TÜBİTAK
UEKAE

E-imza Profilleri

Ferda Topcan
Başuzman Araştırmacı
ferda.topcan@tubitak.gov.tr
(312) 4688486-19

İçerik

- İmza Verisi Formatı
- İmza Tipleri
- İmzalı Belgelerin Uzun Dönem Saklanması
  - Doğrulama Verilerinin Saklanması
  - E-imzanın Arşivlenmesi

E-imza Veri Formatı

ETSI: European Telecommunications Standards Institute

ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

PKCS # 7: Cryptographic Message Syntax Standard

RFC 3852: Cryptographic Message Syntax (CMS)

ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

W3C/IETF Recommendation: "XML-Signature Syntax and Processing".

E-imza Tipleri

- BES (Basic Electronic Signature) : Basit Elektronik İmza
  - İmza tarihi kesin olarak tespit edilemez
- ES-T (Electronic Signature with Time): Zaman Bilgisi Eklenmiş Elektronik İmza
  - BES imzaya zaman damgası eklenmesi ile elde edilir
  - İmzanın hangi tarihten önce oluşturulduğunun kesin olarak tespit edilmesini sağlar
- AdES (Advanced E-Signature): İleri E-imza Tipleri
  - İmzayı doğrulamak için gerekli olan doğrulama verilerinin (ESHS'ye ait sertifikalar, SİL ve OCSP Cevapları) saklanıp imzanın sertifika geçerlilik süresi dolduktan sonra da doğrulanabilmesini sağlar.
  - ES-X-LONG Tipi: İmzayı doğrulamak için gerekli olan doğrulama verilerinin imza dosyasına eklenerek saklanmasına imkan verir.

