TÜBİTAK
BİLGEM

E-İmza Entegrasyon Tasarım Mimarisi

Murat Yasin KUBİLAY
Milli Açık Anahtar Altyapısı (MA3) Projesi Yöneticisi

Kasım 2012

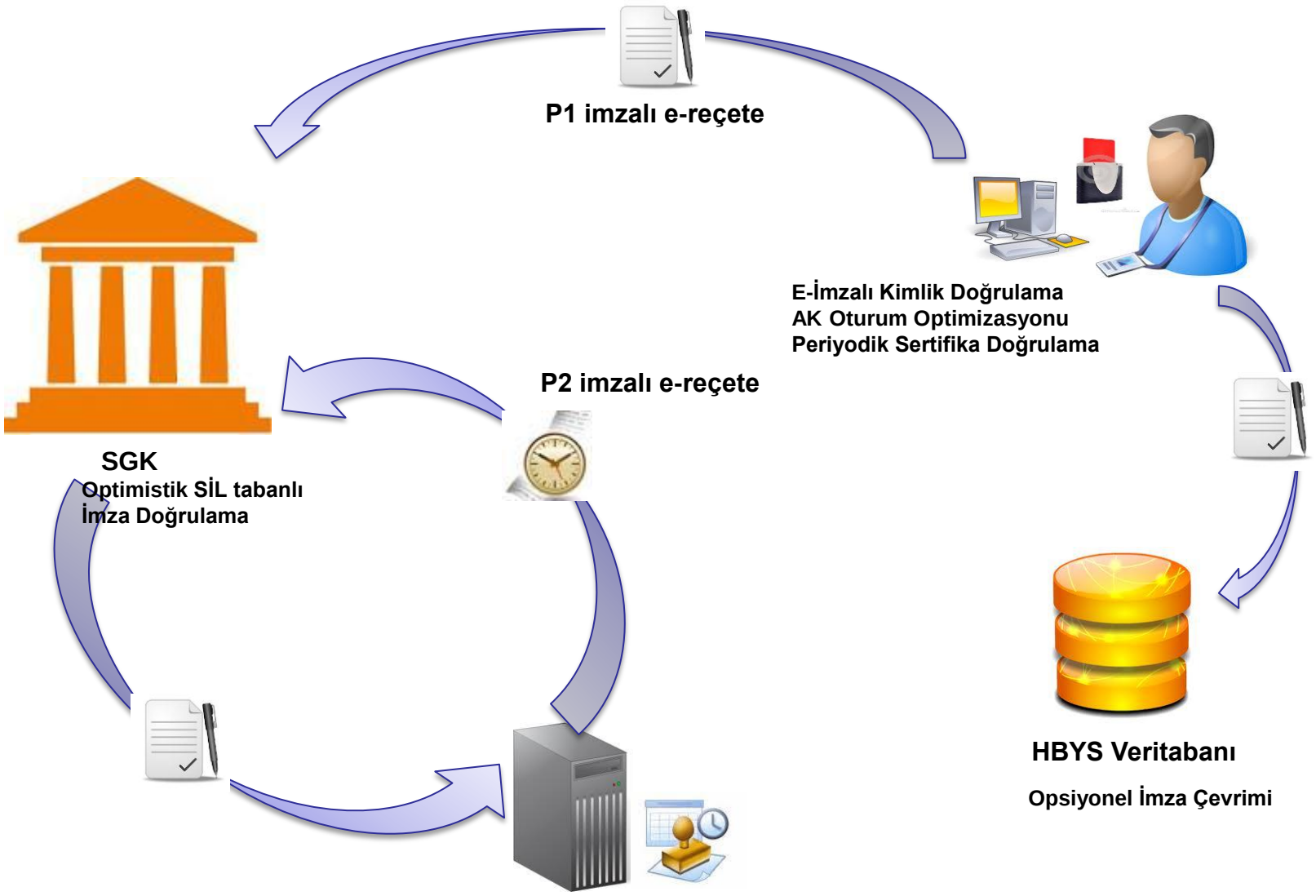
Sunum Planı

- E-İmza Gereksinimleri
- E-İmza Denemesi Nasıl Yapılır ?
- E-İmza Kütüphanelerini Nereden Temin Edebilirim ?
- İmzager

E-İmza Gereksinimleri

- Geçerli sertifikalarla oluşturulmalı
- Oluşturma süreci hızlı ve basit olmalı
- Standartlarla uyumlu olmalı
- Uzun süre doğrulanabilir olmalı
- Doğrulama ve çevrim süreci hızlı olmalı

Büyük Resim



Geçerli Sertifikalarla Oluşturulmalı

- Uygulama açılırken, ilk kimlik doğrulama e-imza ile yapılmalıdır.

