Türkiye Cumhuriyeti Kimlik Kartı (TCKK) ve Elektronik İmza

Vural ÇELİK,
Dr.Oktay ADALIER,
TÜBİTAK BİLGEM

Özet

Bu çalışma, yeni nesil TCKK' nın elektronik imza ile ilişkisini açıklamayı amaçlamaktadır. Çalışma, sadece Türkiye' de TCKK' nın ve elektronik imzanın kullanacağı alanları kapsayacak şekilde tasarlanmıştır. Çalışma, TCKK projesinin çıktısı olarak, proje tecrübelerine ve sonuçlarına dayanmaktadır. Çalışmamızda, nitelikli elektronik sertifika ve anahtarların, uzaktan Kart Erişim Cihazı (KEC) aracılığı ile TCKK' ya yüklenmesi sonucunda, günlük yaşamdaki değişmeler ve elektronik imza kullanımındaki etkilerini tespit etmiştir. Çalışmanın sonuçları, endüstriyel kurumlarla paylaşılmış ve kurumların etkileri süreçlerinde değerlendirmesi için gerekli olan teşvik ve destek sağlanmıştır.

Anahtar Sözcükler: *TCKK, Nitelikli Elektronik Sertifika(NES) ve Anahtarlar (Açık ve Özel Anahtar) Kart Erişim Cihazı.*

Giriş

Son zamanlarda birçok alanda kullanılan elektronik imza, gerek kurumlar gerekse bireyler için birçok yönden avantaj sağlamaktadır. Bu avantajlardan bazıları; kâğıt israfının azalması, iş süreçlerinin kısalması, süreç maliyetlerin azalması, verimliliğin ve etkinliğin artması vb. Ülkemizde ise elektronik imza kullanımı, 2004 yıllında 5070 Sayılı Elektronik İmza Kanunun yürürlüğe girmesi ile başlamıştır. Elektronik imzanın hayata geçmesi ile günümüze kadar kullanım oranı geometrik olarak artmıştır. Elektronik imza kullanımının artmasındaki en büyük etkenler, elektronik imza uygulamalarının yaygınlaşması, elektronik imza fiyatların düşmesi, endüstriyel süreçlerin elektronik imzayı içerecek şekilde yenilenmesi olduğu söylenebilir.

Elektronik imzanın kullanılması ile hem kurumlar hem de bireyler tarafından yeni ihtiyaçların ortaya çıktığı söylenebilir. Bu ihtiyaçların başında elektronik olarak kimlik doğrulama gelmektedir. Bu ihtiyaca cevap vermek için TÜBİTAK UEKAE tarafından yürütülmekte olan e-Kimlik projesi başlatılmıştır. Proje, Türkiye' deki vatandaşların elektronik ortamda güvenilir bir şekilde kimliklerini doğrulamayı ve

doğrulatmayı hedeflemektedir. Proje sonucunda, vatandaşlara elektronik ortamda kimliklerini ispat edebilmeleri için yeni nesil Türkiye Cumhuriyeti Kimlik Kartları (TCKK) ortaya çıkacaktır. TCKK' nın temel işlevi olan elektronik ortamda kimlik ispatının yanında, elektronik imza atabilme özelliği de bulunmaktadır. TCKK' nın içine, Elektronik Sertifika Hizmet Sağlayıcıları (ESHS) tarafından NES ve anahtarların, KEC aracılığı ile yüklenmesinden sonra TCKK ile nitelikli elektronik imza atılması mümkün olmaktadır.

TCKK

TCKK, vatandaşa ait nüfus, fotoğraf ve parmak izi bilgilerinin kart üzerindeki temaslı yongaya güvenli bir şekilde kaydedilmesini ve bu işlemden sonra yetkisiz kimseler tarafından kartın yeniden üretilmesini ya da kart içindeki bilgilerin değiştirilmesini olanaksız hale getirecek şekilde tasarlanmıştır. E-Kimlik projesinde tasarlanmış ve proje paydaşları tarafından onaylanmış olan TCKK' nın genel özellikleri şu şekildedir:

