Elektronik Kimlik Doğrulama Sistemi

Elektronik İmza ile Buluşma Noktanız...

İÇİNDEKİLER

Doküman Tarihçe

Versiyon	Tarih	Yazar	Yorum
1.0.1	17.12.2018	Ümit Yaşar USTA	İlk Yayın
1.0.2	07.01.2019	Ümit Yaşar USTA	Düzeltmeler
1.0.3	01.08.2024	N. Atilla BİLER	Güncelleme

1. Yönetici Özeti

Ürün ve/veya hizmet sağlayan firmaların ve kurumların, doğru kişiye ürün/hizmet verebilmesi için “kimlik doğrulama” en temel ihtiyaçtır. Müşteri sözleşmeleri, abonelik işlemleri, kamu hizmetleri ve sosyal güvenlik hizmetleri gibi pek çok işlem, her zaman kimlik doğrulama ile başlar ve tüm süreçlere hizmet alan kişinin kimliği entegre edilir. Pek çok kanun ve yönetmelik, sunulan hizmetler için kişilerin kimliğinin doğrulanmasını şart koşar. Şahıslar ve kurumlar arasında bir anlaşmazlık durumunda, kurumların verilen hizmete ilişkin yaptığı kimlik doğrulamanın ispatı gerekir. Benzer şekilde işlemi inkâr eden müşterinin de yapılan kimlik doğrulama işleminin geçersiz veya yanlış olduğunu ispatlaması gerekir.

1970’lerde çıkarılan ve bugün halen kullanımda olan nüfus cüzdanları, gelişen teknoloji ve uygulanan pek çok yeni sahtecilik yöntemlerine cevap veremediği için, firmalar ve kurumlar son 40 yılda ilave yatırımlar ile ekstra kimlik doğrulama yöntemleri geliştirmeye çalışmışlardır. Birbirinden kopuk, kapalı çevrim bu ilave kimlik doğrulama yöntemleri, genel olarak geçerli ortak bir standarda dayanmadığı gibi, güvenlik seviyeleri de o kurumların kendi personelinin değerlendirmesi ile sınırlı kalmıştır. Kullanılan çözümler yeni saldırı yöntemlerine cevap verememiş ve sürekli farklı yatırımlar ile yenilenmek zorunda kalmıştır. Bu nedenlerden dolayı özellikle farklı kamu kurumlarında mükerrer yatırıma ve tasarruf zafiyetine sebep olmuştur. Vatandaşlar açısından da bir kurumda avuç içi kimlik doğrulama yapılırken, diğer bir kurumda yüz tanıma, başka bir kurumda da SMS şifre kullanılması gibi yöntemler kafa karışıklığı yaratmış, sosyal mühendislik saldırılarına karşı zafiyet oluşturmuştur. Vatandaşlar kendi adlarına sahte kimliklerle işlem yapan kötü niyetli kişilerce dolandırılma riski taşırken, firmalar ve kurumlar maddi kayıplar ve itibar zedelenmesi ile karşılaşmıştır.

Gelişen teknolojiler, uluslararası standartlar ve düzenlemeler incelenerek, teknik anlamda TÜBİTAK BİLGEM Başkanlığının araştırmaları ve katkılarıyla, tamamen yerli ve milli Elektronik Kimlik Doğrulama Sistemi standartları ve güvenlik kriterleri oluşturulmuş, Türk Standardları Enstitüsü (TSE) tarafından yayınlanmıştır. Bu standartlar kapsamında, kopyalanamayan yeni çipli kimlik kartların kullanımı ve dijital sertifika, PIN, parmak izi, dijital fotoğraf gibi unsurlar ile çoklu kimlik doğrulama yapılması öngörülmüştür.

Bu amaçla T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri (NVİ) Genel Müdürlüğü tarafından 20.10.2020'de "Elektronik Kimlik Doğrulama Sistemi (EKDS) Yönetmeliği" yayımlanmış, elektronik kimlik doğrulama süreçleri ve ilgili Kimlik Doğrulama Hizmet Sağlayıcıların (KDHS) kuruluş ve faaliyetleri düzenlenmiştir.

(EKDS Yönetmeliği: https://www.resmigazete.gov.tr/eskiler/2020/10/20201022-15.htm)

Yeni çipli kimlik kartları aynı zamanda Kişisel Verileri Koruma Kanunu (KVKK) kapsamında, kişilere ait verileri korumakta ve sadece yetkili kurumların yetkili oldukları alanları okuyabilmesini sağlamaktadır. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünce yürütülen çalışmalar ile 2024 yılı itibariyle, 80 (seksen) milyonu aşkın vatandaşımıza yeni çipli kimlik kartları dağıtılmıştır ve ayda ortalama 1 milyon üzerinde kart dağıtımı devam etmektedir.

Bu doküman; her vatandaşımızın kolayca cebinde taşıyabileceği yeni çipli T.C. Kimlik Kartlarının kullanımını ve elektronik ortamda nasıl doğrulanacağını anlatmaktadır. Bu yeni sistemin faydalarını, kullanılan standartları ve çözümün temel bileşenlerini, tüm firmaların ve kurumların ilgili yöneticilerine saygıyla sunarız. Kimlik sahteciliğini önleyebilmek, vatandaşların mağduriyetlerini, kurumların maddi ve itibar kayıplarını azaltabilmek, kamuda mükerrer yatırımları önleyip tasarrufu arttırabilmek temel hedefimizdir.

2. Genel Kimlik Doğrulama Yöntemleri

Kimlik doğrulama, genel anlamda yüz yüze **fiziksel kimlik doğrulama ve elektronik kimlik doğrulama** olarak ikiye ayrılabilir;

- **Fiziksel Kimlik Doğrulama:** Çok eski zamanlardan beri süre gelen bu kimlik doğrulama yönteminde, hizmeti veren kurum çalışanı görevli, hizmeti alacak olan müşteri/vatandaşın kimlik belgesini (nüfus cüzdanı, ehliyet, üye kartı gibi), belge üzerindeki fotoğraf, logo, mühür, soğuk damga, hologram gibi öğeleri **göz ile kontrol ederek doğrulama**ya çalışır. Bu tip kimlik doğrulama yöntemi **insan hatalarına çok açıktır**. Görevli, şahsen hizmet alanı tanımıyor ise veya gözle bakarak sahte belgeyi tanıyabilecek kadar kimlik uzmanı değilse, kolayca sahtekarların hedefi olabilir. Bu duruma nakit paraların kullanımı örnek verilebilir. Vatandaşların büyük çoğunluğu bu konuda uzman olmadığı için iyi taklit edilmiş bir kağıt parayı gerçek zannedebilir ve ürün/hizmeti o kişiye verebilir. Bu nedenle çıkarılan kredi kartları ve banka kartları fiziksel doğrulamayı elektronik doğrulamaya geçirerek, uzman olmayan kişilerin bile sahte işlemleri kolayca tespit edebilmesini sağlamıştır.

- **Elektronik Kimlik Doğrulama:** Kredi kartı kullanımından çok tanıdık olduğumuz bu kimlik doğrulama yönteminde kimlik kartı, görevli kişi tarafından göz ile değil, bir cihaz aracılığıyla elektronik ortamda doğrulanmaktadır. Ödeme kaydedici cihazlar sayesinde kredi kartı sahteciliği önlendiği gibi, Hazine ve Maliye Bakanlığı tarafından denetlenebilmek ve vergi kaçakçılığını önlemek için dijital kayıtlar da oluşturulabilmektedir. Elektronik kimlik doğrulamada 3 (üç) farklı unsur kullanılabilmektedir; **sahip olunan şey**, **bilinen bir şey** ve **kişiye ait biyometrik bir özellik**. Örneğin; kredi kartlarında "Chip & PIN" kullanımında, sahip olunan unsur bankanın vatandaşa verdiği çipli kredi kartı ve bilinen şey ise karta ait PIN numarasıdır. Üç farklı unsurdan herhangi ikisinin kullanıldığı çözümler 2-faktör kimlik doğrulama, her üç unsurun kullanıldığı çözümler 3-faktör kimlik doğrulama olarak sınıflandırılır. Yeni çipli kimlik kartları hem 2-faktör hem de 3-faktör kimlik doğrulamayı (çip, PIN, parmak izi) destekler.

