büyük açık anahtar altyapısı sistemi olacağı görülmektedir.

Bu sistemde diğer önemli bir konu da sertifika durum sorgularına cevap verebilmektir. Güncel KPS (NVİ Kimlik Paylaşım Sistemi) sorgu istatistiklerine bakarak yapılan öngörüye göre talebin en yoğun olduğu mesai saatlerinde saatte 3 milyon adet ÇİSDUP sorgusu yapılabileceği düşünülmektedir. Bu yükü kaldırabilecek altyapı çalışmaları ve testleri halen TÜBİTAK UEKAE tarafından yürütülmektedir. Dünyada bu kadar çok sertifikayı yöneten bir başka sistem olmadığından TÜBİTAK UEKAE tarafından geliştirilen ürün ve çözümlerin başka ülkelere de örnek oluşturacağı tahmin edilmektedir.

4. SONUÇ

E-kimlik kartı projesi veya bir bütün olarak baktığımızda Elektronik Kimlik Doğrulama Sistemi çok yoğun şekilde elektronik sertifika, elektronik imza ve açık anahtar altyapısı hizmetlerinin kullanıldığı bir projedir. e-Devlet hizmetlerinde kimlik doğrulamanın belkemiği olarak hizmet verecek olan bu sistemin uluslar arası standartlara uygun milli ürünlerle, yüksek güvenlikte, kaliteli ve kesintisiz hizmet sunması çok önemlidir. Dünyanın en fazla kullanıcılı açık anahtar altyapısı olması beklenen sistemin, işletimi ve idamesi için TÜBİTAK UEKAE yazılım ve donanım ürünleri, bilgi ve tecrübe birikimi ve yetişmiş insan gücü ile göreve hazırdır.



Akıllı Kartlar ve Uygulamaları

AKILLI KART İŞLETİM SİSTEMLERİ ve UKİS

Mustafa BAŞAK
Aydın KUBİLAY

Akıllı kartlar taşıdığı bilgiler ve kullanım kolaylığı açısından, her geçen gün hayatımıza daha fazla girmektedir. Taşıdıkları bilgi miktarıyla koşut olarak kullanım alanları da artmaktadır. Tersi de doğrudur. Bu döngü böylece sürüp gitmektedir. Son zamanlarda bilginin niceliğiyle birlikte niteliğinin de yükseldiği ve değerinin arttığı ortaya çıkmaktadır. Taşınan bilgi kredi kartlarındaki gibi maddi değer de ifade edebilir, elektronik kimlik kartlarındaki gibi kişinin ömür boyu değiştirilemeyecek olan biyometrik bilgisini de taşıyabilir. Ya da kişiye ait özel bilgileri saklar. Bu nedenle akıllı kartlar artık kişisel doğrulama amaçlı bilgi teknolojileri alanında kullanılmaya başlanmıştır. Bu nedenle, güvenlik önemli bir konu haline gelmiştir. Bu yazıda özellikle akıllı kart tabanlı kimlik kartları için geliştirilen ulusal akıllı kart işletim sistemi ve çalışmalar sırasında hesaba katılması gereken güvenlik önlemleri üzerinde durulmuştur.

1. Giriş

Akıllı kartlar, insanların belli bir mal ve hizmetten yararlanmak amacıyla kişiye özel olarak basılmış plastik kartların evrimi sonucu ortaya çıkmıştır.

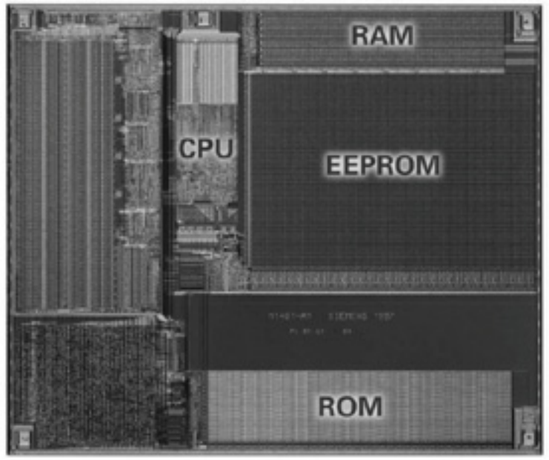
Plastik kartların akıllı kartlara dönüşmesinin altında yatan en önemli etken güvenlik eksikliği ve kopyalanma riskidir. Bu iki olumsuzluğu engellemek ancak kişinin bildiği bir bilginin (PIN) veya sahip olduğu bir özelliğin (biometrik veri) güvenli bir şekilde saklanması ve sorgulanması ile gerçekleştirilir. Bu gereksinmenin işlem gücü gerektirmesi nedeniyle niteliksiz plastik kartlar yerine elektronik tümdevre içeren akıllı kartlar kullanılmaya başlamıştır. Aşağıda Türkiye Cumhuriyeti kimlik kartları için geliştirilmiş ulusal akıllı kart işletim sistemi ile ilgili bilgiler verilmektedir.

2. Ulusal Akıllı Kart İşletim Sistemi (UKiS) Geliştirilmesi

Kimlik kartı projesinin temelinde yine TÜBİTAK UEKAE tarafından geliştirilen açık anahtar altyapısı (AAA) ve sayısal imza projeleri bulunmaktadır. Akıllı kart işletim sistemi (AKiS), ilk olarak sayısal imza uygulamasında başarılı bir şekilde kullanılmıştır. Daha sonra da akıllı kart tabanlı Elektronik Kimlik Doğrulama Sistemi (EKDS) çalışmalarına başlandı. İlk olarak açık anahtar altyapısında kullanılan AKiS işletim sistemi üzerine eID uygulaması konuldu. Böylece geliştirme aşaması daha sağlıklı ve güvenli oldu. Projede, güvenlik onayı CC EAL5+ seviyesinde olan iki ayrı firmanın donanımları kullanıldı. Zamanla, EKDS projesi kapsamında, milli yonganın geliştirilmesiyle, AKiS'in bazı temel yapıları kullanılarak Ulusal Kart işletim Sistemi (UKiS) geliştirildi. TÜBİTAK UEKAE tarafından geliştirilen akıllı kart mikrobilgisayar tümdevresindeki mikroişlemci ünitesinin ve bağlı bulunduğu çevre birimlerinin kullanılması sağlandı. Sonuç olarak, ulusal bir işletim sistemiyle çalışan bir akıllı kart yongası elde edilmiş oldu. UKiS'te ayrıca eID uygulaması da ROM ('*Read-Only Memory*', Salt Okumalı Bellek) bellekte bulunmaktadır. O da AKiS gibi sonradan değişmez "native" yapıdadır.

Elektronik kimlik uygulamaları, zamanla değişim gerektiren uygulama kodları içermediğinden bu yapıyı değiştirmek gerekmez. Bu nedenle sonradan yüklenebilen veya değiştirilebilen Java uygulamaları eID'de kullanılmamıştır. Bu tercihin en önemli gerekçesi güvenliktir. Sonradan yüklenebilen veya değişken kodlar içeren uygulamalar akıllı kartların EEPROM ('*Electronically Erasable Programmable Read-Only Memory*', Elektriksel Silinebilir Bellek) belleğini kullanır. Bu bellek hem fiziksel ömür hemde saldırılar açısından daha risklidir. Ayrıca zaten sınırlı olan EEPROM alanı daha da azalmaktadır. Bu nedenle uygulaması da EEPROM'a yüklenen sistemlerde kişisel bilgiler, fotograf veya biometrik verilere bellek kısıtı oluşmaktadır. Bu nedenlerden dolayı UKiS de AKiS gibi değişmez "native" yapıda tasarlanmıştır.

Akıllı kart donanımı, üzerinde bir işletim sistemi ve onu kullanan bir uygulama olmadan hiç bir işlem görmez. Bu nedenle güvenliği sağlanmış bir donanım üzerinde mutlaka bir işletim sistemi ve en az bir uygulama bulunmalıdır. Genellikle ve yukarıda açıklanan nedenlerden dolayı, işletim sistemleri akıllı kart yongalarının ROM'unda bulunurlar. Bunlar bir bölümü EEPROM'a yüklenen işletim sistemlerine göre çok daha basittir. Çünkü ikinci tiplerde bu işlem, "uygulamanın sertifikalandırılması" adı verilen, güvenlik açısından karmaşık bir sürecin tamamlanması sonrasında gerçekleştirilir. Bu nedenle, AKiS ve UKiS değişmez "native" bir işletim sistemi olarak tasarlanmıştır. Tamamıyla ROM üzerinde bulunmaktadır. Ancak, kullanılacak uygulamaya göre, uygulama verileri EEPROM olarak adlandırılan bellek alanında, AKiS/UKiS Dosya/Bellek yönetim sistemi tarafından, gelişmiş güvenlik önlemleri alınarak saklanmaktadır. Akıllı kart işletim sistemleri dış dünya ile iletişmini iki adet iletişim ucu üzerinden, APDU olarak adlandırılan uygulama protokol veri paketleri aracılığıyla sağlar. Bu iletişim protokolü ISO7816-2/3/4 standartlarıyla tanımlanmıştır. EKDS projesinde geliştirilen AKiS/UKiS işletim sistemleri üzerinde çalışan elektronik kimlik uygulamasıda akıllı kartlar ve uygulamaları için tanımlı tüm standartları sağlamaktadır.



3. Akıllı Kart İşletim Sistemi, AKiS ve UKiS Yazılım Yapısı

Bir işletim sistemi ve uygulama olmadan tek başına anlam taşımaz. Çünkü akıllı kart uygulamaları dış birimler ile etkileşimli çalışmaktadır. Akıllı kart kullanan uygulamalar tarafından gereksinim duyulan birçok işlevin çalıştırması ve kullandığı EEPROM belleğinin belli bir yapıda düzenlenmesini gerekir.

Öncelikle akıllı kart işletim sistemi ile akıllı kart uygulamaları arasındaki farkı belirtmekte yarar var. Akıllı kart işletim sistemi akıllı kart içerisindeki verilerin, uygulama da dış birimdeki uygulamaya özgü verilerin yönetimi görevlerini üstlenmektedir.

AKiS, UKiS ve elektronik kimlik uygulamasının ROM'da olduğunu belirtmiştik. Elektronik kimlik uygulamasının belli bir sistematikte çalışabilmesi için AKiS/UKiS gerekli hiyerarşik yapıyı sağlar. İşletim sistemi yapısında dört ayrı yazılım bileşeni bulunmaktadır:

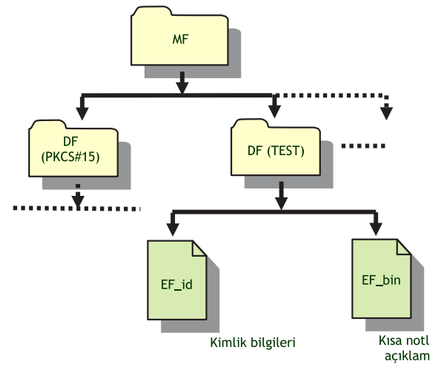
1. Bellek Yöneticisi (*Memory Manager*)
2. Dosya Yöneticisi (*File Manager*)
3. Komut yorumlayıcı (*Command Interpreter*)
4. İletişim arayüzü (*Communication Handler*)

Bunlar haricinde donanıma ait bazı arayüz işlevleri de vardır. Ancak bunlar yonga tasarımcılarınca sağlandığından işletim sistemi bileşenlerine dahil edilmemiştir.

4. Dosya / Bellek Sistemi

AKiS/UKiS işletim sisteminin en önemli özelliği özgün ve kolay yönetilebilir bir Dosya/Bellek Yönetim Sisteminin olmasıdır. Aşağıda bir örneği gösterilen yapıdaki dosya ve dizinlerin oluşturulması ve oluşturulan dosyalara değişik evrelerde verilerin kaydedilmesine olanak tanıyan bir mimariye sahiptir. Böylece akıllı karttaki dosya sistemi önkişiselleştirme birimi, kişiselleştirme ise başka bir birim tarafından gerçekleştirilebilir.

Aşağıda tipik bir akıllı kart uygulamasına ait dosya yapısı gösterilmektedir. AKiS/UKiS de bulunan EEPROM'da dosyalar (EF) ve dizinler (DF) aşağıdaki mantıksal yapıda tutulur. Bu dosya ve dizinlere erişim, anahtarlar ve erişim koşulları ile kısıtlanmaktadır.



AKiS/UKiS, AAA uygulaması için PKCS#15 standartında veri yapısı, elektronik kimlik kartı uygulaması için de TÜBİTAK UEKAE'de oluşturulan EKDS veri yapısı yüklenerek her iki uygulamayı da çalıştırabilir.

Bunların yanında uygulamanın ihtiyaç duyduğu bellek miktarı olanak verdiği sürece başka uyulamalar için de gereksinim duyulan veri yapılarını yükleyip ISO 7816-4 komutları ile gerçekleştirme olanağına sahiptir.

5. Güvenli Bir Akıllı Kart Nasıl Olmalıdır?

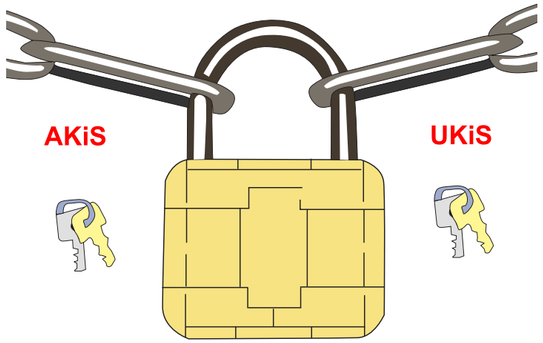
Akıllı kartlara yönelik geliştirilen saldırılara karşı akıllı kart tarafında hem donanımsal hem de yazılımsal önlemler alınmaktadır.

Aşağıda AKiS/UKiS'in sağlıklı ve güvenli çalışması için gerekli donanımsal ve daha sonra da işletim sistemi düzeyinde uygulanan güvelik önlemleri iki ayrı başlıkta sıralanmıştır.

Akıllı kart tümdevresindeki güvenlik önlemleri

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

Akıllı kart tümdevresinin yüzeyinin kazılarak analiz edilmesini önlemek için değişik yöntemler uygulanmaktadır. İlk olarak silikon yapıda oluşturulan RSA, DES veya RNG gibi önemli bloklar tümdevreye rasgele yerleştirilirler. Bir başka yöntem de etkin koruyucu kalkandır. Tümdevrenin lazerle kesilmesi saldırısına karşı tümdevre üzerine ikinci bir metal tabaka konarak kart içerisindeki yapıların ortaya çıkması engellenir. Ayrıca daha güçlü akıllı kart yongalarında, tümdevre yüzeyinden değerli verileri okumayı engellemek için, etkin kalkan da kullanılır. Bu özel yapıda tümdevre yüzeyinde gelişigüzel dizilmiş ve rasgele sayı üretecinden elde edilen verilerle beslenen çok ince veri yolları bulunmaktadır. Etkin kalkan bu veri yollarındaki değişken verilerin doğruluğunun denetlenmesi ilkesine göre çalışır. Eğer bu yüzey aşındırılacak olursa veri yollarındaki veriler hatalı olacağından mikrobilgisayar kendisini güvenli konuma sokacaktır (güvenli bekleme durumu).



Akıllı kart işletim sisteminin güvenlik önlemleri

Aşağıda maddeler halinde AKiS/UKiS işletim sistemlerinin güvenlik önlemleri anlatılmaktadır.

- Algoritmaların işlem süreleri sabitlenerek yan kanal ve zamanlama analizleri ile gizli bilginin açığa çıkarılması önlenir. Eğer herhangi bir işlemin gerçekleşme süresi gizli bilginin içeriğine bağlı olarak değişiyorsa, bu bilgi güç analizi ile ortaya çıkabilir. Bu nedenle giriş değerleri ne olursa olsun işlem süreleri sabit tutulmalıdır. Bunun için gerekiyorsa algoritmaya rasgele gecikmeler eklenir.

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

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

- Algoritmalarda gerçekleştirilen kritik karşılaştırma işlemlerine çifte denetim konulup sonuçlar karşılaştırılarak hatanın önüne geçilebilir.

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

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

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

- DES algoritmasının zayıflığından dolayı veri şifreleme ve deşifreleme için 3DES ve hatta AES algoritmasının kullanılması önerilir.

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

Akıllı kartlardan en temel beklenti güvenliktir. Bunun yanısıra dayanıklı bir sistem olması gerekir. Akıllı kartların güvenliği için hem akıllı kart donanımının (mikrobilgisayarının) hem de onun üzerinde çalışan işletim sisteminin uyması gereken kuralların bulunduğu vurgulanmıştı. Bu bölümde akıllı kart güvenliğini belirleyen faktörlerin neler olduğu ve, nasıl belirleneceği sorularına cevap vermeye çalışılacaktır. Akıllı kart benzeri şifreleme cihazlarının ne kadar güvenli olduğu üzerinde fikir birliği sağlamak için birçok çalışma yapılmış ve uyulması gereken bazı ölçütler oluşturulmuştur. Bu ölçütler zamanla Ortak Ölçütler (*Common Criteria*, CC) adı ile sınıflandırılmış ve yayımlanmıştır. Bunları sağlayan donanım ve yazılımlara bulunduğu sınıfa göre CC sertifikası verilerek gerçeklenen ürünün ne kadar güvenli olduğu ifade edilmiştir. Günümüzde akıllı kart donanım platformu olarak, CC EAL5+ onayı almış yüksek güvenliğe sahip mikrobilgisayarların (örneğin AKiS'in SLE66CLX800PE ve P5CD081 tümdevreleri) kullanılması güvenlik için zorunludur. Akıllı kart ürünlerinin CC seviyesi Ortak Kriter Test Merkezleri'nde belirlenmektedir. Buralarda uygulanan testlerin sonucuna göre güvenlik seviyesini belirtir CC sertifikası verilmektedir.

CC sertifikası, akıllı kart donanımına verilebildiği gibi üzerinde çalışan işletim sistemine de verilmektedir. Akıllı kart kullanarak geliştirilen uygulamalar için kart donanımı, işletim sistemi ve o işletim sistemi üzerinde çalışan uygulamalar ayrı ayrı sertifikalandırılabilir. Bu sertifikalar değişik güvenlik seviyelerine de sahip olabilir. Burada uygulamanın ve uygulamayı kullananların istediği güvenlik seviyesi önemlidir. Örneğin Türkiye Cumhuriyeti Ulusal Kimlik Kartları için bu seviyeler donanım için CC EAL5+, işletim sistemi ve kimlik uygulaması için CC EAL4+ olarak belirlenmiştir.

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

Yukarıda anlatılanlar, akıllı kart kullanımının yaygınlaşmasının güvenliğinin yeterli düzeye çıkması ile olanaklı olduğunu göstermektedir.

6. AKiS ve UKiS İşletim Sistemli Akıllı Kartların Kullanım Alanları

- **Elektronik Kimlik (e-ID) Uygulaması**

Elektronik kimlik uygulaması, akıllı kart tümdevresi içeren bir elektronik kimlik kartının kişinin ülke sertifikası ile doğrulanması ve geçerlenmesi uygulamasıdır. Bu uygulamanın kişiselleştirilmesi ve kullanıma alınması süreci son derece önemlidir. Bu konuda TÜBİTAK UEKAE enstitüsü çok iyi bir deneyime sahiptir. Türkiye Cumhuriyeti Ulusal Kimlik Kartı da bu şekilde gerçekleştirilmiş bir uygulamadır.

- **Sayısal İmza Açık Anahtar Altyapısı (AAA, '*Public Key Infrastructure*', PKI) Uygulaması**

Kişinin ıslak imzadan daha güvenli elektronik imza ile doküman imzalaması veya gelen dokümanın doğru kişiden ve güvenli olarak geldiğinden emin olunması amacıyla geliştirilmiş bir uygulamadır.

- **Elektronik Pasaport Uygulaması**

Gümrüklerde ve ülke giriş/çıkışlarında uygulanan pasaport denetiminde kağıt pasaportlara ek olarak kullanılması planlanan uygulamadır. İşlemlerin daha güvenli, çok daha hızlı ve kolay yapılmasını sağlayacaktır. Bu uygulamada her ülkenin kendisine ait sertifikası yonga içerisine konulur ve pasaportu denetleyen birimin bunu geçerlemesi istenir. Eğer elektronik sertifika geçerlenir ise pasaport doğru, güvenli ve geçerli bir pasaporttur.

- **Sürücü Belgesi Uygulaması**

Yakın gelecekte trafikte araç kullanımı için gereksinim duyulacak bu uygulamanın da AKiS ve UKiS tabanlı işletim sistemleri üzerinde çalıştırılması son derece kolay olacaktır. Tıpkı elektronik pasaport uygulamasında olduğu gibi sürücü belgesini veren kurum kendi sertifikasını yonga içerisindeki uygulamaya yerleştirir ve daha sonra bu sertifika denetlenerek sürücü belgesnin asıl olduğu ve geçerli olduğuna karar verilir.

7. Sonuçlar

Bu yazıda öncelikle ulusal akıllı kart işletim sisteminin geliştirilmesi, mimarisi, dosya bellek yönetim yapısı ve güvenlik önlemleri anlatıldı. Ayrıca bu işletim sistemleri üzerinde koşan uygulamalar hakkında da bilgiler verildi. Şurası bir gerçek ki ulusal işletim sistemine sahip olmak ve özellikle de bunu kendi tasarladığımız bir yonga üzerinde çalıştırmak önemli bir teknolojik seviyeyi göstermektedir.

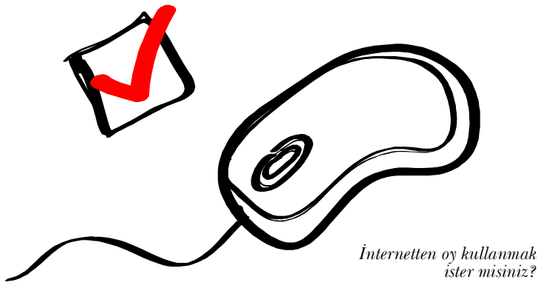
ELEKTRONİK SEÇİM

YÖNTEMLER, UYGULAMALAR, KRİPTOLOJİ ALTYAPISI VE ÜLKEMİZDEKİ GELECEĞİ

Mehmet Sabır KİRAZ
Fatih BİRİNCİ
Umut ULUDAĞ

Tüm dünyada, akademik, kamusal ve endüstriyel sahalarda, elektronik seçim sistemleri incelenmeye başlandı. Bu sistemlerin, kâğıt tabanlı seçim sistemleri yerine ya da onları geliştirmek için kullanılması düşünülmektedir. Böylece, çok daha kısa zamanda seçim sonuçlarının onaylanması, uzun vadede maliyetlerin düşürülmesi ve kâğıt tabanlı sistemlerdeki bazı güvenlik açıklıklarının bertaraf edilmesi hedeflenmektedir. Ancak, birçok uzmanın "kriptolojinin en zor uygulaması" diye nitelendirdiği elektronik seçim sistemi, tamamıyla sorunsuz da değildir. Bu uygulamaların karşılaşabileceği saldırılar ve çözümleri araştırılmaktadır. Ayrıca, bu sistemler büyük ölçeklerde kendini ispatlamamıştır. Dergimizin ileriki sayılarında da devam edilecek bu yazı dizisinde, elektronik seçim sistemlerinin genel tanıtımı, uygulamaları, kriptografik altyapısı, kâğıt tabanlı sistemlerle karşılaştırılması ve hızla gelişen bu teknolojinin ülkemizdeki geleceği ile ilgili değerlendirmeleri bulacaksınız.

Seçimlerde, sandıklarının çalınması, çöpten oy pusulalarının çıkması, mükerrer oy kullanımı veya oyların yanlış/tekrar sayılması gibi haberler, gündemi hayli meşgul eder. Tatilde olduğumuz için oy kullanamadığımız veya oy kullanabilmek için yollara düştüğümüz çok olmuştur. Yurtdışındaki vatandaşlarımızın (ki sayıları milyonlarla ifade edilmektedir) ülkemizdeki siyasi hayata etkisi ne kadardır, kaçta kaçı gümrük kapılarına gidebilmekte ve seçimlere katılabilmektedir? Hatalı veya geçersiz oy verdiğimizi fark ettiğimizde bunu düzeltemediğimize üzülmez miyiz?



İnternetten oy kullanmak ister misiniz?

Yukarıdaki problemler, geleneksel olarak kullanılan "oy merkezinde oylama/kâğıt tabanlı pusula" tekniğinin bazı sonuçlarıdır. Hayli yüksek maliyetler (para, zaman, mekân, insan gücü) ve seçim sonuçlarının açıklanmasının günler alabilmesi de cabası.

Tüm dünyada artan nüfus -ve dolayısıyla artan seçmen sayısı-, insanların, giderek, çok daha az boş zamanlarının olması, teknolojinin gelişmesi ve benzeri sebepler, alışılagelmiş iş modellerinin değişmesine yol açmaktadır. Bir dönüşüm yaşanmaktadır: artık, dersler ve sınavlar elektronik ortamlarda yapılabiliyor, finansal işlemler bilgisayarlar üzerinden yürüyor, vatandaşın kullanımına açılan e-Devlet uygulamalarının sayısı hızla artıyor. Bu değişimin nirengi noktalarından biri de, seçimlerin elektronik ortamda yapılmasıdır. Böylece insanların fikirlerini özgürce belirtmesi ve kendi geleceklerinde söz sahibi olabilmeleri çok kolaylaşacaktır. Bu yazıda alternatif seçim sistemleri tanıtılarak, toplumumuzdaki farkındalık artırılmaya çalışılacaktır. Bu yolla elektronik seçimin artı ve eksilerinin irdelenmesi sağlanacaktır.

1. GİRİŞ

Elektronik Seçim (e-Seçim), geleneksel kâğıt tabanlı oy verme sistemlerinin bazı veya tüm işlevlerini elektronik araçlar kullanarak gerçekleştirmeyi amaçlar [1]. Stratejik bir alan olduğundan her ulus kendi seçimini (elektronik veya kağıt tabanlı) kendi olanakları ile yapmak ister. Bu konuda bilgi ve deneyim geliştirilmesi elzemdir. Çoğu ülkede e-Seçim araştırmaları devlet tarafından desteklenmektedir. Şimdiden, birçok devlet bu konuda araştırma altyapısı kurma çalışmalarını başlatmış, gerekli fonları, hukuki düzenlemeleri sağlamak suretiyle bir tartışma/geliştirme süreci oluşturmuştur [2].

Oylama sistemlerinin demokrasi için hayati derecede önemli bir bileşen olduğu açıktır. Çünkü oyların kayıt ve sayımı bugünün demokratik toplumlarında çok önemlidir. Yaygın olarak Stalin'e atfedilen bir tümceyi anarak bu konunun hayatiyetini vurgulayalım: "Oy veren kişileri ve nasıl oy verdiklerini tamamıyla önemsiz buluyorum, asıl olağanüstü önemli olan şey oyları kimin ve nasıl saydığıdır."[3]

Cep telefonlarının dinlenmesi ve elektronik dolandırıcılık gibi haberleri sıklıkla duyduğumuz bir zamanda elektronik seçim denince birçok kişinin aklına "Kime oy verdiğim anlaşılır mı?", "Verdiğim oy değiştirilir mi?", "Verdiğim oy sayılır mı?" veya genel olarak "Seçimde manipülasyon yapılabilir mi?" gibi sorular gelebilir. Seçimlerin âdil ve güvenilir olarak yapılmasının yanında seçmenlerin sisteme güveninin sağlanması da çok önemlidir. Bazı problemlerine rağmen klasik seçimlerde seçmenler tüm seçim sürecini rahatlıkla anlayabilmekte ve izleyebilmektedir. Elektronik seçimlerde ise seçmenlerin geneli, seçim sürecinin bazı kısımlarının işleyişi hakkında hiçbir fikre sahip olmayacaktır. Ayrıca, banka hesaplarının boşaltılması, dinleme ve takip edilme gibi sorunlar da halkın yeni teknolojilere mesafeli durmasına neden olmaktadır. Görüldüğü gibi elektronik seçim sisteminin önünde seçim probleminin kendisi dışında başka zorluklar da vardır.

Seçmenin sisteme güveninin sağlanabilmesi için geliştirilen sistemin şeffaf olması ve geniş çevreler tarafından incelenmesi sağlanabilir. Bazı seçim sistemleri karmaşık donanım ve yazılıma sahiptir. Tüm bu bileşenlerin güvenliği ve güvenilirliğini sağlayarak tamamıyla şeffaf bir sistem geliştirmek hiç de kolay değildir. Seçmenlerin güveninin kazanılması açısından sistemin olabildiğince basit ve anlaşılır yapıda olması da önemlidir.

Sizce gelecekte hala bu yöntemlerle mi oy kullanılmalı?

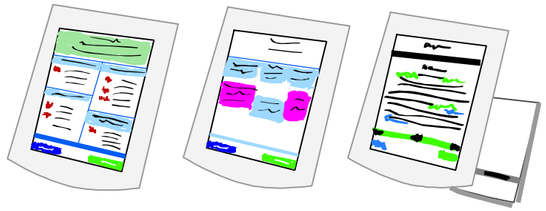
Geçmişte çözülmesi zor hatta imkânsız gibi görünen bazı problemler, bugün teknoloji ve kriptografi kullanımı ile beraber çözülebilmektedir. Bu yazı dizimizde, seçim problemlerinin de bu şekilde çözülüp çözülemeyeceğini inceleyeceğiz. Bunun yanında elektronik sistemler kullanılarak yapılacak seçimlerin, klasik seçimler ile sağlanamayan bazı özelliklerine de değinmeye çalışacağız.

Günümüzde dünyada gelişmiş ülkelerin hemen hemen tamamında başlamış ve geliştirilmeye devam eden e-Seçim

sistemi ülkemizde de farklı merkezlerde/araştırma gruplarında konuşulmaya ve çalışılmaya başlanmıştır. Geniş çaplı konferansların içerisinde bir parça olarak başlayan e-Seçim çalışmaları kendi başlarına özerk bir yapıya bürünerek e-Seçim çalıştay veya konferanslarının düzenlenmesine kadar gitmiştir. Tüm dünyada yerel yönetimlere (belediye vb.) daha çok yetki verilerek sorunları kaynağında hızlı ve düşük maliyetle çözme isteği uyanmaktadır. Bu da gelecekte daha sık seçim ihtiyacı doğurabilecektir.

Yazı dizimizin bu bölümünde, e-Seçim'in altyapısını oluşturan kriptografinin matematiksel detaylarına girmektense genel bilgi vermeye çalışacağız. e-Seçim'in amacı, kriptografik tabanlı sistemleri kullanarak mevcut geleneksel seçim sistemini daha ileri seviyelere getirmektir. e-Seçim sistemi sadece gizlilik ve doğruluk gerektiren diğer kripto tabanlı sistemlere göre çok daha karmaşıktır. Ayrıca sonuçlarının etkileri (ülkenin geleceği, yanlış sonuçların yaratacağı yıkım, insanların güveni vb.) ve oylama yönteminin basitliğine rağmen arka planda yer alan karmaşık teknik yapısı nedeniyle gerçeklemesi zordur.

e-Seçim, dört yılda bir yapılan milletvekili seçimleriyle birlikte referandumlar, belediye seçimleri, oda seçimleri, futbol takımlarının başkanlık seçimi, rektörlük seçimleri gibi onlarca örnekte uygulama alanı bulabilir.



PDA veya cep telefonlarıyla oy kullanmak ister misiniz?

e-Seçim uygulamasında, geleneksel kâğıt tabanlı oylamadan çok farklı yöntemler kullanılmaktadır. POS[1]/ Kiosk[2] makinelerine gidilerek oylama yapılabildiği gibi evden çıkmadan internet aracılığı ile de oy kullanılabilmektedir. Farklı ülkelerde, mevcut teknik sistemlerine, önceliklerine, eğitim seviyelerine, ekonomik durumlarına, yaş ortalamalarına hatta kültürlerine göre farklı sistemler tasarlanmıştır. Örneğin, Estonya, internet ortamında oy kullanma sistemi uygulamaktadır. Oy satılmasını engellemek için seçmenlerin oylarını seçim sonuna kadar değiştirebilmelerine imkân sağlanmıştır. Fakat en son atılan oy resmi olarak kabul edilmektedir. Estonya'da geleneksel kâğıt tabanlı seçim sistemi de hala geçerlidir. Klasik sistemden gelen oy önceliklidir ve geçerli sayılır [4]. İspanya, İtalya gibi Güney Avrupa ülkelerinde ise belirli oy merkezleri kullanılarak seçimler yapılmaktadır [5]. Kiosktan oy kullanılırken doldurulan oy pusulası seçmene gösterilir, onaylarsa elektronik oy sisteme kâğıt da sandığa gönderilir.

1 POS (*Point of Sale*): Genellikle alışveriş merkezlerinde bulunan kartlı satış noktası.

2 Almanya'da ve bazı Avrupa ülkelerinde gazete, sigara vb. satan büfeye verilen ad. Kiosk, Avrupa dillerine Türkçe "köşk" kelimesinden geçen bir sözcüktür. Dokunmatik ekranlı kısıtlı bilgi girişi olan bir bilgisayardır.

2. E-SEÇİM VE KRİPTOGRAFİ KULLANIMI

Değişik seçimlerin farklı özellikte olması istenilebilir. Örneğin, genel seçimlerde aranan bazı özellikler oda seçimleri için gerekmeyebilir. e-Seçim sisteminin güvenli ve güvenilir olması için aşağıda listelenen özelliklerden gerekli olanlarını içermelidir. Bu özelliklerin belirlenmesi için de, uygulanması düşünülen seçim sistemi tüm yönleriyle irdelenmelidir.

Açıklamalarda üyesi olduğumuz Avrupa Komisyonu'nun 2004 yılı tavsiyelerinden faydalanılmıştır [6].

2.1. Seçim Hakkı

2.1.1. Hak Sahipliği

Sadece seçmen olanlar oy kullanabilmelidir. Seçmenlerin seçime katılmaları önünde engel bulunmamalıdır. Engelli/hasta vatandaşların seçime katılmaları sağlanmalıdır.

2.1.2. Seçim Arayüzü

Seçim sisteminin arayüzü anlaşılır ve kullanımı basit olmalıdır. Engelli seçmenlerin kullanımına da uygun olmalıdır.

2.1.3. Seçmenin Olanakları

Seçmenlerin olanakları dikkate alınmalıdır. Uzaktan e-Seçim herkes tarafından ulaşılabilir değilse ancak ek veya seçimlik (ör. yurtdışındaki vatandaşlar için) olarak sunulabilir.

2.2. Eşitlik

2.2.1. Tek Oy Hakkı

Seçmenler birden fazla seçim kanalı (ör. kiosk ve internet) kullansa dahi birden fazla oy sayılması engellenmelidir. Birden fazla seçim kanalının kullanıldığı sistemlerde (örn. hem klasik ve hem de elektronik oy) seçim sonucu güvenli ve güvenilir olarak hesaplanmalıdır.

2.2.2. Seçmenlerin ve Adayların Eşitliği (Eşit Oy/Aday)

Bütün oyların sonuca eşit etkiyi yapması gerekir. Bütün seçmenler aynı resmi şekilde oylarını kullanabilmelidir. Ayrıca, hiçbir adayın diğerlerine karşı avantajlı olmaması gerekir (ör. oy pusulası üzerindeki sıralama, aday resimlerinin büyüklükleri).

2.3. İfade Özgürlüğü

2.3.1. Özgür İfade İmkânı

Seçim sisteminde seçmenin oyunu özgürce ve etki altında kalmadan kullanmasına olanak sağlanmalıdır. Seçim öncesinde oy verme süreci anlatılmalı ve gerekirse seçmene deneme imkânı sunulmalıdır. Kâğıt tabanlı ve uzaktan seçim birlikte kullanılıyorsa, uzaktan seçim, seçim merkezlerindeki oylamadan önce başlayıp bitebilir; fakat merkezlerdeki oylama bittikten sonra devam etmemelidir.

2.3.2. Etkileme Olmaması

Oy kullanma süreci seçmenin oyunu etkileyecek şekilde olmamalıdır.

2.3.3. Değişiklik Hakkı

Seçmenin nihai onayından önce oyunu değiştirmesine izin verilmelidir. Böylece, ifade özgürlüğünün yanında küçük dikkatsizlikler sonucu yanlış işaretlenen oy pusularının düzeltilmesine de olanak sağlanmış olur. Ayrıca, seçmenler son onay anına kadar yaptıkları işlemlerin başkası tarafından anlaşılmayacak şekilde oylamayı iptal edebilmelidir. Seçmenin nihai onayı sonrasında ise artık oy değiştirilememelidir.

2.3.4. Çekimser/Boş Oy Hakkı

Seçmen isteği doğrultusunda çekimser veya boş oy kullanabilmelidir.

2.3.5. Süreç Bitişi Net Olmalı

Oyun başarıyla verildiği, seçmene açıkça belirtilmelidir.

2.4. Güvenlik

2.4.1. Anonimlik, Mahremiyet ve Gizlilik

Seçmenin kime oy verdiği ile ilgili hiçbir bilgi sızmamalı ve tüm e-Seçim süreci boyunca kimse tarafından anlaşılamamalıdır.

Seçim sürecindeki belirlenmiş bir aşamada, kimlik doğrulama bilgileri ile seçmenin kullandığı oy birbirinden ayrılmalıdır. Oylar sayım aşamasına kadar gizli tutulmalıdır. Depolanacak veya kontrolsüz ortamlarda iletileceklerse gizlilikleri sağlanmalıdır.

Seçmenin hak sahipliğinin anlaşılması için yapılan kimlik doğrulama şekli çok önemlidir. Klasik seçimlerde kimlik doğrulandıktan sonra oy verilmektedir. Yani kimlik doğrulama işlemi ile oy verme işlemi arasında ilişki yoktur. Dolayısıyla, klasik seçimlerde, sandıktan sadece bir adaya oy çıkmadığını varsayarsak, kimlik doğrulamadan sonra seçmen oyunu anonim olarak kullanabilmektedir. Benzer şekilde elektronik seçimlerde de kimlik doğrulama süreci ile oy verme süreci birbirinden ayrılarak anonimlik sağlanabilir. Fakat dikkat edilmesi gereken noktalar vardır. Örneğin, kullanılan oylar, oy verme sırasına göre saklanmamalıdır; aksi halde kimlik denetim ve oy verme sıralamasının karşılaştırılması ile kimin kime oy verdiği öğrenilebilir. Klasik seçimlerde ise kimlik doğrulama elektronik olsa bile, oylar sandıkta karıştığından, bu konu ciddi bir problem oluşturmaz.

Evrensel doğrulanabilir seçim sistemlerinde (Madde 2.5.3) kimlik doğrulama ve oy verme süreci birlikte yapılmaktadır. Bu sistemlerde seçmenin kime oy verdiğini anlamak, teorik olarak şifreli mesajları çözmekle aynı zorluktadır.