- 10 yıllık dayanıklılık ömrüne sahip polikarbon malzemeden üretilmiş kart gövdesine sahiptir.
- Kişinin rahatlıkla taşımasına ve kullanmasına olanak verecek kimlik kartı, standart bir akıllı kart boyutlarında olmakla birlikte, kadın ve erkek kişiler için tek tip kart tasarımına sahiptir.
- Taklit edilemez olmakla beraber, tahrip ya da tahrif edildiğinde tespit edilmesine imkân veren görsel ve elektronik güvenlik özelliklerine sahiptir.

o Fiziksel önlemler (Rainbow, guilloce, OVİ, UV, DOVİD, Micro yazı, raster, MLI, Relif)

o Elektronik önlemler (CC EAL 5+ Yonga, CC EAL4+ İşletim Sistemi)

- Ön ve arka yüzünde yer alan kısımlar ve bu kısımlar içerisindeki bilgiler, Uluslarası Sivil Havacılık Örgütü (ICAO-International Civil Aviation Organization) ICAO 9303-3 standardına uygundur.
- ICAO 9303 standardına uygun MRZ baskı ve karttaki temassız yonga sayesinde seyahat kartı olarak kullanılabilmesine olanak sağlamaktadır.
- Kişiye ait yazılan veriler, güvenli olarak saklanır ve değiştirilemez özelliktedir.
- Kişiye ait nüfus bilgilerinin ön ve arka yüzünde bulundurması ile kolay, hızlı ve güvenli görsel kullanım sağlamaktadır.
- Standart bir akıllı kartın sunduğu bütün güvenlik özelliklerini desteklemektedir. Kart içerisinde yer alan elektronik veriler, kriptografik anahtarlar ile korumalı olarak saklanabilmektedir.
- Farklı yöntemler (11 farklı yöntem bulunmaktadır) ile kart sahibi doğrulanmaktadır.
- Uluslararası ISO/IEC 14443 (Temassız) ve ISO/IEC 7816 (Temaslı) standartlarını desteklemektedir.

TCKK üzerindeki yonganın içinde bulunan ve kimlik doğrulamaya ve elektronik imza atmaya yarayan bilgilerin tümü Tablo 1' de verilmiştir.

Tablo 2: TCKK Temaslı Yonga İçindeki Bilgiler

Kişisel Ait Kimlik Bilgileri	**Kişiye Ait Bilgileri**	**Kart Durum Bilgisi**	**Sertifikalar**
Adı	Sayısal Yüz Resmi (ISO 19794-5)	Kişisel Mesaj	Kimlik Doğrulama sertifkası
Soyadı	Islak İmza Resmi (ISO 19794-7)	Rüşt Mesajı	CVC sertifikası
Baba Adı	Parmak İzi	Biyometrik hata sayacı	Kart yayıncı sertifikası
Anne Adı	Damar İzi		Elektronik imza sertifikası (isteğe bağlı) NES ve anahtarlar
Doğum Yeri	MRZ		
Doğum Tarihi			
Cinsiyet			
Medeni Hali			
Önceki Soyadı			
T.C. Kimlik Numarası			

TCKK ve NES

Elektronik imza uygulaması, TCKK'da yer alan ve kart sahibinin nitelikli elektronik sertifikası ile kanuni geçerliliği olan elektronik imza işlemlerinin yapılabilmesini sağlar. Kişi, sahip olduğu kart üzerindeki elektronik imza uygulaması sayesinde, elektronik ortamda gerçekleştirilen işlemlerde ıslak imzası gibi birebir olarak hukuksal bağlayıcılığı olan elektronik imzasını da atabilecektir. Elektronik imza özelliğinin kullanılması için Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (NVİ) tarafından kişiye teslim edilecek olan TCKK temaslı yongasında özel bir alan bulunmaktadır. Bu alana yine Elektronik Sertifika Hizmet Sağlayıcılarına (ESHS), NVİ tarafından verilen Rol Sertifikaları ve anahtarları ile erişim yapılabilmektedir. Bu sayede TCKK üzerindeki elektronik imza alanına yetkisiz kişilerin ve/veya kurumların erişmesi engellenmektedir. TCKK' nın elektronik imza özelliğini kullanmak isteyen kart sahibinin, e-imza konusunda faaliyet gösteren bir ESHS' den (Başvuru yapılacak olan ESHS, başvurunun kamusal veya bireysel olmasına göre değişmektedir) TCKK' sına elektronik imza sertifikasını ve anahtarlarını, KEC aracılığı ile yükletebilmesine olanak tanınmıştır.