BES İmza

Hesaba
10 000 TL
aktarıyorum

E-imza Oluşturma Yazılımı

ETSI 101 733

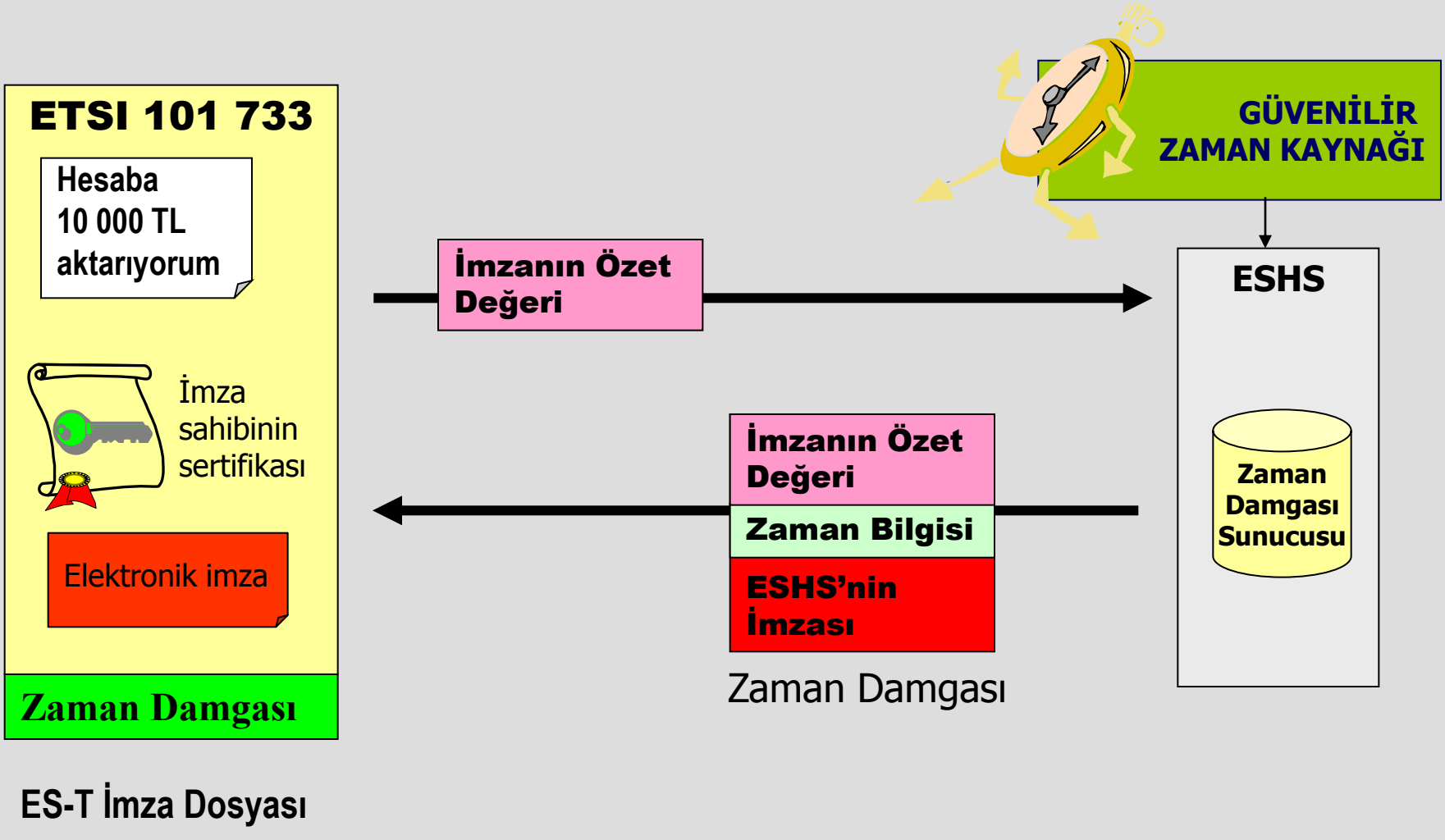
Hesaba
10 000 TL
aktarıyorum

İmza
sahibinin
sertifikası

Elektronik imza

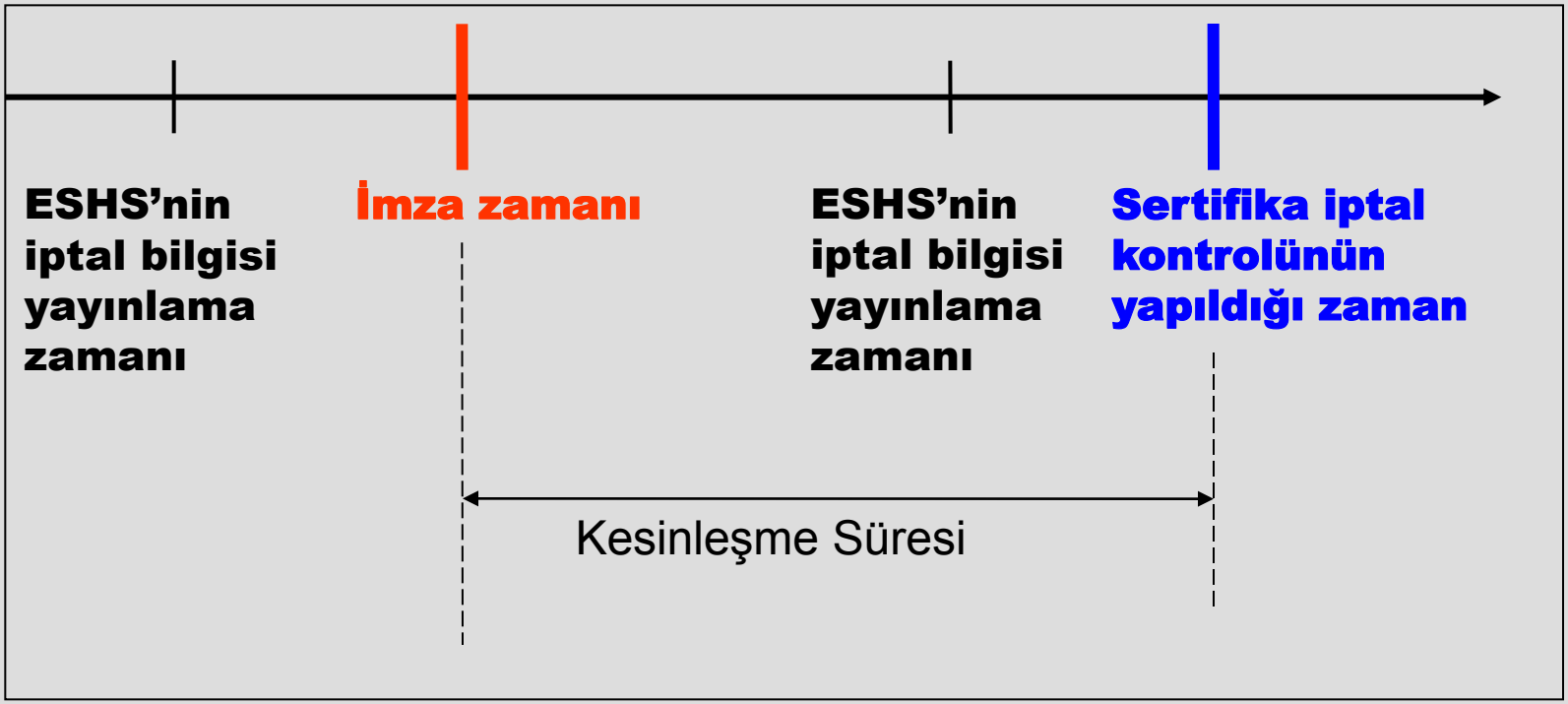
BES İmza Dosyası

ES-T İmza


ETSI 101 733
Hesaba 10 000 TL aktarıyorum
İmza sahibinin sertifikası
Elektronik imza
Zaman Damgası
ES-T İmza Dosyası
GÜVENİLİR ZAMAN KAYNAĞI
ESHS
İmzanın Özet Değeri
Zaman Damgası Sunucusu
İmzanın Özet Değeri
Zaman Bilgisi
ESHS'nin İmzası
Zaman Damgası

Kesinleşme Süresi

- İmza doğrulama imza oluşturulduktan kesinleşme süresi (grace period) kadar zaman geçtikten sonra gerçekleştirilir.



İlk İmza Doğrulama ve Doğrulama Verilerinin Toplanması

- Kesinleşme süresi sonrasında gerçekleştirilir.