Biyometrik kimlik doğrulama sınıflandırması ise genel anlamda **çevrimiçi ve çevrimdışı biyometrik kimlik doğrulama** olarak ikiye ayrılabilir:

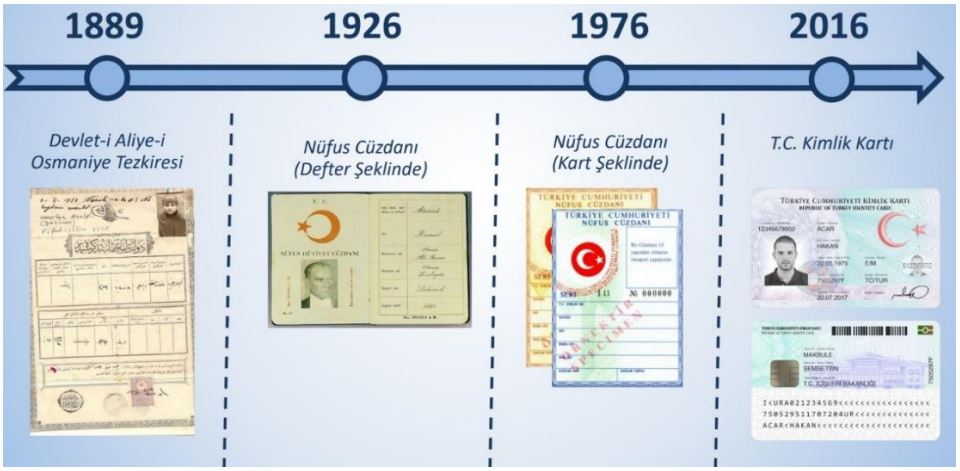
- **Çevrimiçi Biyometrik Kimlik Doğrulama**: Kişilere ait biyometrik veriler (parmak izi, dijital fotoğraf, avuç içi izi, vb.) veya bu verilerden bir algoritma ile türetilmiş veriler, merkezi veri tabanlarında kayıt edilir. Kişi kimlik doğrulama noktasında biyometrik verisini bir cihaza (biyometrik sensor ve/veya kamera gibi) tanıtır ve bu veriler merkeze iletilerek merkezde eşleştirilir. Bu tip sistemlerde en büyük tehlike, verilerin uç noktalardan merkeze iletilirken veya merkezde depolanırken kötü niyetli başka kişilerin eline geçebilme riskidir. Kurumda çalışan **kötü niyetli bir çalışan veya bilgisayar korsanları bu merkezi veri tabanlarına veya iletişim hatlarına saldırabilir**, kişilere ait biyometrik verileri veya türetilmiş verileri ele geçirebilir, kopyalayabilir ve başka amaçlar için kullanabilir. Ayrıca biyometrik verinin

sahibi kişiler, hizmet aldıkları kuruma parmak izini, fotoğrafını vermek istemeyebilir ve bu talep Kişisel Verileri Koruma Kanunu (KVKK) kapsamında bireylerin hak ve özgürlüğüdür.

- **Çevrimdışı Biyometrik Kimlik Doğrulama**: Kişilere ait biyometrik veriler veya bu verilerden türetilmiş hiçbir veri merkezde kayıt ve kontrol edilmez. Kişiye ait biyometrik veri, yine o kişiye ait kopyalanamayan ve güvenlikli çipli bir kartta saklanır. Kimlik doğrulama yapması gereken kişi, güvenlik onaylı bir cihaza hem çipli kimlik kartını hem de biyometrik verisini verir. Eşleştirme işlemi kişinin gözetiminde güvenlik onaylı cihazda çevrimdışı gerçekleşir. **Kişisel veri hiçbir yere kaydedilmez, gönderilmez ve saklanmaz**. **Kişisel Verileri Koruma Kanununa (KVKK) da uygun** olan bu yöntemde kişiye ait biyometrik veri yine kişiye ait çipli kartta kalır. Çevrim dışı gerçekleşen biyometrik kimlik doğrulama sonucu (pozitif/negatif), güvenlik onaylı cihazda yer alan başka bir çipli kart (Güvenli Erişim Modülü) ile elektronik olarak imzalanıp kurum merkezine iletilir. Kurum merkezi doğrulamanın sonucunun değişmeden iletildiğini elektronik imzayı kontrol ederek değerlendirir ve sonucu pozitif/negatif olarak kayıtlarına geçirir. Elektronik imzalı sonuç kaydı ileride oluşabilecek anlaşmazlıklarda delil niteliği taşır. Bu yöntem yeni çipli kimlik kartlarının temelini oluşturmaktadır.

3. Türkiye'de Nüfus Cüzdanının Tarihçesi ve Yeni Çipli Kimlik Kartları

Ortalama her 40 yılda yeni bir nüfus cüzdanı formatı, gelişen teknolojilere uygun olarak tanımlanmıştır. Aşağıdaki şekilde (Şekil-1) nüfus cüzdanlarının geçirdiği evreler görülebilir. Halen az sayıda da olsa kullanılmakta olan **eski nüfus cüzdanları, 1976'da kullanılmaya başlanmıştır** ve o günün güvenlik unsurları baz alınarak hazırlandığı için günümüz ihtiyaçlarına cevap verememektedir. Bu nedenle, uzun süren araştırmalar sonucunda, uluslararası standartlar ve güvenlik kriterleri de dikkate alınarak, ülkemizin en önemli Ar-Ge kurumu TÜBİTAK BİLGEM tarafından yeni çipli kimlik kartları tasarlanmıştır. Projede **Ortak Kriterler (CC) EAL 4+ güvenlik seviyesine sahip** ve **20 (yirmi) yıla yakın bir süredir elektronik imza (e-imza) için de kullanılan milli akıllı kart işletim sistemi (AKİS) kartları** kullanılmaktadır.



Şekil-1: *Nüfus Cüzdanlarının Tarihçesi*

Yeni çipli kimlik kartları kopyalanamaz özelliğe sahiptir. E-imza'da olduğu gibi, kişiye ait özel kriptografik anahtar, kart sahibine özel üretilir ve kart dışına çıkarılamaz. Sadece kart sahibinin bildiği PIN ile kimlik doğrulama amaçlı dijital imza oluşturulabilir. Kimlik kartlarına istenirse yetkili Elektronik Sertifika Hizmet Sağlayıcılarından (ESHS), Nitelikli Elektronik Sertifika (NES) yüklenebilir.

20 (yirmi) yıla yakın bir süredir e-imza alanında güvenliği ispatlanmış AKİS kartları aynı zamanda, **kimlik kartı projesine özel ek güvenlik fonksiyonları** içerir:

- **Kişiye ait özel veriler** (Anne Adı, Baba Adı, Doğum Yeri ve Tarihi, Cinsiyeti, Medeni Hali, Dini, Kan Grubu, Anne Kızlık Soyadı, Veriliş Tarihi, Acil Sağlık Bilgileri, Dijital Fotoğrafı) rol yetki mekanizması ile korunur. Kimlik kartından bu özel verileri okumak isteyen kurumların Nüfus ve Vatandaşlık İşlerinden (NVİ) **okuma izni ve rol sertifikası** almaları gerekir. Gerekli yetki sertifikası ve kriptografik özel anahtara sahip olmayan kurumlar AKİS'ten kişiye özel verileri okuyamaz. **Acil sağlık bilgileri** gibi özel verileri karta yazma işlemi için de benzer şekilde **yazma izni ve rol sertifikası** gerektirir.

- Kişiye ait parmak izi verisi, Nüfus ve Vatandaşlık İşleri (NVİ) tarafından üretilen ve sadece yetkili Kart Erişim Cihazı (KEC) üreticilerine verilen, Güvenli Erişim Modülü (GEM) kartları ile okunabilir. İlerleyen bölümlerde açıklanan bu cihazlar **biyometrik veriyi cihaz üzerinde anlık doğrular, kaydetmez, cihaz dışına çıkarmaz ve herhangi bir merkeze göndermez**. Bu sayede yeni çipli kimlik kartları ile 3-faktör kimlik doğrulama yapılabilir.

4. Nüfus Cüzdanlarının Kullanım Alanları

Nüfus cüzdanları, kimlik doğrulama ve kişiye ait verileri okuyup kayıt etme amacıyla kullanılmaktadır. Sayısız alanda kullanılan nüfus cüzdanlarının bazı **kullanım noktaları ve senaryoları**:

- Sözleşmeleri imzalarken kimlik bilgisi,
- Noterde bir işlem gerçekleştirirken (araç satmak/almak, şirket kurmak, vekaletname çıkarmak vb.),
- Tapu dairelerinde (gayrimenkul alım/satım işlemleri vb.),
- Sınav merkezlerinde,
- Zorunlu mesleki kursların devamlılık takibinde,
- Sosyal Güvenlik Kurumu (SGK) hizmetlerinde,
- Hastanelerde,
- Eczanelerde,
- Okullarda kayıt işlemlerinde,
- Abonelik sözleşmelerinde (elektrik, su, doğalgaz dağıtım, telekomünikasyon ve kablolu TV yayın kuruluşları vb.),
- GSM bayilerinde SIM kart işlemlerinde,
- Banka şubelerindeki hesap işlemlerinde,
- Sigorta işlemlerinde,
- Kargo gönderi ve teslimatlarında,
- Belediye hizmetlerinde,
- Askerlik şubelerinde,
- Kolluk birimleri kontrollerinde (Polis, Jandarma, Sahil Güvenlik, Askeriye),
- Adli işlemlerde,
- Ziyaretçi kabul işlemlerinde,
- NES e-imza başvurularında,
- Üye işyerlerinde ve kredi sözleşmelerinde,

ve daha pek çok kamu hizmetinde, nüfus cüzdanları ile kimlik doğrulama gerekmektedir.