Seçim merkezlerindeki oylama cihazlarında, seçmenin oyunu açığa çıkarmaması için başka tedbirlerin de alınması gerekmektedir. Örneğin, bazı elektronik seçim cihazları elektromanyetik yayılıma karşı korunmadığı için bu cihazlar ile kullanılan oyların uzaktan öğrenilebildiği raporlanmıştır [7].

Görüldüğü gibi anonimliğin (ve gizliliğin), birçok boyutuyla ele alınması gerekmektedir.

2.4.2. Bütünlük/ Bozulmamışlık

Verilen oylar hiçbir şekilde sonradan değiştirilememeli ve silinememelidir.

2.4.3. Oy Satışına Dayanıklılık

Seçmen, kendi oyunu nereye nasıl verdiğini ispat edememelidir. Bunun için sistemin, seçmenin bunu kanıtlayamayacağı şekilde tasarlanması gerekmektedir. Seçmen, oyunu verdiği yeri kanıtlayabilirse başkaları da onu zorlayarak oy verme şeklini etkileyebilir. Video kayıt ve iletişimdeki gelişmeler, oy satışı ve zorlamayı kolaylaştıracağı yönünde kaygıları arttırmaktadır.

2.4.4. Zorlanamazlık

Seçmenin iradesi dışında kişilere zorla oy verdirilmesi önlenmelidir. Bunun için seçmenin kime oy verdiğinin başkaları tarafından anlaşılamaması gerekmektedir.

Önlem alınmadığı takdirde kâğıt tabanlı seçimlerde de zorlama veya oy satışı mümkündür [8]. Örneğin, boş bir oy pusulasıyla zorlama kolaylıkla başlatılabilir. İşaretlenmiş (damgalanmış) oy pusulası seçmene verilerek oylama zarfının içine koyması ve boş oy pusulasını getirmesi istenir. Getirilen boş oy ile sahtekârlığa devam edilir. Fotoğraf veya görüntülü kayıt kullanımının da bu sahtekârlığı destekleneceği düşünülebilir.

Yazımızın girişinde de söylediğimiz gibi Estonya'da seçmenlerin internet ortamında istediği kadar oy kullanabilmesiyle bu sorun bir ölçüde giderilmiştir.

2.4.5. Güvenli Yol

Oylar sunucuya zamanında güvenilir bir mekanizma ile ulaştırılmalıdır. Sistem bileşenleri arasında güvenilir bir iletişim ağının kullanılması gerekmektedir. Oyların gizlilikleri açığa çıkmadan ve değişmeleri engellenecek bir şekilde sunucuya ulaştırılmalıdır.

2.4.6. Orijinallik

Seçim öncesinde seçim otoritesi, e-Seçim sisteminin orijinal olduğunu ve doğru çalıştığını (ör. oylama makinelerinin kötü niyetli kod içermediğini) doğrulamalıdır.

Uzaktan seçim uygulamalarında, seçmenler, sağlanan yazılımların kaynağını ve değişikliğe uğramadığını doğrulayabilmelidir. Seçmenler dilediği takdirde kendine ait veya istediği başka yazılımla da oy kullanabilmelidir.

2.4.7. Erişim Denetimi ve Yetkilendirme

Sadece seçim otoritesi tarafından yetkilendirilmiş kişiler merkezi altyapıya, sunuculara ve seçim verisine ulaşabilmeli ve sadece müsaade edilen işlemleri yapabilmelidirler. Kritik teknik işlemler, birden fazla kişi tarafından yapılmalıdır ve zaman zaman bu kişiler veya sorumlulukları değiştirilmelidir.

2.5. Güvenilirlik

2.5.1. Doğruluk/Hatasızlık

Kullanılan oylar hatasız olarak kaydedilmelidir. e-Seçim sistemi düzgün çalıştığını ve işlevlerini düzgün yaptığını düzenli olarak kontrol etmelidir.

Kullandığınız oyların doğru bir şekilde sayıldığından emin misiniz?

2.5.2. Bireysel Doğrulanabilirlik

Seçmenin, oylama sırasında verdiği oyun alındığını ve seçimden sonra da doğru bir şekilde sayılacağını teyit edebilmesidir. Doğrulanabilirliğin sağlanması için elektronik ortamda verilen oy, aynı zamanda kâğıda basılarak seçmene teyit ettirilebilir. Eğer oy doğru ise seçmenden onay alınması ile oy pusulası otomatik olarak veya seçmen tarafından sandığa atılabilir. Böylelikle hem seçmen verdiği oyun doğruluğu konusunda ikna olmakta hem de itiraz durumunda oylar tekrar sayılabilmektedir [9]. Fakat bu tür sistemlerde bile güveni zedeleyici senaryolar oluşturulabilir. Örneğin, sistem düzgün çalıştığı halde, kullandığı oy ile kâğıda basılan oyun (veya seçimden sonra açıklanan doğrulama bilgisinin) uyuşmadığını iddia ederek seçimi sabote etmek isteyen kişiler çıkabilir. Sandık sorumlusu sadece sistemde problem olup olmadığını kontrol edebilir fakat anonimliliği ihlal edemeyeceği için itiraz eden kişi oy verirken yanında bulunamayacaktır. Bu durumda bu kişinin sahtekâr olup olmadığı nasıl anlaşılabilir veya bu problem nasıl bertaraf edilebilir? [10].

Bireysel doğrulanabilirlikte, oy kullanan kişi haricindekilerin seçmenin oyunu kime verdiği hakkında ipucu elde edememesi gerekmektedir. Aksi takdirde oy satışı veya zorlama gibi istenmeyen sorunlara açık kapı bırakılmış olur.

2.5.3. Evrensel Doğrulanabilirlik

Yayınlanan sonucun gerçekten kullanılan tüm oyların toplamı olduğunun yeterince işlem gücü olan herkes tarafından kontrol edilebilmesine olanak sağlanmasıdır. Doğrulama sadece bağımsız denetçiler tarafından da yapılabilir.

Seçmenlerin verdikleri oyların, yayınlanan oyların içinde olduğunu teyit etmesiyle bireysel doğrulanabilirlik de sağlanabilir. Bunun için kullanılan oyların sonucunu ve doğruluğunu ispat eden mesajların herkesin ulaşabileceği bir yere (örneğin bir web sitesi) konması gerekmektedir. Burada en önemli mesele herkesin teyit etmesinden öte teyit edebilme olanağının sağlanmasıdır. Bunlar yapılırken oy satışı veya zorlama gibi istenmeyen sorunlara açık kapı bırakılmamalıdır. Ayrıca, anonimliğin sağlanmasına da dikkat edilmelidir (bkz. Madde 2.4.1. Anonimlik, Mahremiyet ve Gizlilik).

2.5.4. Seçim Bölgesinin Mahremiyeti

Oylar sayılırken veya sonuçlar açıklanırken, oy kullanılan bölgenin verdiği oyların dağılımının açığa çıkmasının engellenmesidir. Örneğin, bu özelliği sağlayan seçim sistemlerinde, bir köyden veya mahalleden kime ne kadar oy verildiği anlaşılamaz. Böylelikle seçimlerden sonra kazanan tarafın kendine oy verenlere daha fazla hizmet sunması, vermeyenleri ise cezalandırmasının önüne geçilebilir.

2.5.5. Şeffaflık

e-Seçim sisteminin işlevleri hakkındaki bilgiler herkese açık olmalıdır. Kanunların izin verdiği her gözlemci seçim sürecini izleyebilmelidir. Sistem açık-kaynaklı olmak zorunda değilse de, tasarımı / kaynak kodu en azından belirlenmiş güvenlik uzmanlarına açık ve belgelendirme/ denetim işlemi için kullanılabilir olmalıdır.

e-Seçim sistemi tanıtılmadan önce, belirli aralıklarla ve özellikle sistemde değişiklik yapıldıktan sonra seçim kurulu tarafından belirlenmiş tarafsız kurumlar tarafından, düzgün çalıştığı ve gerekli tüm güvenlik önlemlerinin alındığı test/analiz edilmelidir. Denetim sonucunda ortaya çıkan sonuçlar bir sonraki seçimlerde dikkate alınmalıdır.

e-Seçim sisteminde gözlenebilirliğinin sağlanması için yeterli veri saklanmalıdır. Sistemde bir olay/eylem gerçekleştiğinde inceleme verileri güvenli ve güvenilir şekilde kaydedilmelidir. Bu kayıtlar için sistemde güvenilir zaman kaynağı bulunmalıdır. Zaman kaynağı seçimlerin başlangıç/bitişinin belirlenmesi gibi amaçlar için de kullanılabilir.

e-Seçim cihazı veya sandığı açıkken sistemi etkileyecek müdahaleler, en az, yetkilendirilmiş iki kişi tarafından yapılmalı, raporlanmalı ve gözlemciler tarafından izlenebilmelidir.

e-Seçim sistemi, seçimin kısmi veya tamamen tekrarlamasına olanak sağlamalıdır.

2.5.6. Sağlamlık

e-Seçim sistemi arıza, yanlış çalışma ve servis dışı bırakma saldırılarına karşı güçlü olmalıdır. Oy verme cihazlarında meydana gelebilecek arızalar veya internet (ağ) bağlantısı problemleri gibi birçok başarısızlık karşısında bile sistem doğru çalışabilmeli ve herhangi bir oy kaybı olmadan seçim tamamlanabilmelidir. Örneğin, bir seçim merkezinde bin kişi oy verdikten sonra seçim cihazının arızalandığını düşünelim. Oy veren kişileri tekrar geri çağıramayacağımıza göre cihazların olabildiğince arıza yapmayacak şekilde tasarlanması gerekmektedir. Arıza durumunda ise verilen oyların heba olmaması için gereken tedbirler alınmalıdır. Ayrıca, bir bölgedeki yerel arızalar tüm sistemi etkilememelidir.

2.5.7. Âdiliyet

Seçimler tamamlanmadan sonuçlar elde edilemez (seçim sürerken o anki durumun öğrenilmesi seçmenleri etkiler veya kaybedeceğini anlayan taraf(lar) seçimleri sabote etmeye çalışabilir).

2.5.8. Tekrar Sayma ve Denetleme

İtiraz durumunda kullanılan oylar tekrar sayılabilmelidir. Bunun için oylama makinelerinde kullanılan oyların kâğıt çıktısı alınarak itiraz halinde sayılabilir.

Bu özelliğe sahip bir seçim sisteminde tekrar sayım sonucunun farklı çıkması aşağıdakilerden en az birinin gerçekleştiği anlamına gelir.

- Oy verme cihazı hatalı,
- Oy verme cihazının yazılımı değişmiş,
- Sandıktaki kâğıt oylar değiştirilmiş,
- Oy sayanlar hata yapmış.

Aslında bu tür kâğıt destekli makinelerin asıl amacı seçmenlerin oyları fiziksel olarak görmesini ve güvenini sağlamaktır.

2.5.9. Gerçek Zamanlı Yedekleme

Ana sunucunun gerçek zamanlı yedeklenmesiyle olası hatalara ve fiziki saldırılara karşı güvenlik sağlanmış olur.

2.6. Kullanışlılık

2.6.1. Mekândan Bağımsızlık

Seçmenler istedikleri bölgede oylarını kullanabilmelidir.

2.6.2. Seçmen Bilgileri

Seçmenler seçim öncesi kayıtlarına kolayca erişebilmeli ve gerekirse düzeltme talep edebilmelidir.

SSH[3] , e-İmza[4] gibi kapsamı dar güvenlik araçları genellikle sadece gizlilik, bütünlük ve kaynak doğruluğu gibi kriptografik özellikler ile sağlanabilmektedir. Fakat e-Seçim sisteminin birçok özelliği içinde barındırması gerekmektedir. Dolayısı ile bu özelliklerin birlikte sağlanması için kriptografik yapıtaşlarının kullanılması kaçınılmazdır. Bu amaçla şifreleme ve imzalama gibi bilindik kriptografik yapı taşlarının dışında homomorfik şifreleme[5] , kör imza[6] (*blind signatures*) , gizem/anahtar paylaşımı[7] (*secret sharing*) ve mixnet[8] gibi ileri kriptografik yapı taşlarına da ihtiyaç duyulabilmektedir. Dizinin sonraki bölümlerinde bu değişik kriptografik yöntemlere daha detaylı temas edeceğiz.

Temel kimlik doğrulama yöntemlerine ek olarak, alışkanlıklar, parola girme yöntemi (girilen karakterler arasındaki zaman farkı) ve konum gibi bazı bilgiler kullanılarak kimlik doğrulama desteklenebilmektedir. Alışkanlık tabanlı kimlik denetimlerinde, denetim yapılan kişi daha önce öğrenilen alışkanlıklarına uygun davranışlar sergilemiyorsa, örneğin geçmiş senelerin aksine bu sene oy vermeye çok erken gitmişse, sistem bu kişinin daha sıkı bir kimlik denetiminden geçirilmesi için yetkilileri uyarabilir. Bir başka örnek olarak seçmen, geçmiş senelerde oy verdiği bölge dışında oy veriyorsa söz konusu kullanıcı için de ek kimlik doğrulama denetimleri uygulanabilir. Ek denetimlerin insanları yormaması ve seçim kuyruklarına yol açmaması gerekmektedir. Alışkanlık tabanlı kimlik denetimi için seçmenlerin sürekli izlenmesi gerekmektedir. İnsanların, kendileri hakkında bilgi toplanmasına mesafeli yaklaşmaları bu tip kimlik doğrulama sistemlerinin önündeki en büyük engellerden biridir.

3. E-SEÇİM SÜREÇLERİ VE METOTLARI

Elektronik seçim, kâğıt tabanlı seçim ile bazı önemli ve alışılmış adımları paylaşmaktadır. Bu süreçler aşağıda anlatılmaktadır.

3.1. Kayıt / Kimlik

Sadece oy verme hakkı olanların ve doğru kişinin oy vermesini sağlama sürecidir. Kimlik verme/sorgulama statüsüne sahip bir kurumun (nüfus idaresi, vb.) özgün belgesi (nüfus cüzdanı, ehliyet, pasaport vb.) kullanılarak kimlik doğrulanır, bunun sonucunda geçerli bir seçim belgesi (seçmen kayıt belgesi vb) düzenlenir.

e-Seçim sisteminde seçmenleri tanımlamak için kimlik doğrulama yöntemleri şunlardır:

- Kullanıcı adı ve/veya şifre [Bilgi]

  – Her seçmene özel, ayrı bir kullanıcı adı ve seçmenin gizli tutması gereken bir şifre kullanımı ile sağlanan kimlik doğrulama işlemi

- Fiziksel kimlik kartı [Sahiplik]

  – Akıllı kart tabanlı bir e-Kimlik kartı olacaktır. Kartın belli bir güvenlik seviyesini sağlaması için şifre/PIN kullanılır. e-Kimlik kartı içerisinde imza anahtarını da barındırmaktadır.

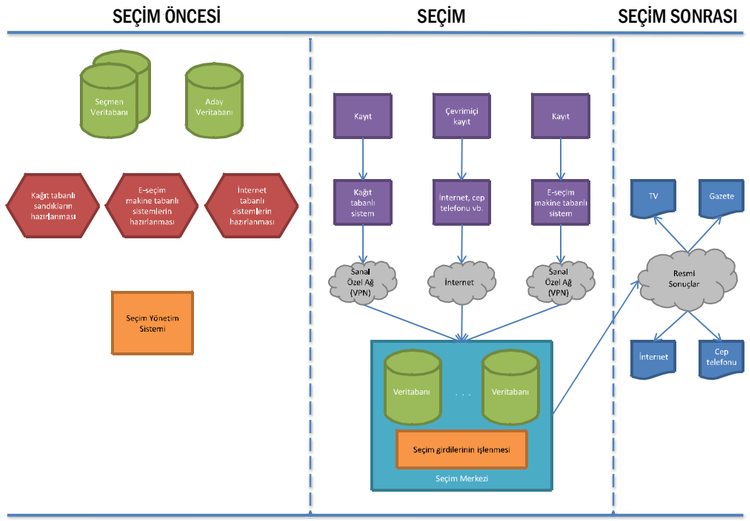
  – Kartlar seçmen veya işlem numarası (TAN - *Transaction Authentication Number*) içerebilir.

- Biyometrik özellikler (Parmak izi, İris vb.) [Bedensel Özellikler]

  – Kişi ile temel seviyede bağlantı kuran bu tür biyometrik özellikler, sistemin güvenliğini artırabilir.

Yukarıda anlatılan temel kimlik doğrulama yöntemlerinden sadece biri kullanılıyorsa sistemlere tek faktörlü denilmektedir. Kimlik doğrulama sistemleri iki veya daha fazla faktörlü de olabilmektedir. Örneğin, Türkiye'de gerçeklenmekte olan e-Kimlik projesinde olduğu gibi fiziksel kimlik kartı, kartın şifresi ve de parmak izi birlikte kullanılabilir.

[3] Telnet ve rlogin gibi ağ üzerindeki başka bir sunucuya uzakta bulunan bir başka makineden bağlantı sağlayan bir güvenlik protokolüdür.
[4] Sayısal imza olarak da bilinen bir kriptografik sistem olup her insan için benzersiz olan ancak sanal dünyada kullanılan kimlik belirtecidir.
[5] Kriptografide yaygın olarak bilinen özel bir açık anahtar şifreleme yöntemidir. Şöyle ki, şifrelenmiş mesajlar cebirsel işlemler yapılarak deşifre edilmeden mesajların cebirsel işlemleri yapılabilir.
[6] Bir kimsenin, bir belgeyi içeriğini görmeden/bilmeden imzalamasına olanak tanıyan sayısal imza protokolüdür.
[7] Gizli bir mesajın (örneğin anahtar) bir topluluk içerisinde paylaştırılmasıdır. Topluluk sadece ve sadece toplanıp bilgilerini birleştirerek mesajı ortaya çıkarabilir.
[8] İngilizce mix network adıyla bilinen kriptografik bir yöntemdir. David Chaum tarafından 1980'lerde ortaya çıkarılmıştır. Vekil sunucularda (proxy server) bulunan mesajlar üzerinden iz sürülmesini engellemek için bunların karıştırılarak gizlenmesi olayıdır.



Bir elektronik seçim sistemi yapısı.

3.2. Oylama Süreci

Belirli bir günde (ya da belli bir süreye yayılmış süreçte), kayıt/kimlik belgesine haiz seçmenlerin oy haklarını kullanmaları sürecidir. Bu süreçte kullanılan bileşenler aşağıda açıklanmıştır.

- **Seçim Yönetim Sistemi ('*Election Management System*', *EMS*).** Sistem bileşenlerinin başlatılmasından, oyları kaydetmekten ve oy sayım işlemlerinden sorumludur ve genellikle seçim merkezinde bulunur. Dağıtık yapıda da olabilmektedirler.

Uzaktan oy kullandıran sistemlerde seçmenlerin yazılımı bu merkezler ile etkileşimde bulunmaktadır. Bu tür sistemler kendi içlerinde, seçmenlerin kaydı ve/veya bilgilerinin kontrolü, kimlik doğrulama, oylama, oy toplama ve oy sayma gibi bileşenlere ayrılabilmektedir.

- **Doğrudan Elektronik Oy Kaydeden Makine ('*Direct Recording Electronic voting machine*', *DRE*).** Seçmenlerin oylarını kullandıkları ve kullanılan oyların kaydedildiği cihazlardır. Genellikle dokunmatik bir ekran aracılığıyla seçmen oyunu kullanır. Seçim merkezlerinde genellikle birden fazla DRE bulunmaktadır.

Amerika'dakilerin aksine Belçika gibi bazı ülkelerdeki DRE cihazları çok basit yapıdadır. Böyle tasarlanmalarının nedeni, seçim sisteminin daha anlaşılır olması ve kolaylıkla kurcalanmaması içindir. Cihazların basit yapıda olmaları onların kolayca değiştirilebileceği anlamına gelmez. Yüz binlerce satır koddan oluşan karmaşık yazılımlı bir sistemin hata ve/veya açık içerme ihtimali binlerce satır koddan oluşan daha basit bir sistemden fazladır. Örneğin, zamanla tespit edilen açıklar ve bunları kullanan virüsler nedeni ile devasa boyuttaki işletim sistemlerinde sürekli güncellenmeler yapılmaktadır.

DRE cihazları sadece seçim sırasında kullanılmakta ve kullanılmadıkları zaman depolanmaktadırlar. Tekrar kullanılacakları zaman değiştirilmediklerinden veya düzgün çalıştıklarından emin olmak gerekmektedir. Bundan dolayı, cihazların kurcalanamamaları veya değişikliğe uğradıklarında (yazılım/donanım olarak) bunun anlaşılması için bazı ek tedbirlerin alınması gerekmektedir.

- **Kullanılan Oyun Seçmen Tarafından Kâğıtla Teyidi ('*Voter-Verified Paper Audit Trail*', *VVPAT*).** Kâğıt tabanlı olarak teyit edilebilen bir elektronik seçim cihazıdır [11].

DRE makinesine bağlı bir yazıcı bulunduran bu sistemler farklı şekilde kullanılabilmektedir. Örneğin, bazı ülkelerde seçmen tarafından kullanılan oy kâğıt üzerinde görülebilir, ancak şeffaf bir örtü (ekran) dolayısıyla klasik yöntemlerle değiştirilmesi engellenmiştir. Seçmenin teyit etmesiyle oy sandık içerisine atılır.

Bu sistem iki yarar sağlar. 1) Seçmene oyunu teyit etmesi için olanak verir. 2) Herhangi bir problemle karşılaşılırsa oyların tekrar sayımı sağlanır. Bu sistem de tamamıyla sorunsuz değildir. Örneğin, kötü niyetli kişiler hata olmadığı halde kâğıda basılan oy pusulasının verdikleri oydan farklı olduğunu iddia edebilirler. Seçim görevlisinin (anonimlik ihlali yaratacağından dolayı) oylama sırasında işlemi izleme ihtimali yoktur. Seçim görevlisi ancak cihazdaki hata kodlarını inceleyebilir veya deneme oyu vererek sistemin çalışıp çalışmadığını kontrol edebilir [10].

- **Optik Okuyucu (*Optical scanner*) veya Manyetik Kart.** Bazı e-Seçim sistemlerindeki DRE'lerde kullanılan oy kâğıda basılır ve seçmenin kontrolünden sonra sandığa atılır. Sandıkta bulunan bir optik okuyucu, kâğıt oy pusulalarını sayar. Böylelikle sandıktaki oyların sayımı yapılır. Oy kullanma makinelerinin sayısına bağlı olarak seçim merkezlerinde bir veya daha fazla optik okuyuculu sandık bulunabilir.

Oy merkezlerinde klasik sandıklar yerine güvenilir makineleri kullanmak ister misiniz?

Belçika'da 2003 yılında yapılan seçimlerde, test amaçlı olarak mevcut sisteme yazıcı eklenerek seçmenlerin verdikleri oyları kâğıt üzerinde de görmeleri sağlanmıştır. Seçim bittikten sonra tüm kâğıt oylar sayılarak elektronik sayım ile karşılaştırılır. Kanunlara göre uyuşmazlık durumunda kâğıt oylar esas alınacaktır. Fakat elektronik sayım ile kâğıt oy sayımının tutmadığı görülmüştür. Sayım farklılıklarının insan hatasından kaynaklandığı düşünülmektedir [12]. Bu yüzden, yapılan bazı çalışmalarda kâğıt oyların barkod şeklinde de basılarak makine yardımı ile okunması önerilmiştir [13].

Belçika'da 2007 yılında yapılan yerel, eyalet ve Avrupa Parlamento seçimlerinde seçmenlerin %44'ü elektronik seçim sistemini kullanmıştır. Belçika'daki oy verme işlemi iki kısma ayrılmıştır. Kimliği doğrulanan seçmene boş bir manyetik kart verilir. Seçmenler oylarını oy kullanma cihazlarında [13] kullandıktan sonra oyları şifreli ve bütünlüğü korunmuş olarak manyetik karta yazılır ve seçmene verilir. Seçmen isterse manyetik kartın içeriğini başka bir cihazda kontrol edebilmektedir. Seçmeni tanımlayacak fiziksel bir işaret konmadığı anlaşıldıktan sonra manyetik kart sandığa atılır. Manyetik kartlar sandığa atılırken otomatik olarak sayılmaktadır. İtiraz durumunda ise sandıkta saklanan manyetik kartlar tekrar sayılabilmektedir [13].

E-Seçim için kullanılabilecek bir kiosk makinesi.

Sistemlerin farklı bileşenleri arasında veri aktarmak için çevrimiçi (IPSec vb.) veya çevrimdışı veri taşıma cihazları (DTD: *Data Transport Device*) kullanılabilir.

Yukarıda anlatılan e-Seçim cihazları ile şu şekilde oylama yapılabilir:

1. Belirli seçim merkezlerindeki kiosk makineleri kullanılarak. Her seçmen oturduğu yere yakın, önceden belirlenen seçim merkezine giderek oyunu kullanır.

2. Herhangi bir seçim merkezindeki kiosk makineleri kullanılarak. Seçmenin oy kullanmak için seçim merkezine gitmesi gerekir, fakat oyunu istediği merkezde kullanmakta özgürdür.

3. Herhangi bir yerde oy kullanılarak. Seçmen, seçim merkezi olmayan yerlerde bulunan DRE makinelerinde oyunu kullanır.

Anlaşılması için örneklendirirsek alışveriş merkezlerine, istasyonlara, postanelere, havaalanlarına konan kiosk makinelerinde oy kullanılabilir. Bu cihazların kurcalanmaya, değiştirilmeye karşı güçlü olmaları çok önemlidir.

4. Seçim merkezlerine gitmeden uzaktan oy kullanılarak. Oy istenilen her yerde kullanılabilir. Bundan dolayı seçmen evinden, işyerinden veya herhangi bir yerden oyunu kullanabilir. Bu amaçla kullanılan teknolojiler farklı olabilir:

- İnternete bağlı herhangi bir bilgisayardan,
- Cepten SMS (*Short Message Service*) yoluyla,
- Telefonla arayarak telefon tuşlarını kullanarak,
- İnteraktif TV yoluyla.

3.3. Oyların Toplanması & Sayılması

Yasal oy kullanma süresinin sonunda, seçim sandıklarından gelen oylar seçim otoritesi tarafından doğruluklarının kontrolü yapılarak toplanır. Bu kontrollerde örneğin, sandıktan çıkan oy ile o sandıkta kayıtlı seçmen sayısının karşılaştırılması veya verilen oyun merkeze ulaştırılana kadar geçen süre içerisinde değiştirilmediğinin kontrolü yapılabilir. Daha sonra, kullanılan oylar seçim otoritesi tarafından seçimin gerektirdiği şekilde sayılır (örneğin, referandumlarda "Evet-Hayır" oyların sayısı, parti seçimi gerektiren durumlarda her partiye düşen oy/milletvekili sayısı).

3.4. Oyların Açıklanması

Belki de seçime katılan yurttaşlar için en önemli ve en heyecanlı kısım sonucun açıklanma sürecidir. Klasik sistemlerde oylama bitmeden oyları sayma ihtimali yoktur. Elektronik seçimlerde ise oylama devam ederken bir taraftan da toplam sayılabilir. Fakat açıklanmaz; çünkü henüz oyunu kullanmamış kişiler etkilenebilir, hatta kimin kime oy verdiği bile anlaşılabilir. Dolayısıyla, oylama bitmeden sayılan oylar hakkında hiçbir bilginin açığa çıkmaması çok önemlidir. Bu da kriptografi kullanımı ile sağlanabilmektedir. Örneğin, oy verme işlemi sırasında oyların şifrelenip otoritenin izni (anahtar(lar)ı) olmadan deşifre edilmesi engellenebilir.

Seçimlerin kesin sonucunu deşifre etmek için sadece bir gizli anahtar kullanılabilir (sadece bir kişi deşifre edebilir). Bir başka olasılık ise gizli anahtarın seçim kurulundaki üyeler arasında eşit olarak dağıtılmasıdır. Örneğin, Yüksek Seçim Kurulu'nun 7 asil üyesi tarafından paylaşılabilir ve herhangi salt çoğunluk bir araya gelmeden şifresi çözülemez. Bu işlem kriptografide yaygın olarak bilinen gizem paylaşımı (*Secret Sharing* [14]) kullanılarak sağlanabilir. Sonraki yazılarımızda bu yöntemi daha detaylı ele alacağız.

Evrensel doğrulanabilir seçim sistemlerinde sonuç açıklanacağı zaman kullanılan oyların doğrulama bilgileri de ilan panosunda duyurulur.

3.5. İtirazların Değerlendirilmesi

İtiraz durumunda oyların tekrar sayılması ve seçim sahtekârlıklarının araştırılması yapılır. Seçim yasalarının kullanılan sistem ile uyumlu olması gerekmektedir. Tekrar sayımın prosedürleri belirlenmiş olmalıdır. Kullanılan oyun seçmen tarafından kâğıtla teyidinin yapıldığı durumlarda açıklanan sonuç ile tekrar sayımın farklı çıkması durumunda hangi sayımın kabul edileceği belirlenmelidir.

3.6. Oyların İmhası veya Arşivlenmesi

Kesin sonucun açıklanması sonrasında, oyların kâğıt veya elektronik olarak arşivlenmesi veya imha edilmesi sürecidir.

4. E-SEÇİMDE ORTAYA ÇIKAN PROBLEMLER

Kâğıt tabanlı olsun, elektronik olsun, tüm seçim sistemlerinde çeşitli problemler olabilir. Ayrıca, bu problemlerin bazıları bilinen ve zamanla değişmeyen karakteristiklere sahipken (ör. seçmenin seçim yerine ulaşımının fiziki olarak engellenmesi atağı), bazıları ise gelişen teknoloji ile ilgili değişen yaşam tarzı gibi sebeplerden oluşmakta (seçmenin cep telefonuna hatalı SMS mesajları atılıp yanlış seçim sandığına yönlendirilmesi) ve zamanla değişmektedir. Teknolojinin hangi ortamlarda hangi seviyelerde gelişebileceği ve toplumun bunları ne kadar benimseyeceği/kullanacağı tam olarak kestirilemediğinden, adı geçen bu tür problemlerin tümünün sınıflandırılması mümkün olmamaktadır. Bu sebeple, aşağıda verilen liste eksiksiz olarak düşünülmemeli, sadece olası problemler için bir ipucu olarak değerlendirilmelidir. Ortaya çıkabilecek problemler çevresel ve teknik olarak ikiye ayrılabilir.

4.1. Çevresel problemler

- Demografik yapıdan kaynaklanan sıkıntılar
  - Oy ticareti
  - Etkiyle oy kullandırma
  - Bir grubun zorla bir odaya alınıp, belirli bir kişi veya gruba oy kullanmaları yönünde telkinde bulunması gibi hadiseler de internet oylamada karşılaşabileceğimiz unsurlar arasındadır. Özellikle az sayıda internet bilgisayarının olduğu coğrafi yerleşimlerimizde (örneğin, köyler) bu yöntem sorun teşkil edebilir.
- Uzaktan Elektronik Oylama ile ilgili sorunlara klasik fakat imkânsız çözüm internet üzerinden oylama esnasında her kişinin başına bir güvenlik görevlisi dikmektir.
- Teknolojiyi ve internet kullanmayı bilmeyenlerin engellemelerini kırmak için özellikle teknolojiye hâkim olanlardan olumlu tepki alınmalıdır.
- Kanunların e-Seçimi destekleyecek yönde değiştirilmesi gerekir. Örneğin, yasal olmayan e-Seçim davranışları hakkında uygulanacak cezalar belirlenmelidir.
- e-Seçim sisteminin ülkemizde kullanması için öncelikle yasal mevzuatın buna uyarlanması gerekmektedir.

4.2. Teknik problemler

- Seçimlerdeki teknik problemlerle ilgilenmesi için teknik elemanların görevlendirilmesi gerekir. Seçim merkezlerinde oylama cihazları ile yapılan seçimlerde bu görevlilerin sayısı fazla olabilir. Bu kişiler, olaylara hızlı bir şekilde müdahale edebilmeleri için eğitilmelidirler.
- Birçok e-Seçim cihazının oyları yanlış hesapladığına dair örnekler bulunmaktadır [12,15].
  - Bu cihaz üreticilerinin güvenilirliği konusunda çok büyük şüpheler vardır.
  - Seçimler çok kritik konulardır ve güvenilirlik kesinlikle bir grup insana emanet edilmemelidir.
  - Hiçbir ürünün tam anlamıyla oturmuş olmadığı, ülkeden ülkeye değişen problemlerin ortaya çıktığı bilinmelidir.
- Kapalı kutu (*black-box*) e-Seçim cihazlarıyla ilgili bir sıkıntı da oyların tekrar sayılamamasıdır.
  - Kâğıtlı sistemlerde, oylar sandıkta fiziki olarak bulunduğu için çıkan sonuçlarla ilgili herhangi bir şüphe durumunda tekrar sayılabilir.
  - Elektronik oylamalarda ayrı bir fiziki materyal oluşturmadan tekrar sayım söz konusu değildir. Bu da şüphelerin sorgulanamaması ve güvensizliğin artması anlamına gelmektedir.
- Dışarıdan veya görevli kişilerce elektronik seçim makinelerine kötü niyetli yazılım yerleştirilebilir. Örneğin, Hollandalı aktivistler bir e-Seçim makinesindeki yazılımı oyun yazılımıyla birkaç dakika içerisinde değiştirebildiklerini göstermişlerdir [16]. Bu şekilde mevcut ve bağlı olduğu ağda bulunan tüm seçim cihazları etkilenebilir.

ABD'de ortaya çıkan sorunlar [17]

2000 yılında Volusia County'de, elektronik oylama makinesi sayımı sonucunda Al Gore'a eksi 16.022 oy çıktı (sıfırın altında bir değer!).

2001 yılında San Bernardino County'de, bir programlama hatası yüzünden 33 bölgede seçmen pusulasının bir kısmı yanlış çıktı. Oy sayımı tekrar elle yapılarak düzeltildi.

2003 yılında Boone County'deki, 4 Kasım belediye seçiminin sonucunda toplamda 140.000'den fazla oy çıktı. Ancak o yörede sadece 50.000 insan yaşıyordu ve onların yarısından daha azının oy kullanma hakkı vardı.

2003 yılında Fairfax County'de, elektronik oylama makineleri bir programlama hatası nedeniyle belirli bir adayın aldığı toplam oyun 100 oy eksik çıkmasına neden oldu.

Ülkelerin e-Seçim haritaları

Yasal olarak elektronik oy makinelerini kullanan ülkeler
Avusturalya, Brezilya, Kanada, Fransa, Hindistan, Japonya, Kazakistan, Peru, Rusya, ABD, Birleşik Arap Emirlikleri, Venezüella.

Yasal olarak uzaktan elektronik oylama yapan ülkeler
Avusturya, Avustralya, Kanada, Estonya, Fransa, Japonya, İsviçre, Norveç.

Pilot uygulamaları olan ülkeler
Arjantin, Azerbaycan, Beyaz Rusya, Bulgaristan, Şili, Çek Cumhuriyeti, Finlandiya, Yunanistan, İtalya, Letonya, Litvanya, Meksika, Nepal, Nijerya, Polonya, Portekiz, Romanya, Slovakya, Slovenya, Güney Afrika, İspanya, Güney Kore, İsveç, İngiltere.

e-Seçim projelerini askıya alan ülkeler
Almanya, İrlanda, Hollanda.

Not: *Anılan sistemlerin detaylı değerlendirmeleri yazı dizimizin sonraki bölümlerinde yer alacaktır.*

• Yazılım hataları olağandır. Bilgisayar programları bazen şaşırtıcı şekilde arıza verebilir. Bu hatalar bilgisayar tabanlı tüm yazılımlar için geçerli olduğu gibi oylama cihazları için de geçerlidir. Bu sorunun olası bir çözümü bu yazılımların açık kaynak kodlu olmasıdır. Böylece yazılımın analiz edilmesi, düzeltilmesi ve ilerletilmesi daha kolaydır. Ayrıca açık kaynak kodu olmasıyla insanların sisteme olan güveni artar. Ancak, unutulmaması gerekir ki açık kaynak kodu aynı zamanda kötü niyetli kişilerin de sistemi analiz ederek açık bulmasını kolaylaştırabilir. Kaynak kod bu nedenle sınırlı sayıda gözlemciye/denetçiye açılabilir.

• Ülkemizde seçimlerden sorumlu kurum olan Yüksek Seçim Kurulu, oy pusulası ve kâğıtlarını seçimlerden belirli bir süre sonra imha etmektedir. Ancak e-Seçim sistemiyle beraber şifrelenmiş mesajlar elektronik ortamlarda rahatlıkla başka yerlere kopyalanabilir ve yıllarca saklanabilir. Bu durumda bile anonimliğin korunması için sistemin sağlam kriptografik temeller üzerine kurulmuş olması gerekmektedir.

• Yetersiz tümleştirme güvensizliğe sebep olur (donanım, yazılım vb).

– Örneğin EMS en az dört farklı programlama dili kullanılarak yazılmıştır. Daha kötüsü, hemen hemen her modülün kendine ait bir veri tabanı ve kendine ait kimlik doğrulama sistemi vardır.

– Modüllerin bağımsız olarak güvenli olması tümleştirdikten sonra da güvenli olması demek değildir.

• Yazılıma karşı saldırı yapılabilir. Geliştirilme sırasında veya daha sonra bir saldırgan tarafından değiştirilebilir. Yazılımı değiştirmek, cihazın donanımını değiştirmekten çok daha kolaydır ve bu değişiklikler kolay saptanamaz. Yazılım güvenliği için güvenli hesaplama çiplerinin kullanıldığı cihazlarda ise bu çiplerin içindeki anahtarların okunamadığından veya çiplerin değiştirilemediğinden emin olunması gerekmektedir.

• Bazı çevreler ATM benzeri dokunmatik ekranların altyapısının oylamada kullanılmasını savunmuşlardır [18]. Destek olarak da genç/yaşlı, eğitimli/eğitimsiz her kesimden milyonlarca kişinin her gün ATM'leri kullanmasını göstermişlerdir. Fakat finansal sistemler, oylama sistemlerinden farklı bir özelliğe sahip olup anonimliği yok sayarlar. Eğer bir olaydan şüpheleniliyorsa, denetçiler sistemin tüm kayıtlarına rahatlıkla gidebilir ve kimin hangi işlemleri yaptığını kolaylıkla anlayabilirler. Seçimlerde ise anonimlik sağlanması gerektiğinden dolayı bu mümkün değildir.

• Kaynak kodunu ve derleyiciyi doğrulamak da yeterli değildir. Ayrıca, bu teyit edilmiş yazılımın her sistemde yüklü olduğunu da garanti etmek gerekir.

5. E-SEÇİMİN YARARLARI

Elektronik seçim sistemi, ilk kurulum aşamasındaki planlama, tanıtım, donanım, yazılım, kullanıcı eğitimi vb. maliyetlere rağmen, uzun vadede ve kullanımın artmasıyla birçok açıdan yarar sağlayacaktır. Bunlardan bazıları şunlardır:

• Mevcut sistemin aksine e-Seçimde seçmenler oylarının doğru bir şekilde sayıldığından emin olabilirler.

