

bio_ona4

Elektronik Kimlik Doğrulama Sistemi



Elektronik İmza ile Buluşma Noktamız...

İÇİNDEKİLER

| | |
|--|----|
| Doküman Tarihçe | 3 |
| 1. Yönetici Özeti | 4 |
| 2. Genel Kimlik Doğrulama Yöntemleri | 5 |
| - Fiziksel Kimlik Doğrulama..... | 5 |
| - Elektronik Kimlik Doğrulama | 5 |
| - Çevrimiçi Biyometrik Kimlik Doğrulama..... | 5 |
| - Çevrimdışı Biyometrik Kimlik Doğrulama..... | 6 |
| 3. Türkiye’de Nüfus Cüzdanının Tarihçesi ve Yeni Çipli Kimlik Kartları | 7 |
| 4. Nüfus Cüzdanlarının Kullanım Alanları..... | 9 |
| 5. Eski Nüfus Cüzdanlarında Yaşanan Başlıca Sorunlar | 10 |
| 6. Yeni Çipli Kimlik Kartlarının Faydaları..... | 11 |
| - Vatandaşlar İçin Faydaları | 11 |
| - Kurumlar İçin Faydaları | 11 |
| - Ülkemiz İçin Faydaları | 11 |
| 7. Uluslararası Standartlar, Milli Çözüm ve Kurumların Katılımı | 12 |
| - Elektronik Kimlik Doğrulama Sistemi (EKDS) Standartları..... | 12 |
| - Kart Erişim Cihazı (KEC) Standartları | 12 |
| 8. Yeni Sistemin Temel Bileşenleri | 14 |
| - Uç Birim Bileşenleri (E-Kimlik ve Kart Erişim Cihazı) | 14 |
| - Arka Ofis Sistemleri (Elektronik Kimlik Doğrulama Sistemi) | 15 |
| 9. Yeni Sistemde Kullanım Senaryoları..... | 18 |
| - Kimlik Doğrulama | 18 |
| - Karttan veri okuma / yazma..... | 19 |
| 10. Sistem Sertifikasyonları ve Özdenetim (Otodenetim) Mekanizması | 21 |
| 11. Sistemin Oluşturduğu Dijital Kayıtlar | 23 |
| 12. E-imza İle Benzerlikler | 24 |
| 13. E-Kimlik ile E-İmza Uygulamaları..... | 25 |
| 14. Bugünkü Durum ve Önümüzdeki Süreç | 26 |
| Elektronik Güvenlik Altyapısı (EGA) A.Ş. Hakkında | 27 |
| İletişim Bilgileri..... | 28 |
| Kısaltmalar ve Açıklamalar | 29 |



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 | Düzeltilmeler |

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 müşteri 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 geçerli ortak bir standarda dayanmadığı gibi, güvenlik seviyeleri de o kurumların kendi personellerinin 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. 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 Müdürlüğüne yürütülen çalışmalar ile 2018 yılı itibarıyla, 32 milyonu aşkın vatandaşıma yeni çipli kimlik kartları dağıtılmıştır ve ayda ortalama 1 milyon üzerinde kart dağıtımı devam etmektedir.

Bu doküman; her vatandaşımızın kolayca cebinde taşıyabileceği yeni çipli 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 doğrulamaya** 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 önlediği gibi, Hazine ve Maliye Bakanlığı tarafından denetlenebilmek ve vergi kaçakçılığını önlemek için dijital kayıtlar da oluşturulabilmektedir. Elektronik kimlik doğrulamada 3 farklı unsur kullanılabilir; **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 doğrulamayı sınıflandırırken 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

