BİYOMETRİK İMZA VE NİTELİKLİ ELEKTRONİK İMZA KARŞILAŞTIRMASI

Biyometrik İmza ve Nitelikli Elektronik İmza

5 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu elektronik imza konusunda Türkiye'deki temel yasal düzenlemedir. Avrupa Birliği (AB) 1999/93/EC Direktifini model alan 5070 sayılı Elektronik İmza Kanunu'nda güven hizmetleri kapsamı elektronik imza ve zaman damgası ile sınırlı tutulmuştur. 2014 yılında ise günümüz gereksinimlerini karşılamak için elektronik kimlik tanımlama ve güven hizmetleriyle ilgili bir AB tüzüğü olan eIDAS (910/2014/EC) yayımlanarak güven hizmetleri çeşitlendirilmiştir.

eIDAS; basit, gelişmiş ve nitelikli olmak üzere birbiri üzerine yapılanan üç farklı elektronik imza türü tanımlar. Bu imza türleri ve sağlaması gereken koşullar;

Basit Elektronik İmza: Başka bir elektronik veriye eklenen veya mantıksal olarak bağlı olan elektronik veridir.

Başka bir deyişle imzalayanın, belgeye kabul veya onayının kanıtı olarak sunulabilecek elektronik biçimdir. Bu, taranmış bir imza imgesi ya da "Kabul ediyorum" butonuna tıklanması olabilir. Basit elektronik imza tüm elektronik imzalar için temel oluşturur.

Sağlaması gereken koşullar:

- İmzalanan veri elektronik biçimdedir.
- İmza değeri diğer elektronik verilere eklenir veya mantıksal olarak ilişkilendirilir.
- İmza değeri elektronik biçimdedir

Gelişmiş Elektronik İmza: Daha yüksek düzeyde imzalayan kimliği doğrulama, güvenlik ve bilgi sızdırmazlığı sağlayan özel gereksinimleri karşılaması gereken bir elektronik imza türüdür. Bu imza türü, basit elektronik imzanın sağlaması gereken koşullara ek olarak içerik ile imza ve imza ile imzacı arasında eşsiz bir bağ olmasını zorunlu kılar.

Sağlaması gereken koşullar:

- İmzacı ile benzersiz şekilde bağlantılıdır.
- İmzacıyı belirleme yeteneğine sahiptir.
- İmzacının kendi kontrolünde benzersiz veriler kullanılarak oluşturulur.
- Veri değişiklikleri tespit edilebilecek şekilde ilgili olduğu veriye bağlanır.

Nitelikli Elektronik İmza: AB üye devletlerinde özel bir yasal statüye sahip olan ve **ıslak imzanın yasal karşılığı olan tek elektronik imza türüdür.** Bu imza türü, gelişmiş elektronik imzanın sağlaması gereken koşullara ek olarak imzacı sertifikasının akredite bir Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) tarafından verilmesini ve kriptografik anahtarların nitelikli elektronik imza oluşturma aracı içerisinde tutulmasını zorunlu kılar.

Sağlaması gereken koşullar:

- Nitelikli elektronik imza oluşturma cihazı tarafından oluşturulur.
- Elektronik imzalar için nitelikli sertifikaya dayanan elektronik imza oluşturma verileri kullanılarak oluşturulur.
- Nitelikli elektronik imza oluşturma cihazı ve nitelikli elektronik sertifika gereksinimleri, eIDAS tüzüğünde tanımlanmıştır.
- Islak imzayla eşdeğerdir.

Biyometrik imza, imza sahiplerinin belirli biyometrik verilerini kullanarak imzalarını özel bir tablet/ped üzerinde oluşturmaları ve genellikle bu verilerin imzalanan belgeye çözülemez biçimde bağlanmasıyla elde edilir.

Biyometrik imza çözümlerinin uygulanması için imzacının biyometrik verilerini yakalayabilecek kabiliyete sahip özel bir cihaza bağlantı olması gereklidir. Bu cihazlar hem statik verileri (imzanın resmi gibi) hem de dinamik verileri (hızlanma, hız, eğim açısı, basınç vb.) yakalayabilir ve kaydedebilir. Sonuç olarak, hem statik hem de dinamik veriler elektronik belgede saklanır.

