ELEKTRONİK İMZA

Dr. Günay TEMÜR

E-imza

- Elektronik ortamda gönderilen veya alınan bilgilerin bunları gönderen kişi veya kuruma ait olduğunun doğrulanmasını, iletilen veya alınan verilerin kimler tarafından gönderildiğinin belirlenmesini, verileri gönderenlerin gönderdiğini ve alanların aldığını inkar edememesini, gönderilen veya alınan bilgilerin içeriğinin değiştirilmemesini, başkaları tarafından elde edilse bile, içeriğin başkaları tarafından anlaşılmamasını sağlamayı garanti eden, elektronik ortamda bit katarlarından oluşturulmuş güvenli haberleşme ortamına verilen addır.

Elektronik imza,

- Finans sektörü başta olmak üzere kamu sektöründe, sağlık sektöründe ve iletişimde sıklıkla kullanılmaya başlanmıştır.
- Hayata geçirilen uygulamaların başlıca örnekleri:
  - Bankacılık işlemleri,
  - Sigorta işlemleri,
  - e-devlet uygulamaları,
  - Her türlü başvuru işlemleri,
  - Vergi ödemeleri,
  - Elektronik oy verme,
  - Sağlık bilgileri ve
  - Elektronik ofisler olarak sıralanabilir.

Elektronik İmza Teknik Altyapısı

1 Şifreleme (Kriptografi)

2 Özetleme Algoritması

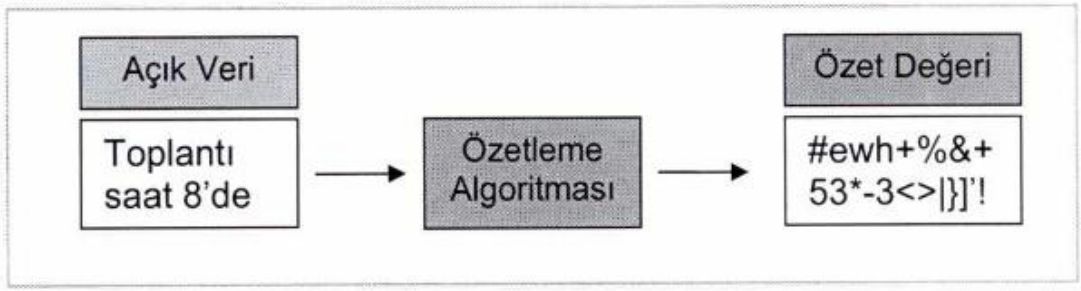
3 Elektronik İmzalama ve Doğrulama

Elektronik İmzalama ve Doğrulama

- Elektronik İmzalama, açık anahtar şifrelemesi tekniği kullanılarak yapılmaktadır. İmzalama ve doğrulama işlemleri adımlar halinde detaylı olarak aşağıda açıklanmıştır. **Adım 1** ve **Adım 2** İmzalama yapan kişi tarafında, **Adım 3** ise doğrulama yapan kişi tarafında gerçekleşmektedir.