• Seçmenler istedikleri yerde oy kullanabilirler.

• Kâğıt tabanlı sistemlerde oy pusulasının işaretli, yırtılmış, mürekkebin pusulanın diğer tarafına geçmiş olması gibi durumlarda oy geçersiz sayılabilmektedir. E-Seçimle birlikte oyların geçersiz olması engellenerek bu konuda yapılabilecek usulsüzlüklerin de önüne geçilebilir (ör. sayımda taraflı davranmak).

• Kâğıtla yapılanın aksine zarfların yakılması, atılması, kutuların kaçırılması vb. dolandırıcılıklar engellenebilir.

• Oylar güvenli, güvenilir ve hızlı bir şekilde seçim merkezine taşınabilir.

• Oy pusulasında karşılaşılabilecek sorunları ortadan kaldırabilir (ör. çok uzun olması, gereksiz ve karmaşık sayılar içermesi vb.).

• Ülkemizdeki mevcut sistemde bulunmayan boş (çekimser) oy seçeneği ek maliyet getirmeden sunulabilir.

• Oylama sonucu hızlı bir şekilde ilan edilebilir.

• Kâğıt tabanlı oylamada yapılan hata ve dolandırıcılıkları minimum seviyeye indirir.

• Oy verme süreci kısalabilir (ör. oylarının damgalanması ve sandığa atılması gerekmez).

• Genç seçmenler bilgi teknolojilerinin düzenli kullanıcıları olduğundan e-Seçim, onların seçimlere katılımını teşvik edebilir. Araştırmalar da gençlerin bu konuda daha fazla istekli ve eğilimli olduğunu göstermektedir.

• Kamu ve siyasi hayatın modernizasyonuna katkıda bulunabilir.

• Seçmen görüşündeki eğilim yansıtılmasını, siyasi katılım ve etkileşimin hızlanmasını teşvik eder.

• Kâğıt tabanlı sistemlerdeki masraflar internet tabanlı sistemlerle beraber azalacak ya da tamamen ortadan kalkacaktır. Bunlardan bazıları şunlardır:

– Elektronik oylama merkezlerinin iş yükünü azaltır ve basitleştirir.

– Oy pusulası hazırlanması ile ilgili masraflar: Pusulanın kâğıda basımı, her pusulanın doğruluğunun kontrolü, pusulaların geçerlilik kazanması için tek tek damgalanması, pusulaların yerleştirileceği zarfların hazırlanması.

– Oylama sırasında doğan masraflar: Tüm sandıkların güvenliğini sağlamak için gerekli personel (sandık başkanı, kolluk kuvvetleri vb.) harcamaları.

– Oylama sonrasında ortaya çıkan masraflar: Oyları içeren zarfların açılıp teker teker sayılması, sayım sonuçlarının güvenli bir şekilde ara ve ana merkezlere gönderilmesi.

• Yönetim ile ilgili masraflar: Seçim yönetim merkezinde istihdam edilmesi gereken personel, koruma, enerji, ulaşım vb. masraflar.

Bu listeden de anlaşılacağı gibi e-Seçim, sosyal hayatın modernleşmesinden ekonomiye kadar birçok alanda katkı sağlayabilir.

Tatilinizi bölmeden oy kullanmak ister misiniz?

6. ÜLKEMİZDE E-SEÇİM

Elektronik seçim sistemleri, ülkelerin kendilerinin geliştirmek isteyecekleri stratejik teknolojilerdendir. Çünkü bir ülkede rahatlıkla kullanılabilecek seçim özellikleri başka ülkeler için sakıncalı olabilir. Örneğin bazı ülkelerde belirli şartlarda seçmenlerin oylarını kullanmaları için başkalarına vekâlet vermelerine müsaade edilmektedir [7,23]. Bu yöntemde genellikle seçim öncesinde seçmenin seçim kurumuna başvurarak, yerine başkasının oy vereceğini bildirmesi istenmektedir. Bu ülkeler, zorla vekâlet verdirmeyi bir risk olarak görmemektedirler. Ülkemizde ise böyle bir seçim özelliği suistimale yol açabilir. Dolayısı ile ülkemize uygun elektronik seçim özelliklerinin belirlenmesi amacı ile bu konuda uzman kurum ve kişiler tarafından e-Seçim sistemi tüm boyutları ile ele alınarak risk analizi yapılmalıdır. Örneğin, NIST (Amerikan Ulusal Teknoloji ve Standartlar Enstitüsü), Amerika'daki elektronik seçim sistemlerinin test ve izlenmesinde rol almasının yanında, risk analizi yapmakta ve teknik kılavuzlar yayımlamaktadır. Ayrıca bunları geniş kitlelerin yorumlarına açarak biçimlendirmektedir [2]. Ayrıca, üyesi olduğumuz Avrupa Komisyonu'nun e-Seçim ile ilgili yasal, operasyonel ve teknik standartlar konusundaki tavsiyeleri dikkate alınmalıdır [6].

Ülkemizde de, TÜBİTAK'ın koordinasyonunda, kamu kurumları ve özel kuruluşlar, üniversiteler ve sivil toplum kuruluşlarıyla birlikte yürütülen ve 2023 yılında bilim ve teknoloji ile bütünleşerek gelişmiş bir topluma ulaşma amacını güden, "Vizyon 2023" Teknoloji Öngörüsü Projesi'nde e-Seçim ile ilgili bazı alanlar kapsanmıştır [19]. Örneğin, gelecekte önem kazanacak temel eğilimler bölümünde;

(1) İnsan-makine arayüzünün, insanın doğal uzantısı haline gelmesi,

(2) Dağılmış işleme ve bilgiye erişim sistemlerini kullanma, eğitim gibi bir vatandaşlık haklarının yasal/etik korumaya sahip olması,

öngörüleri yer almaktadır. "Milletvekili ve belediye seçimlerinde oy kullanmanın, seçim merkezlerinde sandık yerine internete bağlı bilgisayarlarla/herhangi bir internete bağlı bilgisayarlar üzerinden yapılması" da yukarıda anılan alanlardandır.

Seçim sisteminde yer alan tüm paydaşların güveninin kazanılması çok önemlidir. Örneğin, Hollanda'daki e-Seçim cihazının donanımsal açıdan zayıf olduğu kanıtlanmıştır. Seçmenin güveni kırıldığından elektronik seçim sistemi askıya alınarak kağıt tabanlı oylamaya geri dönülmek zorunda kalınmıştır [16, 20].

Elektronik seçim sistemlerinin kriptolojinin en zor uygulamalarından biri olduğunu belirtmiştik. Dolayısıyla geniş kitlelerin katılacağı elektronik seçim sistemlerinden önce oda seçimleri gibi daha küçük çaplı seçimler yapılarak deneyim kazanılabilir. Ayrıca, bu konudaki araştırma projeleri desteklenerek genel seçimler gibi geniş çaplı oylama sistemlerine zemin hazırlanabilir.

e-Seçim sisteminin etkin bir şekilde uygulanabilmesi için altyapısının da uygun olması gerekmektedir. Örneğin, TÜBİTAK UEKAE tarafından Elektronik Kimlik Doğrulama Sistemi (EKDS) projesi kapsamında geliştirilen yeni nesil T.C.

Kimlik Kartı, yakın gelecekte kanuni olarak nüfus cüzdanının yerine geçerek vatandaşlık kartı olarak kullanılmaya başlanacaktır. Bu elektronik kartların kimlik doğrulamada kullanılması ile başkasının yerine oy verme gibi sahtekârlıklar önlenebilir. EKDS, Elektronik Kimlik Kartı, Kart Erişim Cihazı, Kimlik Doğrulama Sunucusu, Politika Sunucusu ve Arabirim yazılımlarından oluşmaktadır [21]. EKDS, hizmete katılan ve hizmetten yararlanmak isteyen kişilerin gerçekten öne sürdükleri kişi olduğunu ve kimliği çalan ya da taklit eden başka biri olmadığını doğrulamaktadır. Diğer taraftan, Bilgisayar Destekli Merkezi Seçmen Kütüğü Sistemi (SEÇSİS) ile seçmen kütüklerinin bütün bilgileri tutulmaktadır ve bunlara hızlı bir şekilde erişilebilmektedir [22].

Bir başka önemli bileşen olarak Açık Anahtar Altyapısını da örnek verebiliriz. Ülkemizde elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları 5070 numaralı kanun ile düzenlenmiştir. Mobil imza kullanımı ile de yaygınlaşmaya başlayan elektronik imza, e-devlet uygulamalarının önemli yapıtaşlarından biridir. Estonya gibi bazı ülkeler, elektronik seçim sistemlerinde elektronik imza kullanmaktadırlar. Islak imza yerine geçen (nitelikli) elektronik imzanın seçim sisteminde kullanılabilmesi için her bir seçmene elektronik imza dağıtılması gerekmektedir. Islak imza yerine geçmeyen elektronik imzalar da kimlik doğrulama sistemlerinde (örn. web tabanlı kimlik doğrulama) kullanılabilmektedir.

EKDS sisteminin yakın gelecekte kullanılmaya hazır olması, Nitelikli İmza Altyapısı ve SEÇSİS sistemiyle tüm seçmen kayıtlarının elektronik ortamda olması ülkemizdeki e-Seçim altyapısının çok önemli yapı taşlarının hazır olduğunu göstermektedir.

Ülkemizin bulunduğu bölgesel kalkınma ve internet kullanımı/kullanabilirlik göz önüne alındığında sadece teknolojik çözümü kullanmayı istemek doğru bir mantık değildir. Problemler yukarıda da belirtildiği gibi detaylı bir şekilde ele alındıktan sonra ülkemiz için uygun kısa, orta ve uzun vadeli planlar yapılmalıdır. Estonya'da olduğu gibi kısa vadede hem kâğıt tabanlı hem de elektronik seçim sistemi birlikte kullanılıp vatandaşların sistemi özümsemesi beklenebilir. Bu arada süreç içerisinde meydana gelebilecek hatalar, eksiklikler, kanuni düzenlemeler, değişiklikler yapılabilir.

e-Seçim ile birlikte insanlar belirli seçim merkezlerine hapsedilmekten kurtarılabilir ve seçimlere katılım arttırılabilir. Bunun yanı sıra, seçimlerin elektronik ortama taşınmasıyla birlikte baskı ve zorlama ile oy kullanımının engellenmesinin de önüne geçilebilir. Ayrıca yurtdışında bulunan vatandaşlarımızın oylarını uzaktan kullanması sağlanabilir. Oy kullanacak olmaları, ülkelerindeki gelişmeleri daha yakından takip etmelerini de sağlayacağından, böylelikle ülkelerine bağlılıklarının arttırılması da mümkündür. Başlangıçta gençlerin daha çok ilgi gösterdiği internet kanalıyla oy kullanımına daha sonraki yıllarda farklı kesimlerin de ilgisinin arttığı görülmektedir [4].

- Siyasi seçimler için:

  – Oy satma gibi saldırıların önünü açabileceğinden internet kanalıyla uzaktan elektronik oylama tek çözüm olmamalıdır. Her seçmen istediği seçim merkezlerindeki DRE makinelerinde de oyunu kullanabilmelidir.

  – Yerel referandumlar için uzaktan elektronik oylama uygulanabilir.

  – Yurtdışında yaşayan Türk vatandaşları internet aracılığı ile oy kullanabilir.

  – Devlet, elektronik oylama sistemi donanımlarının belirli maliyetlerini yüklenmek zorundadır.

  – Devlet tasarım, organizasyon ve operasyondan sorumlu olmalıdır.

- Profesyonel seçimler için:

  – Özel Sektör: Uzaktan elektronik oylama veya DRE makinelerinde kullanılan oylama sistemi yetkililerce resmiyet kazandırılarak güvenilirliği sağlanabilir. Bunun için, iş hukuku hükümlerini değiştirmek gerekli olacaktır.

  – Kamu sektörü: Uzaktan elektronik oylama sistemleri, kamu tarafından atanan yönetim ve teknik birimler tarafından oluşturulmalıdır.

  – Uzaktan elektronik oylama (internet, cep telefonu vb.) şirketlerin yönetim kurullarını seçmede kullanılabilir (ör. Real Madrid Futbol Kulübü'ndeki seçim).

  – Uzaktan elektronik oylama ticaret odaları, sanayi, tarım, dernekler, sendikalar vb. yapılan seçimlerde de kullanılabilir.

E-Seçimin ülkemizde uygulanmasının bazı yararları şunlar olabilir: İnsanların kendilerini dünya ölçeğinde gelişmiş hissetmeleri ve geleceğe daha umutlu bakabilmeleri, seçim gibi geleceklerini doğrudan etkileyen bir aracın doğru, güvenilir, tarafsız ve şeffaf olarak kullanılması ile sağlanabilir. Ayrıca e-Seçim, sosyo-politik anlamda toplumun gelişmesine katkıda bulunabilir. Birey kendini, sisteme karşı güveninin artmasından dolayı, yönetime önemli katkılar sağlayan biri olarak hissedebilir. Hızlı bir şekilde seçimler yapılabilir ve sonuçlandırılabilir. Bu sayede 2-4 ay gibi uzun tarihli seçim hazırlıkları ortadan kalkar. Başlangıçta ciddi manada donanım masrafı çıkmasına rağmen uzun vadede masraflar ciddi miktarda azaltılabilir.

Ülkemizde e-Seçim uygulanmasıyla, kâğıt tabanlı sistemlere göre çok daha hızlı ve az masrafla birçok istatistiksel analizler yapılabilir. Örneğin, anket veya güven oylaması gibi güvenilirliği sürekli tartışma konusu olan seçenekleri doğrudan internet ortamında uygulayarak toplumun genel hissiyatı ölçülebilir. Gençlerin oy verdikleri üzerinden ülkenin 20-30 yıl sonrası okunabilir ve bu sonuçlara göre özgün politikalar geliştirilebilir. Belki de, seçmenlerin bir partiye oy vermesi esnasında aday kişiye de oy vermesi istenebilir. Böylece, halkın demokratik isteklerini yansıtan bir aday listesini seçmenler belirleyebilirler.

Bununla beraber, verilen oy dağılımlarına göre adaylara parlamentoda karar alma gücü verilebilir. Örneğin, 10 bin oy alanla 100 bin oy alan adayın platformdaki güçleri farklı olabilir. Yukarıdaki örneklerin kâğıt tabanlı sistemlerde olabilmesi için oy pusulaların seçimlerde kullanılamayacak kadar büyük ölçülerde olması gerekebilir. Örneğin, Belçika'daki her oy pusulası, yaklaşık 20 listeden, her liste için 30-40 aday ve 30-40 yedek aday içermesiyle yaklaşık 1 metre × 0.5 metre boyutlarda pusulalar olabilmektedir [13].

Bu yazı dizisinin ilk bölümünde e-Seçim ile ilgili ana öğeler açıklanmıştır. İzleyen bölümlerde, dünyada ve ülkemizde önemi giderek artan bu teknolojinin kriptolojik altyapısı, artı ve eksileriyle beraber diğer ülkelerdeki uygulamaları ve ülkemiz için uygulanabilir yöntemler hakkında detaylı bilgiler verilecektir.

KAYNAKÇA

[1] Voting Resources- http://theory.lcs.mit.edu/~rivest/voting

[2] http://www.nist.gov/itl/vote/

[3] Stalin's speeches, writings and authorized interviews- http://en.wikiquote.org/wiki/Joseph_Stalin

[4] Internet voting in Estonia- http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf

[5] Bringing Confidence to Electronic Voting- http://www.ejeg.com/volume-1/volume1-issue-1/issue1-art5-riera-brown.pdf

[6] COUNCIL OF EUROPE - Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting https://wcd.coe.int/ViewDoc.jsp?id=778189

[7] http://www.coe.int/t/dc/files/themes/forum_democratie/netherlands_en.pdf http://www.freedom-to-tinker.com/blog/felten/dutch-e-voting-system-has-problems-similar-diebolds

[8] http://vote.nist.gov/threats/papers/ChainVoting.pdf http://vote.nist.gov/threats/papers/threats_to_voting_systems.pdf

[9] http://en.wikipedia.org/wiki/Voter_Verified_Paper_Audit_Trail http://www.schneier.com/blog/archives/2004/11/the_problem_wit.html

[10] http://votingmachines.procon.org/view.answers.php?questionID=292.

[11] Voter Verified Paper Audit Trail- http://en.wikipedia.org/wiki/VVPAT

[12] Electronic voting in Belgium http://en.wikipedia.org/wiki/Electronic_voting_in_Belgium

[13] Danny De Cock, Bart Preneel: Electronic Voting in Belgium: Past and Future. VOTE-ID 2007 (üyelik gerekmektedir)

[14] Secret sharing- http://en.wikipedia.org/wiki/Secret_sharing

[15] India's electronic voting machines are vulnerable to attack-http://www.physorg.com/news191779395.html

[16] European e-voting machines cracked by Dutch group- http://www.edri.org/edrigram/number4.19/e-voting

[17] What's Wrong With Electronic Voting Machines? http://www.schneier.com/essay-068.html

[18] http://ww.techdirt.com/articles/20080304/134146430.shtml

[19] TÜBİTAK, Vizyon 2023 Teknoloji Öngörüsü Projesi, Bilgi ve İletişim Teknolojileri Paneli Sonuç Raporu, Şubat 2004, http://www.tubitak.gov.tr/tubitak_content_files/vizyon2023/bit/bit_panel_sonuc_rapor.pdf

[20] http://en.wikipedia.org/wiki/Electronic_voting_examples#Netherlands

[21] http://www.ekds.gov.tr/

[22] SEÇSİS http://www.ysk.gov.tr/ysk/SecsisProjesi/SecsisIndex.htm

[23] Proxy voting- http://en.wikipedia.org/wiki/Proxy_voting, http://www.elections.ca/loi/com2000/Voting/vot06_e.html

Türkiye'de Sosyal Mühendislik Saldırıları Çözümlemesi

Tolga Mataracıoğlu

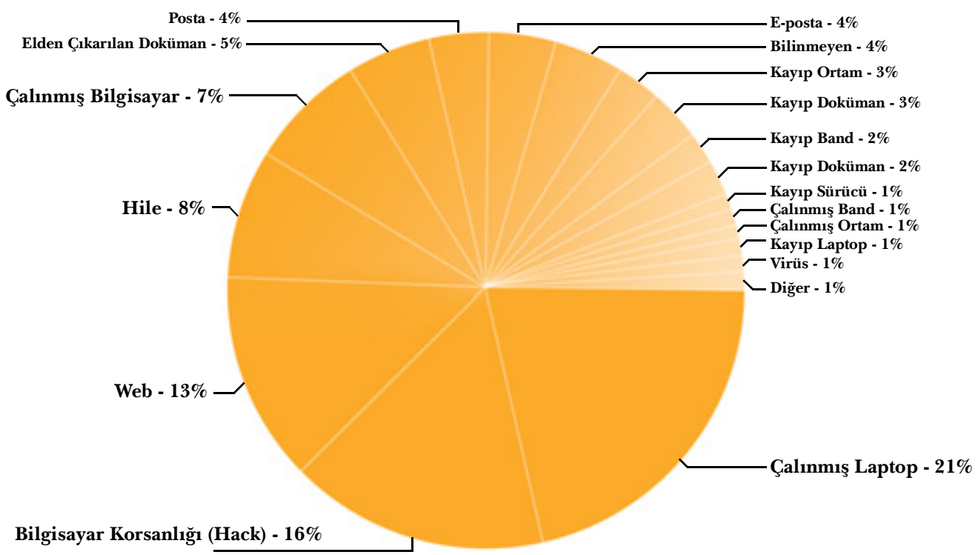
Giriş

Günümüzde oldukça popüler halde olan sosyal mühendislik saldırılarından korunabilmek amacıyla öncelikle saldırı tekniklerini ve sonra da korunma yöntemlerini bilmek artık bir zorunluluk halini almış durumda. TÜBİTAK UEKAE Bilişim Sistemleri Güvenliği Bölümü olarak kamu kurumlarına “Bilgi Güvenliği Testleri” çatısı altında sosyal mühendislik saldırıları gerçekleştirmekteyiz. Bu yazıda gerçekleştirdiğimiz sosyal mühendislik testlerinin bir çözümlemesini (analizini) yapacağız. “Sosyal Mühendislik” terimi bu yazıda, bireylerin davranışlarını etkileyen "Toplumsal Mühendislik" anlamında kullanılmakta olup, geniş kitleleri yönlendirmeyi hedefleyen "Toplumsal Mühendislik" ya da diğer deyişle, "Toplum Mühendisliği" kavramıyla karıştırılmamalıdır.

Hepimizin bildiği üzere bilgi güvenliğinin sadece küçük bir yüzdesi teknik güvenlik önlemleri ile sağlanmakta olup büyük yüzdesi ise kullanıcıya bağlı durumdadır. Kurumda bilgi güvenliğinden sorumlu olan kişiler kimler peki? Başta bilginin sahibi ve bilgi işlem personeli olmak üzere tüm kurum personeli aslında bilgi güvenliğinden sorumludur. Bilgi güvenliğinin düzeyini belirlemek için en zayıf halkaya bakılır. En zayıf halka da çoğu durumda maalesef insan olmaktadır.

Peki kurumunuzda bir bilgi güvenliği zafiyeti oluştuğunda kurumunuzun başına neler gelebilir?

- Bilgileriniz başkalarının eline geçebilir.
- Kurumun onuru, toplumdaki imajı zarar görebilir (ki en kötü durum).
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir.
- Önemli veriye zamanında erişememe sorunları ortaya çıkabilir.
- Parasal kayıplar meydana gelebilir (görece olarak bakıldığında en hafif durum).
- Vakit kayıpları kaçınılmaz olur.
- Hatta can kaybı bile meydana gelebilir.



Şekil 1. *ABD’deki bilgisayar olaylarının türlere göre dağılımı.*

Şekil 1’de 2001-2009 yılları arasında Amerika Birleşik Devletleri’nde meydana gelmiş bilgisayar olaylarının türlerine göre dağılımı gösterilmektedir [1]. Grafiğe baktığımızda çalınmış dizüstü bilgisayarların %21’lik bir oranla birinci sırada yer aldığı görülür. Sosyal mühendislik tekniklerini kullanarak yapılan saldırıları “Bilgisayar Korsanlığı (Hack)” ve “Hile” başlıkları altında toplayacak olursak, bu olaylar %24’lük bir oranla suçların önemli bir bölümünü oluşturmaktadır.

Biraz da sosyal mühendislik hakkında bilgi verelim: Sosyal mühendislik etkileme ve ikna yöntemlerinden yararlanarak, normal koşullarda insanların vermemeleri, paylaşmamaları gereken bir bilgiyi ele geçirme sanatı olarak tanımlanabilir. Çoğu insan, kandırılma olasılığının çok düşük olduğunu düşünür. Bu ortak inancın bilincinde olan saldırgan isteğini o kadar akıllıca sunar ki, hiç kuşku uyandırmaz ve kurbanın güvenini sömürür [4][6].

“En emniyetli bilgisayar, kapalı olandır.” şeklinde klişeleşmiş bir laf vardır. Peki, art niyetli bir kişinin ofise gidip bilgisayarı açması için birini ikna edebileceğini hiç düşündük mü? Artık günümüz bilgi güvenliğine bakış açımızın bu tür durumları da içerecek biçimde genişlemesi gerekiyor.

Şekil 2. *Sosyal mühendislik saldırılarında kullanılabilecek bazı donanımlar.*

Sosyal mühendislik saldırılarında kullanılabilecek bazı donanımlar, fiyatlarıyla birlikte Şekil 2'de görülmektedir. Bu tür ucuz donanımların temininin çok kolay olabileceği ortadadır. Bu durum da kurumunuzda sosyal mühendislik saldırılarının gerçekleştirilme olasılığını ciddi oranda arttırmaktadır.

Saldırı Teknikleri

Bu bölümde, sosyal mühendislerin (beyaz şapkalılar) ya da sosyal mühendislik tekniklerini kullanan kötü niyetli kişilerin (siyah şapkalılar) kullandıkları saldırı tekniklerini inceleyeceğiz [2][3][5].

1. Zararsız Gibi Görünen Bilgiler

Bir kurumun güvenliğinin aşılması, genellikle kötü adamın kurumdaki pek çok insanın korunması ve sınıflandırılması için bir neden görmediği, son derece masum, günlük ve önemsiz görünen bir bilgiyi ya da bir belgeyi elde etmesiyle başlar. Çoğu sosyal mühendis, bir kurum için zararsız gibi görünen bilgileri el üstünde tutar; çünkü bu bilgiler kendilerini daha inandırıcı kılabilmelerinde can alıcı bir rol oynayabilir.

2. Doğrudan Saldırı: Yalnızca İsteyivermek

Çoğu sosyal mühendislik saldırısı karmaşıktır. Fakat bazı saldırganlar amacına basit ve lafı dolandırmadan ulaşabilirler. Bilgiyi doğrudan istemek bazı durumlarda yeterli olabilir.

3. Güven Uyandırmak

Sosyal mühendislerin başarılarının sırrı insanların aldatılmaya fazlasıyla açık olmasıdır. Çünkü insanlar belli şekillerde yönlendirilirlerse yanlış şeylere güven duyabilirler. İyi bir sosyal mühendis, kurbanın sorabileceği soruları önceden tahmin eder ve bu sorulara karşı hazırlıklı olur.

4. “Size Yardımcı Olabilirim”

Bir sorununuz var ve size yardım etmek isteyen birisi var. Bu yardımı reddeder miydiniz? Kabul etmekle kalmaz, saldırgana minnet bile duyardınız. Sorunun kaynağının da büyük ihtimalle saldırgan olduğundan şüpheniz olmasın.

5. “Bana Yardımcı Olabilir misiniz?”

Saldırgan kendini acındırarak kurbandan yardım ister. Zor durumda olan insanlara hep acımışızdır. Sonuç: Hep başarı!

6. Düzmece Siteler ve Tehlikeli Ekler

Bedava indirilebilen yazılımlar! Neden bu yazılımları indirmek bedava diye hiç düşündünüz mü? Bu türden olup da art niyet içermeyen pek çok yazılım da mevcut tabii, onları ayrı tutuyorum. Saldırganlar insanların bedava şeylere duydukları hevesten faydalanıyorlar ya da içeriği cazip gelen e-posta eklerinden. Örneğin, “zamlı maaşınızı öğrenmek için lütfen ekteki dosyaya tıklayın” konulu bir e-posta alıyorsanız eğer, ekini açmadan önce bir kez daha düşünün.

7. Acındırma, Suçluluk Duygusu ve Sindirme Tekniğini Kullanmak

Hem kendimiz hem de başkaları adına zor durumlardan kaçınma eğilimindeyiz. Bu olumlu dürtüden yola çıkarak saldırgan, kişinin acıma duygusuyla oynayabilir, onun kendini suçlu hissetmesini sağlayabilir ya da silah olarak sindirmeyi kullanabilir.

8. Ters Dalavere

Geleneksel sosyal mühendisler belli bir yol izlerler. Bazı durumlarda ise oyun ters yönde oynanır. Buna da ters dalavere denir. Bu yöntemde kurban, yardım için saldırganı arar. Kurbanın saldırganı aramasının altında yatan durum, saldırganın, kurbanın direkt etkileneceği bir sorun çıkartması ve bir şekilde önce kurbana telefondan ulaşması ve telefon numarasını bırakarak kurbanın kendisini aramasını beklemesinden kaynaklanmaktadır.

9. İçeriye Girmek

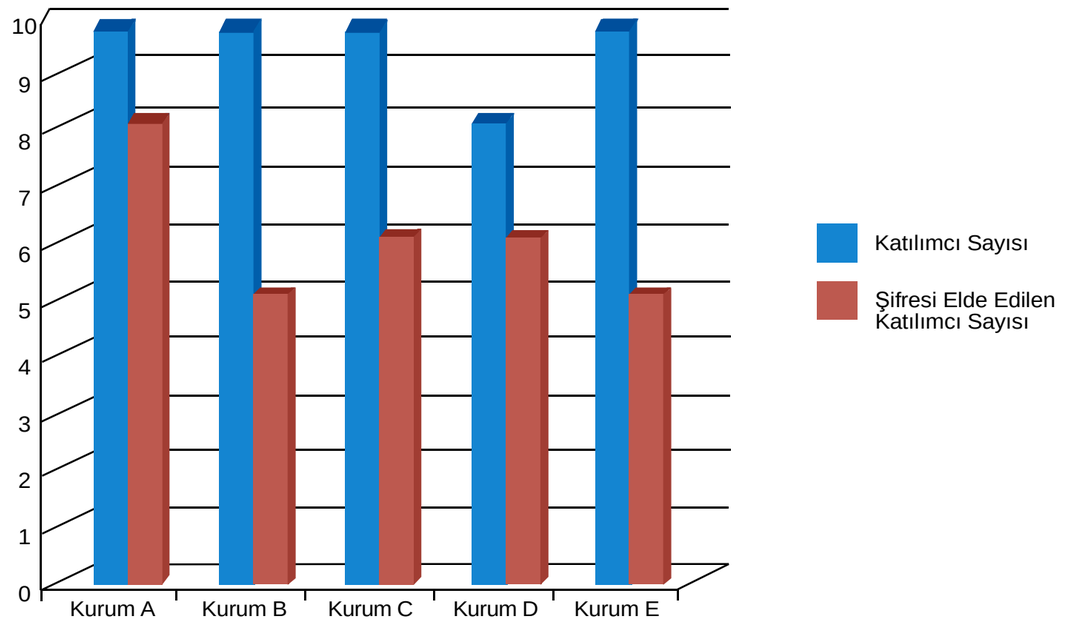
Dışarıdan birinin kurum çalışanı kimliğine bürünmesi tekniğidir. En basitinden, içeriye bir kez girdikten sonra klavyelerin altına ya da monitörlere yapıştırılmış not kağıtlarına bakarak pek çok şifre elde edilebilir. Daha da vahimi, kullanıcısı başında bulunmayan, ekranı kilitlenmemiş ve şifreli ekran koruyucusu bulunmayan bilgisayarlardır.

10. Teknolojiyi ve Sosyal Mühendisliği Birlikte Kullanmak

Başarılı sosyal mühendisler sadece telefonu ya da insanların zafiyetlerini kullanmanın yanı sıra teknolojiyi de kullanarak saldırıyı daha etkin hale getirirler. Bu kapsamda şifre kırma programları, klavyeden girilen tüm bilgiyi kaydeden casus yazılımlar ve zararlı kod içeren dosyalar hazırlamaya yarayan programlar örnek olarak verilebilir.

11. İşe Yeni Girenlere Yapılan Saldırılar

Başarılı bir sosyal mühendis çoğunlukla kurum içi yetki sıralamasında alt düzeylerde olan çalışanları, özellikle de yeni işe başlayanları hedef alır. Peki neden işe yeni başlayanlar? Çoğu zaman kurum bilgilerinin ya da bazı hareketlerinin olası sonuçlarının farkında olmamaları ve kolayca etki altınagirebilmeleri bu soruya yanıt olarak verilebilir.



Şekil 4. *Kamu kurumlarında gerçekleştirilen sosyal mühendislik sonuçları.*

Şekil 3'te sosyal mühendislik saldırısı süreci gösterilmiştir. Sürecin ilk evresinde araştırma yer almaktadır. Bu aşamada saldırı gerçekleştirilecek kişi ya da kurum hakkında edinilebildiği kadar bilgi elde edilir. Daha sonra dostluk ve güven uyandırma aşamasına geçilir. Sosyal mühendis, bir önceki evrede edindiği bilgileri kullanarak kurbanın güvenini kazanmaya çalışır. Eğer başarılı olursa bir sonraki aşamaya geçilir ve güven kötüye kullanılır. Elde edilen hassas bilgiler değerlendirilir. Eğer bu bilgi yeterli ise saldırı sonlandırılır. Edinilen bilgi yetersiz ise tekrar araştırma evresine dönülür ve döngü sosyal mühendis tarafından bir kez daha yinelenir.

Şekil 3. *Sosyal mühendislik döngüsü.*

Sosyal Mühendislik ve Türkiye

TÜBİTAK UEKAE Bilişim Sistemleri Güvenliği Bölümü olarak yaklaşık 1,5 yıldır kamu kurumlarına sosyal mühendislik saldırıları gerçekleştirmekteyiz. Bu kapsamda bugüne kadar toplam 5 kamu kurumunda bu testi gerçekleştirdik. Bu kapsamda toplam 48 kullanıcı ile telefon görüşmesi yapıldı ve 30'una ait şifre elde edildi. Kurum A'da 10 kullanıcı ile görüşülüp 8'inin hassas bilgisi elde edildi. Kurum B ve E'de ise 10 kullanıcı ile görüşülüp 5'inin şifresi elde edildi. Kurum C'de 10, Kurum D'de 8 kurum çalışanı ile görüşülüp 6'sının şifresi elde edildi. (Şekil 4) Kurum A'da başarı oranı (şifresi elde edilen katılımcı sayısı/katılımcı sayısı) %80 iken, Kurum B ve E'de bu oran %50, Kurum C'de %60 ve Kurum D'de %75 olmuştur ki bu oranlar ciddi derecede yüksek oranlardır. Aslında burada kurum bazında başarı oranına bakmak pek de doğru olmayabilir; çünkü siz saldırgan olarak kurumdan sadece bir kişinin bile hassas bilgisini ele geçirseniz, bu hassas bilgiyle pek çok bilgiye ulaşabilmeniz mümkün olabilir. Sonuçlar çözümlendiğinde, maalesef kamu kurumlarımızdaki personelde bilgi güvenliği bilincinin pek oturmamış olduğu gözükmektedir.

Sosyal Mühendislik Testleri

Yaklaşık 1,5 yıldır kamu kurumlarına gerçekleştirdiğimiz sosyal mühendislik saldırılarında kullandığımız bazı senaryoları aşağıda bulabilirsiniz. Bu testi gerçekleştirmeden önce kurum yetkilisinden izin alınmakta ve test boyunca bir bilgi işlem personeli testi gerçekleştiren personele refakat etmektedir. Test sonunda şifreleri ele geçirilen kullanıcılara, bilgi işlem personeli tarafından ulaşılmakta, şifrelerini değiştirmeleri yönünde bilgi verilmektedir. Böylelikle ele geçirilen şifrelerin hassasiyet ya da kritiklik derecesi sıfırlanmış olur.

Senaryo 1:

Bu senaryoda kullanılan veri tamamen kurum dışından (*Facebook*, *Google*, *MSN* vb.) elde edilir. Saldırgan kurumla ilgili telefon bilgilerini internetten topladıktan sonra bu numaraları arayarak kendisinin bilgi işlem departmanında yeni işe başladığını ve aktif dizinde bir güncelleme yapmak amacıyla kullanıcı adı ve şifreye ihtiyacı olduğunu söyler.

Senaryo 2:

Bu senaryoda kullanılan veri tamamen kurum içinden (bilgi işlem departmanından alınan telefon listeleri, kritik personelin listesi vb.) elde edilir. Saldırgan ilgili telefon numaralarını arayarak kendisinin bilgi işlem departmanında yeni işe başladığını ve aktif dizinde bir güncelleme yapmak amacıyla kullanıcı adı ve şifreye ihtiyacı olduğunu söyler.

Senaryo 3:

Saldırgan kendini, denetçi olarak tanıtır ve şu an kurum başkanının yanında olduğunu söyleyerek devam eder. Başkanın emriyle bir inceleme yapmak için kullanıcı adı ve şifreye ihtiyacı olduğunu söyler.

Senaryo 4:

Bu senaryoda kullanılan veri tamamen kurum dışından (ör. *Google*) elde edilir. Saldırgan kurumun santralini arayarak muhasebe departmanından birisiyle görüşmek istediğini söyler. Amaç, öncelikle bir isim ve dahili numara elde etmektir. Bu bilgiyi aldıktan sonra ilgili kişiyi arayarak kullanıcı adı ve şifresini almaya çalışır.

Senaryo 5:

Eğer kurumda var olan kritik yazılımlardan herhangi biri dışarıdan bir kurumun işletimi altındaysa, saldırgan kendisini o kurumdan bir yetkili olarak tanıtıp, bir güncelleme yapmak için kullanıcı adı ve şifre almaya çalışır.

Senaryo 6:

Çeşitli yazılımlar yardımıyla ekinde zararlı yazılım bulunan ve içeriği kullanıcılara çok cazip gelecek e-posta hazırlanır ve tüm kullanıcılara gönderilir.

Örnek 1: Maaşlara yapılan son zammı görmek için ekteki dokümana tıklayınız.

Örnek 2: Ben aaa firmasında teknik destek grubu çalışanıyım. Firmamızın bbb yazılımında meydana gelen kritik bir açıklığın bir an önce kapatılması için lütfen ekteki yamayı bilgisayarınıza kurunuz.

Sosyal Mühendislik Eğitimleri

Sosyal mühendislik konusunda Türkiye'de verilen eğitimlerin noksanlığından yola çıkarak 2009 yılının son çeyreğinde 2 gün süreli "*Sosyal Mühendislik: Saldırı ve Korunma Yöntemleri*" isimli yeni eğitimimizi Bilişim Sistemleri Güvenliği Bölümü Eğitim Kataloğu'na ekledik.

Sosyal mühendislik eğitimlerinin ana hedefi, kurum personelinin, günümüzde oldukça yaygın olan ve başta "*kurumun prestiji*" olmak üzere pek çok farklı yönden kuruma zarar verebilme potansiyeline sahip sosyal mühendislik saldırılarına karşı bağışıklık kazanması olmalıdır. Bu türden bir eğitimi alan personel, hem alacağı teorik bilgiyle hem de eğitim boyunca yapılacak olan uygulamalarla, kendi kurumunda diğer çalışanlara benzer bir eğitimi verecek bilgi birikimine sahip olacak konuma gelmelidir.

Korunma Yöntemleri

Aşağıdaki maddeleri içeren kullanıcı bilinçlendirme eğitimleri tüm kurum personeline belirli periyotlarda verilmelidir [2][3][5]:

- Prosedürlerin ve uygulanmalarının önemi,
- Bilgisayara giriş ve şifre güvenliği,
- Bilgisayarda donanım ve yazılım değişiklikleri yapma,
- Dizüstü bilgisayar kullanımı,
- Dosya erişim ve paylaşımı,
- Yazıcı kullanımı,
- Taşınabilir medya kullanımı,
- Virüsten korunma,
- İnternet erişim güvenliği ve 5651 sayılı yasa,
- E-posta güvenliği,
- Yedekleme,
- Bilgisayar güvenlik olayları ihbarı,
- Sosyal mühendislik.