5. Eski Nüfus Cüzdanlarında Yaşanan Başlıca Sorunlar

Kopyalanması ve sahtesinin hazırlanması son derece basitleşen eski kimlik kartları, sadece yüz yüze görüşmeyle ve fiziksel olarak gözle kontrol yöntemi ile doğrulanabilmektedir. İnsan hatalarına son derece açık olan bu kimlik doğrulama yöntemi nedeniyle;

- Başkası adına sahte kimlik ile işlem yapılması, banka hesabı açılması, cep telefonu için GSM SIM kartı çıkarılması, abonelik başlatılması, noterde araba satışı, tapu dairesinde gayrimenkul satışı gibi **vatandaşın mağduriyeti** ile sonuçlanabilecek pek çok sahtecilik mümkündür.
- **Kurumlar maddi kayıplar** yaşayabilmekte, ürün ve hizmetlerini hak sahipleri yerine, kötü niyetli yanlış kişilere sunabilmektedir.
- Ortaya çıkan mağduriyetler ve maddi kayıplar nedeniyle oluşan **adli işlemler** zaman ve ek maddi kayıplar getirmektedir.
- Basında yer alan haberler nedeniyle **kurumlar itibar kaybı** yaşayabilmektedir.
- Kurumlar kendince (standart olmayan) ilave önlemler ve **mükerrer yatırımlar** yapmak zorunda kalmaktadır.
- Kurumlar **pek çok manuel süreci** operasyonlarına ilave etmek zorunda kalmaktadır.
- Kurumlar kimlik tespiti için **kişiye ait verileri (fotoğraf, parmak izi gibi) merkezde saklamaya yönelerek** KVKK adaptasyon zorlukları ve ek güvenlik endişeleri yaşamaktadır.
- Farklı farklı kimlik doğrulama yöntemleri **vatandaşlarda kafa karışıklığı** yaratmakta ve kötü niyetli **sosyal mühendislere yeni zafiyet alanları** yaratmaktadır.
- Basılı belge olması ve elektronik iletişim sağlayamaması nedeniyle, kimlik kartlarının fotokopisi çekilmekte ve kanıt amaçlı saklanmaktadır. **Fotokopi yöntemi ile yetkisiz kurumlar da vatandaşa ait pek çok kişisel bilgiyi depolamaktadır**. Her kurumda bilgilerin kopyalanması ve saklanması yeni tehditleri beraberinde getirmektedir.
- Kurumlar, nüfus cüzdanlarının kopyalarının saklanması için ekstra **kurye ve arşivleme gibi ek maliyetlere** katlanmaktadır.
- **E-imza ile entegre olamadığı için** e-imza sahipleri ek cihaz/kart taşımak zorunda kalmakta, maliyet ve taşınabilirlik sorunları nedeniyle **e-imza yaygınlaşamamaktadır**.

6. Yeni Çipli Kimlik Kartlarının Faydaları

Yeni sistemin sunduğu faydalar vatandaşlar, kurumlar ve kamusal alan için ayrı ayrı değerlendirilebilir:

- **Vatandaşlar İçin Faydaları**:
  - Herhangi bir kurumda kendi adlarına **sahte işlem gerçekleştirilemeyeceği**nden emin olur.
  - Kendi çipli kartlarından **yetkisiz kurumların kişisel verileri okuyamayacağını** bilir.
  - Parmak izi verileri **herhangi bir merkezde veya cihazda saklanmadığı** ve **başka amaçlarla kullanılamayacağı** için huzurlu olur.
  - Her yerde **aynı kullanıcı deneyimi** yaşanacağı için kolay adaptasyon sağlar. (SGK, hastane, noter, banka şubesi, tapu dairesi, sigorta şirketi, GSM bayii, adliye, okul, sınav merkezi gibi tüm kurumlarda aynı kimlik doğrulama mekanizması ve kullanım şekli uygulanır)

- **Kurumlar İçin Faydaları**:
  - Hizmet verdikleri **kişinin kimliğinden emin** olur.
  - Sahte kimlikle yapılan işlemler nedeniyle uğranılan **maddi kayıplar ve itibar kayıpları**ndan korunur.
  - Kimlik doğrulama sürecini dijital süreçlerine entegre edip **manuel süreçleri kaldırarak verimliliği arttırıp, tasarruf sağlar**.
  - Ekstra kimlik doğrulama yöntemleri geliştirmek ve **ilave yatırımlar yapmak zorunda kalmaz**.

- **Ülkemiz İçin Faydaları**:
  - Kamusal alanda **farklı kimlik doğrulama yöntemleri ile kapalı ve tek bir kurumca kullanılabilen sistemler yerine**, tüm kurumlarda çok daha güvenli yeni e-Kimlik kartlarının (T.C. Kimlik Kartları) elektronik doğrulanmasına geçilir ve bu sayede **mükerrer yatırımlar ortadan kalkar**.
  - Kimlik ile ilgili **süreçlerin dijitalleşmesi sağlanır, verimlilik artar ve tasarruflar sağlanır.**
  - **Sahteciliğin ve mağduriyetlerin önüne geçilerek** adli işlemlerde azalma sağlanması gibi ülkemize sayısız fayda sağlar.

7. Uluslararası Standartlar, Milli Çözüm ve Kurumların Katılımı

Yeni çipli kimlik kartları farklı kurumların görüşleri ve farklı alanlardaki katkıları göz önüne alınarak hazırlanmıştır. Bu kurumlardan bazıları; Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (NVİ), TÜBİTAK BİLGEM, Türk Standardları Enstitüsü (TSE), Bilgi Teknolojileri ve İletişim Kurumu (BTK), Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Kişisel Verileri Koruma Kurumu (KVKK), Hazine ve Maliye Bakanlığı Mali Suçlar Araştırma Kurumu (MASAK). Pek çok özel sektör kurum ve kuruluşu da görüş bildirmiş ve pilot çalışmalara katılmıştır. **Çoğulcu bir katılım sağlanması, farklı görüş ve bakış açılarının sisteme dahil edilmesiyle standartların olgunlaşmasında önemli bir rol oynamıştır**.

Geliştirilen Elektronik Kimlik Doğrulama Sistemi için 8 farklı TSE standardı yayınlanmıştır;

- **Elektronik Kimlik Doğrulama Sistemi (EKDS) Standartları**
  - **TS 13678** (Genel Bakış)
  - **TS 13679** (Kimlik Doğrulama Sunucusu)
  - **TS 13680** (Kimlik Doğrulama Politika Sunucusu)
  - **TS 13680** (Rol Sunucusu)
- **Kart Erişim Cihazı (KEC) Standartları**
  - **TS 13582** (Genel Bakış)
  - **TS 13583** (Arayüzler ve Özellikleri)
  - **TS 13584** (Güvenlik Özellikleri)
  - **TS 13585** (Uygulama Yazılım Özellikleri)

Bunların dışında Kart Erişim Cihazları (KEC) için uluslararası geçerliliği olan **Ortak Kriterler (CC) EAL 4+ güvenlik seviyesinde** Koruma Profili (PP) tanımlanmıştır: (*Protection Profile For Application Firmware of Secure SmartCard Reader For National Electronic Identity Verification System v2.8*).

KEC geliştiren firmaların TSE Uygunluk belgesini almasının yanı sıra, yukarıda belirtilen koruma profilindeki güvenlik gereksinimlerini karşılaması, TSE'den akredite olmuş bağımsız bir güvenlik laboratuvarından CC EAL 4+ güvenlik sürecinden geçmesi ve TSE'den Ortak Kriterler EAL 4+ sertifikası alması gerekmektedir. Bu sayede üretici firmaların geliştireceği KEC cihazlarının güvenlik denetimi sağlanmaktadır.

Sistemde kullanılan kriptografik algoritmalar (RSA 2048, AES 256, SHA 256) ve anahtar uzunlukları, uluslararası standartlardadır ve güvenlik seviyeleri günlük hayatımızca sıkça kullanılan web sayfaları (SSL/TLS bağlantılarda kullanılan) ve kredi kartları (bankalarda

kullanılan) ile aynıdır. Bu algoritmaların zafiyeti ve kırılması, mevcut çevrimiçi tüm sistemlerin kırılması anlamını taşımaktadır. Bu algoritmalar sadece ulusal kurumlarımızca değil, aynı zamanda tüm **dünyadaki araştırma merkezleri, üniversiteler ve laboratuvarlar tarafından test edilmekte ve güvenliği teyit edilmektedir**. Ayrıca, sistemin milli olması sayesinde, gerektiğinde ileride oluşabilecek ihtiyaçlara göre, daha güçlü algoritmalara ve/veya anahtar uzunluklarına geçiş yapılabilecektir.

Yatırım yapmak isteyen tüm özel sektör firmaları, yukarıdaki standartlara uygun sistem bileşenlerini geliştirebilirler. Geliştirilen ürünler TÜBİTAK BİLGEM e-Kimlik Laboratuvarı testlerinden geçmek ve TSE Uygunluk Belgesi almak zorundadır. Bununla birlikte KEC cihazlarının, güvenlik testlerinden geçmesi ve CC EAL 4+ sertifikası alması gerekir. Bu standartlar ve testler, güvenlik ve uyumluluk açısından büyük önem taşımaktadır.

8. Yeni Sistemin Temel Bileşenleri

Yeni sistemde kimlik doğrulama noktalarında (örneğin; banka şubesi) kullanılması gereken **uç birimi bileşenleri** ve kimlik doğrulamanın teyit edilip kayıt edildiği (örneğin; banka merkezi) **arka ofis sistemleri** mevcuttur.