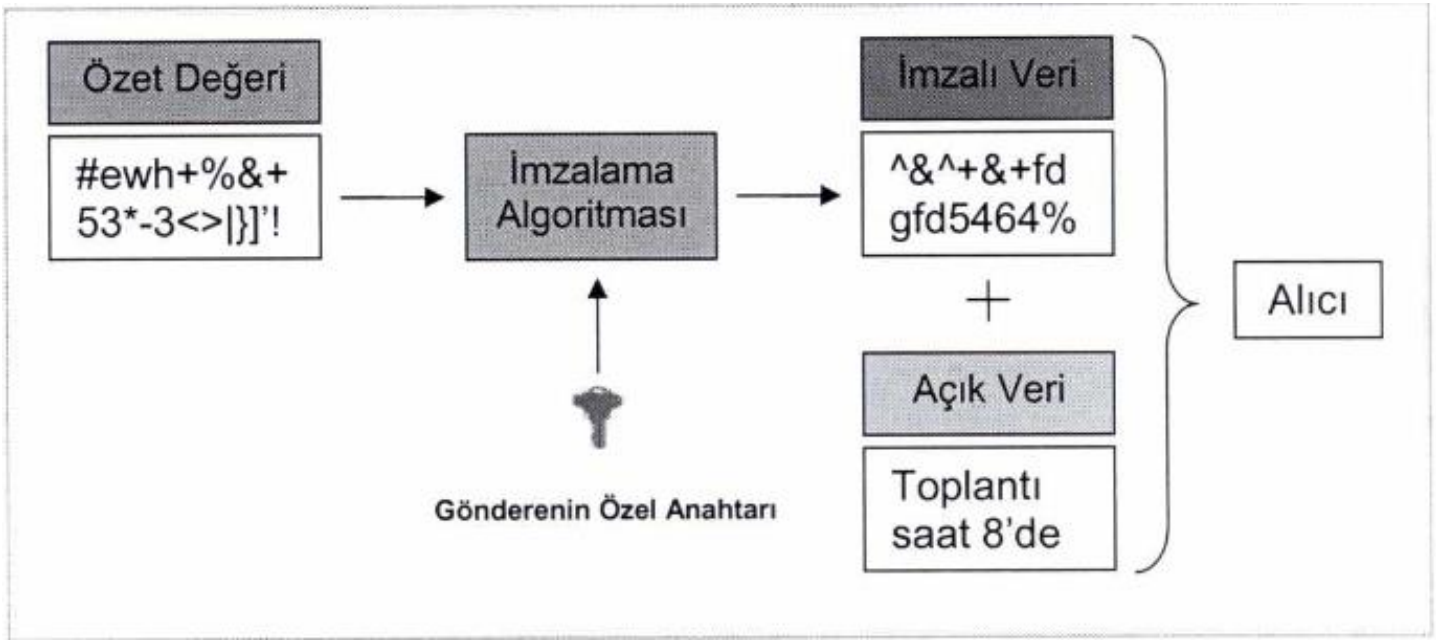
Elektronik İmzalama ve Doğrulama

- **_Adım 1**: imzalanacak veri özetleme algoritmasından geçirilerek sabit uzunlukta olan bir özet değeri elde edilir. Özet değeri hem bütünlük kontrolü için kullanılır hem de gönderilecek verinin büyük olması durumunda İmzalama süresini önemli miktarda kısaltır.



Elektronik İmzalama ve Doğrulama

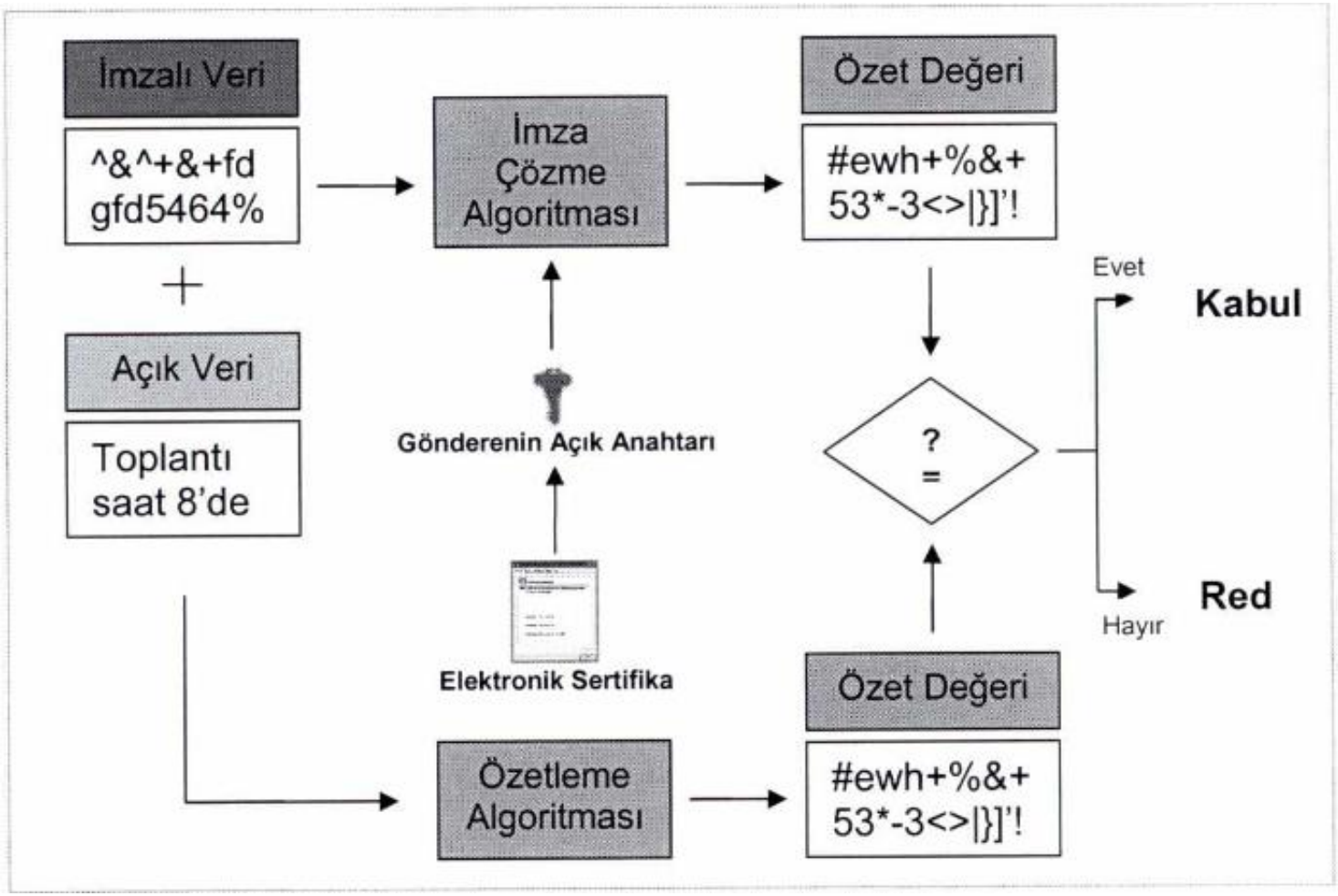
- **_Adım 2:** Özet değeri, İmzalama yapacak kişinin özel anahtarıyla şifrelenir ve imzalanan verinin orijinali ile birlikte alıcıya gönderilir.