Sonuç

TÜBİTAK UEKAE ve Endüstri ile yapılan çalışmalar sonucunda, TCKK'yı nitelikli elektronik imza aracı olarak kullanmak, kurumlara ve kullanıcılara bazı kazançlar sağladığı görülmüştür. Bu kazançlardan başlıcaları; Maliyet, Kolay Başvuru Süreci ve Elektronik İmza kullanımının yaygınlaşmasıdır.

Maliyet

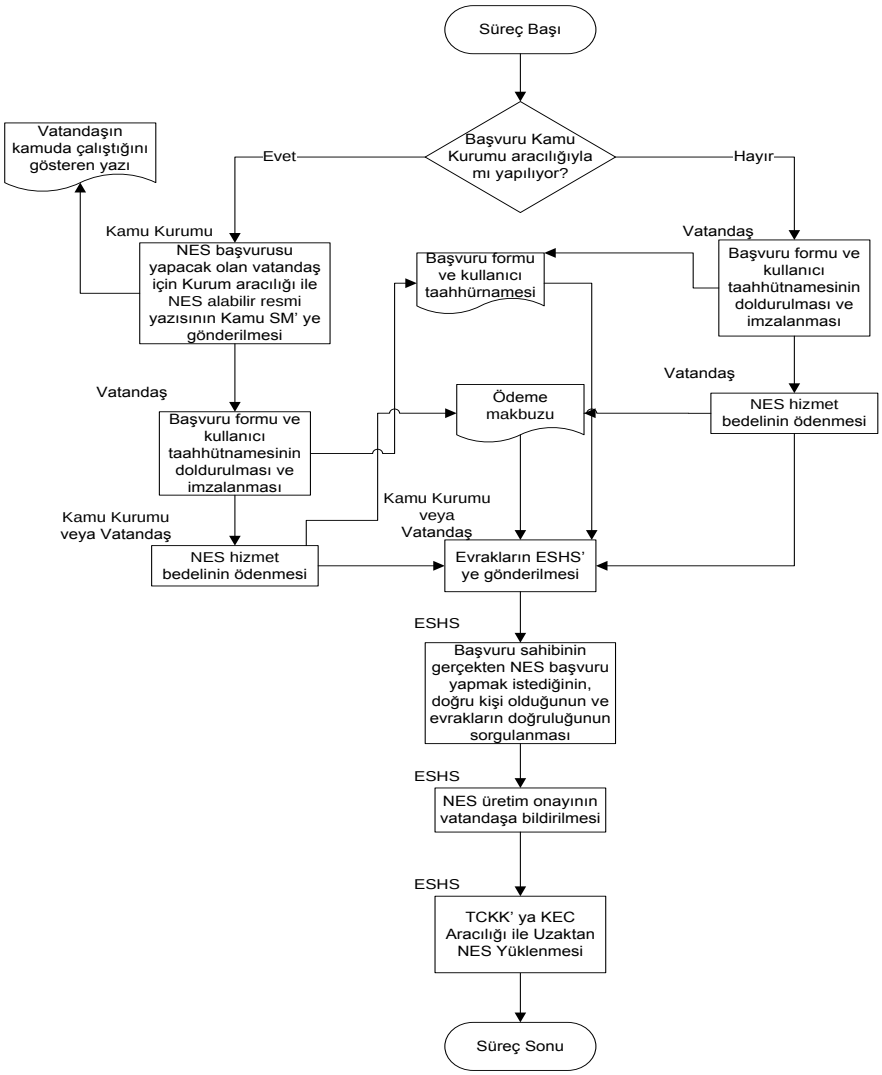
Mevcut durumda, NES' in ve anahtarların yüklenmesi için bir akıllı kart gerekmektedir. Akıllı kart için TCKK' nın kullanılması, ikinci bir kartın kullanılmamasını sağlamakta ve maliyetleri kartın maliyeti kadar düşürmektedir. Bunun yanında, mevcut NES başvurularında, NES' in sahibine teslim edilmesi için lojistik (Kargo, özel teslimat vb) maliyeti söz konusudur. Fakat, NES' in TCKK' da kullanılması söz konusu olduğunda, lojistik maliyetleri ortadan kalkmaktadır. Çünkü TCKK' nın içine elektronik imza anahtarları ve NES yüklenmesi uzaktan KEC aracılığı ile yapılmaktadır. TCKK' nın içine elektronik imza yüklenmesine ilişkin süreç Şekil 1 de gösterilmiştir.