"Sürekli Bilinç Programı" kapsamında kurumun intranet sayfasına bilgi güvenliğiyle ilgili karikatürler, ipuçları koyma, ayın güvenlik çalışanının resmini asma, bülten panolarına duyurular asma, çeşitli bilgi güvenliği posterleri asma, hatırlatma amaçlı e-postalar gönderme, bilgi güvenliğiyle ilgili internet sitelerinin takibi, broşürler dağıtma ve güvenlikle ilişkili ekran koruyucular ve arka plan resimleri kullanma gibi önlemler alınmalıdır.

Ayrıca kurumda risk analizi çalışmalarının yapılması gerekmektedir. Bu kapsamda kurumun bilgi varlıkları, bu varlıklara gelebilecek tehditler ve bu tehditlerin oluşturabileceği zararların tespit edilmesi gerekir. Kurumda veri sınıflandırması çalışmaları yapılmalıdır.

Yukarıda bahsedilen önlemlerin haricinde personel kimlik kartlarını tüm çalışanlar yakalarına takmalıdır. Kurumda bilgi güvenliği şubesi ve olay bildirme merkezi kurulmalıdır. Kurumda periyodik olarak bilgi güvenliği testleri yapılmalıdır. Antivirüs yazılımları mutlaka tüm bilgisayarlara kurulmalı ve tanım dosyası güncel tutulmalıdır. Çöpe atılması gereken kurum için önemli dokümanlar, kırpıcılardan geçirilmelidir. Bilgisayarlarda şifre korumalı ekran koruyucular kullanılmalıdır. İşten ayrılan çalışanların uyması gerekenleri içeren prosedürler hazırlanmalıdır. Kuruma ziyaretçi olarak gelen kişilerden kimlik alınmalı ve kurum içerisinden bir çalışan bu kişiye refakat etmelidir. Kurumda mutlaka ve mutlaka güçlü şifreler kullanılmalı ve bu şifreler kesinlikle bir yerlere yazılmamalı ya da başkalarıyla paylaşılmamalıdır.

Sosyal Mühendislik Saldırılarının Tespit Edilmesi

En çok kullanılan sosyal mühendislik yöntemleri; kurum çalışanı gibi davranmak, ortak iş yürütülen bir şirketin çalışanı gibi davranmak, yetkili biri gibi davranmak, yardıma ihtiyacı olan, işe yeni girmiş biri gibi davranmak, bir sistem yaması yükletmek için çalışan bir sistem üreticisi gibi davranmak, önce

sorun yaratmak, sonra sorunu çözmeye çalışmak, e-posta ekinde zararlı yazılım göndermek ve kurum içi terimleri kullanmak olarak sıralanabilir [3][7].

Eğer tanımadığınız bir kişiyle yaptığınız görüşme esnasında, bir geri arama numarası vermekten kaçınılması, sıra dışı taleplerde bulunulması, yetkili olduğunun öne sürülmesi, aciliyetin üzerine vurgu yapılması, isteğin yerine getirilmemesi durumunda kötü sonuçlar doğacağının söylenmesi, soru sorulduğunda rahatsız olunması, bilinen adların sıralanması ve iltifat edilmesiyle kur yapılması gibi durumlarla karşı karşıya kalıyorsanız bir sosyal mühendislik saldırısına maruz kalıyor olabilirsiniz.

Sonuç

Tehlike hiç ummadığınız bir anda, hiç ummadığınız bir yerden gelebilir. Tanımadığınız kişilerden gelen isteklere karşı temkinli davranın ve size özel bilginizi (ör. şifrenizi) sistem yöneticisi, mesai arkadaşınız, hatta yöneticileriniz dahil, kimseyle paylaşmayın. Kurumdaki tüm personele periyodik olarak bilgi güvenliği bilinçlendirme eğitimleri verin. Ve son olarak da kurumunuzda periyodik olarak, sosyal mühendislik saldırı testini de içeren, bilgi güvenliği testleri gerçekleştirin.

KAYNAKÇA

[1] "Data Loss Statistics", *Datalossdb*, Ekim 2009: http://datalossdb.org/statistics.

[2] T. Mataracıoğlu, "Sosyal Mühendislik: Saldırı ve Korunma Yöntemleri Kurs Notları", *TÜBİTAK UEKAE Bilişim Sistemleri Güvenliği Bölümü*, Ekim 2009.

[3] K. D. Mitnick ve W. L. Simon (çev.: N. E. Tezcan), "Aldatma Sanatı", Ankara: *ODTÜ Geliştirme Vakfı*, 2009.

[4] C. Bican, "Sosyal Mühendislik Saldırıları", *TÜBİTAK UEKAE* – Ulusal Bilgi Güvenliği Kapısı, 20 May. 2008: http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/sosyal-muhendislik-saldirilari.html?Itemid=6

[5] M. B. Arslantaş, "İnternette Bilişim Suçlarında Kullanılan Metotlar", *MEB Bilgi Teknolojileri Gn. Md. - EğiTek H@ber*, 24 Kas. 2004: http://egitek.meb.gov.tr/EgitekHaber/EgitekHaber/s75/bılsım sucları.htm

[6] "What is Social Engineering?", *Microsoft*, 2010: http://www.microsoft.com/protect/terms/socialengineering.aspx

[7] "CERT's Podcasts: Security for Business Leaders: Show Notes", *CERT*, 2008: http://www.cert.org/podcast/notes/20080429hinson-notes.html

SKAAS

SAYISAL KAYIT ARŞİV VE ANALİZ SİSTEMİ

MERDAN METİN

Sayısal Kayıt Arşiv ve Analiz Sistemi; uydu, kablo, karasal ve internet üzerinden yayın yapan televizyon ve radyo kanallarını sayısal olarak arşivlemek, kayıtlar üzerinde ses ve görüntü analizleri yapmak amacıyla Radyo ve Televizyon Üst Kurulu (RTÜK) için TÜBİTAK UEKAE tarafından geliştirilmiştir. Sistem, UEKAE'nin bilgi güvenliği ve ülke savunması ile ilgili donanım, yazılım üretimi ve entegrasyonu gerektiren büyük taahhüt projelerini gerçekleştirme kabiliyetinin farklı alanlara uygulanmasına güzel bir örnek oluşturmaktadır.

Ülkemizde televizyon ve radyo yayınlarını denetlemek ve düzenlemekten sorumlu olan RTÜK ile 2006 yılının şubat ayında sözleşmesi imzalanarak başlanan proje çalışmaları 22 aylık bir sürede tamamlanmıştır. Sistemin işletmeye alınması ile RTÜK mevcut tüm yayın biçimlerini kapsayan ve gelecekte ortaya çıkacak yeni teknolojilere kolay uyum sağlayabilecek, büyüme imkanına sahip, uluslararası standartlara göre hazırlanmış bir altyapıya sahip olmuştur.

Sistem aynı anda ulusal 120 televizyon ve 120 radyo yayınını kaydedebilmekte ve 100'den fazla kullanıcıya hem canlı olarak hem de arşivden izletebilmektedir. Kurumun gelecekte yerel yayınları da sisteme dahil etme ihtiyacı düşünülerek, altyapısı 400 televizyon ve 1500 radyo yayınını canlı olarak izletebilecek ve en az 6 ay saklayabilecek biçimde gerçeklenmiştir.

Geliştirilen yayın alış alt sistemi ile televizyon ve radyo kanallarının uydudan, kablodan, karasal antenden hiyerarşik olarak alınabilmesi yani kaydedilen kanalın uydu üzerinden alınamaması durumunda sırası ile kablodan ve karasal ortamdan alınmaya başlanarak yayının kesintisiz kaydı sağlanmaktadır. Ayrıca yayın alış donanımları aktif – pasif yedekli çalışmakta, yayınların sinyal seviyesi takip edilerek arıza durumunda saniyeler bazında yedek cihazın otomatik devreye girmesi sağlanmaktadır.

Televizyon ve radyo yayınlarının alınması için üçü sabit bir tanesi hareketli dört uydu anteni, iki karasal anten ve bir radyo anteni kullanılmaktadır. Yayın sinyallerinin kesintisizliği uygulama yazılımları içinden dinamik olarak yönetilen 2 anten matrisi ile sağlanmaktadır.

Tasarlanan esnek yapı sayesinde hem mevcut hem de gelecekte ortaya çıkabilecek analog ve sayısal yayın teknolojileri (uydu, kablo, karasal ve *IPTV* platformları) yayın alış alt sistemi tarafından kaydedilebilmektedir. Televizyon yayınları H.264 kodlama algoritması ile istenen çözünürlükte ve ekran boyutunda, radyo yayınları MP3 kodlama algortiması ile istenen örnekleme ve bit hızında saklanabilmekte aynı anda da kurulan ağ altyapısı üzerinden MPEG2 *Transport Stream* (ISO/IEC 13818-1) standardında kullanıcılara canlı olarak izletilmektedir.

Oluşturulan kayıt dosyaları en az altı ay depoda saklanmaktadır, ancak kanallara göre tek tek bu süre sınırsız olarak

uzatılabilmektedir. Depo alt sistemi yaklaşık 750 terabayt fiziksel büyüklüğe sahip iki aşamalı saklama mimarisinde yapılandırılmıştır. 15 günden eski olmayan kayıtlar daha hızlı erişim sağlayan FC (*Fiber Channel*) diskler üzerinde daha eski kayıtlar ise FATA diskler üzerinde tutulmaktadır. Depolama alt sistemi kurumsal (*enterprise*) seviyede, RAID desteği olan tümüyle yedekli donanım bileşenlerinden oluşturulmuştur ve neredeyse sınırsız büyütülebilme potansiyeline sahiptir. Depo alt sisteminin doluluk oranının izlenmesi, otomatik yük dengelemesinin yapılması geliştirilen yazılımlarlar ile açık kaynak kodlu PostgreSQL veritabanı kullanılarak yapılmaktadır. Bu büyüklükteki bir deponun açık kaynak kodlu bir veritabanı ile kontrol edilmesinin ilk ve tek örneğidir. Veritabanının kesintisiz olarak birden fazla sunucu üzerinde hizmet verebilmesi için UEKAE tarafından yazılım geliştirilmiştir. Böylece kurumsal seviyede hizmet veren ticari veritabanı kullanım gereksinimi giderilmiştir. UEKAE'nin bundan sonraki projelerinde de rahatlıkla kullanılabilecektir.

Canlı olarak stream edilen (ethernet ağı üzerinden gönderilen) televizyon yayınlarının görsel olarak kontrolü için her birinde 6 adet 67 inç DLP küp kullanılarak iki ekran duvarı oluşturulmuştur. Ekran duvarlarının yönetimi için UEKAE tarafından geliştilen yazılım sayesinde istenen boyutta ve adette pencere açılabilmekte, hem canlı yayın hem de kayıt dosyası oynatılabilmekte ve yayın gelmemesi durumunda uyarı verilebilmektedir.

Sistem tarafından kaydedilmeyen yayınların depoya atılabilmesi ve çeşitli amaçlarla depodan çıkartılabilmesi için yayın giriş – çıkış yazılımı geliştirilmiştir. Yetkilendirilmiş kullanıcılar VCD, DVD, USB, HDD, VHS, teyp kaseti ortamından sisteme kayıt dosyası atabilmekte ve kayıt dosyalarını VCD, DVD formatında dışarı çıkartabilmektedir. Çıkan kayıtlar üzerine istenen şeffaflıkta fligran eklenebilmekte ve elektronik olarak imzalanabilmektedir.

Yine geliştirilen Medya Varlık Yönetim (MVY) yazılımı sayesinde sistem kullanıcıları,

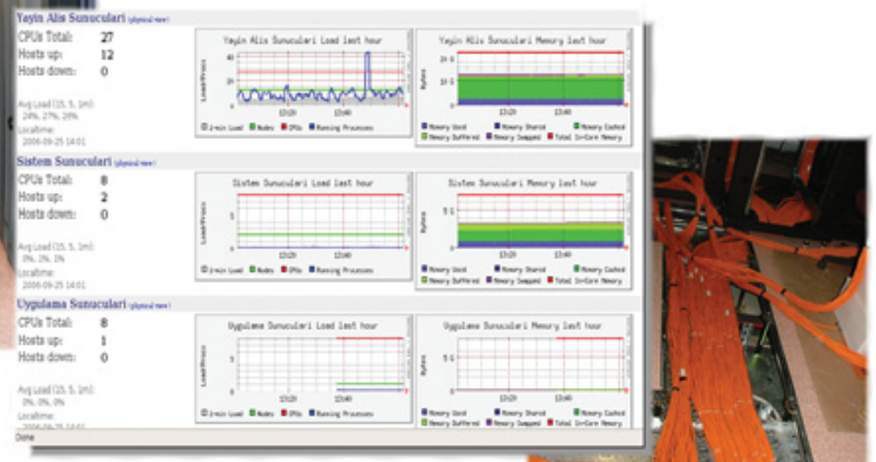
- Birden fazla canlı yayının aynı anda izleyebilmekte,
- Arşiv yayınlarını sorgulayabilmekte ve izleyebilmekte,
- Anahtar kareler üzerinden sahne seçimi yaparak istenen yere hızla konumlamabilmekte,
- Sınırsız sayıda klip oluşturabilmekte ve klip bazlı arama yapabilmekte,
- Açıklama notu koyabilmekte ve rapor yazabilmekte,
- Hazırlanan araçları kullanarak deşifre yapabilmekte
- İş akışı tanımlayabilmekte,
- Görüntü ve ses analiz görevi verebilmektedir.

TÜBİTAK Uzay Bilimleri Enstitüsü tarafından bu proje için geliştirilen görüntü ve ses analiz yazılım paketi kullanılarak;

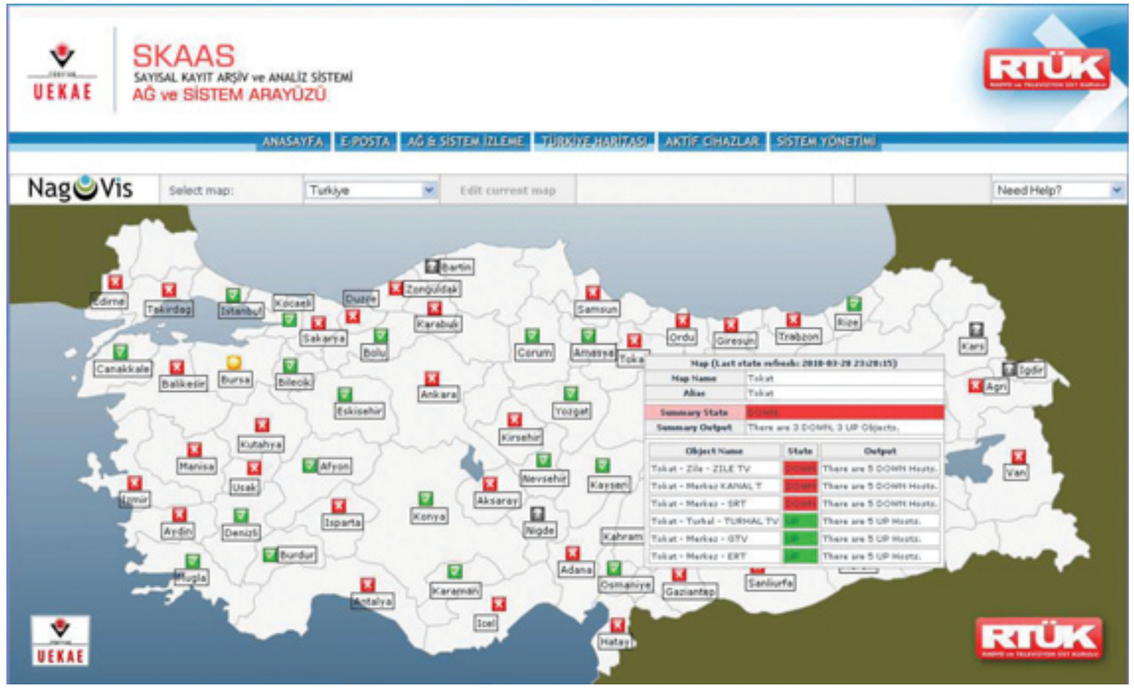
- Sahne geçişlerine veya zamana göre anahtar kare üretimi yapılabilmekte,
- Kayıtlar üzerinde görüntü klibi aranabilmekte,
- Görüntü üzerine bindirilmiş, duran veya hareketli yazılar metine dönüştürülebilmekte,
- Kanal logosu, fragman ve cıngılı tanınarak hem televizyon hem de radyo kanallarının reklam süreleri otomatik olarak belirlenebilmekte,
- Verilen listedeki anahtar kelimeler televizyonda veya radyoda telaffuz edildiğinde yakalanabilmektedir.

Sistemde kullanılan, kurumun ihtiyacı tüm yazılımlar TÜBİTAK tarafından geliştirilmiştir. Açık kaynak kodlu veritabanı (Postgre SQL), işletim sistemleri (Linux/Pardus, Centos) ve sunucu-ağ cihazı yönetim programları kullanılarak yazılım lisansından milyonlarca dolarlık tasarruf sağlanmıştır.

Sistemin donanım ihtiyacı ticari olarak satılan genel amaçlı donanımlardan, sistemin genişlemesi gerektiğinde marka bağımlılığı yaratmayacak biçimde kullanılarak karşılanmıştır.



SKAAS'ın ikinci aşaması sayılabilecek, yerel televizyon kanallarının mahallinde kaydedilerek RTÜK'ün Ankara'daki merkez binasında kurulmuş olan sistem odasına aktarılması çalışmalarına 22 Ocak 2009 tarihinde başlanmıştır. Bu proje ile, Ankara'dan izlenemeyen 185 yerel televizyon kanalının yerinden kaydının alınması, telekom hatları üzerinden aktarılması, ulusal yayınlarda olduğu gibi izlenebilmesi ve üzerinde analizler yapılabilmesi mümkün olacaktır. Şu anda çalışmaların son aşamasına gelinmiş ve 180 yerde yayın alış sistemi kurulumu tamamlanmıştır. 2010 yılı içinde işletme testlerinin tamamlanması ile RTÜK ülkemizde yayın yapan tüm televizyon kanallarını ve ulusal radyoları canlı veya arşivden izleyebilme kabiliyetine sahip olmuş olacaktır.



makaleler

Eşitlik Karakterinin Matematiksel İşlevleri

C. Nezih GEÇKİNLİ

Özet - *Çoğu matematiksel bağıntının eylemi olan eşitlik (‘=’) karakteri, temel olarak, “atama veya hesaplama”, “tanımlama”, “denklem kurma” ve “özdeşini yazma” olarak adlandırabileceğimiz dört değişik işlevi gösterir. Dolayısıyla, karşılaşılan bağıntıların doğru algılanabilmesi için, bu ayrımın doğru yapılabilmesi gerekir. Öte yandan, birbirinden ayrı dört kavramın hep aynı biçimde gösteriliyor olması, özellikle matematikçi olmayanların algılama yeteneğini zayıflatabilir. Bu nedenle, okuyucu bu konuda uyarılmakta; okuyucunun algılama kaybı olup olmadığını sınaması, varsa bunu yeniden kazanabilmesi için, sınıflandırılan ve* Mathematica *programlama dilinde kullanılan dört karakter grubu (‘=’, ‘:=’, ‘==’, ‘===’) ile gösterilen örnek bağıntılar verilmektedir.*

Anahtar Sözcükler - *Eşitlik, denklem, özdeşlik, matematik eğitimi.*

1 GİRİŞ

Matematik size Çince gibi mi geliyor? Çok haklısınız! Çünkü matematikte de

$\mathbb{Z}$ (tam sayılar kümesi),

$\in$ (kümenin elemanı),

∞ (sonsuz),

π (çember uzunluğunun çapa oranı [1]),

i (-1’in karekökü, $\sqrt{-1}$, [2]),

e ($(1+1/n)^n$’nin n sonsuza varırken aldığı değer [3])

gibi anlam yüklü karakterler;

$n!$ (n tam sayısından büyük olmayan pozitif tam sayıların çarpımı),

$\pi(x)$ (x’den büyük olmayan pozitif asal sayıların sayısı),

gibi karakter grupları;

$\approx$ (yaklaşık olarak eşit),

$\sim$ (asimptotik olarak eşit)

$(a \mid p)$ (Legendre)

gibi simgeler (semboller);

$+$ (sayılar için toplama),

Σ (sayı serileri için toplama),

$\cup$ (kümeler için toplama, bileşim),

gibi işlemler;

$\cos(x)$ (kosinüs)

$\Gamma(s)$ (gamma),

$\mu(x)$ (Möbius);

$\zeta(n)$ (Riemann Zeta)

gibi fonksiyonlar; hatta, belirli bir yazıya ya da kitaba özgü pek çok işaret [4] kullanılmaktadır.

Matematikteki çoğu cümlenin eylemi olan eşitlik (‘=’) karakteri ise, kullanıldığı yere göre değişik anlamlara gelmektedir:

1°) “... değerini taşır; ... değerine eşittir”;

2°) “... olarak tanımlanır; ... olarak tanımlansın”;

3°) “... değişkenlerin bazı değerleri için eşittir”;

4°) “... değişkenlerin tüm değerleri için eşittir; özdeştir”.

Bu nedenle, nasıl ki Çinceyi kolayca okuyup doğru anlayabilmek için uzun yıllar Çince eğitim görmüş birisi olmak gerekirse, matematiği kolayca ve doğru anlayabilmek için de uzun yıllar eğitim görmüş bir matematikçi olmak gerekir.

Matematik işlemlerini hem sayısal hem de simgesel olarak yapabilen ve sayı kuramı konusunda çalışan matematikçilerin de değer verdiği bilgisayar programlarından olan *Mathematica*’da [5]-[6], eşitlik karakterindeki belirsizliği giderebilmek için, kullanıcının niyetini anlayacak yapay zekâ (*artificial intelligence*) programları yerine, yukarıda sıralanan anlamlara karşılık gelen ‘=’, ‘:=’, ‘==’, ‘===’ karakter gruplarından birisi kullanılır. Bu yazıda da, *Mathematica*’nın önerdiği karakter grupları kullanılarak, eşitlik karakterinin matematikteki dört değişik anlamı örneklerle tartışılmaktadır.

Mathematica dayanak alındığında, eşitlik karakterinin yukarıda verilen dört anlamına karşı düşen eylemler şöyle adlandırılabilir:

1°) Atama veya hesaplama (‘=’),

2°) Tanımlama (‘:=’),

3°) Denklem kurma (‘==’),

4°) Özdeşini yazma (‘===’).

2 DEĞER ATAMA, HESAPLAMA, TANIMLAMA

Dikdörtgen bir levhamız olsun. Bu levhanın enine x_1, boyuna y_1 diyelim. Levhamızın kenarlarını bir cetvelle

ölçtüğümüzde, enini 2 cm, boyunu 3 cm bulmuş olalım. Bu sonuçları

$$x_1 = 2\,, \qquad y_1 = 3 \tag{1}$$

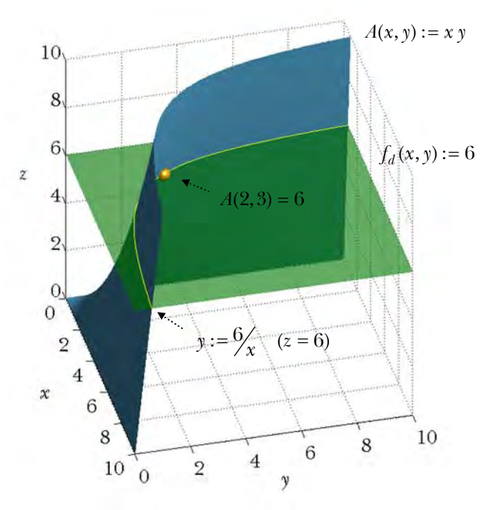
olarak gösterelim. Yani, levhamızın eni x_1’e 2, boyu y_1’e 3 sayılarını atayalım.

Dikdörtgen levhanın alanını, levhanın eni ile boyunun çarpımı olarak tanımlayalım ve bunu x ve y bağımsız değişkenlerinin fonksiyonu olarak, Şekil 1’deki gibi

$$A(x,y) := x\,y \tag{2}$$

biçiminde gösterelim. Böylece, levhamızın alanı A_1’e 6 sayısını atamış oluruz:

$$A_1 = A(x_1, y_1) = A(2,3) = 2 \cdot 3 = 6 \tag{3}$$



Şekil 1. *İki değişkenli fonksiyonlar ve arakesitleri.*

Fonksiyon tanımlamanın yanı sıra, fonksiyonlar üzerine tanımlanmış işlemler ve fonksiyonlar da bulunmaktadır. Örneğin, bir $f(x)$ fonksiyonunun $x = a$’da $0/0$, ∞/∞, $0\cdot\infty$, $\infty-\infty$, 0^0, ∞^0, 1^∞ türü bir belirsizliği varsa ve bu fonksiyon; x a’ya, a’dan daha küçük ya da a’dan daha büyük değerle başlayıp yaklaşırken aynı değere ulaşıyorsa, bu değer o fonksiyonun $x = a$’daki limit değeri olarak tanımlanır [7]:

$$\lim_{x\to a} f(x) := \{f(x)\ \textit{fonksiyonunun},\ x\ a\text{'}ya\ \textit{yaklaşırken ulaştığı değer}\} \tag{4}$$

Euler’in tanıttığı ve çalışmalarında sıkça kullandığı e sayısını göz önüne alalım. Bu sayının tanımı

$$e := \lim_{n\to\infty} (1+1/n)^n = 2{,}718281\ldots \approx 2{,}71828 \tag{5}$$

limiti ile verilebilir. Bu limit ifadesi hesaplandığında, (5) bağıntısındaki ikinci eşitlikle verilen irrasyonel sayı elde edilir. Bu değerin virgülden sonra 5 anlamlı basamağa yuvarlatılmasıyla elde edilen yaklaşık değer de (5) bağıntısında, en sağda görülmektedir.

(Levhamızın kenarlarını ölçtüğümüzde bulduğumuz 2 cm ve 3 cm değerleri tam olamaz; çünkü, bir ölçümü ne kadar doğru yapmaya çalışırsak çalışalım, ancak elimizdeki aletin duyarlığı ölçüsünde hatasız yapabiliriz. Ölçüm sonuçlarımızın rasgele hatalı olması kaçınılmazdır [8]. Yine de (1) bağıntısında, x_1’e ve y_1’e 2 ve 3 değerlerini atarken, yaklaşık değer karakteri yerine eşitlik (‘=’) karakterini kullandık. Öte yandan, eğer atanan değer, virgülden sonra gösterilemeyecek kadar çok ya da sonsuz sayıda basamağı olan bir sayı ise, gösterilemeyen hanelerin varlığı, (5) bağıntısında olduğu gibi ya üç nokta ile belirtilir ya da sayının yuvarlatılmış bir karşılığı yaklaşık değer işareti (‘≈’) ile atanır.)

Bu e sayısını kullanan doğal üstel fonksiyon “exp” ve ters fonksiyonu olan (e’nin kuvvetini bulan) doğal logaritma fonksiyonu “ln” ($\log_e$ olarak da gösterilip “e tabanına göre logaritma” diye okunan fonksiyon) şöyle tanımlanmaktadır:

$$\exp(x) := e^x\,, \tag{6}$$

$$\ln(\exp(x)) := x \tag{7}$$

Yarıçapı 1 birim olan çember üzerindeki A noktasıyla çemberin merkezi O’yu birleştiren doğrunun, çemberin merkezinden geçen yatay eksenle saat yönünün tersinde yaptığı açı θ olsun. Şekil 2’de görülen bu açının sinüsü, kosinüsü ve tanjantı, A noktasının düşey ve yatay koordinatları $h(A)$ ve $a(A)$ aracılığıyla aşağıdaki gibi tanımlanır:

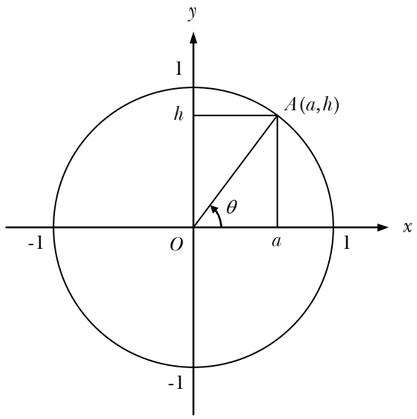
$$\sin(\theta) := h(A) \tag{8}$$

$$\cos(\theta) := a(A)\,, \tag{9}$$

$$\tan(\theta) := \frac{\sin(\theta)}{\cos(\theta)} = \frac{h(A)}{a(A)} \tag{10}$$

3 DENKLEMLER

İlk örneğimizdeki dikdörtgen levhaya geri dönelim. Her dikdörtgen levha için tek bir alan değeri söz konusu iken, alan değeri aynı olan dikdörtgen levhaların sayısı sonsuzdur. Alanı aynı, örneğin 6 olan dikdörtgen levhaların en ve boylarının geometrik yeri



Şekil 2. *Birim çember.*

$$A(x,y) == 6 \tag{11}$$

denklemini, yani

$$x\,y == 6 \tag{12}$$

denklemini çözen, sonsuz sayıdaki

$$(x, 6/x) \tag{13}$$

noktalarının xy dik koordinat sisteminde oluşturduğu eğridir. Bu eğri, geometrik olarak (2) ile tanımlanan yüzey ile, Oxy düzlemine paralel ve bu düzleme uzaklığı 6 olan

$$f_d(x,y) := 6 \tag{14}$$

düzleminin kesişme yeri olup, Şekil 1'de yüzeylerin arakesiti olarak gösterilmektedir.

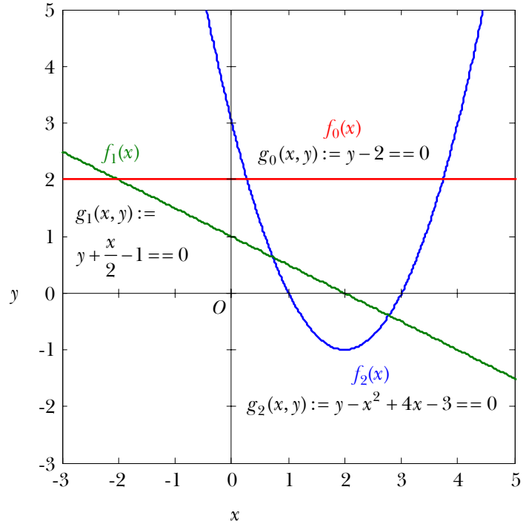
Eğriler, fonksiyonlar ile, açık (*explicit*) olarak tanımlanabildiği gibi, denklemler aracılığıyla, kapalı (*implicit*) olarak da ifade edilebilir [7]. Örneğin, Şekil 3'te görülen eğriler, fonksiyon olarak

$$\begin{aligned} f_0(x) &:= 2\,, \\ f_1(x) &:= -\frac{x}{2}+1\,, \\ f_2(x) &:= x^2 - 4x + 3\,, \end{aligned} \tag{15}$$

biçiminde ya da denklemler aracılığıyla

$$\begin{aligned} g_0(x,y) &:= y - 2 == 0\,, \\ g_1(x,y) &:= y + \frac{x}{2} - 1 == 0\,, \\ g_2(x,y) &:= y - x^2 + 4x - 3 == 0\,, \end{aligned} \tag{16}$$

eşitlikleriyle gösterilebilir. Ancak, denklemler ile ifade edilen kimi eğrileri fonksiyonlar aracılığıyla



Şekil 3. *Eğrilerin gösterilimi.*

tanımlayabilmek için birden fazla fonksiyon kullanmak kaçınılmaz olabilir. Örneğin, Şekil 4'ten de görülebileceği gibi,

$$g_c(x,y) := (y-4)^2 + (x-3)^2 - 4 == 0 \tag{17}$$

denklemiyle tanımlanan bir çemberin üst ve alt yarıları, her x değerine tek bir değer karşı düşüren

$$\begin{aligned} f_a(x) &:= 4 + \sqrt{-x^2 + 6x - 5}\,, \\ f_b(x) &:= 4 - \sqrt{-x^2 + 6x - 5}\,, \\ 1 &\le x \le 5\,, \end{aligned} \tag{18}$$

fonksiyonları ile ayrı ayrı tanımlanmak zorundadır.

Denklemlerin transandantal fonksiyonlarla birlikte kullanımına örnek olarak,

$$\ln(x) == 0 \tag{19}$$

denklemini göz önüne alalım. Bu denklemin çözümü, (6) ve (7) tanım bağıntıları aracılığıyla

$$x_0 = \exp(0) = e^0 = 1 \tag{20}$$

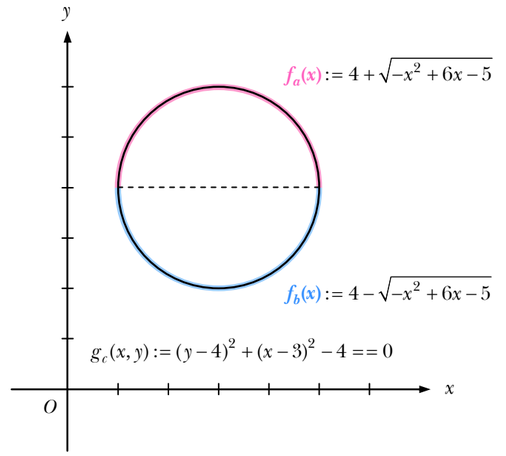
olarak yazılabilir. Benzer biçimde,

$$\ln(x) == 1 \tag{21}$$

denkleminin çözümü de

$$x_1 = \exp(1) = e^1 = e \tag{22}$$

olarak bulunur.



Şekil 4. *Çemberin denklem ve fonksiyonlar aracılığıyla gösterilimi.*

Trigonometride de denklemler kullanılır. Örneğin,

$$\cos(x) + \sin(x) == 1 \tag{23}$$

denkleminin $0 \le x \le 2\pi$ aralığındaki temel çözümleri

$$x_1 = 0 \tag{24}$$

ve

$$x_2 = \frac{\pi}{2} \tag{25}$$

radyandır[1].

4 ÖZDEŞLİKLER VE DİĞERLERİ

Bağımsız değişkenlerin her değeri için sağlanan (sol yanı sağ yanına denk olan) eşitliklere özdeşlik (*identity*) denir. Binom açılımı:

$$(x-y)^3 === x^3 - 3x^2y + 3xy^2 - y^3, \tag{26}$$

çarpanlarına ayrılmış polinom:

$$x^3 - y^3 === (x-y)(x^2 + xy + y^2)\,, \tag{27}$$

seri açılımı:

$$\frac{1}{1-x} === 1 + x + x^2 + x^3 + \ldots\,, \quad -1 < x < 1\,, \tag{28}$$

[1] Trigonometride açıların değeri "derece"den çok, "radyan" cinsinden ölçülür. Bu da, birim çemberde x açısının gördüğü yayın uzunluğuna denktir. Bu durumda 360°'lik tam açının değeri, 2π radyan olmaktadır.

hep birer özdeşliktir.

Örneğin, $x = 1$'de $0/0$ belirsizliğine sahip

$$f(x) := \frac{x^3 - 1}{x^2 - 1}\,, \tag{29}$$

fonksiyonunu göz önüne alalım. $f(x)$'in özdeşi yazılarak, belirsizliğe neden olan $x-1$ çarpanları ayrıştırılabilir:

$$f(x) := \frac{x^3 - 1}{x^2 - 1} === \frac{(x-1)(x^2 + x + 1)}{(x-1)(x+1)}\,, \tag{30}$$

$x \ne 1$ ise, bu iki çarpan birbirini götüreceğinden,

$$\lim_{x \to 1} \frac{x^3 - 1}{x^2 - 1} = \frac{3}{2} \tag{31}$$

bulunur.

Euler, doğal üstel fonksiyon ve doğal logaritmanın limitle ifade edilen, birbirinden bağımsız özdeşlerini de vermektedir [3]:

$$\exp(x) === \lim_{n \to \infty} (1 + x/n)^n\,, \tag{32}$$

$$\ln(x) === \lim_{n \to \infty} n\left(x^{1/n} - 1\right) \tag{33}$$

b ve c değişkenleri

$$b == \exp(c) \tag{34}$$

denklemini sağlıyor olsun. İki yanın doğal logaritması alınıp doğal logaritmanın (7) ile verilen tanımı kullanıldığında,

$$\ln(b) == \ln(\exp(c)) = c \tag{35}$$

denklemi bulunur. Bu iki denklemden, doğal üstel fonksiyonun, doğal logaritma fonksiyonunun tersi olduğunu gösteren şu özdeşlik yazılabilir:

$$b === \exp(\ln(b)) \tag{36}$$

Bu özdeşliğin x'inci kuvveti alındığında da

$$b^x === \left[\exp(\ln(b))\right]^x === \left(e^{\ln(b)}\right)^x === e^{x \ln(b)} \tag{37}$$

özdeşliği elde edilir.

İki bilinmeyenli (35) denklemi (34) denkleminden, iki yanın doğal logaritması alınarak elde edildiği için, bilinmeyenler üzerine yeni bir bilgi taşımaz; yani, iki denklem birbirine özdeştir. Dolayısıyla, (35) denklemindeki c, (34) denkleminde yerine konulduğunda, b bilinmeyeninin çözümü yerine, b bağımsız değişkenini içeren (36) özdeşliği, bir başka deyişle, iki taraf birbirini götürdüğü için, $0 == 0$ denkliği elde edilmektedir.

Trigonometride de birçok özdeşlik vardır. Bunlara örnek olarak

$$\cos^2(x) + \sin^2(x) === 1\,, \tag{38}$$

$$\cos(x+y) === \cos(x)\cos(y) - \sin(x)\sin(y)\,, \tag{39}$$

$$\sin(x+y) === \sin(x)\cos(y) + \cos(x)\sin(y)\,, \tag{40}$$

$$\cos(x) + i\,\sin(x) === \exp(i\,x) \tag{41}$$

özdeşlikleri verilebilir [7]. Son özdeşlik, Euler tarafından 1748'de tanıtılan ünlü Euler özdeşliğidir. Bu özdeşlikten;

- özdeşliğin iki yanının logaritması alınarak, Euler'den 34 yıl önce Cotes tarafından yayımlanan

$$\ln(\cos(x) + i\,\sin(x)) === i\,x \tag{42}$$

özdeşliği;

- (37) özdeşliği kullanılarak, $b > 0$ için

$$\begin{aligned} b^{i\,x} &== \exp(i\,x\,\ln(b)) \\ &=== \cos(x\,\ln(b)) + i\,\sin(x\,\ln(b)) \end{aligned} \tag{43}$$

özdeşlikleri;

- x yerine $\pi/2$ konularak, önce

$$i = \exp(i\,\pi/2) = e^{i\,\pi/2}\quad, \tag{44}$$

sonra, iki yanın i'inci üssü alınarak şu ilginç değer

$$i^i = e^{-\pi/2} = 0,207879... \approx 0,20788 \tag{45}$$

ve son olarak da,

- x yerine π konularak, klasik matematiğin dört önemli alanını (analiz, cebir, geometri, aritmetik konularını) temsil eden beş katsayı $(e, i, \pi, 1, 0))$ arasında matematiğin üç önemli işlemi (üs alma, çarpma, toplama) ile oluşan şu düşündürücü, matematikçilerce çok sanatsal bulunan eşitlik elde edilmektedir [3]:

$$e^{i\,\pi} + 1 = 0 \tag{46}$$

Eşitlik karakterinin matematikteki işlevleri, yukarıda tartışılan dört işlevle sınırlı değildir. Örneğin, güçlüğü nedeniyle olsa gerek, *Mathematica*'nın kapsam dışı bıraktığı, yalnızca tam sayı çözümleriyle ilgilenilen Diophantine denklemlerini de değişik bir denklik işaretiyle ('=+=') göstermek gerekir. Nitekim,

$$x\,y == 6 \tag{47}$$

denkleminin çözümleri, sonsuz sayıdaki $(x, 6/x)$ koordinat değerlerinden oluşan bir eğri iken (Şekil 1),

$$x\,y = + = 6 \tag{48}$$

Diophantine denkleminin çözümleri, bu eğrinin üzerindeki $(-6,-1)$, $(-3,-2)$, $(-2,-3)$, $(-1,-6)$, $(1,6)$, $(2,3)$, $(3,2)$, $(6,1)$ noktalarıdır.