Elektronik İmzalama ve Doğrulama

- _**Adım 3:** Alıcı, kendisine gelen imzalanmış veriyi gönderen kişinin sertifikasında bulunan açık anahtar ile çözer. Ayrıca imzalanan verinin orijinali özetleme algoritması ile işlenerek özet değeri bulunur ve imzalanan özet değeri ile karşılaştırılır. Bu iki özet değeri arasında yaşanacak bir uyuşmazlık mesajın bütünlüğünün bozulduğunu gösterir.

Elektronik İmzalama ve Doğrulama



Açık Anahtar Altyapısı (AAA)

- Açık Anahtar Altyapısı, açık anahtar şifrelemesini destekleyen protokol, hizmet ve standartlardan oluşmaktadır. Literatürde AAA için, açık anahtar sertifikasyonu üzerine kurulmuş güven zinciri veya şifreleme ve elektronik imza hizmetlerinin son kullanıcılara sunumunu sağlayan sistemler şeklinde farklı tanımlamalar da yapılmaktadır.

AAA İşlevleri

- Açık anahtar altyapısı, elektronik imzanın kullanılabilmesini sağlayan temel yapıyı oluşturmaktadır. Elektronik imza ile hayata geçirilen işlevlerin birçoğu AAA tarafından sağlanmaktadır. Bunlar arasında en önemli üç tanesi aşağıda detaylı bir şekilde açıklanmaktadır.

AAA İşlevleri

- **Kimlik Doğrulama**: Kimlik doğrulama; bir kullanıcının veya bilgisayarın kendisine ait olduğunu iddia ettiği kimliğin doğrulanması ve onaylanmasıdır. AAA`da kimlik doğrulama işlemleri özel ve açık anahtarla yapılmaktadır. Özel anahtarın gizli tutulması gerektiğinden, yapılan işlemlerin sadece ilgili tarafça gerçekleştirilebileceği kabul edilir. Bunun yanı sıra açık anahtarın ilgili kişiye ait olup olmadığının kontrolü de elektronik sertifikalarla yapılır.

AAA İşlevleri

- **Gizlilik**: Gizlilik, iletilen verilerin yetkisiz kişilerden gizlenmesi olarak tanımlanabilir. AAA`da gizlilik; simetrik ve asimetrik şifreleme kullanarak sağlanmaktadır.
- **Bütünlük**: iletilen verilerin doğruluğunun ve eksiksizliğinin sağlanması işlemidir. Gönderilen verinin hedef ve kaynak tarafından karşılıklı olarak özetleme algoritmasından geçirilerek özet değerinin hesaplanması ve çıkan sonuçların karşılaştırılması ile gerçekleştirilir.

Açık Anahtar Sertifikası

- Açık anahtar sertifikası, bir açık anahtarın kime veya neye ait olduğunu gösteren elektronik doküman olup, açık anahtar kullanılarak yapılan işlemlerin doğrulanabilmesini sağlar.