Biyometrik imza çözümleri belirli bir standart çerçevesinde tanımlanmadığından farklı kurgusal özelliklere sahiptir. En iyi yeteneklere ve güvenlik düzeyine sahip cihaz ile oluşturulmuş biyometrik imza ancak gelişmiş elektronik imzaya karşılık gelebilir, ıslak imza ile eşdeğer olan nitelikli elektronik imza isterlerini nitelikli elektronik imzanın tanımı gereği karşılamaz.

Gelişmiş elektronik imza koşullarını sağlayan biyometrik imza ile nitelikli elektronik imza, sahip oldukları özellikler bakımından karşılaştırılmış ve avantaj/dezavantajları aşağıdaki tabloda verilmiştir.

Dezavantajlı Durum *Avantajlı Durum*

Özellikler	Biyometrik İmza	Nitelikli Elektronik İmza
Islak imzaya denklik	eIDAS tüzüğüne göre yasal olarak geçerli olmasına rağmen ıslak imzayla denk sayılmamaktadır.	eIDAS tüzüğüne ve 5070 sayılı Elektronik İmza Kanunu'na göre ıslak imza ile eşdeğer olan tek elektronik imza türüdür.
İmza oluşturma verisinin güvenliği	Biyometrik veriler, imza tableti/pedi tarafından imzacının tanınması veya imzanın doğrulanması amacıyla kaydedilmektedir. Bu durum imza oluşturma verisini güvenlik zafiyetlerine karşı açık hale getirmektedir.	İmza doğrulama verisiyle (açık anahtar) matematiksel olarak ilişkilendirilmiş imza oluşturma verisi (özel anahtar), güvenli elektronik imza oluşturma aracı içerisinde tutulmaktadır. Özel anahtara yalnızca imzacı tarafından erişilmektedir.
İmzalayanla benzersiz bağlantı	Biyometrik imza, kişiye özel olan ve bir başkası tarafından taklit ve tekrar edilemeyen verilerin (hız, eğim vb.) birleşiminden oluşur. Ancak imza oluşturma verisinin güvenliğinin tehlikeye girmesi durumunda biyometrik imzanın imzacıyla olan bağlantısı da riske girecektir.	Nitelikli elektronik imza açık anahtar kriptografisine dayanır. Açık anahtarlı kriptografide kullanılan özel anahtar sadece sahibi tarafından kullanılabilir. Herkesin erişimine ve kullanımına açık olan açık anahtarla matematiksel bağlantısı vardır.
İmzalayanı belirleme yeteneği	Biyometrik imza uygulamaları, aynı kullanıcının farklı zamanlarda oluşturduğu imzaları her defasında önceki örneklerle kıyaslayarak imzacı ile imza arasında eşleştirme sağlar. Ancak imza oluşturma verisinin güvenliğinin tehlikeye girmesi durumunda imzacının belirlenmesi de riske girecektir.	Nitelikli elektronik sertifika, sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşır ve taşıdığı açık anahtar bilgisinin belirtilen kişi veya kuruma ait olduğunu temin eder.
İmzalayanın kendi kontrolü altındaki imza oluşturma verilerini kullanması	İmzalayan kişi ıslak imzaya benzer şekilde imzalama işlemini gerçekleştirir. Ancak imza oluşturma verisinin güvenliğinin tehlikeye girmesi durumunda imza üzerinde tam kontrol sağlanamayacaktır.	İmzacı, güvenli elektronik imza oluşturma aracı içerisinde yer alan imza oluşturma verisine PIN ile giriş yaparak erişim sağlar.