- **Uç Birim Bileşenleri (E-Kimlik ve Kart Erişim Cihazı)**

Uç birim hizmet noktasını temsil eder (Örneğin; şube, ofis, üye iş yeri, noter gibi). Uç birimde Kart Erişim Cihazı (KEC) ve vatandaşın elektronik kimlik kartı kullanılır. **Kimlik doğrulamanın gerçekleştiği ve hizmetin sunulduğu noktadır**.

- **Vatandaş Kimlik Kartı**

Vatandaşın sahip olduğu yeni **çipli e-Kimlik kartı**dır (Şekil-2). Kimlik doğrulama işleminde kullanılan yönteme göre kart sahibinin dijital sertifikası, PIN, parmak izi veya dijital fotoğrafı doğrulanır. İşlem tipine ve riskine göre hem görevli e-Kimlik kartı hem de hizmet alan müşteri/vatandaş e-Kimlik kartı elektronik olarak doğrulanabilir.

Şekil-2: *Yeni Çipli Elektronik Kimlik Kartı*

- **Kart Erişim Cihazı (KEC)**

Standartlara ve güvenlik kriterlerine göre farklı firmalarca geliştirilip TSE tarafından belgelendirilen bu cihazlar genel itibarı ile güvenlikli kart okuyucularıdır (Şekil-3). **Cihaz kimlik doğrulamayı kendi üzerinde gerçekleştirir ve kişiye ait PIN, parmak izi, dijital fotoğraf gibi verileri üzerinde saklamaz, cihazın dışarısına çıkarmaz**. Bu özellikler, TSE Uygunluk testleri ve Ortak Kriterler testleri kapsamında bağımsız laboratuvarlarca test edilir.

  - **Donanım bileşenleri**;
    - Hizmet veren (görevli) ve hizmet alan (vatandaş) için **iki kart okuyucusu**
    - **Güvenli Erişimi Modülü** (GEM) için dışarıdan erişilemeyen kart okuyucusu
    - Çevre birimler ile iletişim için **USB, ethernet, kablosuz ağ** (WiFi veya GPRS) modülleri
    - PIN girişi için **tuş takımı**

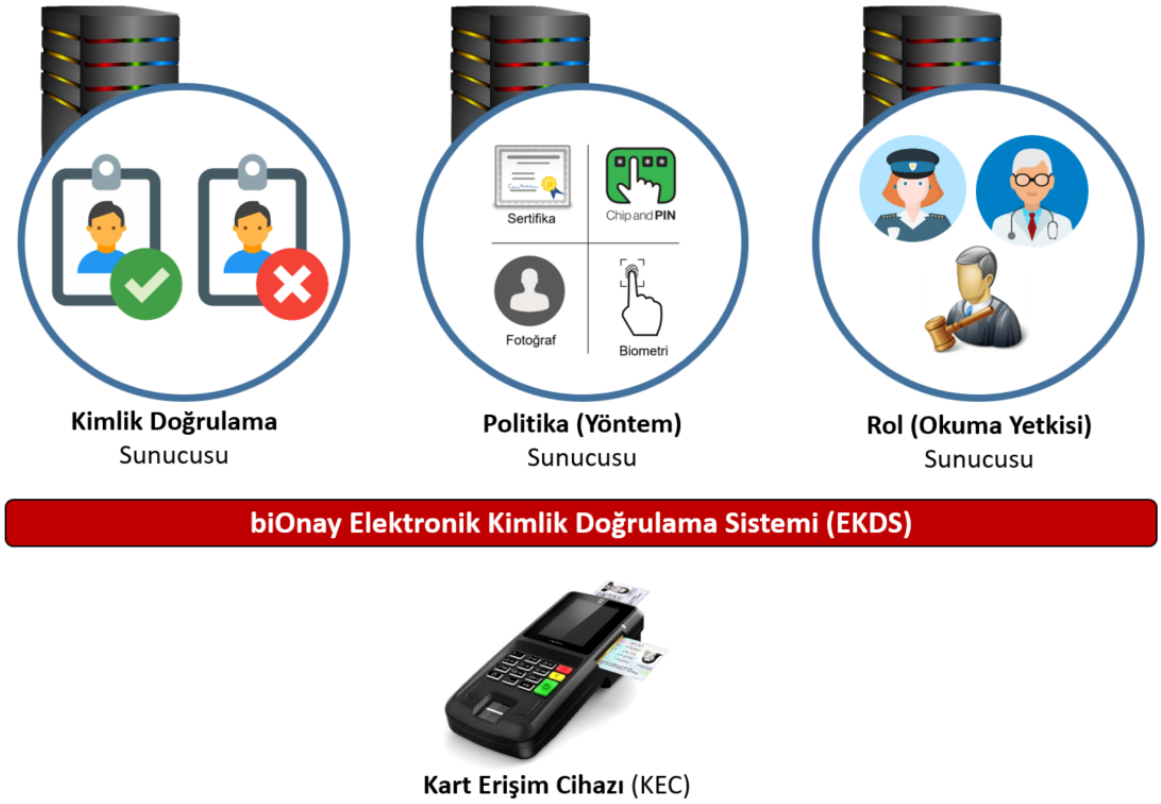
- Parmak izi doğrulama için standartlara uygun (FBI PIV-IQS veya FIPS 201-2 sertifikalarından en az birine sahip) **parmak izi sensörü**
- Fotoğraf doğrulama için **renkli ekran**

- **Güvenlik özellikleri**;
  - Dışarıdan müdahalelere karşı koruma ("**Tamper Protection**"- cihaz kasası açıldığında içerisindeki kripto anahtarlar kullanılamaz duruma gelir)
  - Nüfus İşlerine ait **Güvenli Erişim Modülü** (GEM) kartı ile kriptografik işlemler
  - Yazılım müdahalelerine karşı güvenli yazılım başlatma (**Secure Boot**)
  - **Gerçek zamanlı rastgele sayı üretici** için donanımsal kripto modül
  - Elektronik kimlik kartı sahibinin PIN veya parmak izini cihaza vermeden önce, cihazın orijinal olduğunun, müdahale edilmemiş olduğunun, onaylı bir cihaz olarak içerisinde NVİ'nin onaylı GEM kartını barındırdığının teyidi için kart sahibinin bildiği, **çipli karttaki kişisel mesajın KEC ekranında kart sahibi vatandaşa gösterilmesi**

Şekil-3: *biOnay Kart Erişim Cihazı (KEC)*

- **Arka Ofis Sistemleri (Elektronik Kimlik Doğrulama Sistemi)**

Hizmet noktasının bağlı olduğu kurumun merkezini temsil eder (Örneğin; banka merkezi, Noterler Birliği merkezi, ÖSYM merkezi, SGK merkezi veya kamuya açık hizmet veren yetkili Kimlik Doğrulama Hizmet Sağlayıcıları (KDHS) gibi). Kurumun merkezinde kimlik doğrulamayı teyit eden ve gerçekleşecek işlem için kimlik doğrulama yönteminin yeterli olup olmadığını değerlendiren yazılımlar yer alır. Kurumun merkezi uygulama sunucusu tarafından kullanılmak üzere üç farklı **Elektronik Kimlik Doğrulama Sistemi (EKDS)** sunucusu (Şekil-4) standartlarda yer almıştır. Bu sunucular NVİ'den alınacak sunucu sertifikalarını ve kriptografik özel anahtarlarını güvenli donanım modüllerinde (HSM) saklamak ve donanım üzerinde kullanmak durumundadır.



Şekil-4: *biOnay Elektronik Kimlik Doğrulama Sistemi (EKDS)*

- **Kimlik Doğrulama Sunucusu (KDS)**

Bu sunucu yazılımı sayesinde KEC ile gerçekleşen kimlik doğrulama işlemleri ve üretilen **bildirimler (Kimlik Doğrulama Bildirimi - KDB) doğrulanır ve kayıt altına alınır**. Doğrulama işleminde cihaz tarafından üretilen bildirimde geçerli GEM'in (NVİ kartı) dijital imzası olup olmadığı kontrol edilir. Kullanılan yöntem, zaman, cihaz seri numarası ve hizmet alan/veren kimlik numaraları (TCKN) Kimlik Doğrulama Bildirimi içerisinde yer alır.

- **Politika Sunucusu (KDPS)**

Bu sunucu yazılımı sayesinde KEC tarafından kullanılacak kimlik doğrulama **parametreleri ve yöntemleri** (parmak izi, PIN, dijital fotoğraf, dijital sertifika), işlem tipine göre uzaktan ve güvenli olarak belirlenir. KEC merkezden aldığı politikanın (yöntem ve parametreleri) dijital imzasını doğruladıktan sonra kimlik doğrulamayı gerçekleştirir. Sistemin kullanımını kolaylaştırmak için merkezden ayarlanabilecek olası parametreler; aracı kişinin işlem izni veya hizmet alan kişinin parmak izi doğrulanmadığı durumlarda hizmet veren görevlinin onayı ile işlemin devam ettirilebilmesi vb.