Kolay Başvuru Süreci

NES başvuru süreci, hem bireysel hem kurumsal olarak kısalmaktadır. TCKK' ya uzaktan KEC ile yükleme yapılacağından dolayı lojistik süresi, NES kart basım süresi, başvuru için kimlik doğrulama gibi faaliyetlere ayrılan süre ortadan kalkacaktır. TCKK' nın elektronik imza özelliğinin kullanımında, maliyet başlığı altında bahsedildiği gibi lojistik gerekliliği ortadan kalkmaktadır. Bunun yanında elektronik imza kartı için yeni bir kartın basılması gerekmediğinden, üretim süreside tedarik sürecinin dışında kalmaktadır. Son olarak, yapılacak olan kimlik doğrulama, TCKK ile biyometrik veri ve PIN kullanarak gerçekleştirileceğinden, başvuru sahibi kimliğini elektronik ortamda ispatlamış olacaktır.

NES' in yaygınlaşması

Hem maliyet olarak düşecek olan NES fiyatları hem de kolay başvuru süreçleri, NES' in yaygınlaşmasında çok önemli rol oynayacaktır. Mevcut durumda, NES' in tedarik sürecinin uzun sürmesi, kısa sürede NES sahibi olmak için yüksek maliyetlere katlanma zorunluluğu ve NES' e sahip olmak için gerekli olan maliyet, NES' in yaygınlaşmasını yavaşlatmaktadır. Fakat, hem başvuru süreci olarak hem de maliyetlerdeki azalma, bireyleri ve kurumları elektronik imza kullanma konusunda teşvik etmektedir.



***Şekil 3**: TCKK'ya Uzaktan NES Yüklenmesi*

Şekil 1' de TCKK' ya uzaktan NES yükleme süreci akış olarak verilmiştir. Yeni süreç ile mevcut süreç başvuru evraklarının tamamlanmasına kadar aynı işlemektedir. Süreç, NES' in kişi için üretilmesinde değişiklik göstermektedir. NES' in kişi için üretilmesine onay verildikten sonraki süreci genel hatları ile şu şekildedir:

- NES talep eden kişinin TCKK' sını KEC' e takması
- Kişinin TCKK ile biyometrik veri ve PIN kullanarak kimliğini ispat etmesi
- ESHS' nin anahtarları TCKK' içinde ürettirmesi veya ESHS' nin güvenliğinde üretilmiş anahtarları TCKK' ya yazması
- Üretilen anahtarlara karşılık gelen NES' in ESHS tarafından üretilmesi ve TCKK' ya yüklenmesi
- KEC ekranında, TCKK elektronik imza PIN bilgisinin, NES sahibine gösterilmesi

TCKK' nın KEC' den çıkarılmasından sonra, TCKK' nın sahibi elektronik imzasını istediği gibi kullanabilmektedir.

Teşekkür

Çalışmada, e-Kimlik projesi çıktılarının ve endüstriyel çalışmaların çıktılarının kullanılmasını sağlayan Sayın Proje Yöneticimiz Dr. Oktay ADALIER' e çok teşekkür ederiz.

Kaynakça

Çelik V., (2013). TCKK' ya Uzaktan NES Yükleme Yaşam Döngüsü. *TÜBİTAK UEKAE E-Kimilk Projesi.*

Çelik V., (2013) TCKK Kullanım Eğitim Dokümanı. *TÜBİTAK UEKAE E-Kimilk Projesi.*

Çelik V., (2013) *Rol Sertifikaları Yaşam Süreci, TÜBİTAK UEKAE E-Kimlik Projesi.*