- İmza sahibinin sertifikasının ve güven zincirindeki tüm ESHS sertifikalarının geçerlilik kontrolleri yapılmalıdır.
- ESHS'ye ait diğer sertifikaların (OCSP/SİL İmzalama, Zaman Damgası) geçerlilik kontrolleri yapılmalıdır.
- SİL veya OCSP cevaplarının geçerlilik kontrolü yapılmalıdır.
- Zaman damgasının geçerlilik kontrolü yapılmalıdır.
- Doğrulama verileri toplanmalıdır.
  - ESHS'ye ait sertifikalar
  - SİL/OCSP Cevapları

Doğrulama Verilerinin Saklanması ve ES-X-LONG İmza

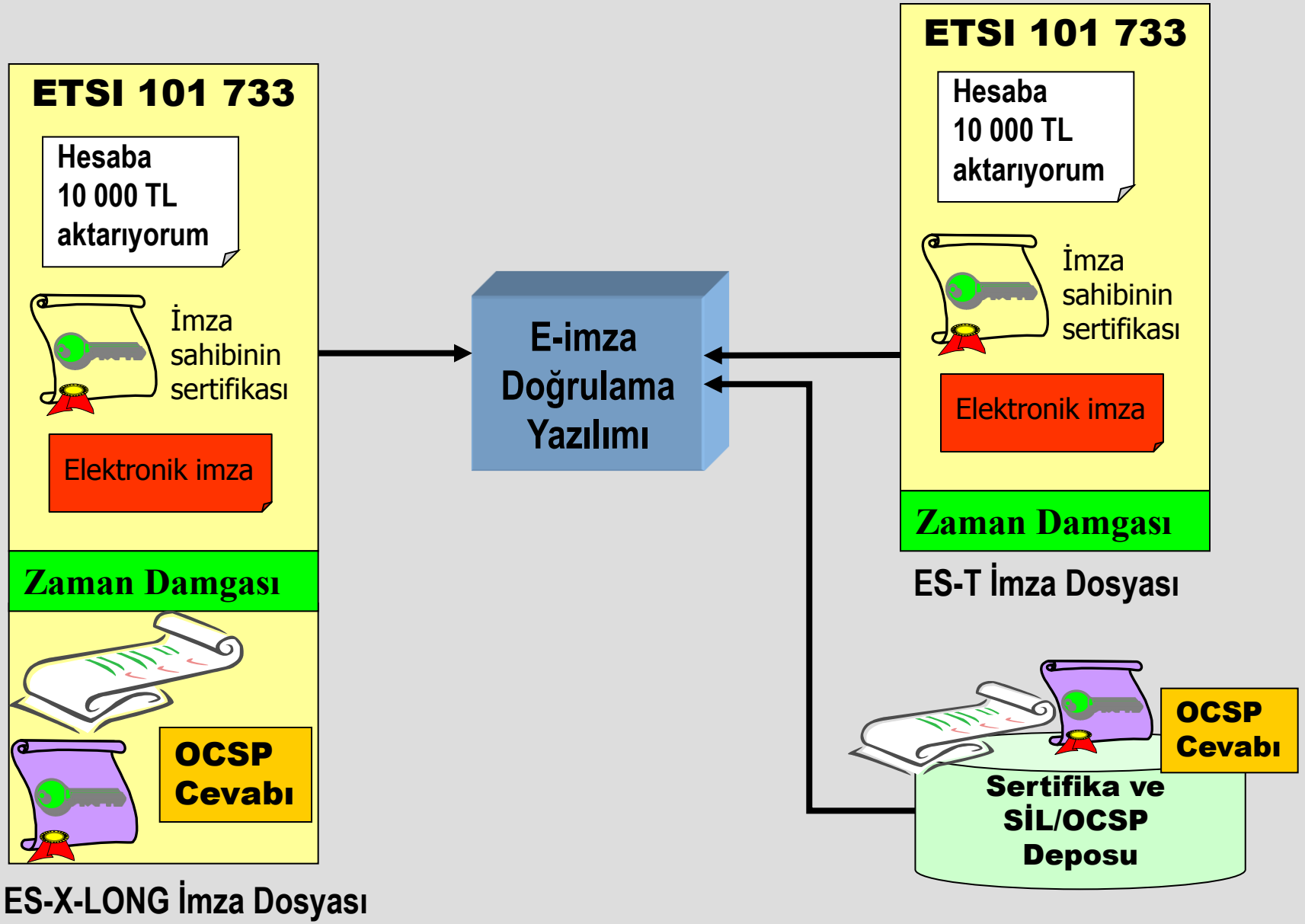
- "Doğrulama verileri" aşağıdaki yöntemlerden birisi kullanılarak saklanır:
  - İmza doğrulaması yapacak tüm kullanıcıların ulaşabileceği ortak bir alanda "doğrulama verileri" saklanır.
  - "Doğrulama verileri" imza dosyasına eklenir.