İmzalanan belgeyle imza arasındaki bağlantı	Bazı biyometrik imza uygulamaları imzalanan belgenin özet değeriyle biyometrik veriyi şifreleyerek paket halinde tutma kabiliyetine sahiptir. Ancak tüm uygulamalarda biyometrik imzanın oluşturulduğu cihazda imzacıya gösterilen belgenin imzalandığı garanti edilemez.	Nitelikli elektronik imza içerisinde imzalanan belgenin özet değeri yer almaktadır. Bu sayede imzanın imzalanan belgeyle ilişkisi koruma altına alınır.
İmzalı verilere bağlı olarak daha sonra yapılacak değişikliklerin tespit edilebilmesi	İmza işlemi sırasında oluşturulan belgeyi şifreleme kabiliyetine sahip biyometrik imza uygulamaları mevcuttur. Ancak şifreleme yapılmadığında imzalı veri üzerinde sonradan değişiklik yapılabilir.	Nitelikli elektronik imza açık anahtarlı kriptografiye dayandığı için imzalı veride yapılacak herhangi bir değişiklik imzanın bozulmasına sebep olur.
İmza doğrulama verisinin erişilebilirliği	İmza doğrulama genellikle anlık değil, itilaf olması durumunda mahkemece imzacının imzasıyla mevcut imzanın kıyaslanması yordamıyla yapılır. Bazı uygulamalar ise imzacının biyometrik verilerini önceden alarak sistemlerinde saklar ve oluşturulan imzaları anlık doğrulayabilir.	İmza doğrulama anlık olarak yapılır. İmza doğrulama verilerine nitelikli elektronik imza içerisinden veya ESHS aracılığıyla erişilebilir.
Standardizasyon	Biyometrik verilerin yakalanmasıyla ilgili uluslararası standartlar bulunmasına karşın biyometrik imzanın oluşturulmasıyla ilgili herhangi bir standart bulunmamaktadır.	Nitelikli elektronik imza formatları uluslararası standartlar ile belirlenmektedir.
Ortak çalışabilirlik	Biyometrik imza standardı olmadığından ortak çalışabilirliğin sağlanması mümkün görünmemektedir.	Nitelikli elektronik imza, uluslararası standartlar kapsamında belirlendiğinden ortak çalışabilirliği sağlar.
İmzanın uzun dönemli doğrulanabilirliği	Belirli bir standart kapsamında olmadığından imza oluşturma esnasında kullanılan cihaza bağlı olarak biyometrik verinin doğrulanmasında farklılıklar oluşabilir. Tanımlanmış bir arşivleme mekanizması bulunmadığından imzanın uzun dönemli korunması garanti edilemez.	Nitelikli elektronik imza belirli formatlarda oluşturulmaktadır. Kullanılan imza uygulaması imza doğrulama sonucunu etkilemez. Uluslararası standartlarda imzanın uzun dönemli korunması için arşivleme mekanizmaları tanımlanmaktadır.
İmza zamanının tespit edilebilmesi	Biyometrik veri içerisine imzalama zamanı eklenerek paket halinde saklanabilir. Ayrıca zaman damgasıyla biyometrik veriyi koruma altına alan uygulamalar da mevcuttur.	Nitelikli elektronik imza içerisine beyan edilen imza zamanı eklenebilir veya imza zaman damgası ile imzanın belli bir zamandan önce var olduğu ispatlanabilir.
İmzanın özgünlüğü	Biyometrik veri ele geçirildiği durumda herhangi bir belgeye iliştirilerek tekrar kullanılabilmesi mümkündür.	Nitelikli elektronik imza değeri, her imzalanan belge için eşsizdir. İmzalanan belge içerisinden elde edilen imza değerinin başka bir belgeye iliştirilerek kullanılması söz konusu değildir.
İmzanın aktarımı	Kullanılan imza tabletinin kabiliyetine göre oluşturulan biyometrik imzanın başka bir ortama aktarılması gerekebilir. İmzanın aktarımı sırasında biyometrik verinin ek güvenlik önlemleriyle korunması gerekir.	Nitelikli elektronik imza oluşturulduğu andan itibaren kriptografik olarak korunduğu için aktarım sırasında ek güvenlik önlemi gerekmemektedir.
Kullanım kolaylığı	İmzacı, imza oluşturma cihazı üzerinde imzalama işlemi için tasarlanmış imza kalemini kullanarak imzasını oluşturur. İmza oluşturma işlemi ıslak imzaya benzer şekilde gerçekleştirildiğinden kullanım kolaylığı sağlanmaktadır.	İmza oluşturma işlemi öncesinde imzacının nitelikli bir ESHS'den nitelikli elektronik sertifika temin etmesi gerekmektedir. Ayrıca imza oluşturma işlemi için güvenli elektronik imza oluşturma aracı kullanımı zorunludur.
Cihaz bağımlılığı	Tablet veya imza pedi gibi biyometrik verileri yakalama kabiliyetine sahip cihaz zorunluluğu vardır. Bu cihazların sağlaması gereken koşullarla ilgili eIDAS tüzüğünde herhangi bir kısıtlama bulunmamaktadır.	Güvenli elektronik imza oluşturma aracı kullanımı zorunludur. Bu aracın sağlaması gereken koşullar eIDAS tüzüğünde tanımlanmıştır.