Açık Anahtar Sertifikası

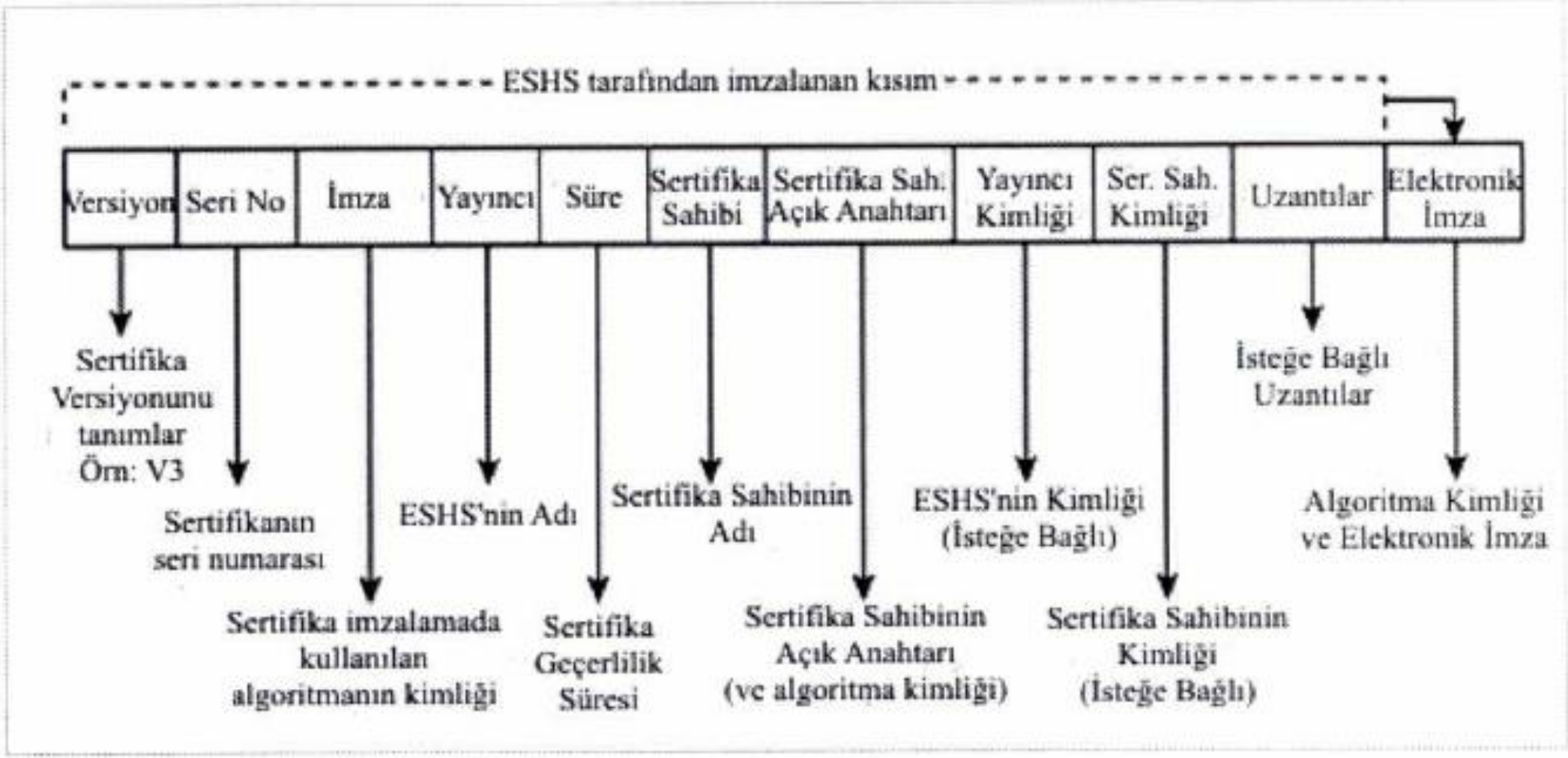
- Elektronik bir sertifika, temelde en az ait olduğu kişinin ad ve soyadı ile açık anahtarını içermek durumundadır. Fakat genelde; sertifikanın son kullanma tarihi, sertifikayı yayınlayan elektronik sertifika hizmet sağlayıcısının (ESHS) adı, seri numarası, ait olduğu bireyin elektronik posta adresi gibi bilgiler de sertifika içerisinde yer almaktadır.