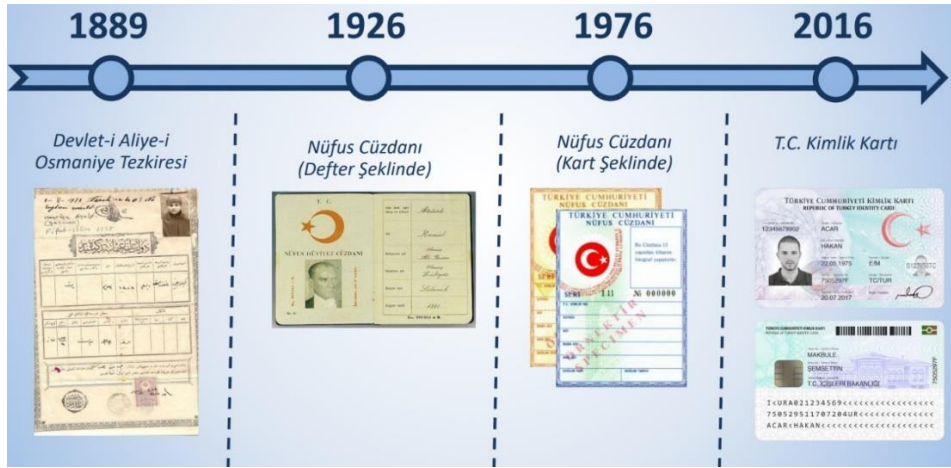


sahibi kişiler, hizmet aldıkları kuruma parmak izini, fotoğrafını vermek istemeyebilir ve bu talep Kişisel Verileri Koruma Kanunu (KVKK) kapsamında bireylerin hak ve özgürlüğüdür.

- **Çevrimdışı Biyometrik Kimlik Doğrulama:** Kişilere ait biyometrik veriler veya bu verilerden türetilmiş hiçbir veri merkezde kayıt ve kontrol edilmez. Kişiyeye ait biyometrik veri, yine o kişiyeye ait kopyalanamayan ve güvenli çipli bir kartta saklanır. Kimlik doğrulama yapması gereken kişi, güvenli onaylı bir cihaza hem çipli kimlik kartını hem de biyometrik verisini verir. Eşleştirme işlemi kişinin gözetiminde güvenli onaylı cihazda çevrimdışı gerçekleşir. **Kişisel veri hiçbir yere kaydedilmez, gönderilmez ve saklanmaz. Kişisel Verileri Koruma Kanununa (KVKK) da uygun** olan bu yöntemde kişiyeye ait biyometrik veri yine kişiyeye ait çipli kartta kalır. Çevrim dışı gerçekleşen biyometrik kimlik doğrulama sonucu (pozitif/negatif), güvenli 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 kullanımda 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 ARGE kurumu TÜBİTAK BİLGEM tarafından yeni çipli kimlik kartları tasarlanmıştır. Projede **Ortak Kriterler (CC) EAL 4+ güvenlik seviyesine sahip ve son 10 yıldır 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.

10 yıldır e-imza alanında güvenliği ispatlanmış AKİS kartları aynı zamanda, **kimlik kartı projesine özel ek güvenlik fonksiyonları** içerir:

- **Kişiyeye 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 (NVi) **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.



- Kişiy e ait parmak izi verisi, Nüfus ve Vatandaşlık İşleri (NVi) 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,
- Sınav merkezlerinde,
- Sosyal Güvenlik Kurumu (SGK) hizmetlerinde,
- Hastanelerde,
- Eczanelerde,
- Okullarda kayıt işlemlerinde,
- Abonelik sözleşmelerinde (Elektrik, su, doğalgaz dağıtım 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 (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 arsa 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.
- Oluşan 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 **kişiyeye 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 mühendisler 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 yaygınlaşmamaktadır**.

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 okuyamayacağı**nı bilir.
- Parmak izi verileri **herhangi bir merkezde veya cihazda saklanmadığı** ve **başka amaçlarla kullanılmayacağı** 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 kayıplarından** 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 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 (NVi), TÜBİTAK BİLGEM, Türk Standardları Enstitüsü (TSE), Bilgi Teknolojileri Kurumu (BTK), Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Kişisel Verileri Koruma Kurumu (KVKK), Maliye Bakanlığı Mali Suçlar Araştırma Kurumu (MASAK). Pek çok özel sektör kurum ve kuruluş 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 de kullanılan) ve kredi kartları (bankalarda kullanılan) ile aynıdır.