5 FONKSİYON TANIMLAMADA EŞİTLİK ÖRNEKLERİ

a) **Türev:** Bir $f(x)$ fonksiyonunun x'e göre türevi, o fonksiyondan türetilen

$$f'(x) := \frac{d}{dx} f(x) := \lim_{\Delta x \to 0} \frac{f(x+\Delta x) - f(x)}{\Delta x} \tag{49}$$

fonksiyonu olarak tanımlanır [7]. $f'(x)$, $f(x)$ eğrisine x'te çizilen teğetin eğimini, yani, $f(x)$'in x'teki değişim hızını verir. Örneğin,

$$\frac{d}{dx}\sin(x) = \cos(x) \tag{50}$$

b) **Belirsiz İntegral:** Bir $f'(x)$ fonksiyonunun belirsiz integrali, türevi $f'(x)$ olan $f(x)$ fonksiyonu ile x'e göre türevi sıfır olan C değişmezinin toplamıdır [7]:

$$\begin{aligned} &\int f'(x)\,dx := \int \left(\frac{d}{dx} f(x)\right) dx := f(x) + C\,, \\ &\frac{d}{dx} C === 0\,. \end{aligned} \tag{51}$$

Bir başka deyişle, belirsiz integral, türev işlevinin tersidir. Örneğin,

$$\begin{aligned} &\int \cos(x)\,dx = \sin(x) + C\quad, \\ &\frac{d}{dx} C ===0\,. \end{aligned} \tag{52}$$

c) **Belirli İntegral:** Bir $f'(x)$ fonksiyonunun $[a,x]$ aralığındaki belirli integrali, türevi $f'(x)$ olan $f(x)$ fonksiyonunun $f(a)$ kadar eksiğidir [7]:

$$\begin{aligned} &g(x) := \int_a^x f'(t)\,dt := \int_a^x \left(\frac{d}{dt} f(t)\right) dt := f(x) - f(a)\quad, \\ &g'(x) === f'(x) \end{aligned} \tag{53}$$

Örneğin,

$$g(x) := \int_0^x \cos(t)\,dt = \sin(x) \tag{54}$$

d) **Fourier Dönüşümü:** Bir $f(x)$ fonksiyonunun Fourier dönüşümü, başka bir değişkene bağlı bir fonksiyondur [9]:

$$F(y) := \mathbb{F}[f(x)] := \int_{-\infty}^{\infty} f(x)\,\exp(-i\,2\pi y x)\,dx \tag{55}$$

$f(x)$ fonksiyonu, $F(y)$ Fourier dönüşümünden, Fourier dönüşümüne çok benzeyen ters Fourier dönüşümüyle elde edilebilir [9]:

$$f(x) := \mathbb{F}^{-1}[F(y)] := \int_{-\infty}^{\infty} F(y)\,\exp(i 2\pi x y)\,dy \tag{56}$$

Örneğin,

$$f_p(x) := \begin{cases} 1\,, & |\,x\,| \le 1 \\ 0\,, & |\,x\,| > 0 \end{cases} \tag{57}$$

dikdörtgen darbe fonksiyonunun Fourier dönüşümü [9]

$$F_p(y) := \mathbb{F}[f_p(x)] = \frac{\sin(2\pi y)}{\pi y}\quad; \tag{58}$$

$F_p(y)$'nin ters Fourier dönüşümü de dikdörtgen darbe fonksiyonu $f_p(x)$'dir.

e) **Fourier Serisi Açılımı:** Periyodu T olan, yani

$$f(x+T) === f(x) \tag{59}$$

özdeşliğini sağlayan periyodik bir $f(x)$ fonksiyonunun Fourier serisi açılımı, frekans değerleri $1/T$ (ana frekans) ve $1/T$'nin katları (harmonikleri) olan kosinüs ve sinüs fonksiyonlarının toplamıdır [9]:

$$f(x) === a_0 + \sum_{k=1}^{\infty} a_k \cos\left(\frac{2\pi k x}{T}\right) + \sum_{k=1}^{\infty} b_k\,\sin\left(\frac{2\pi k x}{T}\right)\,, \tag{60}$$

$$\begin{aligned} a_0 &:= \frac{1}{T}\int_0^T f(x)\,dx\quad, \\ a_k &:= \frac{2}{T}\int_0^T f(x)\,\cos\left(\frac{2\pi k x}{T}\right) dx\,,\quad k = 1,2,3,...\quad, \\ b_k &:= \frac{2}{T}\int_0^T f(x)\,\sin\left(\frac{2\pi k x}{T}\right) dx\,,\quad k = 1,2,3,... \end{aligned} \tag{61}$$

Örneğin, genliği 1, periyodu 1 olan ve

$$\begin{aligned} &f_u(x) := \begin{cases} -4x + 1\,, & 0 \le x < 1/2\,, \\ 4x - 3\,, & 1/2 \le x < 1\,, \end{cases} \\ &f_u(x+1) === f_u(x)\,, \end{aligned} \tag{62}$$

olarak tanımlanan simetrik üçgen dalga fonksiyonu

$$f_u(x) === \frac{8}{\pi^2}\sum_{n=1}^{\infty} \frac{1}{(2n-1)^2}\,\cos\big(2(2n-1)\pi x\big) \tag{63}$$

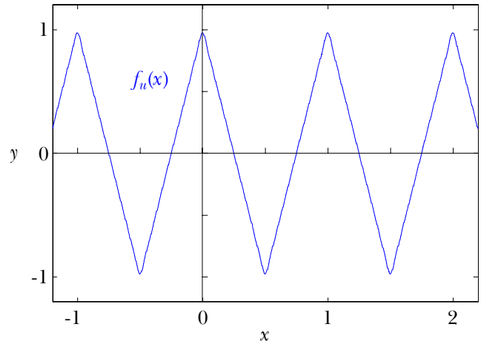
Fourier serisi açılımına sahiptir. Şekil 5'te, bu serinin ilk 8 teriminin toplamı görülmektedir.

f) **Taylor (Maclaurin) Serisi Açılımı:** $f^{(n)}(x)$, $f(x)$'in n'inci türevini göstersin. Analitik (bütün türevleri olan) bir $f(x)$ fonksiyonunun kuvvet serisine açılımı (özdeşi),

$$\begin{aligned} f(x) === f(0) &+ \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 \\ &+ \frac{f^{(\mathrm{IV})}(0)}{4!}x^4 + \cdots \end{aligned} \tag{64}$$

olarak yazılabilir [7]. Örneğin, $1/(1+x)^2$'nin Taylor serisine açılımı, $-1 < x < 1$ aralığında geçerli olan,

$$\frac{1}{(1+x)^2} === 1 - 2x + 3x^2 - 4x^3 + \cdots\quad,\quad -1 < x < 1 \tag{65}$$



Şekil 5. *Simetrik üçgen dalgaya ilişkin Fourier serisinin ilk sekiz teriminin toplamı.*

özdeşliğidir.

6 EŞİTLİĞİ SINIFLANDIRMANIN EĞİTBİLİMSEL ÖNEMİ

Buraya kadar genel açıklamalarla sürdürülen tartışma konusu yazarın duyumsadığı kişisel rahatsızlıklardan kaynaklanmaktadır. Bu rahatsızlıkların *Mathematica*'dan çok önceki yıllarda yaşanmış olması ve *Mathematica*'nın bu rahatsızlıkları doğrulaması, konunun kişiselleştirilmesini kaçınılmaz kılmaktadır.

Eşitlik yerine değişik simgeler kullanmanın, matematik makalesi okuyan bir matematikçi için gereksiz olacağı düşünülse de, matematiği yeni öğrenenler için eğitbilimsel açıdan yararlı olacağı açıktır. Örneğin ben, denklem ile özdeşliğin ayrı kavramlar olduğunu ilk kez lise son sınıfta duyumsamış; kendi başıma çözemediğim bu ayrımı, arkadaşlarıma belli etmeden, ders aralığında, matematik öğretmenimize sormuştum. Öğretmenimizin yanıtlayışını, çok dikkatli izleyip defalarca gözümde canlandırdığım için olsa gerek, hâlâ dünmüş gibi anımsarım. Yine de, bir denklemi çözerken yapılan açılımların, çarpanlara ayırmaların, birbirine özdeş $f(x) - f(x) === 0$ ve $f(x)/f(x) === 1$ özdeşliklerini kullanarak terimleri götürmenin, aslında, eşitini yerine koyma işlemleri değil, özdeşini yerine koyma olduğunun bilincine yeni yeni varıyorum. Eskiden, yüksek matematik (*calculus*) kitaplarında adı pek anılmadığı için olsa gerek (örneğin, Türkiye Bilimler Akademisi'nin bu konuda yayımladığı kitabın [7] dizininde özdeşlikle ilgili, yalnızca "*Green* özdeşlikleri" ve "Trigonometrik özdeşlikler" öğeleri bulunmakta), çok az sayıda olduğunu sandığım özdeşliklerin, şimdi, eşitliklerin önemli bir bölümünü

kapsadığını gördüm. Bu nedenlerden dolayı, özdeşlikleri açıkça belirtmenin, birçok konunun daha iyi kavranmasına yardımcı olacağına inanmaktayım.

Üniversitede okurken zihnimi meşgul eden konulardan birisi de, örneğin, $x=3$'ün kimi zaman bir denklemin çözümünü, kimi zaman bir doğruyu, bir düzlemi, ya da bir hiper düzlemi belirtiyor olmasıydı. Sürekli olarak $x=3$ gibi bir gösterimle karşılaştığımda, ne olduğunu nasıl anlayacağım endişesi duyardım. Şimdi içim rahat. Biliyorum ki,

$$x=3 \tag{66}$$

kendi başına iken, x değişkenine atanan değeri;

$$g_3(x) := x-3 == 0 \tag{67}$$

denkleminin çözümü ise, Ox ekseninde bir noktayı;

$$g_4(x,y) := x-3 == 0 \tag{68}$$

denkleminin çözümü ise, xy koordinat sisteminde, $(3,0)$ noktasından geçen, Oy eksenine paralel doğruyu;

$$g_5(x,y,z) := x-3 == 0 \tag{69}$$

denkleminin çözümü ise, xyz koordinat sisteminde, $(3,0,0)$ noktasından geçen, Oyz düzlemine paralel düzlemi gösterir.

Lisans eğitimim süresince, birkaç değişik derste karşılaştığım Fourier dönüşümü ile Fourier serisi açılımını yürekten duyumsayamıyor olmak beni rahatsız ediyordu. Yurt dışına, lisansüstü eğitimi için çıktığımda, beni rahatsız eden bu durumdan kurtulma umuduyla, Bracewell'in Fourier dönüşümü dersine yazılmıştım [9]. Elime geçen bu fırsatı çok iyi değerlendirebilmek için, ön sırada oturmuş, öğretmenimizin ağzından çıkan her sözü dikkatle dinliyor, o güne kadar duymadığım, beni rahatlatacak şeyler söylemesini bekliyordum. Genel bilgileri sunduğu ilk üç-beş dersten sonra, Fourier dönüşümüne giriş yaparken, beklediğim oldu: Öğretmenimiz, Fourier dönüşümünün bir tanım olduğunu; Fourier dönüşümü ile birlikte, Hankel, Mellin gibi daha pek çok ortogonal dönüşümün olduğunu; belli bir aralıkta ortogonal olma özelliğini sağlayan her çekirdek fonksiyon ile yeni bir ortogonal dönüşümün tanımlanabileceğini; bu nedenle, kuramsal olarak, sonsuz sayıda ortogonal dönüşümün olduğunu; dolayısıyla, kendi adımızı taşıyan yeni bir ortogonal dönüşümü tanımlayabileceğimizi söylediğinde ufkum genişleyiverdi. O gün eve dönerken, kendi kendime, "Hiç de gözümde büyüttüğüm gibi nereden nasıl türetildiğini bilemediğim bir şey değil, yalnızca bir tanımmış!" deyip duruyordum. Birden bir mucize olmuş, Fourier dönüşümüyle aramızdaki duvar yıkılmış, yaşam boyu sürecek bir dostluk kuruluvermişti.

7 SONUÇ

Matematikte kullanılan eşit işaretinin farklı işlevleri, *Mathematica* programlama dilinde de kullanılan farklı eşitlik simgeleri aracılığıyla, örnekler üzerinden ele alınmıştır. Kesin tanımlamalara dayanmayan bu ayrımların tartışmalı olacağı açıktır. Bu aşamada, okuyucunun, eskiden okuduğu matematik kitaplarında alıştırma yaparak, kendi tanımlarını yapması önerilir.

TEŞEKKÜR

Değerli zamanını feda ederek notlarıma hayat veren Sayın Dr. Levent Balamir Tavacıoğlu'na ve resimlerin oluşturulmasında emeği geçen Sayın Mehmet Usta ve Sayın Dr. Murat Akgül'e teşekkür ederim.

KAYNAKÇA

[1] A. S. Posamentier ve I. Lehmann, *π'nin Biyografisi*. İstanbul: Güncel Yayıncılık, 2005.

[2] P. J. Nahin, *An Imaginary Tale: The Story of* $\sqrt{-1}$. Princeton, NJ: Princeton University Press, 1998.

[3] E. Maor, *e : The Story of a Number*. Princeton, NJ: Princeton University Press, 1994.

[4] P. Ribenboim, *The Little Book of Bigger Primes*, 2nd ed. New York: Springer Verlag, 2004, *Index of Notations*, pp. xvii–xxiii.

[5] S. Wolfram, *The Mathematica Book*, 4th ed. Champaign, IL: Wolfram Media, 1999.

[6] M. Erickson and A. Vazzana, *Introduction to Number Theory*. Boca Raton, FL: Chapman & Hall/CRC, 2008.

[7] J. Stewart, *Kalkülüs: Diferansiyel ve İntegral Hesap, Kavram ve Kapsam*. Ankara: TÜBA Yayınları, 2007.

[8] C. N. Geçkinli, "Rasgelelik (Rastlantısallık) kavramına genel bir bakış", *UEKAE Dergisi*, sa. 1, sf. 97–103, Eylül-Aralık 2009.

[9] R. N. Bracewell, *The Fourier Transform and Its Applications*, 3rd ed. Singapore: McGraw-Hill, 2000.

Düzensiz Şifreleme Algoritmasının Gerçek Zamanlı Kriptoanalizi[1]

Esen AKKEMİK PEDERSEN, Orhun KARA

Özet - *"Düzensiz Şifreleme" bir "dizi şifreleme" algoritmasıdır. Algoritmanın tasarımcıları, bu algoritmanın her anlamda "Tek Kullanımlık Koçan" (*One-Time-Pad*) sisteminden daha iyi olduğunu iddia edip, Tek Kullanımlık Koçan sisteminin yerine kullanılmasını önermişlerdir. Bu çalışmada düzensiz şifreleme algoritmasının kriptoanalizini yapıp, algoritmanın anahtar yayılımının zayıf olduğunu tespit ettik. Bu zayıflık kullanılarak biri Sadece Şifreli Metin, diğeri de Bilinen Açık Metin saldırısı olmak üzere "böl ve fethet" tarzında iki tane saldırı yöntemi önerdik. Her iki saldırının da gerek veri gerek işlem karmaşıklığı açısından çok düşük maliyete sahip olduğunu, hatta kâğıt üzerinde bile yapılabileceğini gösterdik. Geliştirilen saldırılara göre anahtarın 4-5 tane bilinen açık metin veya 10-12 tane sadece şifreli metinle elde edilebileceğini tespit ettik. Kripto literatüründe eski kripto sistemleri dışında bu derece düşük veri karmaşıklığına sahip bir saldırı görmek neredeyse olanaksızdır. Bu nedenle, bilim adamları tarafından tasarlanmış ve bilimsel dergide yayımlanmış modern bir şifreleme sisteminin bu derece zayıf olması beklenmeyen bir durumdur.*

Anahtar Sözcükler - *Dizi şifreleme, düzensiz şifreleme, kriptoanaliz, bilinen açık metin saldırısı, sadece şifreli metin saldırısı, böl ve fethet saldırısı, tek kullanımlık koçan.*

1 GİRİŞ

Tek Kullanımlık Koçan (*One-Time-Pad*) 1917 yılında Vernam tarafından tasarlanmış bir şifreleme sistemidir [2]. Bu sistemde, açık metin bitleri ile açık metinle aynı uzunlukta, tamamen rasgele bir anahtar dizisinin karşı düşen bitlerine "ayrıcalıklı veya" (*exclusive or, exor*) işlemi uygulanarak şifreli metin elde edilir. Açık metin P, anahtar dizisi K, açık metin bit sayısı N ise, şifreli metin olan C'nin bitleri şu şekilde belirlenir:

$$C_i = P_i \oplus K_i, \qquad i = 1, \ldots, N \tag{1}$$

Bu sistem mükemmel gizliliği sağlar [2], yani Sadece Şifreli Metin saldırısı uygulamak sonsuz hesap gücü sahibi olunsa bile olanaksızdır. Yalnız, mükemmel gizliliği sağlamak için anahtar dizisinin sadece bir kere kullanılması şarttır.

[1] Bu yazı ABG 2008 Bildiriler Kitabı'nda yayımlanan "Düzensiz Şifreleme Algoritmasının Gerçek Zamanlı Kripto Analizi" adlı makaleden [1] yararlanılarak hazırlanmıştır.

Düzensiz Şifreleme Algoritması (DŞA) Taş, Alataş ve Akın tarafından *ELECO*'2002 sempozyumunda sunulmuş [3], 2004 yılında da İstanbul Üniversitesi Elektrik-Elektronik Mühendisliği dergisinde yayımlanmış bir "dizi şifreleme" (*stream cipher*) tekniğidir [4]. Tasarımcıları, algoritmanın anahtar dizisini tekrar kullanabilmesinden dolayı tek kullanımlık koçana karşı üstünlük sağladığını iddia etmişlerdir [3]–[4].

Bu makalede DŞA çözümlenmiş ve algoritmaya uygulanan iki saldırı örneği anlatılmıştır. Bu saldırılar, algoritmaya geliştirilmiş ilk saldırılardır. Ayrıca, saldırılar karmaşıklıkları açısından değerlendirildiklerinde son derece uygulanabilir türdendir.

Algoritmada "anahtar yayılımı" (*key diffusion*) açısından ciddi sorunlar olduğu gözlenmiştir. Anahtar yayılımındaki zayıflık algoritmaya "böl ve fethet" türünden saldırı geliştirilmesinde kullanılmıştır. Algoritmaya hem Sadece Şifreli Metin saldırısı hem de Bilinen Açık Metin saldırısı düzenlenmiştir. Her iki saldırının da zaman karmaşıklığı yok denecek kadar azdır. Hatta bir bilgisayara bile gerek duymadan saldırıları kâğıt üzerinde gerçeklemek mümkündür. Ayrıca, saldırıların veri karmaşıklıkları da son derece düşüktür. Sadece Şifreli Metin saldırısı uygulamak için yaklaşık 10-12 şifreli metin yeterli olmaktadır. Bilinen Açık Metin saldırısında ise, 4-5 açık metin ile anahtar ele geçirilebilmektedir. Bu sonuçlar DŞA'nın ne kadar güvensiz bir algoritma olduğunu göstermektedir.

Bu makalede §2'de DŞA kısaca anlatılmıştır. Şifreleme sistemlerinde kullanılan bazı saldırı çeşitleri ve algoritmaya geliştirilen saldırılar §3'te verilmiştir. Ayrıca, §EK'te her iki saldırı için birer örnek sunulmuştur.

2 DÜZENSİZ ŞİFRELEME ALGORİTMASI

Düzensiz Şifreleme Algoritması (DŞA) bir dizi şifreleme tekniğidir. Her seferinde bitler düzeyinde şifreleme yapılır. Öncelikle açık metin karakterlerinin kaç bitle (n) simgeleneceği belirlenir. Bu değer belirlendikten sonra $[1,n]$ aralığından rasgele bir k sayısı seçilir. Bu k değerine göre açık metin bitleri k gruba ayrılır. Bu ayırma işleminde her grupta olabildiğince eşit eleman olmasına dikkat edilir. Eşit elemanın olmadığı durumlarda da fazla eleman taşıyan

gruplar, anlamlı bitlerin olduğu tarafta olacak biçimde gruplandırma yapılır. Daha sonra "Başlangıç Vektörü" (BV) adı verilen, rasgele k bit üretilir. Bu bitlerin değeri 1 ise, açık metnin gruplanmış halinde karşılık gelen grup bitleri değiştirilir, aksi takdirde aynen alınır. Bu işlem sonunda elde edilen n bitin arkasına k bitlik rasgele değer eklenerek n bitlik blok için şifreli metinde karşılık gelen $n+k$ bitlik blok elde edilir. Aynı işlemler bir sonraki karakter bloğu için tekrarlanır. Burada anahtar olan gizli değer rasgele seçilen bitlerin (BV'nin) uzunluğudur. Şifreleme yöntemi üzerine aşağıdaki gibi bir örnek verebiliriz:

Açık metin ($P = P_1, P_2$) : 01000101 01000001
Anahtar (k_1, k_2) : {4,3}
BV (BV_1, BV_2) : 1101 011
Gruplama: 01 00 01 01 010 000 01
1 1 0 1 0 1 1
Şifreleme: 10 11 01 10 010 111 10
Şifreli metin ($C = C_1, C_2$) : 10110110110101011110011

Bu çalışmada rasgele üretilen ve şifreli metinde açık şekilde yollanan rastlantısal değerler "başlangıç vektörü" (BV) olarak adlandırılmıştır. Şifreleme işlemlerinde karakterlerin *ASCII* gösteriminin kullanıldığı, yani her açık metin karakterinin en fazla 8 bitle simgelendiği varsayılmıştır.

3 ŞİFRELEME SİSTEMİNİN KRİPTOANALİZİ

Bu makalede DŞA'ya bir Sadece Şifreli Metin saldırısı ve bir de Bilinen Açık Metin saldırısı yapılmıştır. Bu saldırı türlerinin kısa açıklaması aşağıdaki gibidir:

1°) Sadece Şifreli Metin Saldırısı: Saldıran kişi, elindeki şifreli metinleri kullanarak anahtarı veya açık metni bulmaya çalışır. Matsui'nin *DES*'e (*Data Encryption Standard*) yaptığı doğrusal saldırılardan biri de bu türdendir. Saldırının veri karmaşıklığı yaklaşık 2^{54} şifreli metin bloğudur [4]. (Bir blok 64 bit uzunluğundadır.)

2°) Bilinen Açık Metin Saldırısı: Saldıranın elinde bir grup açık metin ve karşılık gelen şifreli metinler vardır. Bu veriler kullanılarak anahtar ele geçirilir. 1994 yılında Matsui tarafından bulunan doğrusal kriptoanaliz bu tür bir saldırıdır [4]. Bu saldırı ile *DES* 2^{47} bilinen açık metin bloğu kullanılarak kırılmıştır.

Her bir karakteri şifrelemek için $2^3 = 8$ anahtar kullanılmaktadır. Dolayısıyla, N karakter uzunluğunda açık metni şifrelemek için $3N$ bit uzunluğunda anahtar bilgisi kullanılır. Anahtar değerinin tek tek denenmesine dayanan kaba kuvvet saldırısının (*exhaustive search*) karmaşıklığı bu algoritma için 2^{3N} olur. Örneğin, 100 karakterlik açık metne karşılık gelen şifreli metinde kaba kuvvet saldırısının karmaşıklığı 2^{300}'dür. 4 GHz hızında bir bilgisayar saniyede 2^{32} anahtar tararsa, 2^{300} anahtarı 2^{268} saniyede dener. Bu işlem bir milyar bilgisayarda yaklaşık $1{,}5 \times 10^{64}$ yıl sürer. Ancak, aşağıda verilen her iki saldırı yöntemi de kaba kuvvet saldırısıyla kıyaslanamayacak kadar düşük karmaşıklığa sahip oldukları için gerçek zamanda uygulanabilir.

3.1 Sadece Şifreli Metin Çözümlemesi

Şifreleme işleminde İngilizce alfabenin kullanıldığı varsayılsın. Bu durumda bütün İngilizce karakterlerin, rakamların ve noktalama işaretlerinin bitsel gösterimi en fazla 7 bit ile yapılır. Eğer şifreleme işleminde her karakter 8 bit ile gösterilirse her karakterin en anlamlı biti 0 olur. Bu ayırt edici özellik yardımıyla aşağıdaki önerme geçerlidir:

Önerme 1: Şifreli metinde bir karakter (8 bit) açık metindeki bir karakterin şifreli hali olduğu zaman, şifreli metindeki karakterin en anlamlı biti ile BV'nin en anlamlı bitinin ayrıcalıklı veyası açık metnin en anlamlı bitine eşittir.

Kanıt: Açık metnin en anlamlı biti 0 olsun. BV'nin uzunluğu, [1,8] aralığında herhangi bir değer olsun. BV'nin en anlamlı biti 1 ise, açık metnin en anlamlı biti değiştirileceğinden, şifreli metinde karşılık gelen karakterde en anlamlı bit 1 olacaktır. BV'nin en anlamlı biti 0 olursa, açık metnin en anlamlı biti değiştirilmeyeceği için, şifreli metinde en anlamlı bit 0 olacaktır. Açık metnin en anlamlı bitinin 1 olması durumunda da önermenin doğruluğu benzer biçimde kanıtlanabilir. □

Önerme 1, yalnızca İngilizce alfabenin kullanıldığı açık metinlerde, şifreli metin karakterinin en anlamlı bitinin BV'nin en anlamlı bitine eşit olması gerektiğini söyler.

Aşağıda anlatılan "böl ve fethet" tekniğindeki saldırı, yani her seferinde şifreli metnin bir karakteri ile işlemler yapıp bir sonraki karakterine geçen saldırı, bu ayırt edici özellik ve Önerme 1 kullanılarak geliştirilmiştir.

Elde S tane şifreli metin olsun. Amaç, sadece şifreli metinler kullanarak "böl ve fethet" tekniği ile anahtar dizisini elde etmektir. Saldırının i'inci adımı şu şekildedir:

$(i-1)$'inci adımdaki anahtar $k_{i-1} = m$ olsun. Bundan önce de şifreli metinlerde t bit ilerlenmiş olsun. $C_{t+1} \ldots C_{t+8}$ bitleri açık metin karakterinin şifrelenmiş hali olarak varsayılıp C_{t+9} bitinin C_{t+1} bitine eşit olup olmadığına bakılır; yani Önerme 1'in geçerliliği kontrol edilir. Bu değerler eşitse Önerme 1 sağlanıyor demektir ve önceki anahtar değerleri doğru varsayılıp $k_i = 1$ kabul edilir ve $C_{t+10} \ldots C_{t+17}$ bitleri bir sonraki açık metin karakterinin şifrelenmiş hali olarak alınır. Eğer C_{t+9} biti C_{t+1} bitine eşit değilse $k_{i-1} = m+1$ olarak kabul edilir. Bu durumda $C_{t+2} \ldots C_{t+9}$ bitleri açık metnin şifrelenmiş hali olarak varsayılıp, C_{t+10} bitinin C_{t+2} bitine eşit olup olmadığına

bakılır. Bu değerler eşitse $k_i = 1$ kabul edilir ve $C_{t+11} \dots C_{t+18}$ bitleri bir sonraki açık metnin şifrelenmiş hali olarak kabul edilir. Saldırı bu şekilde sürdürülür. C ile simgelenen şifreli metin, eldeki bütün şifreli metinlerin her birini ifade eder. Anahtar değeri belirleme işlemi yapılırken şifreli metin bitlerinin karşılaştırılmasında eşit olmama durumunun en az bir şifreli metinde, eşit olma durumunun da bütün şifreli metinlerde sağlanması gereklidir.

Bu saldırı algoritma olarak şu şekilde verilir:

d dizisi açık metin karakterinin olası şifreli halini ve BV'nin en anlamlı bit değerini taşıyan 9 elemanlı diziyi, m değeri de [1,8] aralığında herhangi bir değeri göstersin. m değeri 8'i aştığı zaman algoritma sonlandırılmalıdır. t'nin ilk değeri 0 alınarak saldırıya başlanır.

$k_{i-1} = m$; $\quad j = 0$;
$d = \{C_{t+1}, C_{t+2}, \dots, C_{t+8}, C_{t+9}\}$;
eğer $(d[1] \neq d[9])$ ise {
  $(d[1] \neq d[9])$ iken {
    $k_{i-1} = k_{i-1} + 1$; $\quad j = j + 1$;
    $d = \{C_{t+1+j}, \dots, C_{t+8+j}, C_{t+9+j}\}$; }
}
eğer $(d[1] = d[9])$ ise {
  $k_i = 1$;
  $d = \{C_{t+10+j}, \dots, C_{t+17+j}, C_{t+18+j}\}$;
}

Bu saldırının başarısı, şifre çözme boyunca anahtar için doğru tahminin yapılmasına bağlıdır. Saldırıda bit karşılaştırma işleminde her şifreli metin için herhangi bir adımda Önerme 1 sağlanıyorsa 0, sağlanmıyorsa 1 olacak biçimde bir vektör oluşturulsun. Bir karakter şifre çözme işleminde 8 farklı anahtar değeri için 8 vektör elde edilir. Doğru anahtar için bu vektör 0 vektörü olacaktır. Ancak, yanlış anahtar değeri için de sıfır olabilir. Bu durumu sağlayan anahtar değerleri saldırıda yanlış alarma, yani anahtar değeri yanlış iken doğru kabul etmeye neden olur. Bu durumda, elde olan S tane şifreli metin için herhangi bir adımdaki yanlış alarm olasılığı

$$P_f = 1 - \left(1 - 2^{-S}\right)^7 \qquad (2)$$

olarak hesaplanır.

Bir karakter için birden fazla 0 vektör olması, birden fazla anahtarın şifre çözme işleminde kullanılabileceğinin göstergesidir. Ancak, bu durum sonraki karakterlerin şifre çözümünde uyumsuzluk yaratıp hatayı tespit etme olanağı oluşturabileceği gibi, yapılan bir hata başka hatalarla birleşip doğru karakter-BV çiftine tekrar ulaşabilir. Böyle bir durumda, bir adımdan sonra bir grup anahtar yanlış tahmin edilmiş ancak sonraki bir adımda tekrar doğru anahtar değerlerine ulaşılmış demektir.

(2) bağıntısı ve Tablo 1'deki değerlerle elde edilen şifreli metin sayısı arttıkça saldırıyla tahmin edilen anahtar dizisinin doğru olma olasılığının arttığı sonucuna varılır. Tablo 1'den de görüldüğü gibi yaklaşık 20 şifreli metin, anahtarın neredeyse % 100 olasılıkla ele geçirilmesi için yeterli olmaktadır.

Tablo 1. Sadece Şifreli Metin Saldırısında Şifreli Metin Sayısına (S) Karşılık Saldırının Yanlış Alarm Olasılığı (P_f)

S	P_f
5	0,2
6	0,1
7	0,05
8	0,027
9	0,014
10	0,0068
20	$6{,}6 \times 10^{-6}$
30	$6{,}5 \times 10^{-9}$

3.2 Bilinen Açık Metin Çözümlemesi

Bu bölümde DŞA'ya bir Bilinen Açık Metin saldırısı uygulaması anlatılmaktadır. Bu saldırıda çok daha az veri ile anahtarı bulmak mümkün olabilmektedir.

Saldırıda açık metin bitlerinin değiştirilip değiştirilmeyeceğine karar veren BV bitleri kullanılmaktadır. Saldırının sömürdüğü ayırt edici özellik Önerme 2'de verilmektedir. Tablo 2'de herhangi bir açık metin karakterinin i'inci biti şifrelenirken, anahtar değerine bağlı olarak BV'nin kaçıncı bitinin kullanıldığı gösterilmektedir. Örneğin, anahtar değeri 1 iken her bir i değeri için $k_i = 1$ olmaktadır.

Tablo 2. Anahtar Değerine Göre Açık Metnin Şifrelenmesinde BV'nin Kullanılacak Bitlerinin (k_i) Gösterimi

K	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8
1	1	1	1	1	1	1	1	1
2	1	1	1	1	2	2	2	2
3	1	1	1	2	2	2	3	3
4	1	1	2	2	3	3	4	4
5	1	1	2	2	3	3	4	5
6	1	1	2	2	3	4	5	6
7	1	1	2	3	4	5	6	7
8	1	2	3	4	5	6	7	8

Önerme 2: Herhangi bir açık metin karakteri, karşılık gelen şifreli metin karakteri ve BV'nin bitleri arasında

$$P_i \oplus C_i \oplus \mathrm{BV}_{k_i} = 0 \quad , \quad i = 1, \dots, 8 \qquad (3)$$

eşitliği vardır.

Kanıt: BV_{k_i} değeri açık metin karakterinin i'inci bitinin değiştirilip değiştirilmeyeceğini belirler. $\mathrm{BV}_{k_i} = 0$ iken, açık metin bitleri (değiştirilmeyecekleri için) karşılık gelen şifreli metin bitlerine eşit olacaktır. $\mathrm{BV}_{k_i} = 1$ iken ise açık metin karakterindeki i'inci bit 1 ile ayrıcalıklı veyası alınacaktır. BV değeri de 1 olduğundan, (3) eşitliği bu durumda da sağlanır. □

Dikkat edilecek olursa, Önerme 2 Önerme 1'in genelleştirilmiş halidir. Buna karşın, Önerme 1, Sadece Şifreli Metin çözümlemesinde kullanıldığı için ayrıca vurgulanmıştır.

Bilinen Açık Metin saldırısında da, tıpkı Sadece Şifreli Metin saldırısında olduğu gibi her bir karakter için elde bulunan verilerden aday anahtar değerleri belirlenir. Bu durumda ayırt edici özellik olarak Önerme 1 yerine Önerme 2 kullanılır. Önerme 2'de verilen eşitlik şartını bütün veriler için sağlayan anahtar değerleri aday olarak belirlenir. Diğer taraftan, sadece birkaç tane açık-şifreli metin çifti bile aday olarak sadece gerçek anahtarın kalmasına yeterli olmaktadır.

Algoritma kodu aşağıda verilmiştir. P ile açık metin, d ile olası şifreli metin, BV ile şifrelemede kullanılacak olası BV, m ile açık metin karakter sayısı simgelenmektedir. k_{top}, bulunulan adımdan önceki bütün anahtar değerlerinin toplamını gösterir. Bir dizinin sonuna yeni eleman ekleme "|" ile gösterilmiştir.

$k_{top} = 0$; $\quad t = 0, \dots, m-1$ {
  $d = \{C_{8t+k_{top}+1}, \dots, C_{8t+k_{top}+8}\}$
  $P = P_{8t+1}, \dots, P_{8t+8}$;
  $k_{t+1} = 1$;
  $\mathrm{ind} = 8t + 8 + k_{top} + 1$;
  $\mathrm{BV} = C_{\mathrm{ind}}$;
  $i = 1, \dots, 8$ {
    $d_i \oplus P_i \oplus \mathrm{BV}_{k_i} \neq 0$ ise {
      $k_{t+1} = k_{t+1} + 1$;
      $\mathrm{ind} = \mathrm{ind} + 1$;
      $\mathrm{BV} = \mathrm{BV} | C_{\mathrm{ind}}$;
      $d_i \oplus P_i \oplus \mathrm{BV}_{k_i}$'yi hesapla;
    }
  }
  $t = t + 1$;
  $k_{top} = k_{top} + k_t$;
}

Bu saldırının başarısı, şifre çözme boyunca anahtar için doğru tahminin yapılmasına bağlıdır. Elde S tane açık-şifreli metin çifti olsun. Bu durumda, her bir anahtar adayının (3) denklemi ile verilen denetim mekanizmasından geçme olasılığı 2^{-8S} olmaktadır. Dolayısıyla, belirli bir açık metin karakterini şifreleyen anahtar değeri dışında en az bir tane yanlış anahtar gelme olasılığı

$$P_f = 1 - \left(1 - 2^{-8S}\right)^7 \qquad (4)$$

ifadesi ile verilir.

Tablo 3. Bilinen Açık Metin Saldırısında Açık Metin-Şifreli Metin Çifti Sayısına (S) Karşılık Saldırının Yanlış Alarm Olasılığı (P_f)

S	P_f
5	$6{,}4 \times 10^{-12}$
6	$2{,}5 \times 10^{-14}$
7	$9{,}7 \times 10^{-17}$
8	$3{,}8 \times 10^{-19}$
9	$1{,}5 \times 10^{-21}$

Tablo 3'teki örneklerden de görüleceği gibi saldırının yanlış alarm olasılığı son derece düşüktür. Öyle ki, birkaç tane açık metin-şifreli metin çifti neredeyse 1 olasılıkla anahtarı tespit etmek için yeterli olmaktadır.

Bu saldırıda da, bir önceki saldırıdaki duruma benzer bir durum söz konusu olabilir, yani, yanlış anahtar değeri, ileride tespit edilebilecek bir hataya neden olabileceği gibi, sonradan kendini toparlayan bir duruma da yol açabilir.

4 SONUÇ

Bu çalışmada DŞA'ya biri Sadece Şifreli Metin, diğeri Bilinen Açık Metin olmak üzere iki saldırı anlatılmıştır. Bu saldırılar algoritmaya uygulanan ilk saldırılardır ve karmaşıklıkları son derece düşüktür. Sonuç olarak, DŞA'nın son derece zayıf bir algoritma olduğu anlaşılmaktadır.

EK 1 SALDIRI ÖRNEKLERİ

Bu bölümde Sadece Şifreli Metin ve Bilinen Açık Metin saldırılarına birer örnek verilecektir.

EK 1.1 Sadece Şifreli Metin Saldırısı

Elde aynı anahtar dizisi ile şifrelenmiş 3 tane şifreli metin olsun. Açık metnin ilk bitinin 0 olduğu da bilinsin (alfanümerik karakterler durumu). Bu durumda

Önerme 1'de açık metnin en anlamlı biti yerine 0 değeri konularak işlem yapılacaktır

C_1: 01001000011101110010000000010010

C_2: 11010110110110010101101000000110

C_3: 10110101100001111000110110100 1

BV_i ile i'inci BV değeri simgelensin.