- turkiye.gov.tr portaline e-imzalı giriş örneğinde olduğu gibi bir metin imzalatılabilir.
  - Bu metin dinamik olmalıdır. (Replay Attack'e karşı)

- Bu süreçte uygulama imza kontrolü yaparken sertifika geçerlilik kontrolü muhakkak yapmalıdır. Sertifika İptal kontrolünde OCSP tercih edilmelidir.

Oluşturma Süreci Basit Olmalı

- 5070 sayılı e-imza kanuna göre imzayı atan imzaladığı veriye ulaşabilmelidir.
  - İmzalanan veri imzalama esnasında gösterilebilir
  - Başka bir linkten imzalanan veriye ulaşabilir.

- Arayüz basit olmalı, hata yapmaya imkan tanımamalı

Oluşturma Süreci Hızlı Olmalı(1)

- Akıllı karta oturum 1 kere açılmalı,
  - oturum ölünceye kadar,
  - kart, okuyucudan çıkartılıncaya kadar veya
  - belli bir timeout süresince aynı oturum kullanılmalıdır.

- 1 Akıllı Kart Oturumu boyunca doktor 1 kere PIN girmelidir.

- PIN kesinlikle diskte, memory'de veya başka bir yerde **saklanmamalıdır**.

Oluşturma Süreci Hızlı Olmalı(2)

- Her bir e-imza oluştururken sertifika doğrulama **yapılmamalıdır**.
  - Sadece ilk imza atılırken bu doğrulama yapılmalı
  - Belli bir timeout süresince (politikaya göre değişebilir – örnek 3 saat) doğrulama yapılmamalıdır.

- E-imza oluştururken dış bir sisteme bağımlı olunmamalıdır.
  - P1 profilinde (BES) imza oluşturulmalıdır.

- Mevcut e-imza kütüphanesi ile BES imza 2 saniyenin altında atılabilmektedir.

- Ekran açılırken farklı bir thread'da imza atılabilecek sertifikaların okunması ve cache'lenmesi, ilk akıllı karta erişim sürecini hızlandıracaktır.

- APDU kullanımı
  - Azami hız
  - Driver bağımlılığını engeller

Standartlarla Uyumlu Olmalı

- Oluşturulan E-İmza XADES BES(P1 profili) formatında olmalıdır.
- İmzalama algoritması olarak RSA-SHA256 kullanılmalıdır.
- Eğer SGK'ya iletilmeyecek Sağlık-NET veya HBYS içinde saklanması istenen e-imzalı belgeler varsa, uzun süreli doğrulamanın sağlanabilmesi için sunucu tarafında e-imza formatı profil 4 e uygun XLONG'a çevrilmelidir.

Uzun süre doğrulanabilir olmalı

- BES imza formatında güvenli zaman bilgisi (Date&Time) yoktur.
  - E-imza'nın ne zaman oluşturulduğu kanunen ispat edilemez.

- Kanuni geçerli zaman bilgisi **zaman damgası** ile sağlanır.

- İmza doğrulanırken, sertifikanın imza oluşturma zamanında geçerli olduğunu ispat eden iptal bilgisine (OCSP-SİL) ihtiyaç vardır.

- Uzun süreli doğrulama gerektiren e-imzalı veriler, içinde kanuni geçerli zaman bilgisi ve iptal bilgisi içeren XLONG (P4 profili) formatına çevrilmelidir.

- Bu çevrim sunucu tarafında yapılmalıdır.

E-İmza Doğrulama ve Çevrim Süreci Hızlı Olmalı(1)

- SGK Sunucuları gelen her e-reçeteyi muhakkak **doğrulamalıdır**.
- Doğrulama süreci çok hızlı olmalı ve dış bağımlılığı olmamalıdır.
- Doğrulamada iptal kontrolü SİL üzerinden yapılmalıdır.
- Doğrulamada en güncel SİL kullanılmalıdır. SİL'in en geç 10 dk bir yayınlandığı varsayılmalıdır. (Bu konuda talepde bulunulmalıdır.)
- SİL'de arama sequential olmamalıdır. SİL uygulamanın memory'sinde tutulmalı ve üzerinde O (log n) süresinde arama yapılmalıdır.
- Memory'deki SİL, yayınlanan her bir yeni SİL ile güncellenmelidir.
- Diskte yer kazanmak için sıkıştırma teknikleri uygulanabilir.

E-İmza Doğrulama ve Çevrim Süreci Hızlı Olmalı(2)

- Reçete içinde doktor adı-tckimlik no ile e-imzayı oluşturan sertifikanın içindeki isim-tckimlikno eşleştirmesi yapılmalıdır.
- SGK içine kurulacak bir Zaman Damgası sunucusu ile e-imza formatı P2'ye çevrilmelidir.
- Geriye yönelik doğrulamalar için ya SİL'ler yedeklenmeli ya da KamuSM'nin hizmetinden faydalanılmalıdır.
- Reçete dışında çok daha uzun süreli doğrulanması gereken bilgiler P4'e çevrilmelidir. Çünkü arşiv formatına sadece P3 ve P4'den geçiş yapılabilmektedir.