Bu algoritmaların zafiyeti ve kırılması demek, 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**. Fakat 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.**

o Vatandaş Kimlik Kartı

Vatandaşın sahip olduğu yeni **çipli e-Kimlik kartıdır** (Şekil-2). Kimlik doğrulama işleminde kullanılan yöntemlere 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

o Kart Erişim Cihazı (KEC)

Standartlara ve güvenlik kriterlerine göre farklı firmalarca geliştirilip TSE tarafından belgelendirilen bu cihazlar genel itibarı ile güvenli 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**

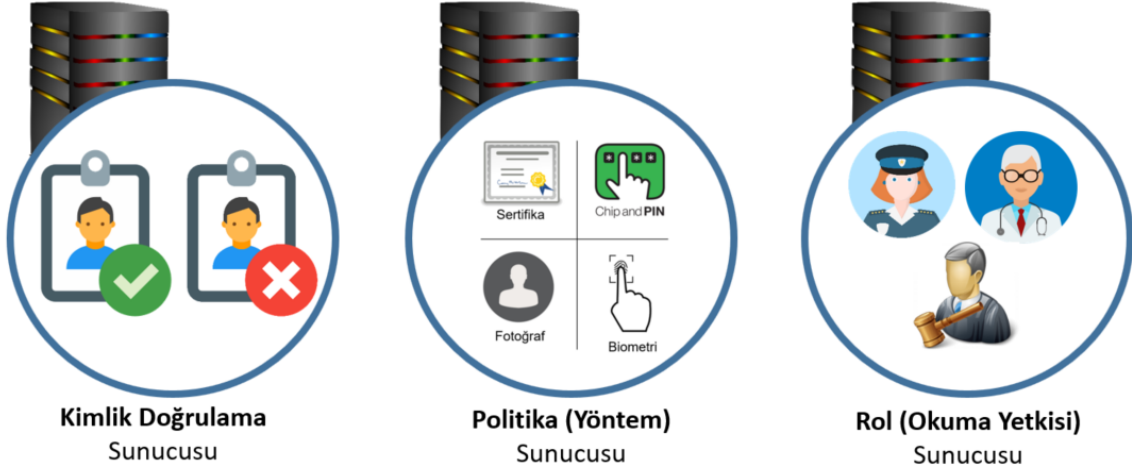
- Parmak izi doğrulama için standartlara uygun (FBI PIV-IQS veya FIPS 201-2 sertifikalarından en az birine sahip) **parmak izi sensörü**
- Fotoğraf doğrulama için **renkli ekran**
- **Güvenlik özellikleri;**
 - Dışarıdan müdahalelere karşı koruma ("**Tamper Protection**"- cihaz kasası açıldığında içerisindeki kriptonahtarlar 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 kriptomodül
 - Elektronik kimlik kartı sahibinin PIN veya parmak izini cihaza vermeden önce, cihazın orijinal olduğunun, müdahale edilmemiş olduğunun, onaylı bir cihaz olarak içerisinde NVI'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 gibi). Kurumun merkezinde kimlik doğrulamayı teyit eden ve gerçekleştirilecek 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 NVI'den alınacak sunucu sertifikalarını ve kriptografik özel anahtarlarını güvenli donanım modüllerinde (HSM) saklamak ve donanım üzerinde kullanmak durumundadır.



biOnay Elektronik Kimlik Doğrulama Sistemi (EKDS)



Kart Erişim Cihazı (KEC)

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 (KDB) doğrulanır ve kayıt altına alınır**. Doğrulama işlemi cihaz tarafından üretilen bildirimde geçerli GEM'in (NVI 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;