Öncelikle, şifreli metinlerin ilk 8 biti ayrılır. Önerme 1'den dolayı her zaman 9. bit şifreli metnin en anlamlı bitine (1. bite) eşittir.

C_1: 01001000**0** 11101110 **0**100000010010

C_2: 11010110**1** 10110010 **1**011010000110

C_3: 10110101**1** 00001111 **0**001101101001

Saldırıya $k_1 = 1$ kabul edilerek başlanır. 9. bitten itibaren ikinci 8 bit, şifreli metin bloğu olarak alınır. Eğer $k_1 = 1$ ise 18. bit BV'nin ilk biti olur. Ancak, C_1'in ilk biti ile BV_2 birbirine eşit değildir; yani Önerme 1 sağlanmaz. Bu durum bir çelişkidir ve $k_1 = 1$ varsayımından kaynaklanmıştır. Öyleyse, $k_1 = 2$ alınır ve işleme devam edilir. Böylelikle, aşağıdaki durum geçerlidir.

C_1: 01001000**01** 11011100 **1**00000010010

C_2: 11010110**11** 01100101 **0**11010000110

C_3: 10110101**10** 00011110 **0**01101101001

$k_1 = 2$ ve $k_2 = 1$ olursa 19. bit BV_2'nin ilk biti olur. Bu durumda, bütün şifreli metinlerin 11. bitleri ve BV_2 değeri Önerme 1'i sağlar. Böylelikle, bitler aşağıdaki gibi olur:

C_1: 01001000**01** 11011100**1** 00000010 **010**

C_2: 11010110**11** 01100101**0** 11010000 **110**

C_3: 10110101**10** 00011110**0** 01101101 **001**

20. bitten itibaren 8 bit alındığında 28. bit BV_3'ün ilk bitidir. Bütün şifreli metinlerin 20. bitleri ve BV_3 değerleri Önerme 1'i sağlar. Öyleyse $k_1 = 2$ ve $k_2 = 1$ değerleri doğru tahmin edilmiş varsayılır ve şifreli metinde en son değerlendirmeye katılmayan bitler en son BV değeri olarak alındıktan sonra anahtar dizisi {2,1,3} olarak bulunur. Burada koyu yazılmış bitler BV değerlerini belirtir.

C_1: 01001000**01** 11011100**1** 00000010**010**

C_2: 11010110**11** 01100101**0** 11010000**110**

C_3: 10110101**10** 00011110**0** 01101101**001**

EK 1.2 Bilinen Açık Metin Saldırısı

Açık metin P ve şifreli metin C ile gösterilsin.

P : 01000111 00100011 00011101 01100111

C : 01001000011101110010000001001101011 01001101

Saldırıya şifreli metinde ilk 8 bit ayrılarak başlanır.

C : 01001000 **0**
111011100100000010011010110100 1101

$k_1 = 1$ varsayılır. Bu durumda $BV_1 = 0$ olur. Şifreli ve açık metnin 5. biti ile BV_1 Önerme 2'yi sağlamadıkları için $k_1 = 2$ alınır. Yeni $BV_1 = 01$ olur. Bu yeni BV, şifreli metnin ilk 8 biti ve açık metnin ilk karakteri Önerme 2'yi sağladığı için $k_1 = 2$ varsayılır.

P : 01000111 00100011 00011101 01100111

C : 0100100**01** 11011100 **1**
00000010011010110100 1101

Şifreli metinden 11. bitten itibaren 8 bit alınır. $k_2 = 1$ alınır ve BV_2'nin değeri 19. bit (1) alınarak saldırıya başlanır. Açık metnin ikinci karakteri, şifreli metnin 11.–18. bitleri ve $BV_2 = 1$ Önerme 2'yi sağladığı için $k_1 = 2$ varsayımı hâlâ geçerlidir ve $k_2 = 1$ alınarak üçüncü basamağa geçilir.

C : 0100100**01** 110111001
00000010 **0** 110101101001101

Şifreli metinde 20. bitten itibaren 8 bit ayrılır. $k_3 = 1$ ise $BV_3 = 0$ olur. Açık metnin 3. karakterinde 4. bit, şifreli metnin 23. biti ve BV_3 Önerme 2'yi sağlamadığından $k_3 = 2$ yapılır. Yeni $BV_3 = 01$ alınır.

P : 01000111 00100011 00011101 01100111

C : 0100100**01** 110111001
00000010 **01** 10101101001101

Bu yeni BV değerine göre şifreli metnin 23. biti, açık metnin 3. karakterinin 4. biti ve BV_3'ün açık metnin bu bloğunun şifrelemesinde kullanılacak 1. biti Önerme 2'yi sağlamadığı için $k_3 = 3$ yapılır. Bu durumda $BV_3 = 011$ olur. Bu yeni BV_3, açık metnin üçüncü karakteri ve şifreli metnin 20.–27. bitleri Önerme 2'yi sağladığından $k_3 = 3$ kabul edilir.

P : 01000111 00100011 00011101 01100111

C : 0100100**01** 110111001
00000010**011** 0101101**01101**

Şifreli metinde 31. bitten itibaren 8 bit ayrılır. Geriye kalan 5 bit BV_4 değeridir. Açık metnin 4. karakteri, şifreli metnin 31.–38. bitleri ve BV_4 Önerme 2'yi sağladığından anahtar dizisi {2,1,3,5} olarak bulunur.

KAYNAKÇA

[1] E. Akkemik ve O. Kara, "Düzensiz şifreleme algoritmasının gerçek zamanlı kripto analizi", *EMO 2. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu (ABG 2008) Bildiriler Kitabı*, Girne, May. 2008, sf. 188–192.

[2] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, 1st ed. Boca Raton, Florida: CRC Press, 1997, p. 42.

[3] O. Taş, B. Alataş ve E. Akın, "Akış şifreleme tekniğine yeni bir yaklaşım: düzensiz şifreleme", *2. Elektrik-Elektronik-Bilgisayar Mühendisliği Sempozyumu ve Fuarı (ELECO'2002) Bildiriler Kitabı*, Bursa, Ara. 2002, sf. 264–267.

[4] O. Taş, B. Alataş ve E. Akın, "A new approach to stream cipher: unsystematic cipher," *IU J. Electrical & Electronics Eng.*, vol. 4, no. 1, pp. 1057–1062, Jan. 2004.

[5] M. Matsui, "Linear cryptanalysis method for DES cipher," *Proc. Workshop on the Theory and Application of Cryptographic Techniques (Advances in Cryptology - EUROCRYPT '93)*, Lofthus, Norway, May 1993, (*Lecture Notes in Computer Science*, 1993), vol. 765, pp. 386–397.

Radar Antenleri – IV: Faz Dizili Anten Kuramına Genel Bakış

Bahattin TÜRETKEN, Koray SÜRMELİ

Özet - *Bu çalışmada, haberleşme, radar ve radyoastronomide sık kullanılan faz dizili antenlerin temel kuramı, mimari yapıları ve anten tasarımları ile ilgili bilgiler verilecek ve örnek bir uygulama üzerinden tasarım teknikleri incelenecektir.*

Anahtar Sözcükler - *Aktif diziler, dizi antenler, elektronik taramalı diziler, faz dizili antenler, pasif diziler, radar.*

1 GİRİŞ

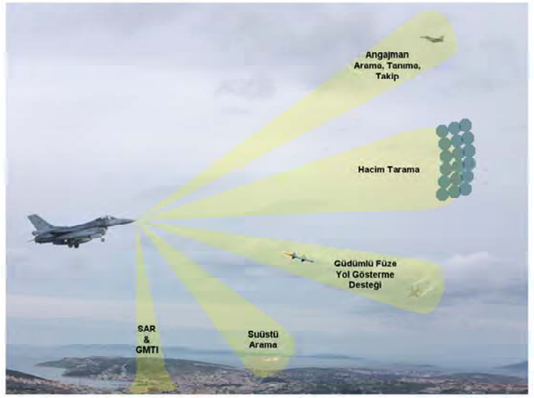
Günümüzde mikrodalga ve yazılım tekniklerindeki gelişmelerle birlikte, radar uygulamalarında kullanılan antenlerden çok daha farklı görevler beklemek olağan hale gelmiştir; zira, klasik radarlar tehditlere karşı etkisiz kalmaya başlamıştır. Bundan dolayı çok fonksiyonlu ve çoklu görev ifa eden akıllı sistemleri kullanmak kaçınılmaz olmuştur. Böylelikle, modern radarlar birçok işlevi yerine getirmek için faz dizili yapılar kullanmaya başlamıştır (Şekil 1).

Bilindiği gibi anten dizileri, istenilen ışıma özelliklerini verecek şekilde uygun genlik ve faz ilişkileri bulunan özdeş antenlerin değişik biçimlerde düzenlenmiş gruplarına denir [1]. Dizi antenler anten hüzmesini daraltmak, hüzmeyi şekillendirmek, yönlendirmek ve kazancı artırmak için kullanılırlar. Dizi antenlerin önemli ışıma özellikleri; ana demet doğrultusu, yan kulakçık düzeyleri ve yarım güç hüzme genişliğidir.

Faz dizili antenler ise, istenilen bir hüzme yapısını oluşturabilmek amacıyla, diziyi oluşturan elemanların her birinin besleme genlik ve faz değerlerinin ayrı ayrı kontrol edilebildiği bir dizi yapısıdır. Hüzmenin konumu diziyi oluşturan elemanların besleme faz değerlerinin ayarlanması ile elektronik olarak kontrol edilir. Böylece ana hüzme anteni fiziksel olarak hareket ettirmeden yönlendirilebilir.

Faz dizili antenlerin mikrosaniye mertebesinde hızlı ve doğru (*accurate*) hüzme tarama (*beam steering*) yapabilme yetenekleri, sistemlerin birçok fonksiyonu birden gerçekleştirebilmesine izin vermektedir. Elektronik olarak hüzme tarama yapabilen radarlar çok sayıdaki hedefleri izleme ve bu hedeflerden bazılarını radyo frekans (RF) enerjisi ile aydınlatabilme yeteneklerine sahiptir. Böyle bir radar yüksek kazançlı hüzmelerini uzak mesafedeki alıcı ve vericilere yönlendirerek, bir haberleşme sistemi olarak da çalışabilir. Faz dizili antenlerde muazzam bir esneklik söz konusudur. Özel durumları en iyi şekilde karşılayabilmek amacıyla tarama ve izleme hızları ayarlanabilir. Örneğin hedeflerin manevraları gibi belirsizlik durumlarında veri hızı artırılmaktadır. Faz değiştirme yoluyla anten hüzme genişliği elektronik olarak değiştirilebilir. Böylece, belirli alanları çok daha hızlı bir biçimde, ancak daha düşük kazançla kapsamak mümkündür. Açıklık boyunca yerleştirilen çok katlı güç üreteçleri sayesinde çok yüksek güç değerleri elde edilebilmektedir. Güç dağılımı, tarama alanında bilgisayar yardımıyla kontrol edilebilir. Elektronik olarak kontrol edilen faz dizili antenler eldeki belirli bir görevi en iyi biçimde yerine getirebilmek için gerek duyulan çeşitli fonksiyonların tamamını gerçekleştirebilme yeteneğine sahiptir. Örneğin ters sentetik açıklık gibi hedef sınıflama fonksiyonlarını desteklerler. Fonksiyonlar sayısal hüzme tarama bilgisayarları ile hızlı bir biçimde programlanabilirler. Faz dizili antenler kargaşayı (*clutter*) daha etkili bir biçimde bastırabilirler [2].

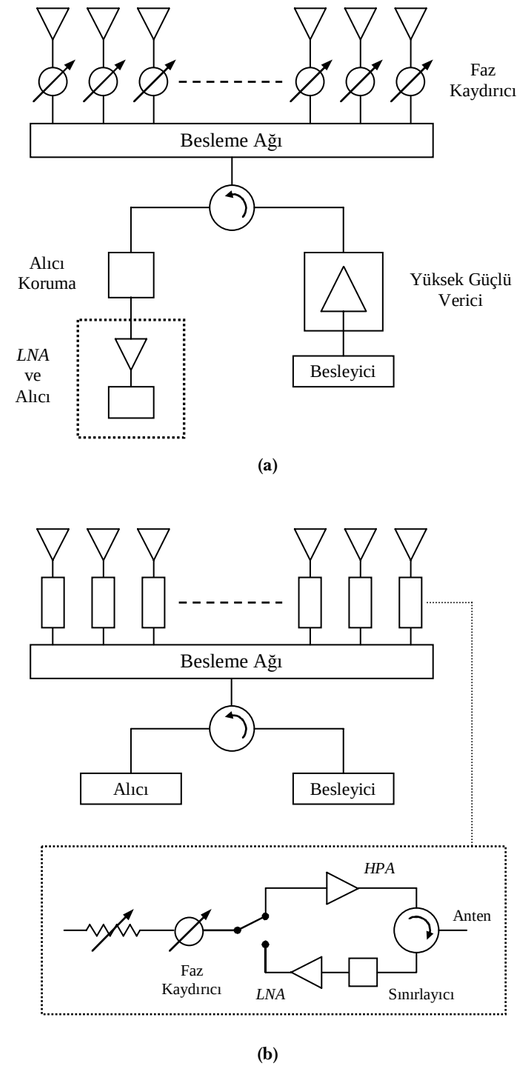
Yukarıdaki avantajlarından dolayı faz dizili radarlar 1950'li yıllardan beri birçok askeri ve sivil radar uygulamalarında yoğun olarak kullanılmaktadır [2]–[6].



Şekil 1. *Faz dizili anten fonksiyonları*

2 FAZ DİZİLİ ANTENLERİN ELEKTRİKSEL MİMARİSİ

Faz dizili antenler, Şekil 2'de gösterildiği gibi iki temel mimariyle ifade edilirler: pasif faz dizileri ve aktif faz dizileri. Her bir yapı kendine has özelliklere, avantajlara ve dezavantajlara sahiptir [7].



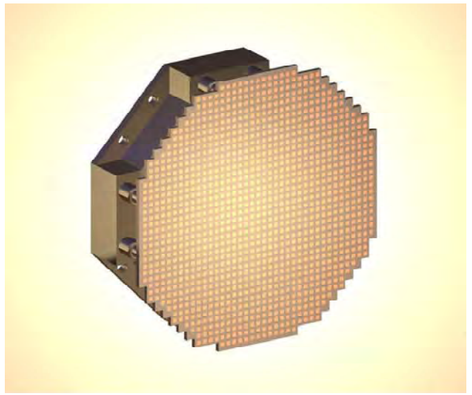
Şekil 2. *Temel faz dizisi mimarileri: (a) Doğrusal pasif dizi, (b) aktif dizi.*

Pasif diziler merkezi bir verici ve bir alıcı birimi kullanırlar. Hüzme tarama yapabilmek için gerek duyulan faz kaymasını sağlamak amacıyla eleman düzeyinde faz kaydırıcılar kullanılır, ancak genellikle bunlar genlik kontrolü sağlamazlar. Pasif dizilerde sistem hassasiyetini ve verimliliğini artırmak için besleme ağı ve faz kaydırıcılar içerisindeki kayıpları en düşük düzeye indirmek gerekmektedir.

Pasif diziler elektronik olarak tarama yapan dizi antenlerin en düşük maliyetli olanıdır; çünkü bileşenlerinin sayısı ve maliyetleri düşüktür. Eğer çok düşük yan kulakçık düzeyleri isteniyorsa, uygun genlik ağırlıklandırılmasının kullanıldığı ayrı bir alıcı besleme ağının kullanılması gerekmektedir.

Aktif dizilerde eleman başına bir verici/alıcı birimi kullanılarak genlik ve faz kontrolü sağlanmaktadır. Pasif dizilerde kullanılan merkezi verici birimi her bir verici/alıcı birimi içerisinde kullanılan ayrı güç kuvvetlendiricileriyle yer değiştirmiştir. Bu kuvvetlendiriciler verici durumda yüksek güç kuvvetlendiricisi, alıcı durumda ise düşük gürültülü kuvvetlendiricidir. Bu durum Şekil 2'deki verici/alıcı biriminin basitleştirilmiş şemasından da görülmektedir. Aktif dizilerde sistem hassasiyeti, sistem gürültü faktörünün ayarlanması ve RF gücünün açıklıkta üretilmesiyle artırılmaktadır. Aktif dizilerde kullanılan verici/alıcı birimleri hem alıcı hem de verici durumda tamamen esnek genlik ve faz kontrolü sağlar. Aktif dizilerde besleme ağının en düşük kayıp için optimize edilmesine gerek duyulmaz. Bu nedenle, aktif diziler tasarım esnekliğine ve sistemin hacim ve ağırlık değerlerinin en düşük düzeye indirilebilme yeteneklerine sahiptir. Aktif dizilerin bu avantajları sistemin karmaşıklığını ve maliyetini de doğal olarak artırmaktadır. 1980'lerden itibaren düşük maliyetli GaAs tek parça mikrodalga tümdevreleri, yüksek hızlı sayısal işleme bileşenlerinin geliştirilmesiyle birlikte, aktif dizilerin birçok radar ve haberleşme uygulamasında tercih edilen dizi yapısı haline gelmesini sağlamıştır. Ancak GaAs teknolojisi, maliyeti, yüksek yoğunlukta tümleştirme yapılamaması, güç tüketiminin yüksek olması nedenleriyle, yerini 1955'lerde başlayan, 2000 yıllarında hızla artan Silisyum-Germanyum (SiGe) teknolojisine bırakmıştır ve bu pazar bu yönde hızla ilerlemektedir [8], [9].

Melez bir faz dizisi yapısı aktif ve pasif dizilerin bazı özelliklerini birleştirir. Pasif faz dizili antenlerde olduğu gibi, merkezi bir verici birimi diziyi besler; fakat sistemin toplam gürültü faktörünü iyileştirebilmek amacıyla her bir faz kaydırıcının önüne bir düşük gürültülü kuvvetlendirici eklenmiştir. Düşük yan kulakçık düzeyleri elde edebilmek için ayrık bir alıcı besleme ağı kullanılmaktadır.

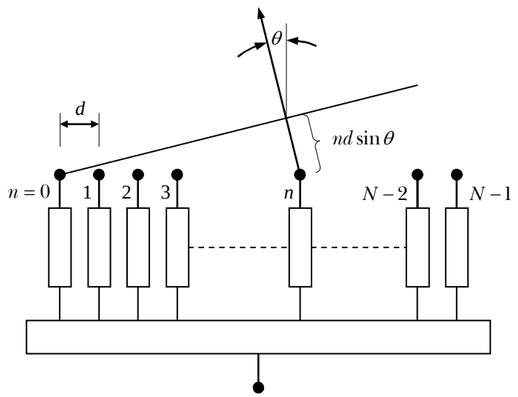


Şekil 3. *Aktif faz dizili atış kontrol radarı.*

3 FAZ DİZİLİ ANTENLERİN FİZİKSEL YAPILARI

Faz dizili antenlerde elemanların nasıl gruplanıp besleneceğine bağlı olarak, geometrik gereksinimleri sağlamak üzere belirli frekans aralıkları için tasarlanmış üç temel dizi yapısı bulunmaktadır. Bu yapılar tuğla, kiremit ve tepsi olarak adlandırılmaktadır. Bu adlandırma verici/alıcı birimlerinin, işaret ve güç dağılımına ve besleme devrelerinin fiziksel yerleşimine göre yapılmıştır.

Bir örneği Şekil 3'te görülen tuğla (*brick)* tipi dizilerde verici/alıcı birimleri tuğlaya benzeyen dikdörtgen bir yapıdadır. Verici/alıcı birimleri; enerji depolama kondansatörleri, işaret ve güç dağıtma devreleri ve doğrusal alt dizileri düzenleyebilmek için kullanılan RF katlarıyla birlikte soğutma biriminin her iki tarafına monte edilirler. Tuğla yapısı düşük maliyetli olarak üretilmektedir. Yapı içerisinde kullanılan elemanlar ise geniş bantlı tasarlanabilmektedir [10].



Şekil 4. *Temel doğrusal dizi yapısı.*

Tepsi (*tray)* tipi dizilerin yapısı temel olarak tuğla yapısına benzer. Ancak tepsi yapısında her bir alt dizi kendi güç kaynağını ve hüzme tarama kontrol birimini içermektedir.

Kiremit (*tile*) mimarisinde verici/alıcı birimleri dikdörtgen kiremit biçimindedir ve açıklığa paralel şekilde soğutma birimi üzerine monte edilirler [11]. Enerji depolama, işaret ve güç dağıtma devreleri ve RF katları verici/alıcı birimlerinin arkasına monte edilir. Bu yapı bir kekin katları şeklinde düşünülebilir. Kiremit mimarisi dizi ağırlığını önemli ölçüde azaltır. Ancak daha gelişmiş soğuk tabaka tasarımlarına ve yeni RF bağlantılarına gerek duyar.

4 DİZİ ANTEN KURAMI

Doğrusal veya düzlemsel dizi antenlerin ışıma diyagramları, genel dizi yapısının (doğrusal, dairesel, düzlemsel vb.), elemanlar arası uzaklığın, elemanların besleme genlik ve faz katsayılarının ve diziyi oluşturan elemanların ışıma diyagramlarının fonksiyonudur [12], [13].

Genellikle özdeş elemanlar eş aralıklı bir şekilde doğrusal olarak, dikdörtgen bir ızgara üzerinde olacak biçimde veya bir daire üzerinde olacak şekilde yerleştirilirler. İlk durumda doğrusal dizi, ikinci durumda düzlemsel dizi, üçüncü durumda ise dairesel dizi yapısı elde edilir.

Özdeş elemanlardan oluşan bir dizi için ışıma diyagramı diyagram çarpım ilkesi yoluyla bulunabilir. Bu ilkeye göre dizinin ışıma diyagramı, dizi elemanının ışıma diyagramı ile dizi faktörünün çarpımından elde edilir. Dizi elemanının ışıma diyagramı diziyi oluşturan elemanların herhangi birinin ışıma diyagramıdır. Dizi faktörü ise dizinin geometrisine ve elemanların besleme katsayısına (genlik ve fazına) bağlı olan bir fonksiyondur. Eğer bir dizi özdeş elemanlardan oluşuyorsa dizi faktörünün anten tipinden bağımsız olduğu düşünülür.

5 DOĞRUSAL DİZİLER

Daha önce de bahsedildiği gibi, doğrusal diziler özdeş elemanların bir eksen üzerine eşit aralıklarla yerleştirilmesi ile elde edilir. Böyle bir dizi yapısı Şekil 4'te gösterilmiştir.

Doğrusal dizilerde bütün elemanlar aynı akım dağılımına sahiptir. Sadece akımın genlik ve faz değerleri değiştirilebilir.

N elemandan oluşan ve elemanlar arasındaki uzaklığın d olduğu bir doğrusal dizi için dizi faktörü, her bir elemanın uzak alanda herhangi bir noktada oluşturduğu elektrik alan ifadelerinin toplanması ile elde edilir. Dizi faktörü,

$$A(\psi) = \sum_{n=0}^{N-1} a_n e^{jn\psi} \tag{1}$$

biçimindedir. Burada a_n n. elemanın besleme genlik katsayısını ifade etmektedir. Eğer antenler

- x eksenine yerleştirilmiş ise

$$\psi = kd\ \sin\theta\cos\phi \quad , \tag{2}$$

- y eksenine yerleştirilmiş ise

$$\psi = kd\sin\theta\sin\phi \quad \text{ve} \tag{3}$$

- z eksenine yerleştirilmiş ise

$$\psi = kd\ \cos\theta \tag{4}$$

olacaktır.

Doğrusal bir dizinin genelleştirilmiş dizi faktörü ise

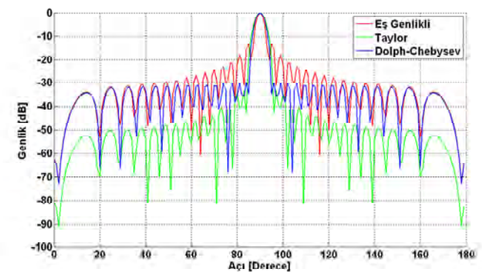
$$|A(\psi)| = \frac{1}{N}\left|\frac{\sin\left(\frac{N\psi}{2}\right)}{\sin\left(\frac{\psi}{2}\right)}\right| \tag{5}$$

olarak ifade edilir.

Doğrusal dizilerin ana hüzme doğrultusu, ilk yan kulakçık düzeyi gibi önemli bazı parametreleri yukarıdaki dizi faktörü ifadesi kullanılarak elde edilir.

Ana hüzmenin doğrultusu dizinin en fazla ışıma yaptığı açı değerini göstermektedir. Bu açı değeri dizi faktöründe ψ'yi sıfır yapan değerdir. Örneğin x eksenindeki bir dizi için yatay düzlemde ($\theta = 90^\circ$)

$$\psi = kd\ \cos\phi \tag{6}$$



Şekil 5. *-30 dB yan kulakçık düzeyi için elde edilen ışıma diyagramları.*

olacaktır ve ana hüzme $\phi = 90^\circ$'de oluşacaktır.

Işıma diyagramında, ana hüzmeye göre ilk yan kulakçık düzeyinin değeri önemli bir parametredir. Bu değer büyük N değerleri için

$$\frac{1}{N}\left|\frac{1}{\sin\left(\frac{3\pi}{2N}\right)}\right| \cong \frac{1}{N}\left|\frac{1}{\frac{3\pi}{2N}}\right| = \left|\frac{2}{3\pi}\right| = 0,212 \tag{7}$$

olarak hesaplanır.

İlk yan kulakçık ana hüzmeden 13,5 dB kadar aşağıdadır. Bu değer N büyük olduğu sürece, N'den hemen hemen bağımsızdır.

Yan kulakçık düzeyleri elemanların besleme genlik katsayısı dağılımının değiştirilmesiyle azaltılabilir. Dizinin merkezindeki eleman en yüksek genlikli akım ile beslenirken diğer elemanların genlik değerleri simetrik olarak değiştirilir. Sonuçta yan kulakçık düzeyleri azaltılır, ancak ana hüzmenin genişliği artar. Dolph-Chebyshev Taylor, Binom, Bayliss vb. çeşitli sentez teknikleri bu amaç için kullanılmaktadır [12]-[14]. Bu teknikler literatürde ayrıntılı bir şekilde incelenmiştir. Eş aralıklarla yerleştirilmiş 32 elemandan oluşan doğrusal bir dizi için sentez teknikleri uygulandıktan sonra elde edilen ışıma diyagramları Şekil 5'te verilmiştir.

5.1 Elektronik Hüzme Tarama

Hüzme tarama dizi antenlerin en önemli özelliklerinden biridir. Diziyi oluşturan antenleri uygun fazlarda besleyerek hüzme belirli bir açıya yönlendirilebilir. Doğrusal dizilerde elemanların faz değerleri doğrusal artırılarak ana hüzme yönlendirilir. Bu durumda dizi faktörü

$$A(\psi) = \sum_{n=0}^{N-1} a_n e^{jn(\psi-\psi_0)} \tag{8}$$

biçimini alır.

Burada ψ_0 eklenen faz faktörüdür ve ana hüzmenin pozisyonunu istenilen açıya yönlendirir. Eğer antenler

- x eksenine yerleştirilmiş ise

$$\psi_0 = kd\sin\theta_0\cos\phi_0 \quad , \tag{9}$$

- y eksenine yerleştirilmiş iseler;

$$\psi_0 = kd\sin\theta_0\sin\phi_0 \quad \text{ve} \tag{10}$$

- z eksenine yerleştirilmiş iseler;

$$\psi_0 = kd\ \cos\theta_0 \tag{11}$$

olacaktır.

5.2 Doğrusal Dizilerin Yönlendiriciliği ve Hüzme Genişliği

Anten yönlendiriciliği ana hüzme doğrultusunda birim açı başına ışıman güç yoğunluğunun ortalama ışıman güç yoğunluğuna oranı olarak ifade edilir. Eğer herhangi bir uyumsuzluk kaybı yoksa kazanç yönlendiriciliğe eşit olacaktır. Bu tanımla birlikte ana hüzmesi θ_0 açısında oluşan bir dizi için yönlendiricilik

$$D(\theta_0)=\frac{\left|E(\theta_0)\right|^2}{\frac{1}{4\pi}\int\limits_{tüm\,uzay}\left|E(\theta_0)\right|^2\cos\theta\,d\theta\,d\phi} \tag{12}$$

biçiminde olacaktır.

İzotropik (özellikleri doğrultudan bağımsız) elemanlardan oluşan ve elemanlar arası uzaklığın dalga boyunun yarısı kadar olduğu bir doğrusal dizide yönlendiricilik ifadesi ana hüzmenin doğrultusundan bağımsızdır.

$$D_0=\frac{\left|\sum a_n\right|^2}{\sum\left|a_n\right|^2} \tag{13}$$

Bu ifadenin en büyük değeri eş genlikli besleme durumunda oluşur ve bu değer eleman sayısına eşittir.

İzotropik olmayan elemanlardan oluşan bir dizi için yönlendiricilik ifadesini hesaplamanın basit bir formülü yoktur. Bu durumda yönlendiricilik sadece integral ifadesinin çözülmesi ile elde edilebilir. Ancak yönsüz anten elemanlarından oluşan bir dizi için yönlendiriciliğin kapalı formda integrali alınabilir. z eksenine yerleştirilmiş bu tipteki bir dizi antenin yönlendiricilik ifadesi

$$D=\frac{\left|\sum a_n\right|^2}{\sum\sum\left|a_n\right|\left|a_m\right|\exp\left[-jkd(n-m)\cos\theta_0\right]\sin c\left[kd(n-m)\right]} \tag{14}$$

biçimindedir.

Dizi antenlerin yarım güç hüzme genişliği, anten elemanlarının besleme genlik dağılımı ile değişmektedir. Örneğin yan kulakçık düzeylerini azaltmak için bir genlik dağılımı seçildiğinde bu dağılım hüzme genişliğini artıracaktır. Bir doğrusal dizinin ışıma diyagramının yarım güç hüzme genişliği radyan cinsinden

$$\theta_3=0{,}866\,B_b\lambda/L \tag{15}$$

$$L=Nd \tag{16}$$

biçiminde ifade edilir.

Burada L dizi açıklığıdır ve B_b hüzme genişletme faktörüdür. Bu faktör eş genlik besleme durumu için bire eşittir. Farklı besleme genlik dağılımları için ise 1'den büyük olacaktır.

Büyük dizilerde hüzme düşey düzlemde belirli bir açıya yönlendirildiğinde hüzme genişliği

$$\theta_3=\theta_3\left(\text{yönlendirmenin olmadığı durum}\right)/\cos\theta_0 \tag{17}$$

biçimindedir.

Bu ifade ϕ açısından bağımsız olan tarama düzlemlerindeki diziler için geçerlidir.

5.3 Izgara Kulakçıklar

Eğer elemanlar arası uzaklık dalga boyu ile karşılaştırıldığında yeteri kadar büyük ise bu durumda ışıma diyagramı içerisinde ızgara kulakçık (*grating lobes*) dediğimiz ikinci bir ana hüzme oluşur. Dizi faktöründe üstel kısım 2π'nin katı olduğunda ızgara kulakçıklar oluşacaktır. Örneğin x eksenine dizilmiş bir dizi için düşey düzlemde ızgara kulakçıklar

$$kd\sin\theta_t-kd\sin\theta_0=2p\pi$$
$$p=\pm(1,2,3,\ldots) \tag{18}$$

açılarında oluşur.

Bir dizi herhangi bir açıya yönlendiğinde ızgara kulakçıkların görünür bölge içerisinde yer almamasını sağlayacak bir kriter söz konusudur. Bu kriter

$$\frac{d}{\lambda}\le\frac{1}{1+\sin\theta_0} \tag{19}$$

biçimindedir.

Izgara kulakçıkların bastırmak amacıyla kullanılan çeşitli yaklaşımlar mevcuttur. Bu yaklaşımlar aşağıdaki gibi sıralanabilir:

- Antenlerin periyodik bir şekilde dizilmesi yerine periyodik olmayan bir diziliş kullanılması;
- Izgara kulakçıkları bastırmak için daha geniş eleman açıklığının ve eleman faktörünün kullanılması;
- Dizi ışıma diyagramının ızgara kulakçıklarında eleman ışıma diyagramını en küçük değerine ulaştırmak amacıyla çoklu durum tekniğinin kullanılması;
- Dizi anten içerisinde farklı açıklığa sahip elemanların kullanılması ve bunların yerleşimlerinin keyfi bir şekilde yapılması;
- Büyük dizilerin alt dizilere ayrılması [15].

5.4 Dizi Fark Işıma Diyagramları

Eğer eş aralıklarla yerleştirilmiş elemanlardan oluşan doğrusal bir dizi içerisindeki eleman sayısı çift ise, iki ana hüzmeden oluşan simetrik bir fark ışıma diyagramı elde etmek mümkündür. Fark ışıma diyagramları dizinin iki yarısının zıt fazla beslenmesi ile elde edilir. Elemanlara hüzmeyi belirli bir açıya yönlendirecek şekilde doğrusal artımlı faz farkları verildiği durumda, dizinin iki yarısı yine zıt fazla beslenirse bu durumda yönlendirilmiş bir fark ışıma diyagramı elde edilir. Eş aralıklarla yerleştirilmiş 16 elemandan oluşan ve eleman besleme genlikleri Bayliss dağılımına göre belirlenmiş doğrusal bir dizi anten için fark ışıma diyagramı Şekil 6'da gösterilmiştir.

Toplam ve fark ışıma diyagramları hedefleri belirlemek ve izlemek amacıyla kullanılırlar. Toplam ışıma diyagramı bir hedefi belirlemek için yararlıdır. Ancak hüzme hedefin konumunu belirlemek için çok geniştir. Hedef toplam ışıma diyagramı ile aydınlatılır. Hedef yeteri kadar yakın olduğunda, alıcı durumda fark ışıma diyagramı kullanılarak hedefin ışıma diyagramının iki ana hüzmesi içerisinde tutulması sağlanır. Hedef iki ana hüzme arasındaki sıfır noktasında olmadığı zaman radar alıcısı ile bir geri dönüş işareti tespit edilir. Bu işaret hüzmenin eğimi ile orantılıdır ve hüzmenin konumuna son derece duyarlıdır. Böylece hedefin açısal konumu doğru bir şekilde belirlenebilir.

6 DÜZLEMSEL DİZİLER

Düzlemsel diziler diziyi oluşturan anten elemanlarının tamamının bir düzlem üzerinde yer aldığı dizi yapısıdır. Doğrusal diziler için daha önce sözü edilen hüzme biçimlendirme ve yönlendirme işlemlerinin temel ilkeleri düzlemsel dizilere genişletilebilir. Ancak, bazı pratik uygulamalarda düzlemsel dizilere özgü teknikler kullanılmaktadır.

Bir dikdörtgen ızgara üzerine ve xy düzleminde yerleştirilmiş bir düzlemsel dizi için dizi faktörü

$$A(\theta,\phi)=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}a_{nm}e^{\,jnkd_x\sin\theta\cos\phi}e^{\,jmkd_y\sin\theta\sin\phi} \tag{20}$$

biçiminde ifade edilir. Burada x doğrultusundaki elemanlar arası uzaklık d_x, y doğrultusundaki elemanlar arası uzaklık da d_y'dir. N, y eksenine paralel olan satır sayısını, M ise her bir satırdaki eleman sayısını göstermektedir. a_{nm} ise ilgili elemanın besleme genlik katsayını ifade etmektedir.

Eğer her bir satır, akım düzeyleri farklı bile olsa aynı akım dağılımına sahipse bu durumda akım dağılımı "çarpanlarına ayrılabilir". Bu durumda dizi faktörü

$$A(\theta,\phi)=A_x(\theta,\phi)A_y(\theta,\phi) \tag{21}$$

olarak yazılabilir. Burada

$$A_x(\theta,\phi)=\sum_{n=0}^{N}a_n e^{\,jnkd_x\sin\theta\cos\phi} \tag{22}$$

$$A_y(\theta,\phi)=\sum_{m=0}^{M}a_m e^{\,jmkd_y\sin\theta\sin\phi} \tag{23}$$

ve

$$a_{nm}=a_n a_m \tag{24}$$

olacaktır.

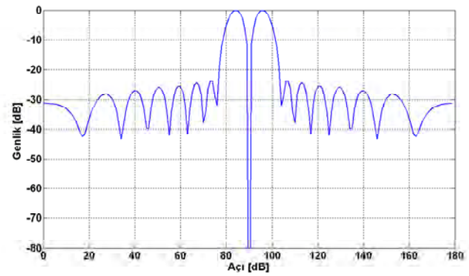
Yukarıdaki ifadelerden de anlaşılacağı üzere akım dağılımının çarpanlarına ayrılabildiği durumda, bir düzlemsel dizinin dizi faktörü iki doğrusal dizinin dizi faktörlerinin çarpımı olarak elde edilir.

Eğer düzlemsel dizide hüzme tarama yapılmak isteniyorsa, doğrusal dizilerde olduğu gibi, elemanlara düzgün artımlı faz farklarının eklenmesi gerekir. Bu durumda dizi faktörü

$$A(\theta,\phi)=\left[\sum_{n=0}^{N}a_n e^{\,jn\left(kd_x\sin\theta\cos\phi-\psi_{0x}\right)}\right]\times\left[\sum_{m=0}^{M}a_m e^{\,jm\left(kd_y\sin\theta\cos\phi-\psi_{0y}\right)}\right] \tag{25}$$

biçiminde olacaktır.

Burada ψ_{0x} ve ψ_{0y}, (9) ve (10)'da verildiği gibidir.



Şekil 6. *Bayliss dizi fark ışıma diyagramı.*

7 ÖZDİRENÇ VE KUPLAJ

Bir dizi içerisindeki bir anten elemanının yapmış olduğu ışıma, anten tek başına iken yapmış olduğu ışımadan farklıdır; çünkü dizi içerisindeki elemanlar arasında kuplaj söz konusudur. Bu da antenin ışıma yapısını değiştirebilir. Dizi kuramı incelenirken akım dağılımlarının tüm antenler için aynı olduğu ve sadece genlik ve faz olarak farklı olabileceği söylenmişti. Sonlu dizilerde elemanlar arasındaki kuplajdan dolayı akım dağılımları değişmektedir. Dizinin merkezindeki ve kenarlarındaki anten elemanları frekansın ve tarama açısının fonksiyonu olan farklı akım dağılımlarına sahip olurlar. Bu koşullar altında kuplajın hesaba katıldığı dizi eleman faktörünün tanımlanması gerekmektedir.

Toplam eleman sayısının kenar eleman sayısından çok daha fazla olduğu büyük diziler sonsuz dizi olarak düşünülebilir. Bu durumda tüm antenler aynı çevre yapısına

sahip olurlar ve akım dağılımları da aynı olur. Dizinin ışıma diyagramı diyagram çarpım ilkesi kullanılarak hesaplanabilir.