- **Rol Sunucusu**

Bu sunucu yazılımı sayesinde NVİ'den kurumun aldığı **karttan veri okuma ve/veya yazma yetki sertifikası** ile KEC üzerinde takılı kimlik kartında yer alan kişisel verileri

(doğum yeri ve tarihi, anne adı, kan grubu, acil sağlık bilgileri vb.) uzaktan ve güvenli okuyabilir ve/veya acil sağlık bilgisi gibi verileri karta yazabilir. Bu işlemler sırasında NVİ'nin kuruma verdiği yetki kart sahibinin onayını gerektiriyorsa, kart sahibinden PIN girerek onay vermesi istenebilir.

- **Yönetim, Entegrasyon ve Ek Hizmet Servisleri**

Standartlarda tanımlanan yukarıdaki 3 (üç) temel sunucu yazılımı dışında, sistemin kolay entegrasyonu, kullanımı ve yönetimi için farklı arka ofis yazılımlarına da ihtiyaç duyulabilir. **Anahtar teslim altyapıları** oluşturan bu bileşenlerden bazıları;

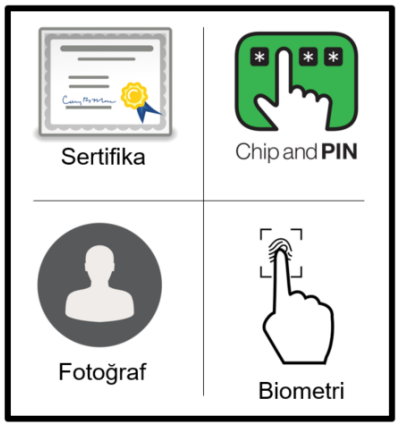
- Merkezi uygulamalara kolay entegrasyon için "**Elektronik Kimlik Kartı (EKK) Servis API**"
- Ağ üzerinden bağlı KEC cihazlarına erişim için "**KEC Ağ Sunucusu**"
- Mobil KEC cihazlarının tek bir noktadan güvenli erişimi için "**KEC Proxy Servisi**", "**APN Servisi**" ve "**RADIUS Kimlik Doğrulama Servisi**"
- KEC cihazlarının sahada yönetimi ve uzaktan güvenli güncellenmesi için "**KEC Yönetim Sistemi**"
- E-Kimlik kartlarına uzaktan güvenli e-imza yüklemek için "**NES Yönetim Servisleri**"
- E-Kimlik kartları ile doküman imzalamak için "**E-İmza Oluşturma ve Doğrulama Servisleri**"

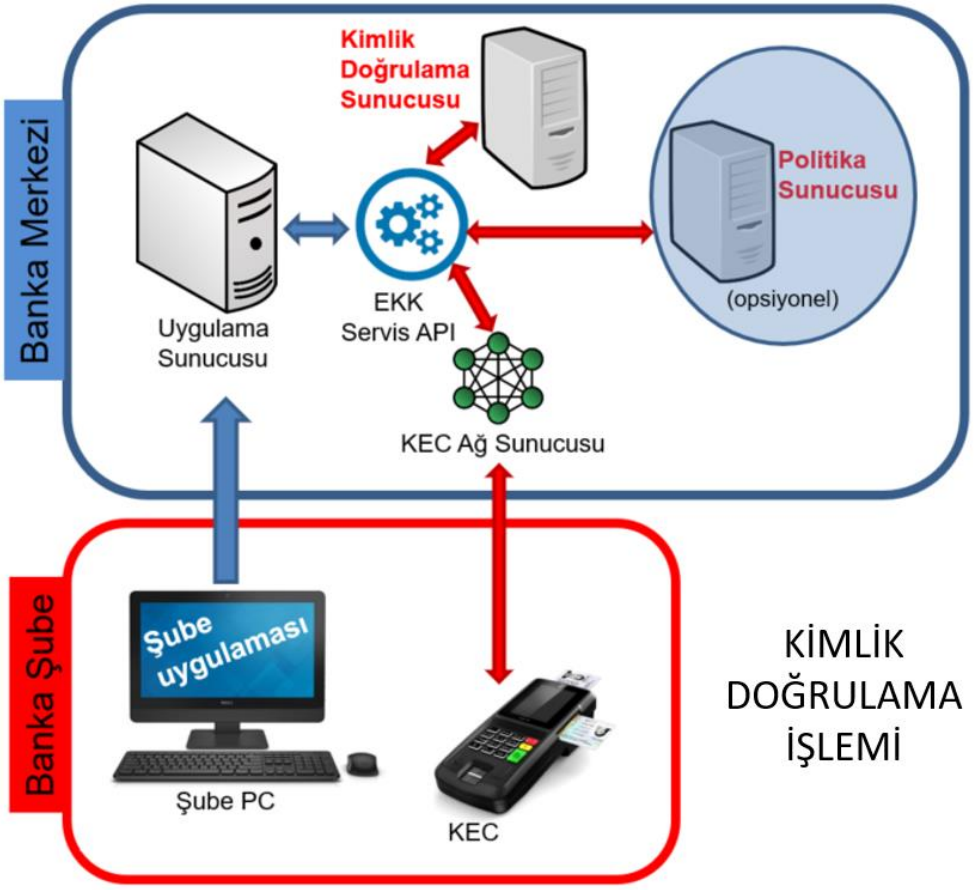
9. Yeni Sistemde Kullanım Senaryoları

Sistemin **2 (iki) temel kullanım senaryosu** vardır: kimlik doğrulama ve karttan veri okuma/yazma.

- **Kimlik Doğrulama**

Sistemin en temel fonksiyonu, hizmet almak isteyen vatandaşın çipli kimlik kartının doğrulanmasıdır. Bu işlem için kimlik doğrulama gerektiren noktada KEC cihazı ve o kurumun merkezinde **Kimlik Doğrulama Sunucusu** (KDS) olması yeterlidir. Kimlik doğrulama sırasında kart sahibi PIN, parmak izi ve dijital fotoğraf yöntemlerinden bir veya birkaçı ile doğrulanabilmektedir. Bu yöntemin seçimi için istenirse kurumların kendi merkezlerinde **opsiyonel** olarak kuracakları **Politika Sunucusu** (KDPS) kullanılabilir (Şekil-5).





Şekil-5: *Elektronik Kimlik Doğrulama İşlemi*

- **Karttan veri okuma / yazma**

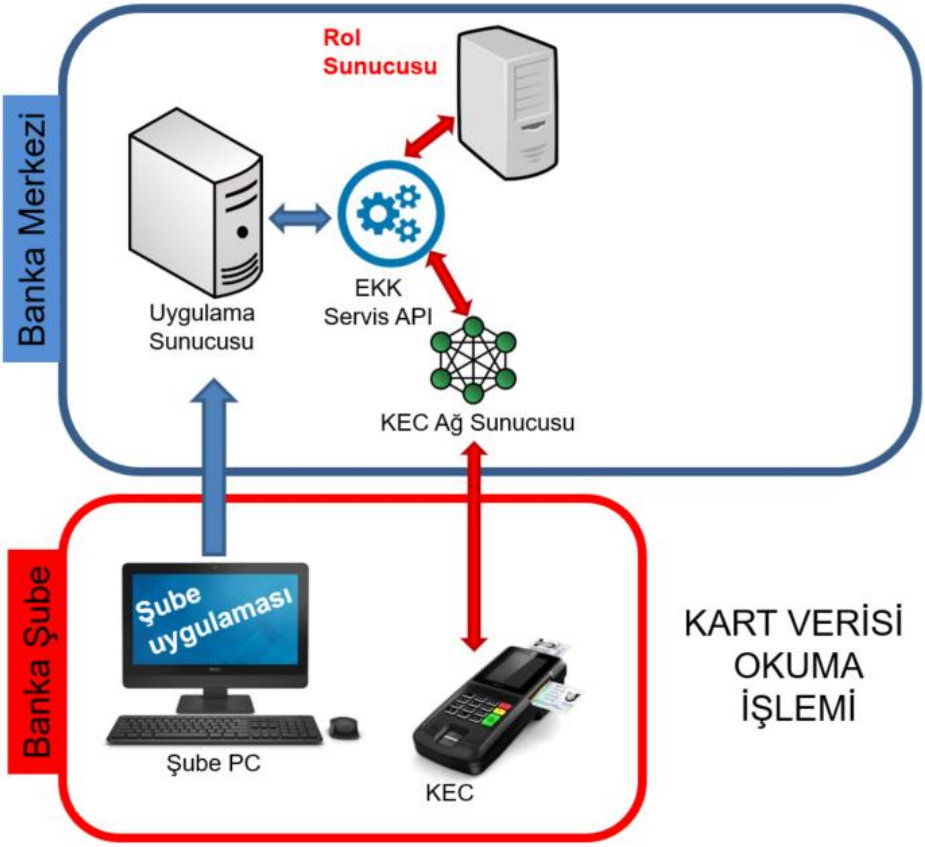
Ana işlev olan kimlik doğrulamanın dışında, ikinci bir fonksiyon olarak, çip içerisinde kişiye ait veriler yetki kontrolü ile okunabilir ve/veya acil sağlık bilgisi gibi veriler yazılabilir.

- **Açık verilerin okunması** (TCKN, Ad ve Soyadı, Kart No)

  Bu verilere erişim için yetki alınması gerekmez.