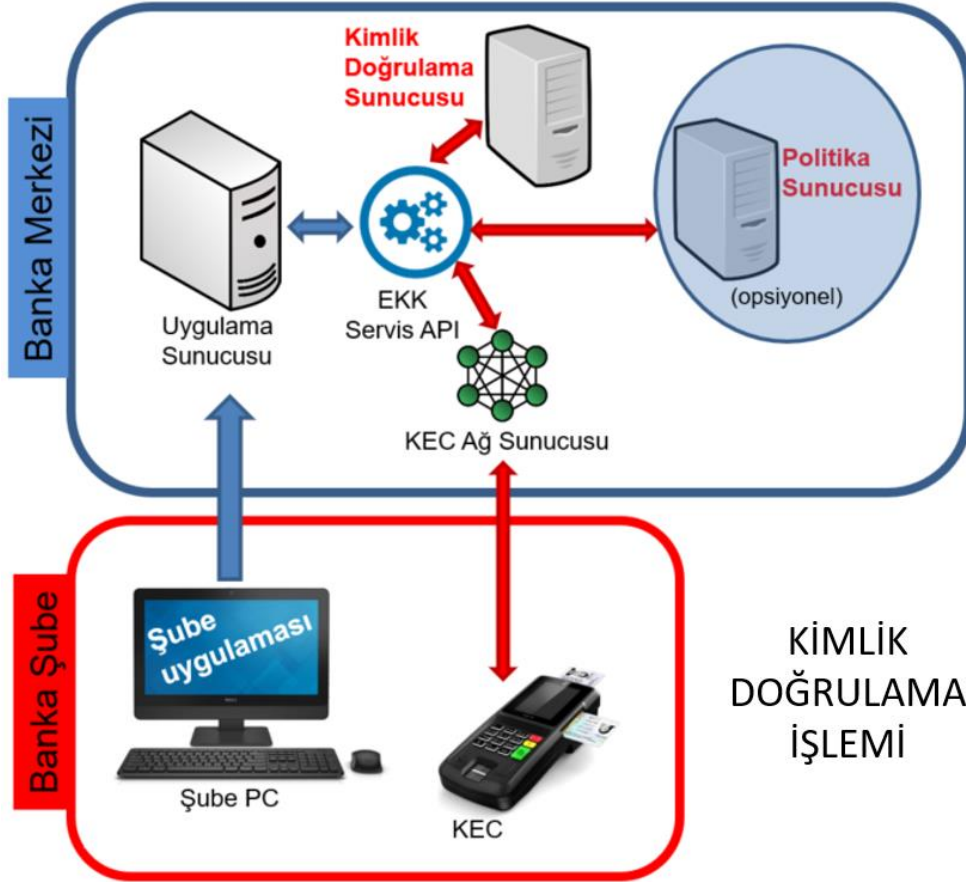
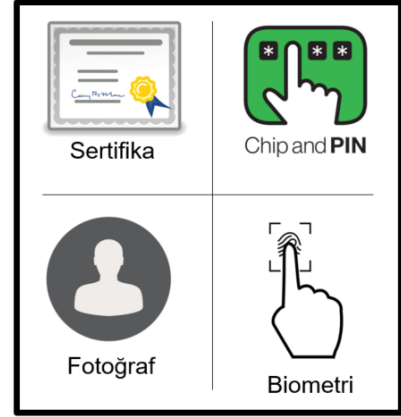
- Merkezi uygulamalara kolay entegrasyon için “**Elektronik Kimlik Kartı (EKK) Servis API**”
- Ağ üzerinden bağlı KEC cihazlarına erişim için “**KEC Ağ Sunucusu**”
- Mobil KEC cihazlarının tek bir noktadan güvenli erişimi için “**KEC Proxy Servisi**”, “**APN Servisi**” ve “**RADIUS Kimlik Doğrulama Servisi**”
- 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