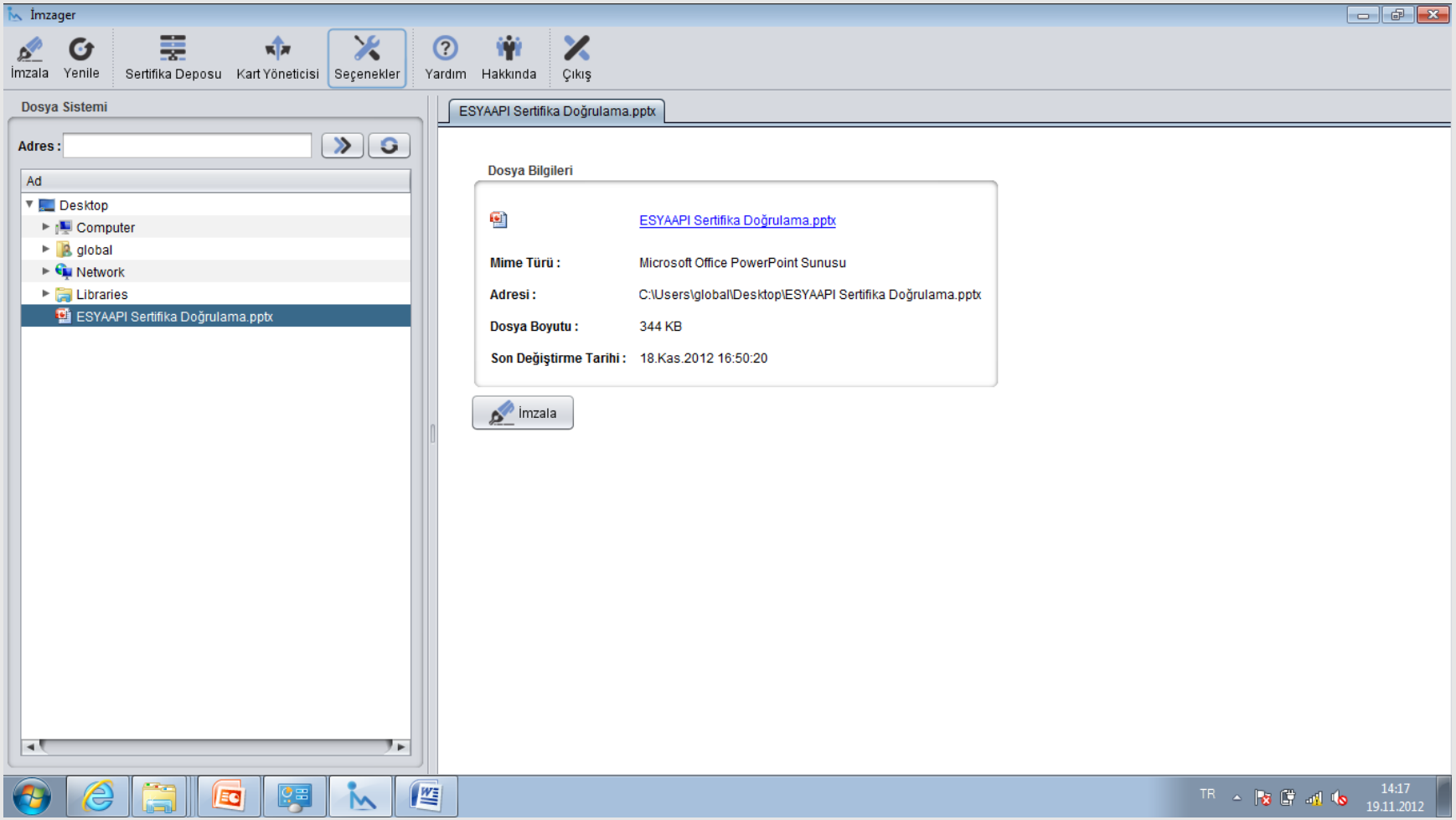
E-İmza Denemesi Nasıl Yapılır ?

- Akıllı Kartsız
  - XADES kütüphanesi içinde PFX formatındaki sertifika/anahtarları kullanarak
- Akıllı Kartlı
  - KamuSM dışındaki bir ESHS'den NES alarak
  - KamuSM'den veya başka bir yerden Akıllı Kart&Kart Okuyucu alarak ve PFX'i akıllı karta yükleyerek

E-İmza kütüphanelerini nereden temin edebilirim ?

- https://yazilim.kamusm.gov.tr adresinden E-İmza kütüphaneleri linkinden indirilebilir.
- Ücretsiz üyelik gerektirmektedir.

İmzager



- CADES, XADES formatında E-İmza oluşturmak/doğrulama
- E-İmza Profillerini destekler
- E-Yazışma formatlı veri oluşturma

Sorular

İletişim :
Tel : (0262) 648 1000 Faks : (0262) 648 1100 e-posta :bilgi@kamusm.gov.tr