- **Kişiye ait özel verilerin okunması** (Doğum Tarihi, Doğum Yeri, Anne Adı, Anne Kızlık Soyadı, Medeni Hali, Dini, Kan Grubu, Acil Sağlık Bilgileri, Rüşt Mesajı…)

  Bu verilere erişmek isteyen kurumların kendi merkezlerine **Rol Sunucusu** kurup, NVİ'den **yetki sertifikası** alması gerekmektedir (Şekil-6).



Şekil-6: *Elektronik Kimlik Kartından Veri Okuma*

- **Kişiye ait özel verilerin yazılması** (Acil Sağlık Bilgileri, Kan Grubu, Bağışıklık Bilgileri, Rüşt Mesajı, Kişisel Mesaj, Nitelikli Elektronik Sertifika)

Bu verileri yazmak isteyen kurumların kendi merkezlerine **Rol Sunucusu** kurup, NVİ'den **yetki sertifikası** alması gerekmektedir.

OPSİYONEL İLAVE KULLANIM SENARYOSU: Uzaktan kimlik doğrulama sayesinde KEC üzerinde takılı e-Kimlik kartına anlaşmalı ESHS ile uzaktan **Nitelikli Elektronik Sertifika (NES)** yüklenebilir ve NES ile yasal geçerli, ıslak imzaya eşdeğer **sözleşme imzalatılabilir.** (Şekil-7)

Şekil-7: *E-imza ve Nüfus Cüzdanı Aynı Kart Üzerinde*

10. Sistem Sertifikasyonları ve Özdenetim (Otodenetim) Mekanizması

Sistemi kullanacak kurumların NVİ'den dijital sertifika temin etmeleri ve bu sertifikaları kendi sistemlerine tanıtmaları gerekmektedir. Bu **sertifikalar NVİ'den alınmadan hiçbir kurum EKDS işletemez ve KEC kullanamaz**. Bir kurumun bu sistemi kullanabilmesi için gereken dijital sertifikalar:

- Uç Birim (şube/ofis/üye iş yeri)
  - **KEC cihazları için GEM kartı** ve içerisinde yüklü ve geçerli dijital sertifika temin edilmesi gerekmektedir. Bu kartlar KEC üreticisi tarafından alınıp cihazlara ilklendirme aşamasında yerleştirilir ve yetkili servis dışında cihazdan çıkarılamaz.

- Arka ofis sistemleri (kurumların ve KDHS'lerin merkezleri)
  - **Kimlik Doğrulama Başarım Onayı** dijital sertifikası
  - OPSİYONEL (yöntem belirlemek için) : **Politika Sunucusu** dijital sertifikası
  - OPSİYONEL (karttan veri okumak için): **Rol Sunucusu** dijital sertifikaları
  - KEC in bağlanacağı **SSL sunucu** sertifikaları

NVİ'nin bir kuruma veya KDHS'ye yukarıdaki sertifikaları kullanma yetkisi verebilmesi için, **her kurumun NVİ / Kamu SM ile bir sözleşme yapması** gerekmektedir. Bu sertifikaları alan **kurumlar sahip olup kullandıkları sertifikalardan sorumludur**. Ayrıca yukarıdaki sertifikaları alabilmek için kurumların **satın alıp kullandığı KEC cihazı ve EKDS sunucuları, aşağıdaki testleri başarıyla geçmiş ve ilgili kurumsal sertifikaları/belgeleri almış olması** gerekmektedir.

- **Kart Erişim Cihazı** (KEC) üreticilerinden istenen belgeler
  - TÜBİTAK testleri ve TSE Standartları Uyumluluk Belgesi
  - TSE Ortak Kriterler Sertifikası (güvenlik seviyesi EAL4+)

- **Elektronik Kimlik Doğrulama Sistemi** (EKDS) üreticilerinden istenen belgeler
  - TÜBİTAK testleri ve TSE Standartları Uyumluluk Belgesi

Yukarıdaki test ve sertifikasyonu geçen **üreticiler ve test merkezleri de kendileri ile ilgili testlerden sorumludur**. Dolayısıyla sistemi kullanan kurumlar, testleri yapanlar ve üreticiler kendi kısımları ile ilgili özdenetimden otomatik olarak geçmektedir.

Elektronik Kimlik Doğrulama Sistemi (EKDS) için ilave güvenlik denetimleri:

- EKDS'yi işletecek kurumların, **TS EN ISO/IEC 27001** standardı kapsamında akredite edilen belgelendirme kuruluşlarınca verilen **Bilgi Güvenliği Yönetim Sistemi (BGYS)** sertifikasyonuna sahip olması zorunludur. Aşağıdaki öz denetimler sayesinde EKDS kullanacak kurumun ayrıca bir denetime ihtiyacı yoktur:

    - **Şartları sağlamayan bir firma** NVİ'ye başvurduğunda NVİ'den **sertifika alamayacak ve kimlik doğrulaması yapamayacaktır**.
    - **Rol yetkisi alamayan bir kurum kartlardan özel veri okuyamayacaktır**.
    - Kullanılan EKDS yazılımı **TSE standart uygunluk belgesine sahip değilse**, sertifika alamayacaktır. Benzer şekilde **KEC üreticisi** gerekli testleri geçip ürünü (CC EAL4+) **sertifikalandıramaz ise NVİ'den GEM kartı alamayacaktır**.
    - EKDS sunucu sertifikalarını NVİ adına Kamu SM yayınladığından, **Kamu SM'nin sertifika dağıtım kontrolü**nden de bu firmanın geçmesi gerekecektir.

- EKDS içerisindeki sunucular aynı kritik işlem setine sahip değildir ve bu nedenle tüm EKDS sunucularının aynı kurallara tabi olduğu düşünülmemelidir:

    - Kimlik Doğrulama Sunucusu **(KDS) sadece işlem saatine, TCKN, Kart No ve Ad-Soyadı verileriine ulaşır**. Opsiyonel yöntem belirleyen **Politika Sunucusu da benzerdir**.
    - **Sadece Rol sunucusu kişiye ait özel verilere ulaşabilir** ki, kurumun karttan okuyacağı her bir veri için NVİ'den yetki içeren Rol sertifikası alması gerekmektedir. Benzer şekilde yazma işlemi için de yetki sertifikası gerekmektedir. Bu nedenle en kritik bileşen Rol sunucusudur, diğer iki sunucu kişisel veriler açısından bu denli kritik değildir.

11. Sistemin Oluşturduğu Dijital Kayıtlar

Yeni sistemde elektronik kimlik doğrulama sayesinde, KEC cihazlarındaki GEM kartları ile dijital olarak imzalanmış **Kimlik Doğrulama Bildirimleri (KDB)** ilgili kurumların merkezlerine gönderilir. Bu bildirimler, denetim amaçlı ve anlaşmazlık durumlarında kanıt amaçlı kullanılabilir. Benzer şekilde kimlik doğrulama sunucusunun yaptığı doğrulama sonucu, yine dijital imzalı olarak saklanır. Kimlik Doğrulama Sunucusu yaptığı doğrulamaya ilişkin **Kimlik Doğrulama Başarım Onayı (KDBO)** üretebilir ve istenirse KDBO arşiv imza atılarak da saklanabilir.

Kimlik doğrulaması için Politika sunucusu kullanılmış ise; **doğrulama yöntemi ve parametreleri üzerindeki dijital imza**, gerçekleşen işlemde kullanılan yöntem ve parametreler için kanıt olarak saklanabilir. Bu veriler KDB içerisinde de yer almaktadır.

Rol sunucusu karttan veri okumak için, Kart Erişim Cihazı (KEC) ile güvenli iletişim kurar ve KEC üzerinde takılı e-Kimlik kartı ile (T.C. Kimlik Kartı) Rol (yetki) doğrulaması yapar. Tüm bu süreçte uçtan uca dijital imzalar kullanılır. **Rol sunucusunun log kayıtları, e-Kimlik kartına erişim ile ilgili izleri tutar**. Hangi KEC cihazına ve hangi karta erişildiği bilgisi dijital olarak saklanabilir.