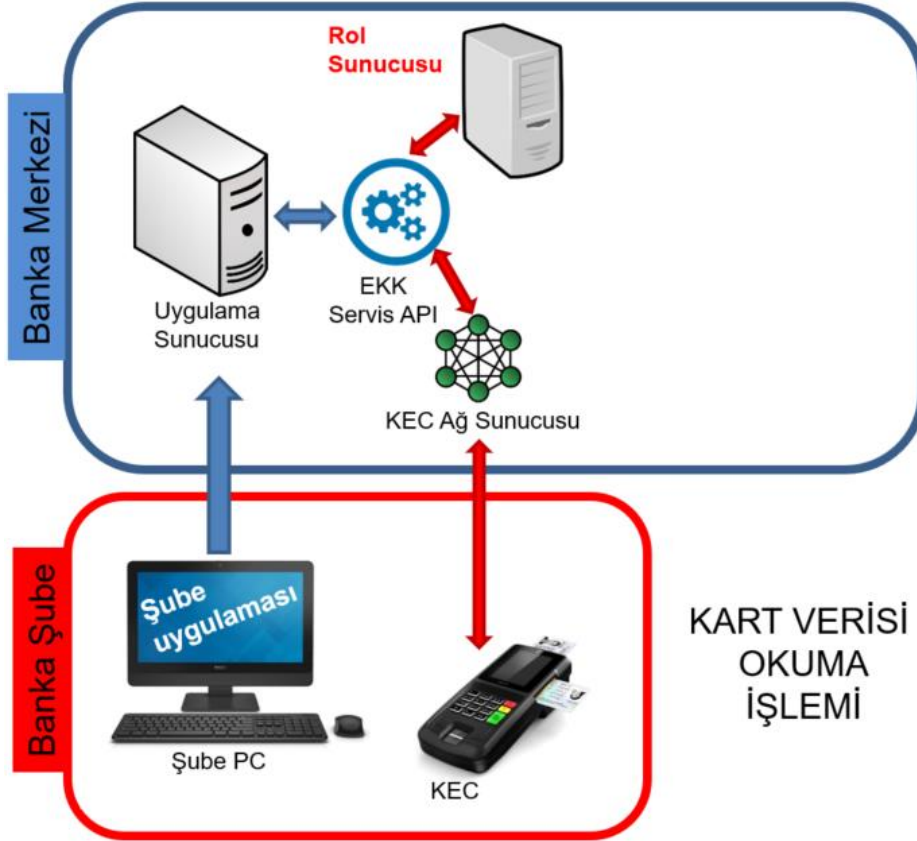
Ana işlev olan kimlik doğrulamanın dışında, ikinci bir fonksiyon olarak, çip içerisinde kişiye ait veriler yetki kontrolü ile okunabilir ve/veya acil sağlık bilgisi gibi veriler yazılabilir.

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

Bu verilere erişim için yetki alınması gerekmez.

- **Kişiye ait özel verilerin okunması** (Doğum Tarihi, Doğum Yeri, Anne Adı, Anne Kızlık Soyadı, Doğum Yeri, 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 KEK 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 tanıtılmaları 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)
 - o **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 merkezleri)
 - o **Kimlik Doğrulama Başarım Onayı** dijital sertifikası
 - o OPSİYONEL (yöntem belirlemek için) : **Politika Sunucusu** dijital sertifikası
 - o OPSİYONEL (karttan veri okumak için): **Rol Sunucusu** dijital sertifikaları
 - o KEC in bağlanacağı **SSL sunucu** sertifikaları

NVİ'nin bir kuruma 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 sertifikaları/belgeleri almış olması** gerekmektedir.

- **Kart Erişim Cihazı (KEC)** üreticilerinden istenen belgeler
 - o TÜBİTAK testleri ve TSE Standartları Uyumluluk Belgesi
 - o TSE Ortak Kriterler Sertifikası (güvenlik seviyesi EAL4+)
- **Elektronik Kimlik Doğrulama Sistemi (EKDS)** üreticilerinden istenen belgeler
 - o 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** standard kapsamında akredite edilen belgelendirme kuruluşlarınca verilen **Bilgi Güvenliği Yönetim** 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 kontrolünden** 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 saatini, TCKN, Kart No ve Ad Soyad verisine 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 kritik Rol sunucusudur, diğer iki sunucu kişisel veriler açısından çok 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.