Dizi eleman faktörü $g_r(\theta,\phi)$; dizi içerisindeki diğer bütün elemanlar, elemanları besleyen iletim hattı ile uyumlu kaynak direnci ile sonlandırıldıklarında beslenen tek bir elemandan elde edilen güç ışıma diyagramı olarak tanımlanır. Bu dizi eleman faktörü bütün kuplaj etkilerini içermektedir.

Büyük bir dizi içerisinde bütün elemanların aynı ışıma diyagramına sahip olduğu kabul edilir. Elemanlar eş genlikle beslendiği zaman, dizinin bir (θ,ϕ) doğrultusunda gerçeklenen kazancı

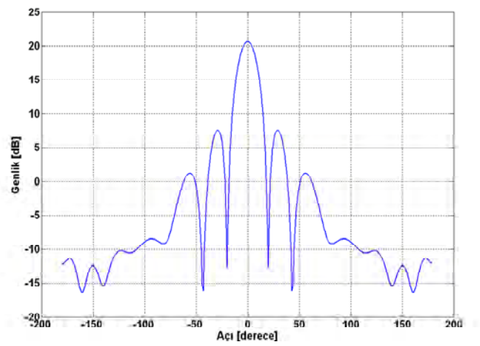
$$G_r(\theta,\phi) = N g_r(\theta,\phi) \tag{26}$$

olarak ifade edilir. Burada $g_r(\theta,\phi)$ aynı doğrultuda tek bir eleman beslendiğinde gerçeklenen kazanç ifadesidir. N ise eleman sayısıdır.

Kayıplardan ve direnç uyumsuzluklarından dolayı antenin gerçeklenen kazancı yönlendiricilik kazancından daha az olacaktır. Eğer anten ile besleme ağı arasında kayıp olmadığını ve sadece uyumsuzluk kayıplarının olduğunu kabul edersek, bu durumda gerçeklenen kazancın yönlendiricilik kazancına oranı

$$G_r(\theta,\phi)/G_d(\theta,\phi) = 1-\left|\Gamma(\theta,\phi)\right|^2 \tag{27}$$

biçiminde olacaktır. Burada $\Gamma(\theta,\phi)$ aktif yansıma katsayısı olarak tanımlanmaktadır. Aktif yansıma katsayısı dizi içerisindeki bütün elemanlar istenilen yönlendirme açısına uygun faz dağılımı ile beslendiğinde belirlenebilir ve bu değer bir elemandan yansıyan gücün ölçümüdür. Böylece, kuplaj etkileri eşdeğer bir aktif yansıma katsayısı ile ifade edilebilir. Bu aktif yansıma katsayısı da geniş bir dizi



Şekil 7. *Düzlemsel dizi anten ışıma diyagramı.*

içerisindeki tüm elemanlar için yaklaşık olarak aynıdır.

Dalga boyuna göre büyük açıklıklara sahip bir düzlemsel dizinin yönlendiricilik kazancı, dizinin elemanları eş genlikle beslendiğinde ve elemanlar ızgara kulakçıklar oluşmayacak biçimde yerleştirildiğinde dizi açıklığının alanı ile ilişkilidir. Bu kazanç

$$G_d(\theta,\phi) = \frac{4\pi NA}{\lambda^2} e_A \cos\theta \tag{28}$$

şeklinde ifade edilir. Burada A tek bir elemanın kapsadığı alandır. e_A ise, "açıklık verimliliği" olarak tanımlanır. Bu ifadelerin sonucu olarak dizi eleman faktörü

$$g_r(\theta,\phi) = \frac{4\pi A}{\lambda^2}\cos\theta\left[1-\left|\Gamma(\theta,\phi)\right|^2\right] \tag{29}$$

olacaktır.

Dizi elemanları arasındaki kuplaj ve bunun anten kazancı ile aktif yansıma katsayısına olan etkileri dizi eleman faktörü içerisinde gömülüdür. Dizi eleman faktörü eleman sayısı yeteri kadar büyük olan bir dizinin merkezdeki elemanlardan biri beslenerek ölçülebilir veya bu değer, dalga kılavuzu simülatörleri kullanarak, sınırlı tarama açıları üzerinde aktif yansıma katsayısının ölçülmesi ile elde edilebilir. Aktif yansıma katsayısı dalga kılavuzu simülatörlerinin bilgisayar modelleri kullanılarak da hesaplanabilir.

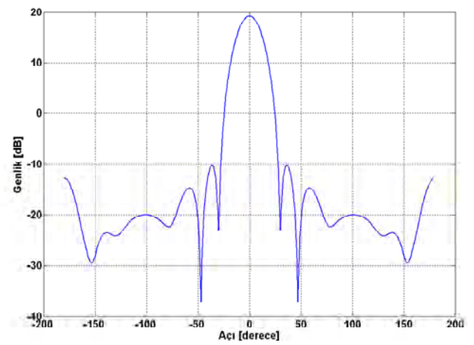
8 ÖRNEK UYGULAMA

Çalışma kapsamında *xy* düzlemine yerleştirilmiş bir düzlemsel dizi anten tasarımı gerçekleştirilmiştir. Düzlemsel dizide *y* eksenine paralel beş satır ve her bir satırda da beş eleman olmak üzere toplamda 25 eleman bulunmaktadır. Bu düzlemsel dizi yapısı faz dizili antenin bir alt dizisi olarak düşünülebilir. Diziyi oluşturan anten elemanları % 30 bant genişliğine sahip olan yığın (*stacked*) yama anten yapısında olup, boyutları $4\times4.5\times1$ cm^3'tür.

Gerçekleştirilen çalışmada düzlemsel dizinin yan kulakçık düzeylerinin bastırılması ve ana hüzmenin belirli bir açıya yönlendirilmesi amaçlanmıştır.

Şekil 7'de düzlemsel dizinin eş genlik ve fazla beslendiği durumdaki ışıma diyagramı görülmektedir.

Tasarlanan dizinin yarım güç hüzme genişliği 17,2°, en yüksek yan kulakçık düzeyi –13 dB ve kazancı 20,6 dB'dir. -13 dB'lik yan kulakçık düzeyi birçok uygulama için uygun bir değer değildir ve azaltılması gerekmektedir. Bu nedenle dizi anten tasarım teknikleri kullanılarak anten elemanlarının besleme genlik dağılımları değiştirilmiş ve yan kulakçık düzeyleri uygun değerlere çekilmiştir. Bu çalışma sonrasında elde edilen ışıma diyagramı Şekil 8'de gösterilmektedir.

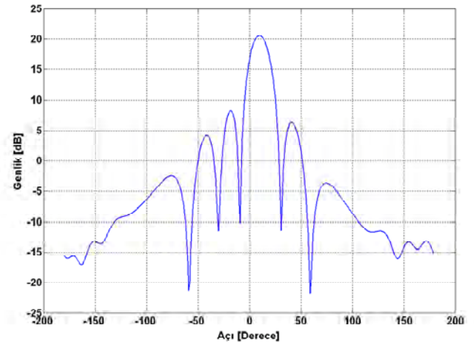


Şekil 8. *Düzlemsel dizinin besleme genlik dağılımının değiştirilmesinin ardından elde edilen anten ışıma diyagramı.*

Elde edilen ışıma diyagramından da görüleceği gibi en yakın yan kulakçık düzeyi –29,4 dB olmuştur. Bununla birlikte dizinin yarım güç hüzme genişliği artarak 21,6° olmuş ve kazancı ise 19,2 dB değerine düşmüştür.

Düzlemsel dizi ile son olarak elektronik hüzme tarama çalışması gerçekleştirilmiştir. Burada elemanların besleme faz değerlerinin uygun bir şekilde ayarlanması ile hüzme 10° döndürülmüştür. Çalışma sonucunda elde edilen ışıma diyagramı Şekil 9'da gösterilmiştir.

Oluşan hüzmenin yarım güç hüzme genişliği 17,4° olmuştur. Bu değer (17) kullanılarak yapılan hesaplama ile aynıdır. Antenin kazancı 20,6 dB olarak kalmış, yan kulakçık düzeyi ise –12,3 dB olmuştur.



Şekil 9. *Düzlemsel dizinin hüzme tarama sonrasında elde edilen ışıma diyagramı.*

9 SONUÇ

Bu çalışmada faz dizili antenlerin genel mimari yapısı, çeşitleri ve çalışma prensipleri incelenmiştir. Dizi antenlerin tasarımında önemli olan konulardan bahsedilmiştir. Örnek bir düzlemsel dizi tasarımı yapılmış, yan kulakçık bastırma, hüzme tarama teknikleri kullanılarak sonuçlar verilmiştir.

KAYNAKÇA

[1] D. K. Cheng, *Field and Wave Electromagnetics*, 2nd ed. Reading, MA: Addison-Wesley, 1989.

[2] J. L. Volakis (ed.), *Antenna Engineering Handbook*, 4th ed. New York: McGraw-Hill, 2007.

[3] R. J. Mailloux, *Phased Array Antenna Handbook*, 2nd ed. Boston: Artech House, 2005.

[4] R. C. Hansen, *Phased Array Antennas*. New York: John Wiley & Sons, 2001.

[5] E. Brookner, *Practical Phased-Array Antenna Systems*. Boston: Artech House, 1991.

[6] J. Colin, "Phased array radars in France: present and future," *Proc. IEEE Intl. Symp. Phased Array Syst. Technol.*, Boston, Massachusetts, Oct. 1996, pp. 458–462.

[7] D. Parker and D. C. Zimmermann, "Phased arrays—part I: theory and architectures," *IEEE Trans. Microwave Theory Tech.*, vol. 50, no. 3, pp. 678–687, Mar. 2002.

[8] G. W. Stimson, *Introduction to Airborne Radar*, 2nd ed. Mendham, NJ: SciTech Publishing, 1998.

[9] D. L. Harame *et. al.*, "The revolution in SiGe: impact on devices electronics," *Applied Surface Science*, vol. 224, no. 1–4, pp. 9–17, 15 Mar. 2004.

[10] S. Panaretos *et al.*, "A broadband, low-sidelobe, dynamic weighting three-channel receive, X-band active array," *IEEE MTT-S Intl. Microwave Symp. Dig.*, San Francisco, California, June 1996, vol. 3, pp. 1573–1576.

[11] R. Sturdivant, C. Ly, J. Benson, and M. Hauhe, "Design and performance of a high density 3D microwave module," *IEEE MTT-S Intl. Microwave Symp. Dig.*, Denver, Colorado, June 1997, vol. 2, pp. 501–504.

[12] S. J. Orfanidis, *Electromagnetic Waves and Antennas*. ECE Dept., Rutgers University, 2008: http://www.ece.rutgers.edu/~orfanidi/ewa/.

[13] R. S. Elliott, *Antenna Theory and Design*. Englewood Cliffs, NJ: Prentice-Hall, 1981.

[14] E. T. Bayliss, "Design of monopulse antenna difference patterns with low side lobes," *Bell Syst. Tech. J.*, vol. 47, pp. 623–650, May-June 1968.

[15] L. Changyuan, D. Shuanyu and H. Guobao, "A limited scan phased array system in circular grid configuration," *Proc. CIE Intl. Conf. Radar*, Beijing, Oct. 2001, pp. 210–213.

Duran LEBLEBİCİ

Başarı Öyküsü / Asım ALTUNBAŞ

Bu sayımızda, öğrencileri ve meslektaşları tarafından "Türkiye'de mikroelektroniğin babası" olarak adlandırılan Prof. Dr. Sayın Duran Leblebici ile keyifli bir sohbet yaptık. İlk cümlelerimizden itibaren anladık bu yakıştırmanın ne kadar doğru olduğunu. Hayatını elektronik alanına adamış Duran Bey. Eşi Yıldız Hanım elektronik alanında emekli öğretim görevlisi. Oğulları Yusuf Bey'e miras kalmış bu sevda. Hatta gelinleri de Anıl Hanım da elektronikçi.

Ortaokulda fizik dersine olan özel ilgisinden, lisedeki amatör radyoculuk merakına, İTÜ'deki yıllarından, TÜBİTAK'taki kariyerine kadar birçok konuya değindik. Bize ülkemizde mikroelektronik alanında yapılan ilk girişimlerden bahsetti, gelecekteki teknolojilere dair ipuçları verdi. Şimdi Duran Bey'e kulak verelim, ne dersiniz?

Öncelikle kişisel olarak merak ettiğim bir soruyla başlayayım. Çorumlusunuz ve soyadınız Leblebici. Aile büyüklerinden leblebi işi ile uğraşan varmıymış?

Bildiğim kadarıyla yok (gülüyoruz). Ailemiz genelde mektepli bir aile. Ama bir Leblebici Hoca varmış, sanırım ondan geliyor.

Elektronik alanına merakınız ne zaman, nasıl başladı?

Ortaokuldayken fizik hocamız vardı, Mahmut Hoca. Bu başka Mahmut Hoca (gülüyoruz). Onunla beraber başladı diyebilirim. Lisede Çorum'daydım, Çorum Lisesi'nde. Çok iyi hocalarımız vardı. Bizim merakımız onların da teşvikiyle beraber deneyler yapmaya, laboratuarda bulunmaya başlamıştım. Sıkı bir radyo amatörüydüm. Fakat bir açıdan da tehlikelidir radyo amatörlüğü. Amatörler genellikle formal öğretimi beğenmezler, amatör olarak hızını alamayıp fakülteyi terk eden bir sürü insan tanıyorum.

Lisedeyim, nasıl öğrendim hatırlamıyorum ama Teknik Üniversite'de (İTÜ) Santur Hoca'yı (Prof. Dr. Mustafa Santur) duymuşum. Onunla çalışmak hayalim.

Ardından Teknik Üniversite'ye gittim. Son sınıftayız. Hocalık yıllarımda beraber çalışmak için iyi öğrencileri gözüme kestirirdim. O zaman da öyleydi, kimlere asistanlık teklifi gelcek diye merakla bekliyorduk. 90 kişi girmiştik bölüme. Zayıf akım kolunda (elektronik bölümü) 12 kişiydik. 4 kişi teklif aldı asistanlık için. Ben de vardım.

Yıldız Hanım'la tanışmanız?

Yıldız'la üniversitede tanıştık, beraber okuduk. Sonra da evlendik.

Oğlunuz Yusuf Bey'in de elektronik alanını seçmesinde sizin yönlendirmeleriniz oldu mu?

Aslında aleni bir yönlendirmemiz olmadı.

Ailece elektronikçisiniz.

Gelinimiz de elektronikçi (gülüyoruz).

Asistanlığa seçildiniz, sonrasında?

Sonrasında İ.T.Ü'de, 1960'ların sonuna doğru mikroelektronikle ilgili ilk dersleri vermeye başladık. 1970'te de rahmetli hocam Prof. Dr. Mustafa Santur'un teşvikiyle üretim teknolojileri konusunda da birşeyler yapma zamanının geldiğine karar verildi. 1971'de İngiltere'de Southampton Üniversitesi'nde bir kursa giderek bu teknoloji ile yüz yüze geldim. Daha sonra 1974'te Hollanda'da Twente Teknik Üniversitesi'nde bir yaz geçirerek MOS transistör ve tümdevre teknolojisinin temellerini laboratuvarda fiilen çalışarak öğrendim.

71'de ve 74'te bir grupla mı gittiniz, tek başına mıydınız?

Tek başımaydım. Grup kuracak adam yoktu ki. Laboratuvar kurma çalışmaları 74'te başladı. Burada şunu da ekleyeyim; İTÜ'deki mikroelektronik laboratuvarını kurarken 2 birim halinde düşündük. Biri kalın film tümdevre birimi, diğeri de MOS transistör ve tümdevre birimi. Kalın film teknolojisi o yıllarda bayağı revaçta idi ve mikro teknoloji için sıçrama tahtası olarak düşünülebilecek bir teknolojiydi. Onun için biz kalın film teknolojisiyle başladık. 1974'te ilk kalın film tümdevreleri çok mütevazi şartlar altında gerçekleştirildi. Bizim bu kalın film tümdevrelerini kolayca gerçekleştirebildiğimizin görülmesi üzerine TELETAŞ kendi kalın film tümdevre tesisini kurmaya karar verdi. Bir genç arkadaşı, TELETAŞ'ta çalışmakta olan Selçuk Özbayraktar'ı bizim laboratuvara gönderdi. Selçuk bizde 15-20 gün kadar çalıştı, teknolojiyi öğrendi. TELETAŞ kalın film tümdevre üretim tesisini lisans, know-how vs. almadan bizdeki birikimden yararlanarak kendisi kurdu ve Avrupa'nın en iyi kalın film tümdevre üretim tesislerinden biri haline geldi kısa zamanda.

Kalın film teknolojisinde Avrupa'nın en iyi üretim yapan laboratuvarlarından biri TELETAŞ'ınkiydi dediniz. Peki o zamanlarda en son teknoloji kalın film teknolojisi miydi?

Duran Bey sorularımızı içtenlikle yanıtladı.

Eşi Yıldız Hanım'la birlikte.

En son teknoloji değil ama revaçta olan, para kazanılan bir teknolojiydi; ancak kalın film teknolojisi kısa zaman sonra öldü. Entegre devre teknolojisindeki gelişmeler kalın film teknolojisini gereksiz hale getirdi.

Şunu merak ettiğimden soruyorum. Biz biliyoruz ki şu an tümdevre teknolojilerinde başı çeken ülkelerden bir iki adım gerideyiz. O zaman aynı seviyedeydik de farkı sonradan mı açtılar? Yoksa o zamanda mı durum öyleydi?

Kalın film teknolojisi konusunda gelişmiş ülkelerdeki teknoloji neyse bizdeki de oydu. Üretkenlik bakımından da, teknolojik düzey bakımından da kalite bakımından da aynı düzeydeydik.

At başı gidiyorduk yani.

Fakat o teknoloji öldü. Yarıiletken teknolojisine de endüstriyel düzeyde geçemedik. Şimdi yarıiletken teknolojisine -daldan dala geçiyoruz- geçmek için Türkiye'nin kaçırdığı birtakım fırsatlar vardır. 1960ların sonlarında Siemens Türkiye'de yüksek frekans güç transistörleri imal eden bir fabrika kurmak üzere teşebbüslerde bulundu. O zamanki genel müdürleri Arnold Hornfeld'in -kulakları çınlasın- anlattığına göre işler hemen hemen son aşamasına gelmişken 1972 darbesi sonrasında planlama üst yönetiminin değişmesi bunun Türkiye'de yapılmasına gerek yoktur diye bir kararın ortaya çıkmasına yol açmış ve konu kapanmış. İkinci şey de şudur; 1980'lerde, yine kulakları çınlasın Teletaş Genel Müdürü Fikret Yücel tarafından, dijital telefon santrallerinde kullanılan tümdevrelerin Türkiye'de imal edilebilmesi için bir tesis kurulması konusu gündeme getirildi ve Uğur Çilingiroğlu arkadaşımız bir fizibilite çalışması yaptı.

Bu projenin yatırım finansmanının önemli kısmını o zamanın başbakanı rahmetli Turgut Özal vermeyi vaat etti. Tam oluyor olacak derken seçimler oldu. Siyasi iktidar değişti ve film koptu. O da kaybedilmiş bir fırsattır. Şimdi üniversitedeki laboratuvarın kurulma hikayesine devam edersek;

Şimdi o yıllar Türkiye'de ithalatın son derece zor olduğu yıllar. Herhangi bir şeyi ithal edebilmek için muhakkak Ankara'dan permi almak gerekiyor. Laboratuvarda kullanacağımız teçhizatın bir kısmını Türkiye'de biz kendi imkanlarımızla gerçekleştirdik ama bir kısmını da ithal etmek zorundayız, çünkü özel teçhizat. Bunların permilerini alabilmek için ben genç bir akademisyen olarak ikinci mevki kuşetli trene atlıyorum, ikide bir Ankara'ya gidiyordum. Maliye Bakanlığı ve Merkez Bankasında kapı kapı dolaşıp permileri almaya çalışıyordum. Bu gidiş gelişler sırasında işleri aşağı düzeyde yapmanın imkansız olduğunu, yapılacaksa yukarıdan halletmek gerektiğini öğrendim. Kısa zaman içerisinde gerek -kulakları çınlasın- Merkez Bankasının o zamanki başkanı Cafer Tayyar Sadıklar, gerek o zamanki Maliye Bakanlığı Müsteşarı Biltekin bey ile gide gele adeta dost olduk. Merkez Bankası Başkanı doçentti. Ben de o zaman demek ki doçent olmuşum ki meslekdaş diye bakardı bana. Bu laboratuvarın kurulması için bizim ithal ettiğimiz cihazların tümünün toplam bedeli 90.000 dolardan ibarettir. Yani olağanüstü ucuza çıkarılmış bir laboratuvardır. Türkiye'de yapılabilecek her şey, bazı cihazlar dahil, kendi imkanlarımızla Kürsü'nün teknisyenlerinin ve asistanlarının el emeği ile gerçekleşmiştir. O kültür aslında YİTAL'in kurulmasında da çok etkili olmuştur. YİTAL'de de bir çok şey kendi imkanlarımızla gerçekleştirilmiştir. Şimdi bu YİTAL ile ilgili olarak size bir şeyden bahsetmek istiyorum; Elektrik Mühendisleri Odası 2006 yılında

Silisyum nitrür ve polisilisyum depolama (LPCVD) cihazı.

elektronik sanayinin Türkiye'de kuruluşu ve gelişmesi ile ilgili olarak bir dizi sohbetler düzenlemişti. Her seferinde 3-5 kişi bir araya geliyordu. Herkes hatıratını anlatıyordu. Bütün bunlar EMO tarafından iki cilt halinde yayınlandı. Bu kapsamda MAM'ın o dönemki başkanlarından biri olan Ömer Kaymakçalan'dan da görüş istemişler. Ömer Bey –kulakları çınlasın- konu ile ilgili görüşlerini yazı olarak göndermiş. YİTAL'le ilgili olarak şöyle diyor: "İşi bilenlerin değerlendirmesiyle oldukça ucuza kurulmuş başarılı bir birimdi. Ancak ben geldiğimde işletilmesi için gerekli işletme sermayesi yoktu. Dışarıdan proje de alınamıyordu ve elemanlarının büyük bir kısmı da ayrılmıştı. Ankara'daki üniversite çevrelerinde ve TÜBİTAK Başkanlığı'nda YİTAL'in eski teknoloji olduğu, işe yaramadığı ve mali yük olduğu söyleniyor, kapatılmasını teklif edenler bulunuyordu. O zamanki Tübitak başkanı Kemal Gürüz bile bana YİTAL'i kapatmaktan bahsetmişti."

Şimdi burada Ankara diyorum ya; Ankara tuhaftır. Bu hükmü vermiş olanların herhangi birinin gelip de YİTAL'i gördüğünü hatırlamıyorum. Yani YİTAL nasıldır, ne yapılıyor.

Sonra devam ediyor ve diyor ki;

"Duran Bey ve Fikret Bey (Fikret Yücel) Önder'i önermeseler (Önder Yetiş'i kastediyor) ve Önder'in çabaları olmasa bugün belki YİTAL kapanacak ve ortada UEKAE de olmayacaktı."

Bu da o yıllarda sorumluluk almış bir yöneticinin yıllar sonra yaptığı bir değerlendirme.

Direkten dönmüş açıkçası YİTAL. Çok net ve çarpıcı olarak açıklamış.

İTÜ'de 1970'lerin başında çok ekonomik olarak bir laboratuvar kurduk ve bu laboratuvarda MOS transistörleri başarıyla gerçekleştirmeye başladık. Burdaki başarı zaten bu alana girmeye niyetlenmiş olan Marmara Araştırma Merkezi (MAM) Elektronik Bölümü'nden bir teklif gelmesine yol açtı. Lütfullah Ulukan ve rahmetli Yılmaz Tokad benden kurmayı planladıkları yarıiletken teknolojisi laboratuvarı için yardımcı olmamı istediler. 1980 yılı başında MAM'a bu projenin yürütücüsü olarak gittim. Danışman olarak haftada 2 gün devam ediyordum. YİTAL'in planlamasında bir başka yön daha vardı. O da Ankara'da kurulmakta olan TESTAŞ transistör ve entegre fabrikasının Ar-Ge birimi olarak planlanmıştı.

TESTAŞ özel teşebbüs mü, devlet kurumu muydu?

Devlet kurumu. Bu kuruluşun Amerika'daki Exar firmasından aldığı know-how bu bağlantı üzerinden bize de verildi. Ve bunun yanısıra İslam Kalkınma Bankası'ndan 1.500.000 dolarlık bir kredi kullanma imkanı ortaya çıktı.

TESTAŞ Amerika'dan "know-how"ı nasıl elde etmiş? Türk mühendislerini mi göndermişler?

Amerika'da çeşitli firmalarla görüşerek bir know-how anlaşması yapmak istemişler ve sonunda Exar firmasıyla mutabık kalmışlar. O tarihte Exar'in başında bir Türk vardı; Alan Bekir Grebene. Firmanın kurucularından biri aynı zamanda. Meblağı hatırlamıyorum ama lisans, bayağı iyi bir paraya TESTAŞ tarafından alınmış. O tarihte geçerli olan teknoloji bipolar teknolojisiydi, henüz MOS teknolojisi yaygınlaşmamıştı. Ve TESTAŞ'ın Ankara'daki fabrikasının amacı da öncelikli olarak Türkiye elektronik sanayiinde kullanılan transistör ve entegre devrelerin Türkiye'de yapılmasıydı. YİTAL'in kuruluş çalışmaları 3 sene içerisinde tamamlandı ve 1983 yılının Nisan ayında ilk deneme üretimini başarıyla tamamladık. Bu dönemde halen Yeditepe Üniversitesi'nde olan Prof. Dr. Uğur Çilingiroğlu mikroelektronik alanında yurtdışında doktorasını yapmış genç bir doçentti. Bu ilk aşamada Uğur Çilingiroğlu'yla beraber çalıştık. Daha sonra Uğur ayrıldı, yurtdışına gitti. Bir süre sonra YİTAL'deki ekibe Prof. Dr. Atilla Ataman dahil oldu. Yakın zamana kadar Atilla'yla beraber devam ettirdik.

YİTAL'in kuruluşunda kaç kişiydiniz?

YİTAL'in kuruluşunda danışman olarak ben ve Uğur'dan başka 3 tane yeni mezun öğrencimiz vardı, bu kadardık. Bir de bizim kürsünün maharetli bir teknisyeni vardı, Allah rahmet eylesin, Hamdullah Örentel. Hamdullah laboratuvarın altyapısının kurulmasında, boruların döşenmesinde, aletlerin monte edilmesinde falan olağanüstü bir performans göstermiştir. Çok emekleri, katkıları vardır. 1983'te dediğim gibi biz üzerimize düşeni yaptık. TESTAŞ o

zamana kadar yetişmiş olsaydı bizden birşeyler isteyecekti, biz de onlara destek verecektik. Fakat TESTAŞ bir türlü ayağa kalkamadı ve dolayısıyla kurulan laboratuvar amaçsız bir duruma düştü. O kurulan altyapıyı ve kadroyu değerlendirmek amacıyla bazı girişimlerimiz oldu. Bunlardan en önemlisi şudur. ASELSAN telsizler üretiyordu o yıllarda. Bu telsizlerde de bayağı pahalı yüksek frekans güç transistörleri kullanılıyordu. ASELSAN'la temas kurduk.

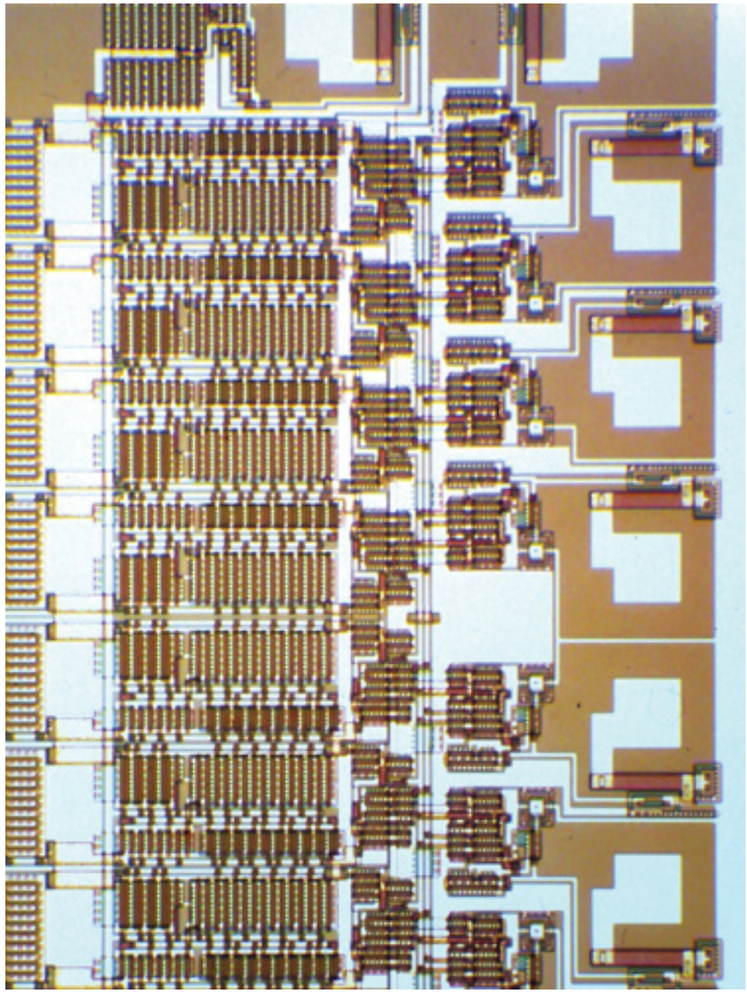
Bu transistörler yurtdışından alınıyor değil mi?

Gayet tabi. En çok kullanılan güç transistörlerinden birkaç örnek istedik. Onları inceledik, üzerinde çalıştık ve güç transistörlerini yapmaya karar verdik. Deneme üretimleri yaptık, denemeleri için ve başarılı olduğu takdirde üretimleri YİTAL'de yapılsın diye yaptığımız örnek üretimlerini ASELSAN'a gönderdik. Yalnız bu diyalog sağlıklı gelişmedi. Burada şöyle birşey vardır. Bizde genellikle bu tür yüksek teknoloji ürünlerinin Türkiye'de iyi bir şekilde yapılacağına pek ihtimal verilmez. Şöyle söyliyeyim, zamanın ASELSAN genel müdür yardımcısıyla diyalog kurarak bu işi başlatmıştık. Ama o ekip bizim kadar heyecanla seferber olmadı. Biz bir örnek yapıyoruz, gönderiyoruz; "Yahu şunu bir ölçeyim, deneyeyim" denmedi, kısacası film koptu.

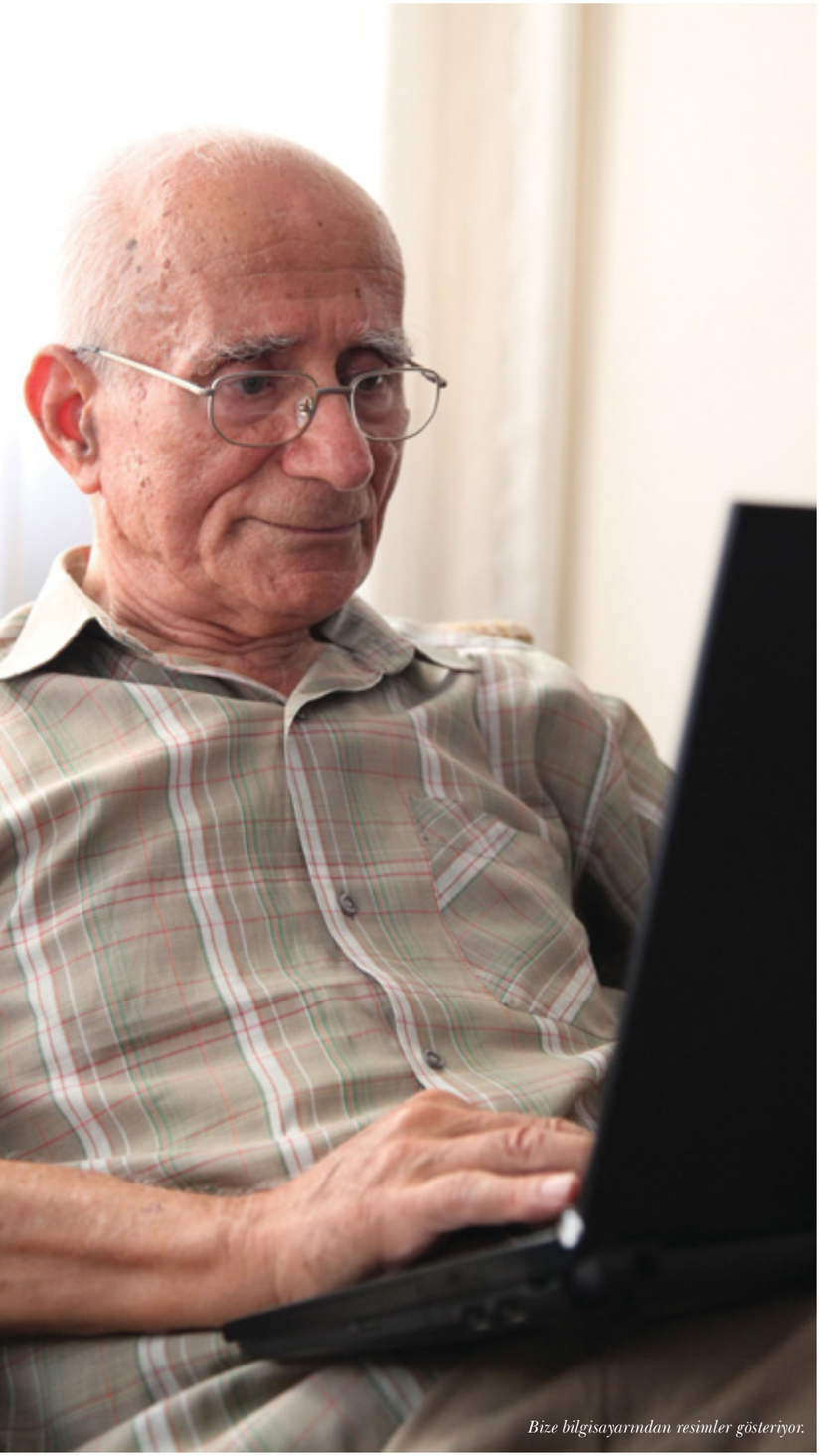
Belki bu transistörleri sizden tedarik etselerdi herşey çok daha farklı olabilirdi.

Olabilirdi. İlk yapılan transistörler gayet güzel çalışıyordu. Bu arada YİTAL sürekli para harcıyor. Laboratuvarın ayakta kalması için devamlı azot kullanması lazım, oksijen kullanması lazım, elektrik harcanıyor. "Kapatsak mı?" düşünceleri ortaya çıkmış. Bir taraftan da biz bu birikim, altyapı boşa gitmesin diye yeni arayışlara girdik. Yeni ve hızlı bir gelişme içine giren MOS tümdevre ve transistör teknolojisini kazanmak üzere bir faaliyet başlattık. Bu faaliyeti desteklemek için de o zaman NATO'nun Science for Stability (SfS) programı vardı. Bu programa maddi destek almak için başvurduk. Bu desteğin kazanılmasında o zamanki Marmara Araştırma Merkezi başkanı Prof. Dr. Nejat İnce'in bir olumlu bir de olumsuz katkısı olmuştur. Olumlu katkısı şudur; NATO SfS programı NATO'nun fukara üyelerine bize, Yunanistan ve Portekiz'e proje destekleri veriyordu. Fakat bu verdikleri proje destekleri genellikle yerel sorunların çözülmesine yönelik desteklerdi. İleri teknoloji desteği verme gibi bir adetleri yoktu. Nejat Bey'in katkısı NATO'da gerektiğinde bağırarak-çağırarak Türkiye'ye ileri teknoloji alanında bir proje verilmesini sağlamak olmuştur. Bu çok önemli bir başlangıç katkısıdır. Olumsuz katkısı ise şudur; bu proje NATO'da olumlu olarak değerlendirildiği sırada Nejat Bey MAM'dan ayrılıp ODTÜ'ye gitme kararı aldı veyahut öyle bir durum ortaya çıktı. Bunun üzerine o projenin bütçesinin yarısını Ankara'ya aktardı. Başlangıçta gerek MOS tümdevre tasarımı gerekse üretimi YİTAL bünyesinde planlanmışken tasarım Ankara'da ODTÜ'de, üretim Gebze'de olacak şekilde ikiye bölündü.

Coğrafi uzaklığın yanı sıra biri MAM biri ODTÜ olmak üzere kurum ayrılığı da ortaya çıktı. İşinizi oldukça zorlaştırmış olmalı.



YİTAL'de üretilen bir CMOS tümdevresi.



Bize bilgisayarından resimler gösteriyor.

Evet. Neticede her birim işi kendi içinde götürdü. Şunu söyleyeyim; bizim o projeden Türkiye'ye kazandırdığımız YİTAL oldu. Fakat projenin diğer yarısının harcandığı ODTÜ'de sürekliliği olan başarılı bir tasarım merkezi oluşmadı.

ODTÜ'deki filizlenmenin devam etmemesi acaba ekonomik sorunlardan mı yoksa kalifiye işgücü yetersizliğinden mi kaynaklandı?

Onu bilmiyorum. Kadro yetersizliğinden de olabilir. YİTAL için alınan "Silicon LSI/VLSI Circuits Fabrication Technologies" adlı projenin başlangıç tarihi 1988'dir. Alınan destek 600.000 dolardır. Bu kaynaktan yararlanılarak YİTAL'in bipolar teknoloji için kurulmuş olan altyapısının MOS transistor ve tümdevreleri de gerçekleştirecek şekilde geliştirilmesi sağlandı. Burada birşeyi söylememem lazım. İlk teknoloji, bipolar teknoloji Exar'dan alınan know-how'ın kullanılmasıyla gerçekleştirilmişti. Ama NATO'dan aldığımız destekle MOS teknolojisinin geliştirilmesi sırasında herhangi bir know-how yahut lisans almadık. Teknolojiyi açık literatürdeki bilgiden yararlanarak kendimiz geliştirdik. Bu başarılı bir projeydi. Zannediyorum NATO'nun başlangıçta gönülsüz verdiği bir proje olmasına rağmen böyle başarıyla sonuçlanması olumlu bir takım etkiler oluşturdu ve NATO'nun aynı konuda arka arkaya iki proje vermek gibi bir adeti olmadığı halde bize bu projenin devamı için ikinci bir proje verdiler 1994'te. Ve bu projeden yararlanarak da başlangıçta 3 mikron teknolojisi için geliştirilen teknolojiyi ve altyapıyı bir kademe aşağıya, 1,5 mikrona çekmek için destek aldık. Yalnız NATO bu desteği verirken bir de koşul ileri sürdü. "Biz 600.000 dolar vereceğiz, en az bunun yarısı kadar da Türk sanayii katkı yapsın." Bunu sağladık. O tarihte TELETAŞ, NETAŞ, BEKO ve Siemens toplam 400.000 dolar civarında bir katkıyı sağladılar.