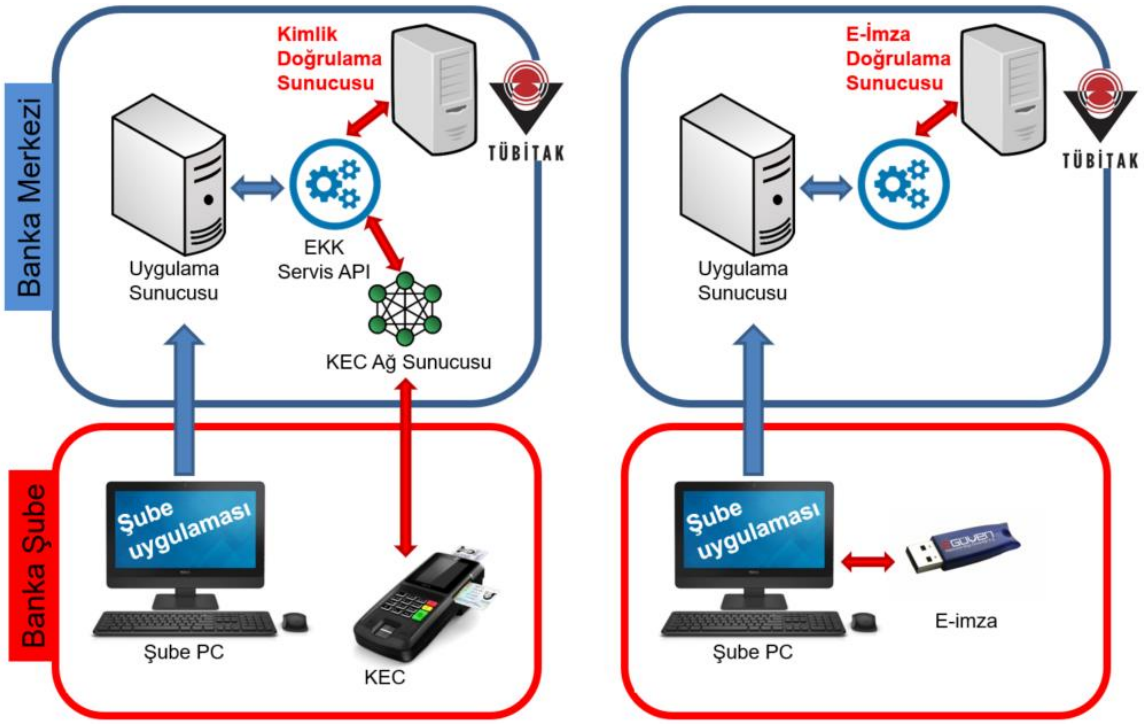
Yeni sistem sayesinde, kimlik fotokopisi ve manuel kontroller yerine tamamen dijital ortamda, otomatikleştirilen süreçler ile denetim daha doğru ve daha verimli bir şekilde gerçekleşebilir. Maliye, BDDK, SGK ve MASAK gibi kurumlar denetimlerini çok daha efektif bir şekilde yapabilir. **Kurumların fiziksel kopya ve arşivleme ihtiyaçları ile ilave maliyetler ortadan kalkar**.

12. E-imza İle Benzerlikler

E-imza doğrulama fonksiyonu yasal geçerliliği olan, ıslak imzaya eşdeğer elektronik kayıt oluşturma yöntemidir. Ülkemizde bugün binlerce kurumda e-imza doğrulaması yapılmaktadır. (Şekil-8)

- **E-imza doğrulama sunucularının hiçbir kurum tarafından denetimi yapılmamakta**, sadece bu yazılımların **TÜBİTAK testlerinden geçmesi beklenmektedir**. Kimlik Doğrulama Sunucusu da TÜBİTAK testlerinden geçmekte ve TSE'den standart uyumluluk belgesi almaktadır ve ilave bir denetim gerekmemektedir.

- **E-imza doğrulama sunucusu, e-imzayı doğrulayan ve kabul eden kurumun kontrolündedir**. Benzer şekilde Kimlik Doğrulama Sunucusu da kimlik doğrulamayı yapan ve kabul eden kurum bünyesinde kurulabilir ve kullanılabilir olmalıdır. NVİ, EKDS sertifikası vereceği kurum ile yapacağı sözleşmelerde sorumlulukları belirtebilir.



Şekil-8: *E-Kimlik Doğrulama ile E-İmza Doğrulamanın Benzerlikleri*

13. E-Kimlik (T.C. Kimlik Kartı) ile E-İmza Uygulamaları

Yeni e-Kimlik kartları (T.C. Kimlik Kartları) Ortak Kriterler CC EAL 4+ güvenlik sertifikasyonuna sahip olduğu için yetkili ESHS'lerden **Nitelikli Elektronik Sertifika (NES) yüklenebilir ve e-imza oluşturmak için kullanılabilir**.

ESHS'lerin bir müşterisine NES verebilmek için, o müşterinin kimliğini doğrulaması gerekmektedir. Kart Erişim Cihazları (KEC) sayesinde **ESHS'ler e-Kimlik sahiplerinin kimliğini uzaktan doğrulayabilir** ve e-Kimliklere uzaktan ve güvenli olarak NES yükleyebilir.

2004 yılında çıkarılan 5070 sayılı Elektronik İmza Kanunu ve ilgili mevzuat çerçevesinde, NES sahibi kişiler **ıslak imzaya eşdeğer elektronik imza** atabilir. Bu sayede kişiler üye iş yerlerinde uzaktan kimlik doğrulaması yapabildiği gibi, e-Kimlik kartlarına uzaktan NES yükleyebilir ve yasal bağlayıcı olarak sözleşmeleri KEC üzerinde imzalayabilir. Bu sayede kimlik fotokopisi ortadan kalkacağı gibi, e-imza sayesinde kâğıt üzerine basılan ve ıslak imza ile imzalanan sözleşmeler de dijital ortama taşınabilir. **Kolay kullanım, süreçlerin dijitalleşmesi, kâğıt ortamı, kurye ve arşiv gibi ek maliyetlerin ortadan kalkması** kurumlara çok sayıda avantaj sağlayacaktır.

14. Bugünkü Durum ve Önümüzdeki Süreç

Bugünkü Durum:

- **80 (seksen) milyonun üzerinde yeni çipli e-Kimlik kartı (T.C. Kimlik Kartı)** dağıtılmış ve ayda 1 milyona yakın kart dağıtımı devam etmektedir.
- T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri (NVİ) Genel Müdürlüğü tarafından 20.10.2020'de **"Elektronik Kimlik Doğrulama Sistemi (EKDS) Yönetmeliği"** yayımlanmış, elektronik kimlik doğrulama süreçleri ve **ilgili Kimlik Doğrulama Hizmet Sağlayıcıların (KDHS)** kuruluş ve faaliyetleri düzenlenmiştir.
- **Kamuya açık hizmet veren özel sektör Kimlik Doğrulama Hizmet Sağlayıcıları (KDHS)** kurulmuş ve işletilmektedir. Tüm ihtiyaç sahibi kurum ve kuruluşlar NVİ tarafından **onaylanarak yetkilendirilmiş**, **tüm güvenlik ve uyumluluk sertifikaları tam ve güncel** olan KDHS'lerden kimlik doğrulama hizmeti alabilmektedir.
- **Son 2 (iki) yılda 4 (dört) milyonun üzerinde Türkiye Cumhuriyeti vatandaşı** yeni çipli T.C. Kimlik kartları ile **parmak iziyle** elektronik kimlik doğrulama işlemi gerçekleştirmiştir.
- **Tapu Daireleri, Noterler, Bankalar, Dershaneler, Belediyeler** gibi pek çok kurum ve kuruluşta Kart Erişim Cihazları (KEC) bulunmakta, Elektronik Kimlik Doğrulama Sistemi (EKDS) kullanımı her geçen gün yaygınlaşmaktadır.
- Bilgi Teknolojileri ve İletişim Kurumu (BTK), EKDS yönetmeliğine atıfta bulunarak "Elektronik İmza Yönetmeliği"ni güncellemiş, EKDS altyapısı aracılığıyla **T.C. Kimlik Kartlarına güvenli elektronik imza kullanımı amaçlı e-imza sertifikaları (Nitelikli Elektronik Sertifika - NES) yüklenmesiyle** ilgili süreci tanımlamıştır.
- Elektronik kimlik doğrulamanın tüm bu avantajlarına rağmen, klasik kimlik doğrulama yöntemi olarak bugün hala pek çok noktada fiziksel gözle kontrol yapılmakta ve pek çok kurum tarafından e-Kimlik kartlarının fotokopisi çekilmekte veya dijital tarama işlemi yapılmaktadır. Bu eski uygulamaların ve alışkanlıkların dezavantajlarından aşağıda kısaca bahsedilmiştir.
  - Fiziksel gözle kontrol **insan hatalarına açıktır** ve **kolay sahteciliğe sebebiyet** verebilmektedir.
  - Fotokopi ve tarama ile kişiye ait özel veriler kart yüzeyinden (**Doğum tarihi, Anne adı, Baba adı, Islak imzası, Son kullanma tarihi, Cinsiyeti, vb.**) kağıda aktarılmakta ve/veya kurumların veri merkezlerinde depolanmaktadır. Bu durum Kişisel Verileri Koruma Kanununa (KVKK) aykırı bir durum teşkil etmektedir. Bu konuda yapılan uyarılara rağmen, maalesef güncel kimlik doğrulama kart fotokopisi ile devam etmektedir.

- T.C. Kimlik Kartlarının merdaneli tarayıcılarda fotokopi çekimi veya tarama işlemine maruz bırakılması durumlarında kartlar üzerindeki dijital çipler yerlerinden çıkabilmekte ve yeniden NVİ'ye başvuru yapılarak yeni bir T.C. Kimlik Kartı alınması gerekebilmektedir.