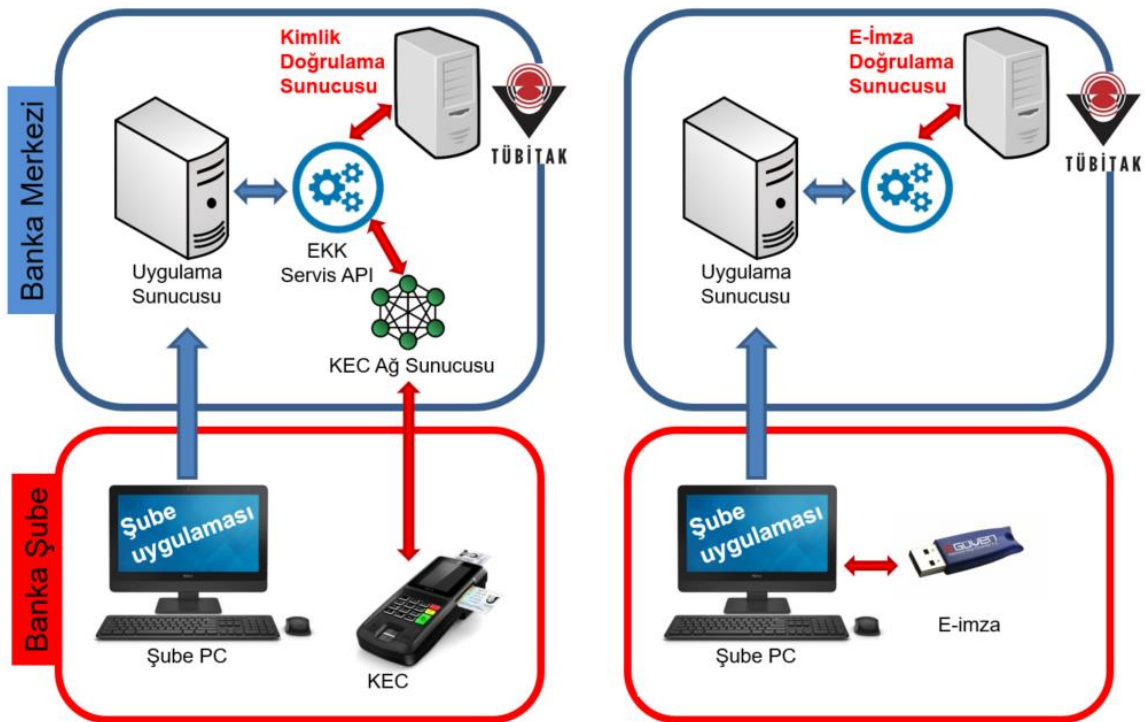
Rol sunucusu karttan veri okumak için, Kart Erişim Cihazı (KEC) ile güvenli iletişim kurar ve KEC üzerinde takılı e-Kimlik kartı ile Rol (yetki) doğrulaması yapar. Tüm bu süreçte uçtan uca dijital imzalar kullanılır. **Rol sunucusunun log kayıtları, e-Kimlik kartına erişim ile ilgili izleri tutar**. 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 gerçekleştirilebilir. 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 dođrulama fonksiyonu yasal geerliliđi olan, ıslak imzaya eřdeđer elektronik kayıt oluřturma yontemidir. Ülkemizde bugun binlerce kurumda e-imza dođrulaması yapılmaktadır.

- **E-imza dođrulama sunucuları hibir kurum tarafından denetimi yapılmamakta**, sadece bu yazılımların **TÜBİTAK testlerinden gemesi beklenmektedir**. Kimlik Dođrulama Sunucusu da TÜBİTAK testlerinden gemekte ve TSE'den standart uyumluluk belgesi almaktadır ve ilave bir denetim gerekmemektedir.
- **E-imza dođrulama sunucusu, e-imzayı dođrularan ve kabul eden kurumun kontrolündedir**. Benzer řekilde Kimlik Dođrulama Sunucusu da kimlik dođrulamayı yapan ve kabul eden kurum bünyesinde kurulabilir ve kullanılabilir olmalıdır. NVİ, EKDS sertifikası vereceđi kurum ile yapacađı sözleşmelerde sorumlulukları belirtebilir.



Şekil-7: E-Kimlik Doğrulama ile E-İmza Doğrulamanın Benzerlikleri

13. E-Kimlik ile E-İmza Uygulamaları

Yeni e-Kimlik kartları CC EAL 4+ sertifikasyonuna sahip olduğu için yetkili ESHS'lerden **Nitelikli Elektronik Sertifika (NES) yüklenebilir ve e-imza oluşturmak için kullanılabilir.**

ESHS'ler 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 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:

- **32 milyon yeni e-Kimlik kartı** dağıtılmış ve ayda 1 milyona yakın kart dağıtımı devam etmektedir.
- NVİ dışında başka bir kurumda henüz Kart Erişim Cihazı (KEC) bulunmamaktadır.
- EKDS kuran bir kurum olmadığı için **elektronik olarak kimlik doğrulama yapan kurum henüz yoktur.**
- İki üretici firma KEC sertifikalarını tamamlamış ve 4-5 firma ise çalışmalarını devam ettirmektedir. Rekabet sayesinde cihaz ve sistem maliyetleri düşecektir.
- **Kimlik doğrulama yöntemi olarak bugün fiziksel gözle kontrol yapılmakta ve pek çok kurum tarafından e-Kimlik kartlarının fotokopisi çekilmekte veya dijital tarama işlemi yapılmaktadır.**
 - 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.
- Mevcut **fiziksel kimlik kontrolünü yeterli bulmayan kurumlar**; SMS şifre, avuç içi el ayası doğrulama, merkezde kişiye ait biyometrik veri depolama ve merkezde eşleştirme gibi hem **KVKK ile uyumsuz** hem de ileride âtil kalabilecek **mükerrer yatırımlara yönelmektedir.**

Önümüzdeki Süreç:

- Kimlik kartlarının dağıtımıyla 2-3 yıl içerisinde tüm vatandaşların yeni çipli kartlara kavuşmasının sağlanması çalışması devam etmektedir.
- İlgili **yönetmeliğin çıkması ile birlikte kurumlar**; test, deneme, pilot projeler yapmaya başlayabilecek ve bu sayede;
 - Sahada e-kimlik kartı olan vatandaşlar ile yeni **elektronik kimlik doğrulama yönteminin denenmesi** pek çok kurumca yapılabilecektir.
 - Kurumlar **uygulamalarına yeni kimlik kartlarını entegre** edebilecektir.
 - **Dijital süreçler** test edilebilecek ve fayda, verimlilik, tasarruf **ölçülebilecektir.**
 - **EKDS ve KEC'e geçiş için 1-3 yıllık dönemin ilk adımları atılacaktır.**



Elektronik Güvenlik Altyapısı (EGA) A.Ş. Hakkında

%100 yerli üretim ve milli yazılım geliştirerek, elektronik güvenlik hizmetleri sunmak amacıyla 2006'da kurulan Elektronik Güvenlik Altyapısı A.Ş; konusunda uzman ekibiyle **E-İmzanın ülkemizde gelişmesine ve yaygınlaşmasına liderlik etmektedir**. Aynı zamanda E-Fatura, E-İhale ve Mobil İmza kavramlarının ülkemizde oluşmasında etkin rol almış, ARGE ve danışmanlık görevi üstlenmiştir. EGA, sunduğu çözümlerinin/ürünlerinin tamamını kendi bünyesinde geliştirmektedir ve kurulduğu günden bu yana 500'ü aşkın kamu ve özel sektör müşterisine anahtar teslimi e-dönüşüm hizmetleri sunmaktadır.

www.ega.com.tr

www.bionay.com.tr

e-İmza Çözümlerimiz

- 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 Şube:**
Avni Dilligil Sok. Çelik İş Merkezi A Blok No:11 Kat:2 Daire:7
Mecidiyeköy, Şişli / İstanbul
- **Teknopark Şube:**
Teknopark İstanbul Sanayi Mahallesi, Teknopark Bulvarı No:1-1C Blok Kat:3 D:1306
34906 Pendik / İstanbul

Tel: 0-216-510 8096

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 |
| 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 |
| KDS | Kimlik Doğrulama Sunucusu |
| KDPS | Kimlik Doğrulama Politika Sunucusu |
| KVK | Kişisel Verileri Koruma |
| KVKK | Kişisel Verileri Koruma Kanununu/Kurumu |
| NES | Nitelikli Elektronik Sertifika |
| NVİ | Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü |
| Protection Profile (PP) | Koruma Profili |
| SSL | Secure Socket Layer |
| TCKN | Türkiye Cumhuriyeti Kimlik Numarası |
| TSE | Türk Standardları Enstitüsü |
| TÜBİTAK BİLGEM | Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi |
| WiFi | Ofis ortamındaki mobil ağ |