Bunu hibe olarak mı verdiler?

Evet, hibe olarak. Bu Türkiye'nin teknolojik geleceğine yapılan bir yatırımdır. Bunun öncülüğünü yapan o zamanki TELETAŞ'ın genel müdürü Fikret Yücel'in, Siemens'ten Arnold Hornfeld'in Netaş'tan Tanju Argun'un, Beko'dan Muvaffak Gözaydın'ın cömert ve ileri görüşlü katkılarını şükranla anmak gerekir. O sıralar TÜBİTAK'ın bütçesi de biraz daha rahatlamıştı. Neticede 1998'de 1,5 mikron teknolojisiyle tümdevreler yapılmaya başlandı.

Peki bunlar sahaya nasıl indi?

Evet, asıl soru "Ne yapacağız?". İşte orada kripto olayı gündeme geldi. Kripto biliyorsunuz en başından en sonuna kadar herşeyiyle size ait olması gereken bir teknoloji alanı. Yani kripto algoritmasını Türkiye'de geliştirip, devrelerinin tasarımını Türkiye'de yapıp ondan sonra bunu yurtdışında imal ettirmeye gönderdiğinizde o kriptonun kriptoluğu kalmaz. Sıfırdan sonuna kadar burada yapılması gerekir.

%100 milli olması gereken bir teknoloji.

Evet. Dolayısıyla bu altyapı kripto tümdevrelerinin (kripto çiplerinin) Türkiye'de yapılması imkanını sağlayan bir proje oldu ve 1999'dan başlayarak, yani proje bitiminden hemen sonra kripto çipleri YİTAL'de seri olarak üretilmeye ve kripto sistemlerinin içine girmeye başladı. Hala da devam ediyor.

Müşteriniz UEKAE idi?

Evet, UEKAE'ydi. Tabi bunun sadece kriptoyla kalmaması gerekir. Yeni müşteriler bulmak, daha büyük üretim hacimleriye üretim yapmak bir amaç olarak hep akıllarda kalmıştır. Büyük bir iç pazar olarak şimdi her yerde kullanılan akıllı kartların çiplerinin yapılması önemli bir konudur. Bu konu ilk defa 5-6 yıl evvel gündeme geldi. Konu gündeme geldiğinde YİTAL'de arkadaşlarla görüştük.

Arkadaşlar derken tabi bir parantez açmam lazım; başta dediğim gibi part-time olarak Uğur ve bu işin asıl yükünü çeken az sayıda genç mühendis vardı. Daha sonra gruba Atilla katıldı, eleman sayısı da arttı. Başlangıçtan itibaren YİTAL'de çalışan mühendisler misyoner ruhu ile çalışmışlardır. Geceleri, gündüzleri yoktur, önemli olan işin yapılmasıdır. Bu kültürü yerleştirdik kurum kültürü olarak. Akşam 5 oldu işi bırakayım diyemezsiniz, o proses bitene kadar başında durmak zorundasınız.

İdealist bir yaklaşımla olmazsa başarılı olamıyorsunuz.

Kesinlikle. YİTAL'in kuruluşundan itibaren hep böyle gençlerle birlikte çalışma fisatımız oldu. Tabi burda şansımız şuydu, bunlar öğrencilerimizdi daha evvel. Nasıl başlangıçta Santur hoca bana "gel"demişse ben de göz koyduğum öğrencilere (gülüyor) "gel burada beraber çalışalım" diyordum. Bir de şunu söylemem lazım, bu uzun zaman içinde, 25 yıl içinde

TÜBİTAK Hizmet Ödülü'nü alırken.

Oğlu Yusuf Leblebici'yle beraber.

tabiatiyle bir eleman hareketi de ister istemez oluyordu. Birileri gidiyordu. Yurtdışına gidiyordu, sağlık sebebiyle ayrılanlar oluyordu, başka işe girenler oluyordu. İlk zamanlarda işi öğrenmiş bir genç ayrılacağı zaman uykularım kaçardı; "eyvah nasıl devam ettireceğiz" diye. Ama bu bahsettiğim kurum kültürü bilginin kopmadan nesilden nesile, elden ele devam etmesini sağladı. Şu anki kadronun içindeki kıdemliler; Aziz Bey, Sema Hanım dükkanın sahibi olarak (gülüyor) devam ettiregeldiler. Yani bu projelerin yürütüldüğü süre boyunca beraber çalıştığım genç arkadaşların niteliklerinin altını çizmek, hepsine çok teşekkür etmek isterim. YİTAL Türkiye şartlarında bazı engellere, olumsuzluklara rağmen başarıyla yoluna devam edebilmiş bir kuruluştur. Bu kuruluşun buraya gelmesinde gerek yöneticiler arasında çok açık destek vermiş olanların, Prof. Lütfullah Ulukan'ın, Prof. Dr. Yılmaz Tokad'ın, Prof. Dr. Nejat İnce'nin, Prof. Dr. Erdoğan Şuhubi ve Ömer Kaymakçalan'nin ve gerekse bu projede fiilen çalışan genç elemanların büyük katkıları vardır.

Akıllı kart çiplerinden bahsediyordum. İşte 5-6 sene evvel gündeme geldiğinde bu işin YİTAL tarafından yapılabileceğine kimse inanmadı.

Türk insanının yüksek teknoloji barındıran ürünleri yapamayacağı önyargısına takıldınız.

Evet. Bana göre yazık olmuştur. Olağanüstü büyük bir pazar. Başlangıçta her Türkiye Cumhuriyeti vatandaşı için bir çip. Bir taneyle de bitmiyor. Akıllı kartlar her yere giriyor. Sağlık hizmetlerinden, pasaporta, ehliyete kadar her yerde var. Yüzlerce milyon çiplik bir pazar söz konusu.

Bunların yenilenmesi de var.

Gayet tabi. Yenilenmesi de olacak. Neticede bu çipler dışarıdan alınmaya başlandı ve de devam edilecek. Keşke zamanında, mesela 10 sene satın alma için harcanacak para kadar bir yatırım YİTAL'e yapılabilseydi bunların Türkiye'de imal edilmesi çok güzel olurdu.

Şimdi burada başka birşeyden daha söz etmek istiyorum. Bir taraftan bu işler devam ederken üniversitede de sanayi kuruluşlarıyla beraber bir İTÜ İleri Elektronik Teknolojileri Vakfı (İTÜ-ETA Vakfı) adında bir vakıf kurduk. Bu vakıf tümdevre tasarımı konusunu Türkiye elektronik sanayine öğretmek gibi bir öncelikli amaç tanımladı. Bir tasarım merkezi kuruldu. Burada çeşitli teknolojilerle sanayi için tümdevre tasarımları yapılmaya başlandı. Bunların çoğu yurtdışında ürettirildi. Çünkü teknolojileri YİTAL'in teknolojisinden daha yüksek bir teknolojiydi. Daha sonra ASELSAN'dan çok yüksek frekanslı devrelerde kullanılan SiGe (silisyum-germanyum) teknolojisiyle yapılmış tümdevrelerin tasarımı talepleri gelmeye başladı. Aşağı yukarı 10 seneden beri bu tasarım merkezinde Si-Ge tümdevre tasarımları yapılıyor. Tasarlanan tümdevreler de yine yurtdışında üretime gönderiliyor. Bu faaliyetler esnasında farkettim ki stratejik teknoloji sayılan bu teknolojiyle tasarımını yaptığımız devrelerin yurtdışında imal ettirilmesi konusunda bir darboğazın ortaya çıkması riski var. Bunu da şurdan gördük. Avusturya'da bir şirketle çalışıyorduk. Teknolojisi biraz daha iyi olan bir Amerikan şirketine başvurduğumuzda "Askeri elektronikte çalışan müşteriniz var mı?" diye sordular. Biz de "Var, ASELSAN var" dedik. O zaman "Kusura bakmayın, biz sizinle iş yapamayız" dediler (gülüyoruz). Bu cevapları alarm zillerini çaldırdı kafamda. Aziz Bey'le beraber Önder Bey'e gittim. Konuştuk ve stratejik bakımdan Türkiye'nin bu teknolojiye sahip olması gerektiği konusunda herkes ikna oldu. Bunun üzerine DPT'den (Devlet Planlama Teşkilatı) bir proje aldılar. Si-Ge hattı kurulmaya başladı. İnşallah bu yıl içinde deneme üretimlerine başlayacak. Böylece stratejik bakımdan bağımlılıktan kurtulma imkanı sağlanmış olacak.

Düşük teknolojilerle çalışırken kimsenin sizi aşağı çekmek gibi bir niyeti yok ama ne zaman zirveye oynuyorsunuz, birileri sizi alaşağı etmeye çalışıyor.

Gayet tabi. Bu girişimi yaptığımızda ben UEKAE'den ayrılmıştım. Kendi kendimi emekli etmiştim (gülüyor). 25 senem tamamlandı, dedim ki "Yeter". Niye kendi kendimi emekli ettim onu da söyliyeyim.

Ben de onu soracaktım.

Evet. Kurumların kişi bağımlı olmaması lazım. Herkesin aktif bir süresi var. Bir doğal ömrü var. Ben oradaki kadronun bu işleri ben olmadan da yürütecek kıvama geldine emin olduğumda huzur içinde ve gözüm arkada kalmadan kendimi emekli ettim. Si-Ge teknolojisi fikrini Önder Bey'e götürdüğümüzde fiilen UEKAE'de çalışmıyordum. Ama bunun bir gereklilik

Oğlu Yusuf'la, yıllar önce.

olduğunu düşünerek götürdük, çok da iyi oldu. SiGe (silisyum-germanyum) prosesi oturduktan sonra GaN (galyum-nitrid) teknolojisini kafalarına sokmaya çalışacağım (gülüyor). O da stratejik bir teknoloji olacak.

Bir de şimdi büyük resmi siz rahat görüyorsunuz. Bu işin Türkiye'de başlangıcını biliyorsunuz. Nereden nerelere geldiğini biliyorsunuz. Peki bundan sonra Türkiye'de bu alanda neler olur, hangi alanlara yönelmeliyiz? Tümdevre alanında yarıiletken alanında neler yapmalıyız? Özellikle hangi teknolojiler daha kritik olacaktır, hayatımıza yön verecektir?

Şimdi iki şey var. Bir tanesi stratejik teknolojiler, mesela; kripto çiplerinin üretim teknolojisi bir stratejik teknolojidir. Teknolojinin kendisi stratejik olmadığı halde. Onu kendiniz yapabiliyorsanız anlamı vardır. Stratejik teknolojilerden ikincisi Si-Ge olayında söylediğim gibi dışarıda yaptıramama riskinin olduğu teknolojidir. Ama siz bunlara sahip olmak zorundasınız. İşte günümüzde Heron'larla ilgili çeşitli şeyler söyleniyor. Mesela bana çok çarpıcı gelen ama hiç de yadırgamadığım zaten tahmin ettiğim, Heron'ların çektiği fotoğraflar önce İsrail'e gidiyormuş ondan sonra ne kadarı verilirse onlar buraya geliyormuş. Böyle bir sistemin gerek donanım olarak gerek yazılım olarak her şeyini siz yapmadığınız takdirde sizin değildir. Seneler evvel bir panelde, bir toplantıda Silahlı Kuvvetlerin askeri uydu satın alması konuşuluyordu ve orada bunun doğru olmayacağını söyledim. Çünkü aldığınız askeri uydu sulh günlerinde tıkır tıkır çalışır fakat harp olduğu takdirde o uydunun ne yapacağına o uyduyu yapan karar verir. Şimdi bu tür stratejik teknolojileri kendin yapamadığın takdirde sahip olmak mümkün değildir. Yani para verip satın almak mümkün değildir. Şimdi bu yarıiletken teknolojisinin, mikroelektroniğin stratejik yönü. Bir de ekonomik yönü var.

O da şu; mikroelektronik artık her şeye girdi. Yani oyuncaktan, saate, otomobile. Bugün mikroelektronikten ekonomik olarak para kazanmak için çok büyük ölçekli üretim yapmak lazım. Bunu sadece Türkiye iç pazarı ile sağlamak mümkün değil. Yani büyük boyutlu yarıiletken endüstrisinin ürettiklerini sadece iç pazarda tüketmek, bu üretim tesisini ekonomik düzeyde tutmak mümkün değil.

Teknolojinin o zaman ihracatçısı da olmamız lazım.

İhracatçısı da olmamız lazım. Yahut üretim teknolojisinin nispeten küçük sayılarda da üretim yapabilecek esnek türlerine geçmek lazım. Bu konuda da dünyada bazı uygulamalar var. Bunlara " mini fab " diyorlar. Küçük fabrika. Bunlar, birkaç milyar dolarlık fabrikalarda yapılan üretim miktarının onda biri, yüzde biri mertebesindeki üretimin daha mütevazi bir yatırımla, birkaç yüz milyon dolarlık yatırımla gerçekleştirme imkanı veren fabrikalar.

Şimdi biraz evvel söz ettiğim bu akıllı kartlar konusu, Türkiye'de böyle bir yaklaşımla gerçekleştirilebilirdi. Hala da gerçekleştirilebilir.

Bakın bu yatırımlar yani birkaç yüz milyon dolar mertebesindeki yatırımlar bugünün Türkiye'si için olmayacak şeyler değil ama olduğu takdirde, devamı da olduğu ve akıllıca yönlendirildiği takdirde Türkiye'ye önemli ekonomik ve teknolojik getiriler sağlayacaktır.

Çok güzel şeylerden bahsediyorsunuz. Öyle güzel tablolar çiziyorsunuz ki yani Türkiye'i hakikaten en üst teknolojiyi üretirken, Atatürk'ün bize tarif ettiği gibi muasır medeniyetler seviyesinde ve daha üstünde görmek istiyoruz. Belki önümüzdeki birkaç yılda değil ama birkaç on yılda Türkiye bu teknolojilerin başını çekecek, amiral gemisi olacak ülkelerden biri neden olmasın?

Şimdi bakın Türkiye'de insan kalitesi çok iyidir. Benim yurtdışında mikroelektronik alanında çalışan yüze yakın öğrencim var. Dünyada özellikle Amerika'nın Silikon Vadisi'nde başarıyla çalışıyorlar, çalışmaktalar, çalıştılar. Bu büyük bir birikimdir. Türkiye bu birikimi Türkiye'de de değerlendirirse çok şeyler yapılabilir.

Umarız onlar da bir gün olur. Yani sizin başladığınız günlerden bugünlere kadar çok şey değişti. "Sermaye azdı, bir şeyleri yurt dışından almak zordu, insan sayısı azdı" dediniz. O günlerden bugünlere geldik.

Türkiye'nin o günleri ile bugünlerini karşılaştırdığımızda arada dağlar kadar fark olduğunu görüyorsunuz. Demek ki bir süre sonra o tarihle bugün arasında da dağlar kadar fark olacak.

Güzel sohbetiniz ve bizi ağırladığınız için çok teşekkür ederiz.

Rica ederim, benim için de bir zevkti.

Duran LEBLEBİCİ kimdir?

14 Mart 1935'te Çorum'da doğdu. İlk ve orta öğrenimini Çorum'da tamamladıktan sonra girdiği İTÜ Elektrik Fakültesi Zayıf Akım Kolu'ndan 1958'de yüksek mühendis olarak mezun oldu. Kara Harp Okulu'nda elektronik öğretmeni olarak yaptığı askerlik hizmetinin ardından 1960'ta İTÜ Elektrik Fakültesi Yüksek Frekans Tekniği Kürsüsü'nde asistan olarak görev aldı. 1962-63 yılları arasında "Philips International Institute of Technological Studies" adlı lisans üstü programına devam ederek diploma aldı. 1966'da İTÜ'de doktora çalışmasını tamamlayarak doktor mühendis ünvanını aldı. 1971'de doçent, 1977'de profesör oldu. 1982-1997 yılları arasında Elektronik Anabilim Dalı başkanlığı yaptı. 1978-79 yıllarında Elektrik Fakültesi dekan yardımcılığı, 1984-85'te Elektronik ve Haberleşme Bölümü başkanlığı, 1985-87'de Elektrik-Elektronik Fakültesi dekanlığı ve 1987-92'de İTÜ rektör yardımcılığı görevlerinde bulundu. Mart 2001'de İTÜ'deki görevinden emekli oldu. Halen İTÜ'de, CMOS Yüksek Frekans Devre Tasarımı dersini vermeye devam etmektedir.

Duran Leblebici 1975-77 yıllarında İTÜ'de Türkiye'nin ilk mikroelektronik laboratuvarının kurulmasında görev aldı. 1980'de Türkiye'de ilk MOS transistörlerin ve MOS tümdevrelerin gerçekleştirildiği Yarıiletken Teknolojisi Araştırma Laboratuvarı'nın (YİTAL) TÜBİTAK-MAE'deki (Marmara Araştırma Enstitüsü) kuruluş çalışmalarında bulundu. 1977-81 yıllarında TÜBİTAK Mühendislik Araştırma Grubu üyesi, 1981-85'te TESTAŞ Yönetim Kurulu üyesi, 1997-2000'de TÜBİTAK Elektronik ve Enformatik Araştırma Grubu üyesi olarak görev yaptı. başlanmış olan de değerlendirildi. 1989'da Türkiye'nin önde gelen elektronik sanayii kuruluşlarının desteği ile, öncelikli amacı Türkiye elektronik sanayiinin tümdevre teknolojilerine yönlendirilmesi olarak tanımlanmış olan İTÜ-ETA Vakfı'nın (İTÜ-İleri Elektronik Teknolojileri Araştırma ve Geliştirme Vakfı) kuruluşuna öncülük etti. Vakıf 1991'de Türkiye'nin ilk profesyonel tümdevre tasarım merkezini kurdu ve burada ülkedeki sanayi kuruluşlarının ihtiyaçlarına uygun tümdevrelerin tasarımları yapılmaya başlandı. Prof. Leblebici halen Türkiye Elektronik Sanayicileri Derneği (TESİD) Yüksek Danışma Kurulu üyesi ve İTÜ İleri Elektronik Teknolojileri Araştırma ve Geliştirme Vakfı (İTÜ-ETA Vakfı) Yönetim Kurulu üyesidir. Vakfın ortak olduğu Mikroelektronik Ar-Ge, Tasarım ve Ticaret Ltd. Şti. yönetiminde vakfı fahri olarak temsil etmektedir.

Duran Leblebici'nin çeşitli tarihlerde İTÜ'de yayınlanmış üç adet Türkçe ders kitabı (Elektronik Elemanları, Elektronik Devreleri, Analog Elektronik Devreleri) ve oğlu Yusuf Leblebici ile yazdığı bir İngilizce ders kitabı (Fundamentals of High Frequency CMOS Analog Integrated Circuits) vardır.

Prof. Dr. Duran Leblebici 1992'de "mikroelektronik teknolojisinin ülkemize kazandırılması yolunda yaptığı ve yapmakta olduğu önderlik ve hizmetler nedeni ile" TÜBİTAK Hizmet Ödülü ile ödüllendirilmiştir.

Evlidir (Yıldız Leblebici), evli bir oğlu (Yusuf-Anıl Leblebici) ve bir torunu (Ebru) vardır.

BİLİMSEL DÜŞÜNCEYİ HAYATA GEÇİRMEK

Nur YANANLI

Bilimsel düşünce deyince ilk olarak aklımıza müspet (pozitif) bilimler geliyor. Fakat bilimsel düşüncenin faaliyet alanı sadece müspet bilimlerle sınırlı kalmamalıdır. Her meslek dalında, akademik olan veya olmayan her ortamda hatta kişisel meselelerde kısacası hayatın tüm alanlarında kullanılmalıdır. Sadece bilim adamının değil her insanın bizzat uyguladığı ve doğru arayışında takip ettiği yol olmalıdır.

Günlük hayatta bilimsel düşüncenin kullanılması düşüncelerimize, davranışlarımıza ve algılayışımıza yerleşmiş ve kendini gizlemiş yanlışların düzeltilmesi açısından çok önemlidir. Çünkü yanlışlar fark edilmediği ve düzeltilmediği takdirde sürekli tekrarlanarak kişilerin algılayışında normalleşir ve zamanla benimsenerek doğru olarak kabul görür. Bu yanlışlar, düşünmeden kabullenilen gelenekler, alışkanlık haline gelmiş sorgulanmayan davranışlar, fikirler ve yaklaşımlar ile hayatımıza girerler. Genellikle masum değerlerin arkasına sakladıkları için fark edilmeleri çok zordur. Farkedilmemelerinin diğer bir sebebi de sorgulanmadan yaşanan hayat tarzıdır. Bu hayat tarzı yanlışların ortaya çıkmasını engelleyerek insanların ömür boyu toplumların ise asırlarca aynı yanlışlar içinde kalmasına sebep olur.

Doğru olarak benimsenmiş bu yanlışların fark edilmesi ancak bilimsel düşüncenin sorgulayan, şüpheci yaklaşımı ile mümkündür. İnsan olarak hedefimiz doğruya ulaşmak olduğuna ve yanlışlarla da doğruya ulaşamayacağımıza göre her insanın fikirleri, algıları ve davranışları sorgulaması gerekir. Sorgulama yanlışların fark edilmesi için gerekli olan ilk adımdır. Sonraki adımlar ise yanlışların tarafsız, önyargısız gözlemler ile analiz edilmesi ve yapılacak akılcı değerlendirmelerle düzeltilmesidir. Böyle bir yaklaşım kişiyi de toplumu da her zaman olduğu noktadan daha doğruya daha ileriye götürecektir.

Bilimsel düşüncenin yalnız müspet bilimlerle veya bilim adamları ile sınırlandırılması, insan hayatının büyük bir bölümünü oluşturan sosyal konuların bilimsel yaklaşımdan ve dolayısıyla akılcılıktan uzaklaşmasına sebep olur. Günlük yaşantıdan bilimsel yaklaşımın ve beraberinde akılcılığın dışlanması ise toplumları felakete sürükleyecek sonuçlar doğurur. Bu felaketi anlayabilmek için kişisel ve toplumsal hayatın bilimsel düşünce ve akılcılıktan yoksun olmasının sakıncalarını birkaç madde ile özetleyelim:

• Aklın girmediği konular dogma haline gelir ve dokunulmazlaşır. Dokunulmaz hale geldiği için bu konular içindeki yanlışlar asla düzeltilemezler. Ayrıca akla dayalı yorumlar yapılmadığı için dogma haline gelen fikirler mana ve derinlikten uzaklaşarak yüzeyselleşir.

• Akıl kullanılmadan, alışkanlık veya gelenek haline gelmiş işler bilinçli olmadığı için değerli ve kalıcı değildir. Yapılan işten olumlu bir sonuç elde edilmiş olsa bile tesadüfidir. Ancak neden, nasıl gibi sorulara bulunan akılcı cevaplar ile yapılan işler başarıya ve hedefine ulaşır.

• Sosyal hayatta aklın kullanılmaması kızgınlık, kin, nefret, hırs gibi duyguların kişilere hakim olmasına neden olur. Böyle toplumlarda cinayetler, incir çekirdeğini doldurmayan konulardan kavgalar, nesilleri etkileyecek kan davaları günlük sıradan olaylara dönüşür. Oysa ki akıl, duyguların frenidir ve onların kontrol edilmesini sağlar.

• Bilimsel düşünce ile manevi olguların birbirinden ilgisiz konular olduğu düşünülür. Ama tam aksine akıl olmazsa ahlak da gelişemez. Ahlak ancak kendinden şüphe eden, davranışlarını sorgulayan, üzerinde düşünen ve doğruyu arayan bir akılla gelişir. Bu yüzden sosyal alanda akılcılığı hayata geçiremeyen toplumlarda büyük ahlaki çöküntüler yaşanır.

• Bilimsel düşüncenin egemen olmadığı toplumlarda kişiler farkında olmadan geleneklerin, çoğunluğun ve güç odaklarının etkisi altına girerler. Bu etkiler altında kişilerin bireyselleşmesi, dolayısıyla özgür bir şekilde düşünmesi engellenir. Bireyselleşmenin olmadığı, toplumsal bakışın hakim olduğu yerlerde yanlışlar görülemez hale gelir. Çünkü kalabalıklar hep aynı yöne bakar, dolayısıyla farklı bir doğrultudaki doğruyu göremez.

• Bilimsel düşünce yöntemi ile yetiştirilmeyen gençler sorgulamadıkları için beyin yıkama faaliyetlerinin hedef kitlesi haline gelir.

Bilimsel düşünce veya bilimsel yaklaşım dediğimiz bu yöntem nedir?

Montaigne "Allah'ın insanlara en adilce dağıttığı nimet akıldır. Çünkü hiç kimse akıl payından şikayetçi değildir," der. Her insan akıllı olduğunu ve düşündüğü her şeyin doğru olduğunu sanır. İşte bu zan, insanın aklını kullanmasına, düşünmesine engel olur. Olması gereken, asıl düşünce yöntemi bilimsel düşüncedir. Bilimsel düşünce eski bildiklerimize, kabullerimize, zanlarımıza şüpheyle yaklaşarak, araştırarak, sorgulayarak, tarafsız gözlem yaparak, önyargılardan arınmış saf aklı kullanarak zamana ve mekana göre değişmeyen mutlak doğrulara ulaşma yolu veya yöntemidir.

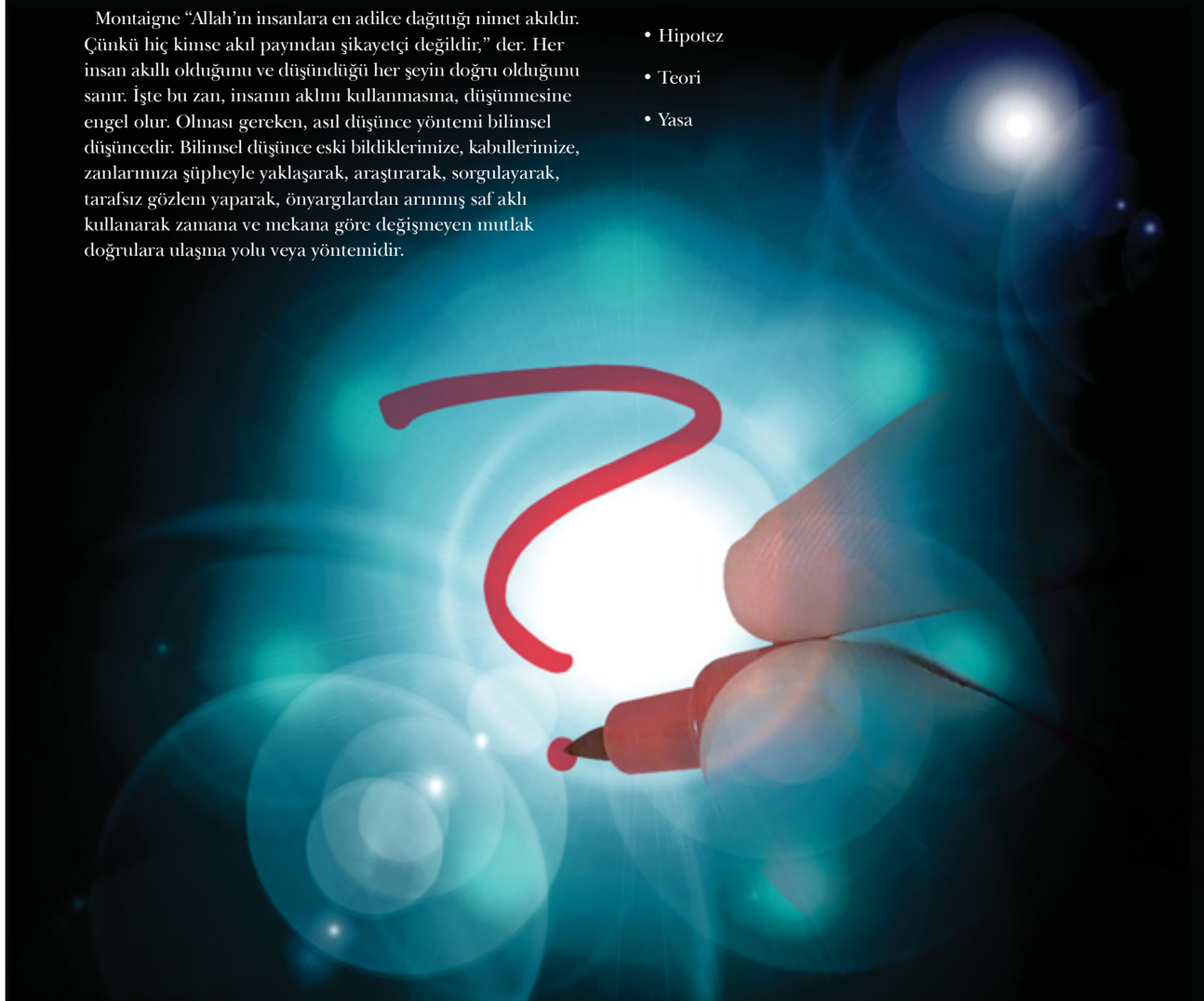
Bilimsel düşünce genellikle şu adımlar ile tarif edilir:

• Tez

• Hipotez

• Teori

• Yasa



Fakat bu adımları gerçekleştirmek için olması gereken başka unsurlar da vardır. Bilimsel düşüncenin ilk adımı bilinenlere şüpheyle yaklaşmaktır. Bir tez ortaya atabilmek için öncesinde bilinenlere şüphe ile yaklaşmak gerekir. Ancak şüpheci yaklaşımı gerçekleştirmek oldukça zordur. Çünkü insan genellikle bildiğinden emindir. Zanlarını bilgi, bu bilgiyi de kayıtsız şartsız doğru kabul eder. Kabullerle gelen bu eminlik hissi insanda şüpheyi ve sorgulamayı ortadan kaldırır. İnsan çoğu zaman kabul ettiklerinden o kadar emindir ki defalarca aynı hatayı yapıp, tökezlese de dönüp bildiğinden şüphelenmez, kendine neden diye sormaz.

Gerçeği arayan, düşüncesini tartmalı şüpheyle
Bulduğundan emin olan, sınırlanır bildikleriyle
Derse hep "Ben bilirim", gidemez öteye, çeker çile
Kuşku duymalı zanlardan yaşamak için gerçeklerle

Şüphe doğruya ve gerçeklere açılan kapıdır. Tabii her zaman tahmin edilen doğruyla bulunan doğru aynı olmayabilir. Bazen de bulunan doğru, eski bilinen doğru olabilir. Sonuç ne olursa olsun bilimsel düşünce sonrasındaki biliş ile öncesindeki biliş arasında fark vardır. Bilimsel düşünce sonunda bilinç oluşur, öncesinde ise körü körüne bir inanış vardır sadece.

Ortaya atılan tezler genelde bilinenlerin dışında veya bilinenlere tezat teşkil edecek şekilde olur. Alışılagelmişin dışında olmaları yeni fikirlerin ve tezlerin her zaman tepkiyle karşılaşmasına yol açar. Bu tarz yaklaşımlar yeni fikirler üretilmesinin yolunu keser. Unutmamalıdır ki; ortaya atılan fikirler veya tezler insanları düşünmeye sevk ettiği, düşünce ufkunu genişlettiği için önemlidir. Yeni fikirlere karşı tutucu yaklaşımı ortadan kaldıracak olan yine bilimsel düşünce yöntemidir. Çünkü bilimsel düşünce baskılardan, tabulardan ve önyargılardan kurtulmuş, özgür, tarafsız düşünce yöntemidir.

Tez kadar antitezler de önemlidir. Çünkü aynı yönden bakmak insanı hataya sürükler. Antitezler farklı bakış açıları sunduğu için üzerinde düşünülen fikrin birçok boyutuyla görülmesine ve dolayısıyla tam olarak kavranabilmesine imkan sağlar. Antitezler değerlendirilirken de yine baskısız, çıkarsız, özgür bilimsel düşünce yönteminin kullanılması gerekir. Önemli olan tezi veya antitezi ispatlamak değil doğruyu bulmaktır.

Doğruya duymalı iştiyak, dürüst olmalı muhakkak
Kendi fikrini kabul ettirenle, sağlanmaz ittifak
Yanlışı anladığında doğruya etmeli iştirak
Duyunca gerçeği, demeli hasmına, haklısın el-hak

Bilimsel düşüncede şüpheden sonra gelen adım sorgulama, araştırma ve incelemedir. Ancak bu sorgulamayı da tarafsız bir şekilde yapmak gerekir. En son aşama ise elde edilen verileri akılcı bir şekilde yorumlamaktır. Yorumlarken de yine bilimsel düşüncenin ilkelerini izleyen, tabulardan ve önyargılardan kurtulmuş, özgür bir yaklaşıma sahip olmak gerekir.

Bilimsel yöntemler müspet bilimlerde zaten kullanılıyor. Asıl önemli olan insan hayatını doğrudan ilgilendiren konularda bilimsel düşüncenin kullanılmasıdır. Geçmişin ve genelin yanlışları içinde doğup büyüyen insan, yanlışlardan ancak bilimsel düşünce yöntemi ile kurtulabilir. Bu sebeple bilimsel düşünce yöntemi kişisel gelişimden, sosyal hayata kadar hayatın bütün alanlarına uygulanmalıdır.

ŞİFRESAYAR

Umut ULUDAĞ

soru 1

Üniversitede aldıkları Kriptoloji dersinde, gizli paylaşım (secret sharing) algoritmaları anlatılırken, Ayşe-Bora-Erol-Güven dörtlüsü, 1.984.909 sayısının asal çarpanlarını bulmaya çalışıyorlar ve konunun özünü kavrayamadan dersleri bitiyor. Akıllarında kalan kısımlarla, kendilerine bir gizli paylaşım algoritması tasarlıyorlar. Bu algoritmaya göre, Ayşe ve Bora,

B U D E R S T E N S I N I F T A K A L D I K

bilgisini,

Ayşe: B D R T N I I T K L I

Bora: U E S E S N F A A D K

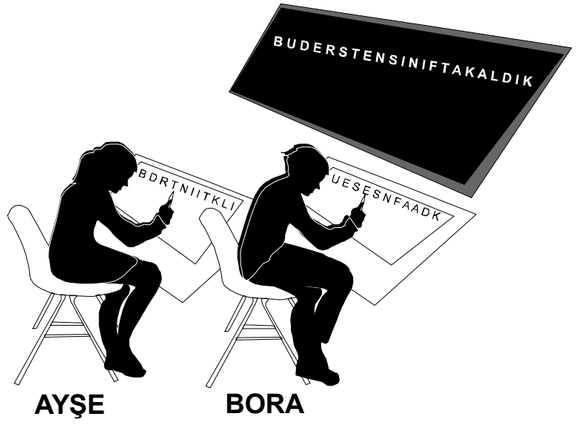
olarak paylaşıyorlarsa, Ayşe-Bora-Erol-Güven dörtlüsü aşağıdaki paylaşım ile hangi bilgiyi saklamaya çalışmaktadır?

Ayşe: V N E Ğ M E R R O İ K L Y A K O Ğ K M E Ğ M A

Bora: E İ Ç İ E R D İ L K N E G N T K İ H E R L A D

Erol: R N T H N Y E P O T İ R U M A D Ş İ T S A K I

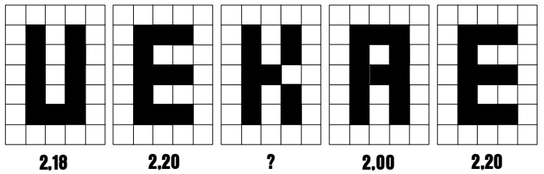
Güven: İ G İ E H E K T J E K U L A Ç E İ Z L A N T R



soru 2

2, 3, 5, 7, 2, 4, 8, 10, 5, 11, 4, 10, 5, 7, ?

soru 3



soru 4

Açık Yazı	Gizli Yazı
İŞTE ŞİFRE	ĞVÜL ĞTHLÜ
?	YÖÇN PRBUÇNLHLVTĞU LCĞNTĞÖ

soru 5

Aşağıdaki olasılıklardan hangisi daha büyüktür?

(i) Melahat'in, bir saniyede 1.000.000.000 anahtarın doğruluğunu deneyebilen makinesini kesintisiz olarak her gün çalıştırdığında, Ayşe'nin 128 bitlik rastgele seçilmiş anahtarını, 1 yıl (365 gün) içinde bulma olasılığı,

(ii) Can'ın, 3 hafta boyunca, her hafta yalnızca 1 kolon sayısal loto oyunu oynayıp, bu 3 haftanın 3'ünde de büyük ikramiyeyi veren 6 numarayı doğru bilme olasılığı.

Not: Sayısal loto oyununda, her hafta, 1-49 arası numaralardan 6 tanesi tekrarsız olarak rastgele seçilmekte, oynanan bir kolonda oyuncunun belirttiği 6 numara, seçilen 6 numara ile aynı ise, büyük ikramiye kazanılmaktadır.

soru 6

Tek alfabeli yerleştirmeyle (monoalphabetic substitution) şifrelenmiş metinlerin çözümünde, uzunluğu belirli, tekrar eden harflerin aynı konumda bulunduğu örnek kelime listelerinden yararlanılabilir. Bu listelerde, eldeki kelimenin harfleri A, B, C,... gibi harflerle gösterilmekte ve tekrarlar olduğunda karşı düşen tekrar harfi kullanılmaktadır:

Yapı	Örnek kelimeler
ABACD	YAYIN, SUSAM, TATLI, ELEĞİ, ARACI...

Bu sisteme göre, aşağıda verilen yapıların her biri için en az 3 adet örnek Türkçe kelime bulunuz.

Yapı	Örnek kelimeler
ABCDB	?
ABCBDB	?

Şifresayar bölümündeki 6 sorudan en az 3 tanesini doğru cevaplayıp, çözümlerini iletişim bilgileriyle birlikte odullusoru@uekae.tubitak.gov.tr e-posta adresine, "UEKAE Dergisi: Şifresayar" konu bilgisi ile 31 Aralık 2010 tarihine kadar gönderenler arasından kura ile belirlenecek 5 kişiye TÜBİTAK Popüler Bilim Kitapları arasından seçilen kitaplar hediye edilecektir. Soruların cevapları derginin bir sonraki sayısında yayınlacaktır. Ödüllü diğer sorulara www.uekae.tubitak.gov.tr adresindeki "Ödüllü Kriptoloji Soruları" bölümünden ulaşabilirsiniz.

TÜRKİYE AKLINI KULLANIYOR

akiş

Akıllı Kart İşletim Sistemi

- TC Kimlik Kartı ile güvenli kimlik doğrulama
- e-Devlet kapısına erişim
- e-Pasaport
- Sayısal imza taşıma aracı

AKiS: Akıllı kartların yönetilebilmesi ve uygulamalarının çalışması için gerekli olan akıllı kart işletim sistemidir.

www.uekae.tubitak.gov.tr

TÜBİTAK
UEKAE