- Mevcut fiziksel kimlik kontrolünü yeterli bulmayan bazı kurum ve kuruluşlar; EKDS dışında farklı yollara başvurabilmekte, güvenliği ve güvenilirliği bağımsız test ve sertifikalarla kanıtlanmamış, mevzuat uyumu bulunmayan SMS şifre, avuç içi el ayası doğrulama, merkezde kişiye ait biyometrik veri depolama ve merkezde eşleştirme gibi hem **KVKK ile uyumsuz** hem de ileride âtıl kalabilecek **mükerrer yatırımlara yönelebilmektedir.**
- An itibarıyla Türkiye Cumhuriyeti genelinde gerek mevzuat uyumu gerekse de standartlara uyum ve belgelendirme bakımından en sağlam temeller üzerine inşa edilmiş **yegane kimlik doğrulama yöntemi Elektronik Kimlik Doğrulama Sistemi (EKDS) olarak öne çıkmaktadır.**

Önümüzdeki Süreç:

- **2024 yılı sonuna kadar tüm vatandaşların** yeni çipli T.C. Kimlik Kartlarına kavuşması beklenmektedir.
- EKDS Yönetmeliği uyarınca faaliyet gösteren **KDHS'ler** ve **KEC üreticilerinin daha çok sayıda kamu kurumu ve özel sektör kuruluşuna ulaşmasıyla** Elektronik Kimlik Doğrulama Sistemi (EKDS) kullanımı daha da yaygınlaşacaktır.
- İlerleyen dönemlerde NVİ'nin düzenlemelerine ek olarak Mali Suçları Araştırma Kurulu (MASAK), Bilgi Teknolojileri ve İletişim Kurumu (BTK), Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) gibi **sektör düzenleyici kurumlarının** EKDS yönetmeliğine atıfta bulunarak, **kendi alanlarındaki regülasyonlarda ve ilgili mevzuatta gerekli güncellemeleri yapması** beklenmektedir.
- Sektörün hazır olması ve uygulama deneyimlerinin artmasıyla pek çok kurum ve kuruluş **uygulamalarına yeni kimlik kartlarını entegre edebilecektir**.
- **Dijital süreçlerin yarattığı fayda, verimlilik, tasarruf** daha çok öne çıkacaktır.

“Elektronik Güvenlik Altyapısı (EGA) A.Ş.” ve “biOnay E-kimlik Doğrulama Hizmet Sağlayıcı A.Ş.” Hakkında

Yüzde yüz yerli üretimle milli yazılım ve donanımlar geliştirerek elektronik güvenlik hizmetleri sunmak amacıyla 2006 yılında kurulan **EGA Elektronik Güvenlik Altyapısı A.Ş. (EGA)**, konusunda uzman ekibiyle mevzuata uygun elektronik kimlik doğrulama çözümleri geliştirmiş, elektronik imza yazılımlarıyla ülkemizde e-imza ve mobil imza kavramlarının yaygınlaşmasında etkin rol almış, bilgi güvenliği ve kriptografi alanlarında Ar-Ge ve danışmanlık hizmetleri yürütmüştür.

Türkiye’yi yeni bir kimlik doğrulama deneyimiyle tanıştıran **EGA**, bu amaçla **biOnay** markasını oluşturmuş, T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü tarafından yayınlanan “Elektronik Kimlik Doğrulama Sistemi (EKDS) Yönetmeliği” ile düzenlenen ve TSE tarafından teknik standartları yayınlanan **Elektronik Kimlik Doğrulama Sistemi (EKDS)** kapsamında Kimlik Doğrulama Hizmet Sağlayıcısı (KDHS) olarak faaliyet göstermek üzere 2018 yılında **biOnay E-kimlik Doğrulama Hizmet Sağlayıcı A.Ş.** firmasını kurmuştur.

Bir **EGA** iştiraki olarak kurulmuş olan **biOnay**, 25.07.2022 tarihinde T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri (NVİ) Genel Müdürlüğü tarafından yetkilendirilerek **Kimlik Doğrulama Hizmet Sağlayıcısı (KDHS)** olarak faaliyetlerine başlamıştır.

EKDS kapsamında **T.C. Kimlik Kartları** üzerinden güvenli elektronik kimlik doğrulama işlemlerini yürütmek üzere tasarlanmış olan, NVİ tarafından onaylanmış ve ilgili tüm TSE sertifikaları ile Ortak Kriterler (CC) EAL4+ güvenlik sertifikasına sahip **biOnay Kart Erişim Cihazlarının (KEC)** üretimi ise 1955 yılından bu yana dünyanın önde gelen otomotiv markalarına elektronik, elektromekanik ve mekatronik ürünler geliştiren, EGA ve biOnay’ın da ana iştirakçisi olan **KAT Mekatronik Ürünleri A.Ş.**’nin **25.000 m2 kapalı alana sahip modern üretim tesislerinde** yapılmaktadır.

Bu yönüyle hem KEC donanımlarının üreticisi hem de EKDS kapsamındaki tüm sunucu yazılımlarının üreticisi konumundaki tek firma olan EGA’nın sağladığı donanım ve yazılım altyapısıyla faaliyet gösteren biOnay, **elektronik kimlik doğrulama alanında bütünleşik çözüm sunan Türkiye’deki ilk ve tek KDHS** olmuştur.

www.ega.com.tr

www.bionay.com.tr

Elektronik Kimlik Doğrulama ve e-İmza Çözümlerimiz

- Kart Erişim Cihazı (KEC) Donanımı (TSE ve Ortak Kriterler (CC) EAL 4+ sertifikalı)
- biOnay Kimlik Doğrulama Sunucusu Yazılımı (TSE Sertifikalı)
- biOnay Politika Sunucusu Yazılımı (TSE Sertifikalı)
- biOnay Rol Sunucusu Yazılımı (TSE Sertifikalı)
- biOnay Kiosk Akıllı Kimlik Kartı Doğrulama Yazılım ve Donanımı (entegre KEC)
- biimza Merkezi E-imza Servisi E-İmza Yazılımı
- biimza Mobil İmza Entegrasyon Servisi E-İmza Yazılımı
- Elektronik İmza Kütüphanesi ve Entegrasyonu (Tüm akıllı kart, akıllı kart okuyucu, zaman damgası, Nitelikli Elektronik Sertifika, HSM'ler ile çalışabilme özelliği)
- Mobil İmza Entegrasyonu (Avea, Turkcell, Vodafone, tüm GSM operatörleri ile çalışabilme özelliği)
- MSSP (Mobile Signature Service Provider) Altyapısı ve Kurulumu
- Zaman Damgası Entegrasyonu (Tüm ESHS'lerin verdiği hizmetler ile uyumlu)
- Merkezi Veri Tabanı Hizmet Sağlayıcı (MTHS) Altyapısı ve Entegrasyonu
- Web Tarayıcı Bağımsız E-imza, Mobil imza ve E-kimlik Doğrulama Çözümü
- E-Fatura Özel Entegratörlük Çözümleri (Birçok ERP ürünü ile entegre)
- E-Defter İmzalama/Doğrulama Entegrasyonu
- KEP (Kayıtlı Elektronik Posta) Entegrasyonu (Tüm KEP Hizmet Sağlayıcılarla çalışabilen altyapı)
- SGK E-Haciz Yönetim Sistemi
- Maliye E-Haciz Yönetim Sistemi
- TMSF E-Haciz Yönetim Sistemi
- EKAP E-İhale Yönetim Sistemi
- ASBİS Araç Tescil Elektronik İmza Entegrasyonu
- PKI (Açık Anahtar Altyapısı) Yazılımı
- Şifreleme Yazılımları
- E-'li tüm süreçlerin eğitim ve danışmanlığı

İletişim Bilgileri

EGA Elektronik Güvenlik Altyapısı A.Ş.

ve

biOnay Elektronik Kimlik Doğrulama Hizmet Sağlayıcısı A.Ş.

Merkez Adres:

Teknopark İstanbul, Sanayi Mahallesi, Teknopark Bulvarı No:1-11C Blok Kat:3 No:301
34906 Pendik İstanbul

Tel: 0 (216) 759 00 60

info@ega.com.tr
info@bionay.com.tr

Kısaltmalar ve Açıklamalar

Çok Faktörlü kimlik doğrulama	Sahip olunan, bilinen ve kişiye ait özellik ile kimlik doğrulama (2-faktör ve 3-faktör olarak ta bilinmektedir)
AKİS	Akıllı Kart İşletim Sistemi
Biyometrik Veri	Parmak izi
Common Criteria (CC)	Ortak Kriterler
EKDS	Elektronik Kimlik Doğrulama Sistemi
e-Kimlik Kartı	T.C. Kimlik Kartı
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
GEM	Güvenli Erişim Modülü
GPRS	GSM operatörlerin sunduğu mobil ağ
Hardware Security Module (HSM)	Donanımsal Güvenlik Modülü
Kamu SM	Kamu Sertifika Merkezi
KEC	Kart Erişim Cihazı
KDB	Kimlik Doğrulama Bildirimi
KDBO	Kimlik Doğrulama Başarım Onayı
KDHS	Kimlik Doğrulama Hizmet Sağlayıcısı
KDS	Kimlik Doğrulama Sunucusu
KDPS	Kimlik Doğrulama Politika Sunucusu
KVK	Kişisel Verileri Koruma
KVKK	Kişisel Verileri Koruma Kanunu/Kurumu
NES	Nitelikli Elektronik Sertifika
NVİ	Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü
Protection Profile (PP)	Koruma Profili
SSL/TLS	Secure Socket Layer/ Transport Layer Security
TCKN	Türkiye Cumhuriyeti Kimlik Numarası
TSE	Türk Standardları Enstitüsü
TÜBİTAK BİLGEM	TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi
WiFi	Ofis ortamındaki mobil ağ