ES-X-LONG İmza Dosyası

Sonraki İmza Doğrulama İşlemi

- İlk imza doğrulamadan sonra yapılan doğrulama işlemleridir.
- İlk imza doğrulamada saklanan “doğrulama verileri” kullanılır.
- “Doğrulama verileri” aşağıdaki yöntemlerden birisi ile elde edilir:
  - Tüm kullanıcıların ulaşabileceği ortak bir alandan elde edilir.
  - İmza dosyasının içeriğinden elde edilir.
- İlk imza doğrulaması sırasında yapılan tüm kontrollerin aynısı imzanın atıldığı tarih referans alınarak tekrar yapılır.

Sonraki İmza Doğrulama İşlemi



Önerilen İmza Profilleri

Profil	İmza Ömrü	Zaman Damgası	İptal Bilgisi [1]	Kesinleşme Süresi	İmza Formatı	İmza Dosya Boyutu
P1	Anlık	Yok	SİL/ ÇiSDuP	Uygulanmaz	BES	Düşük
P2	Kısa	Var	SİL	Uygulanır	ES-T	Orta
P3	Uzun Süreli	Var	SİL	Uygulanır	ES-XL [3,4]	Çok yüksek
P4		Var	ÇiSDuP	Uygulanmaz [2]	ES-XL [4]	Yüksek

[1] İmza sertifikası için iptal bilgisi

[2] Kontrol edilecek ÇiSDuP bilgisinin "gerçek zamanlı" ÇiSDuP olduğu kabul edilmiştir.

[3] İmza ES-T tipinde atılır. Kesinleşme süresi sonrası ES-XL'a çevrilir.

[4] ES-XL formatı [2][3][5][6] da bahsi geçen XAdES-XL Type 1, CAdES-XL, PAdES-LTV formatlarına karşılık gelir.

Elektronik İmzanın Arşivlenmesi

- Elektronik imzalı dokümanların uzun dönem saklanması gerektiğinde arşivleme yapılır.
- Geçmişte kullanılan algoritmaların veya anahtarların artık güvenli kabul edilmediği durumlarda arşivleme yapılır.
- ESHS Zaman Damgası sunucularına bağlanılarak, eskiden oluşturulmuş imza dosyalarına Zaman Damgası alınması yoluyla arşivleme yapılır.
- Arşivleme yapılacak imza dosyasının ES-X-LONG tipinde olması gerekmektedir.
- Arşivleme ilerleyen zamanlarda gerektikçe tekrarlanır.

Arşiv Zaman Damgası