Yazılım geliştiricilerin geliştirdikleri sistemlere e-imza ve mobil imza atma fonksiyonalitesi kazandırmalarını sağlayan platformdur.

Geliştirilecek olan platformun bileşenleri aşağıda listelenmiştir.

e-İmza Aracı

Kişilerin sahip oldukları USB e-imzalar ile e-imza atmalarını sağlayan, son kullanıcı bilgisayarında çalışan uygulamadır. Bu uygulama Windows, Mac OS ve Linux işletim sistemlerinde çalışabilecek şekilde geliştirilecektir.

Uygulamanın son kullanıcı bilgisayarında çalışması için Java veya .Net gibi üçüncü parti bileşenlere ihtiyaç duymayacaktır.

Uygulama BTK tarafından yetkilendirilmiş tüm e-imza sağlayıcılar tarafında üretilen e-imzalar ile uyumlu çalışacaktır.

İmza aracının farklı yazılım geliştiricilerin geliştirdiği platformlarla güvenli şekilde çalışması için sadece izin verilen sistemlerden erişilmesini sağlayacak CORS mekanizması oluşturulacaktır. CORS saldırılarını önlemek maksadıyla, kabul edilen URL bilgileri uygulama içerisinde statik olarak saklanmak yerine, kabul edilen URL bilgileri şifreli şekilde uygulama sunucularında saklanacak, e-İmza Aracı bu şifreli dosyayı indirecektir. İndirilen dosyanın şifresi açılacak ve bu dosyanın güvenilir kaynaktan indirildiği kontrol edilerek sadece verilen URL'lerden gelen isteklere yanıt verilecektir.

İmza aracı ile internet tarayıcı arasındaki iletişim HTTPS olacak şekilde güvenlik mekanizmaları geliştirilecektir. HTTPS iletişim için alınacak sertifikanın ait olduğu URL bilgisi üzerinden e-İmza Aracına ulaşım sağlanması için MacOS ve Window işletim sistemlerinde hosts dosyasının güncellenmesi için gerekli mekanizma kurulacaktır.

İmza aracı son kullanıcı bilgisayarında çalışacağından, imza atılacak dosyanın tümünün son kullanıcı bilgisayarına indirilmeden e-imza atılmasını sağlayan mekanizma oluşturulacaktır. Bu sayede büyük boyutlu dosyaların son kullanıcı bilgisayarına indirilmesi engellenerek ağ kullanımı azaltılacak aynı zaman imzalama işlemi daha hızlı gerçekleşecektir. Ek olarak tüm dosyanın son kullanıcı bilgisayarına inmemesi sayesinde dokümanın bir kopyasına son kullanıcı ve aradaki kişiler (man in the middle) tarafından erişilmesi de mümkün olmayacaktır.

Bu işlemin gerçekleşmesi için her bir imza türü için (cades, pades) imzalanacak verinin içinde tutulduğu ve stateless şekilde imzalama yapılmasını sağlayan e-imza state objesi oluşturulması ile ilgili mekanizma geliştirilecektir.

Javascript Kütüphaneleri

Yazılım geliştiricilerin e-İmza aracına bağlantı sağlayıp e-imza işlemlerini yapabilmeleri için kullanmaları gereken metotları barından kütüphaneler geliştirilecektir.

Web API

e-İmza ve mobil imza işlemlerini gerçekleştirmek için gerekli metotları barındıran servislerdir. Bu servislere yazılım geliştiriciler kendi uygulama katmanları üzerinden erişeceklerdir.

Güvenlik gereksinimleri açısından her bir farklı uygulama kendisine atanmış bir API anahtarı ile servislere ulaşacaktır.

Web API metotları aşağıda sıralanmıştır.

PDF Dönüştürücü

Müşterinin gönderdiği Microsoft Office ve resim dosyalarını görsel özellikleri korunarak pdf formatına çeviren fonksiyondur. Bu sayede e-imza işlemi için uygun olmayan dosya formatları (makro içeren Office dosyası gibi) e-imza için uygun olan pdf formatına çevirebilecektir. Ayrıca dosyanın pdf'e çevrilmesi neticesinde PADES imza atmak da mümkün olacaktır.

CADES İmza Mekanizmaları

e-İmza

CADES B, T, LT ve LTA türünde e-imza atılması sağlanacaktır.

Mobil İmza

Ülkemizdeki tüm operatörler kullanılarak CADES B, T, LT ve LTA türünde mobil imza atılması sağlanacaktır.

PADES İmza Mekanizmaları

e-İmza

PADES B, T, LT ve LTA türünde e-imza atılması sağlanacaktır.

Mobil İmza

Ülkemizdeki tüm operatörler kullanılarak PADES B, T, LT ve LTA türünde mobil imza atılması sağlanacaktır.

PDF Düzenleme Mekanizmaları

Pdf üzerine layer olarak karekod ve doğrulama bilgisi eklenebilecektir. Layer olarak eklenmesi sayesinde orijinal pdf bozulmayacaktır. Karekod ve doğrulama bilgisi içerisinde bulunacak bilgiler müşteri tarafından belirlenecektir.