Açık Anahtar Sertifikası

- Sertifikalar basit yazılımlardır ve farklı formatlarda oluşturulabilmektedir. PGP (Pretty Good Privacy), SPKI (Simple Public Key lnfrastructure - Basit Açık Anahtar Altyapısı) gibi birbirinden farklı yapıda sertifikalar geliştirilmiş olmasına rağmen, halen en yaygın kullanıma sahip olanlar ITU-T'nin(International Telecommunications Union-Telecommunications Standardization Sector - Uluslararası Telekomünikasyon Birliği-Telekomünikasyon Standardizasyon Sektörü) X.509 standardına uygun biçimlendirilmiş sertifikalardır. X.509 sertifikaları →

- Versiyon
- Seri numarası
- İmza Algoritması
- Yayınlayıcı
- Geçerlilik Süresi
- Sertifika Sahibi
- Sertifika Sahibinin Açık Anahtar Bilgisi
- Yayinlayıcının Tekil Kimliği
- Sertifika Sahibinin Tekil Kimliği gibi standart alanları içermektedir

X.509 v3 Sertifika Yapısı



Elektronik Sertifika Hizmet Sağlayıcısı

- Literatürde geçen; “Sertifikasyon Kurumu", “Yayınlayıcı Kurum" veya “Sertifika Yayınlayıcı" şeklindeki farklı terimlerin tamamı, 5070 sayılı Elektronik imza Kanununda tanımlanan elektronik sertifika hizmet sağlayıcısı ile aynı kavramı ifade etmektedir.

ESHS'nin Sunduğu Hizmetler

- ESHS'ler, elektronik imzanın kullanılmasına yönelik olarak; kayıt, sertifika oluşturma, sertifika dağıtımı, iptal ve iptal durum bilgisi gibi çeşitli hizmetler sunmaktadır:

Türkiye’de E-imza Çalışmaları

- Türkiye’de Ana Sertifika Merkezi Türk Telekomünikasyon kurumudur. Alt Sertifika Merkezleri olarak da Türktrust, E-Tuğra ve E-Güven sertifika hizmet sağlayıcıları, e-imza çalışmalarını sürdürmektedirler. Kamuya ait sertifikaların teminini TÜBİTAK-UEKAE üstlenmiş durumdadır. Bir AAA yapısının nasıl olması gerektiği ile ilgili standartlar ve teknik nitelikler 5070 Sayılı Elektronik İmza Kanunun’ da belirtilmiştir.

Nitelikli Elektronik Sertifika (NES)

- ESHS ‘ nin e-imza kullanıcısına verdiği sertifika, 5070 Sayılı Elektronik İmza Kanunun’ da Nitelikli Elektronik Sertifika olarak aşağıdaki özellikleri ile ifade edilmiştir. Sertifikanın nitelikli olması, e-imza uygulamalarında kullanıcı açısından çok önemlidir. Çünkü kullanılan basit sertifikalarla gerçekleştirilen imzalama olaylarında problem çıkabilir. Elektronik sertifika, e-imza kullanıcısının elektronik ortamdaki kimlik kartıdır. 5070 Sayılı Elektronik İmza Kanunun’ a göre elektronik sertifika;

Elektronik Sertifika

- “İmza sahibinin, imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydıdır.” Nitelikli elektronik sertifikada; Sertifikanın “nitelikli elektronik sertifika” olduğuna dair ibarenin, Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının, İmza sahibinin teşhis edilebileceği kimlik bilgilerinin, Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin, Sertifika geçerlilik süresinin başlangıç ve bitiş tarihlerinin, Sertifika seri numarasının, Sertifika sahibi diğer kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin, Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgilerin, Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzanın, bulunması zorunludur.[

ELEKTRONİK SERTİFİKA	
Sertifikanın Seri Numarası:	
Sertifika Sahibinin Kimlik Bilgileri:	
Sertifikanın geçerlilik tarihi:	
Sertifikanın geçerlilik Süresi:	
Kullanılacak algoritmalar	
Açık Anahtar bilgisi:	
Sertifikayı Yayınlayan ESHS:	
Sertifikayı Yayınlayan ESHS’ nin Elektronik İmzası:	

Elektronik İmzada Güvenlik

- Elektronik imza güvenliği, kullanılan yazılım ve donanımdan fiziksel korumaya kadar birçok faktöre bağlıdır.
- Elektronik imza güvenliğinde, klasik güvenlik önlemlerinin yanı sıra kullanılan algoritmaların ve anahtarların güvenilir olması da büyük önem taşımaktadır.
- 5070 sayılı Elektronik İmza Kanununun 5inci maddesinde yer alan "*Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur*." hükmü uyarınca ilgili tüm taraflar kullanım koşulları ve güvenliğe azami önemi göstermelidir.

Elektronik İmzada Güvenlik

- Yanda Elektronik imzanın güvenliğine etki eden en önemli unsurlar sıralanmıştır.

- Özetleme algoritmaları güvenilirliği
- İmzalama algoritmaları güvenilirliği
- İmza oluşturma araçları güvenliği
- İmza doğrulama araçları güvenliği
- ESHS güvenliği

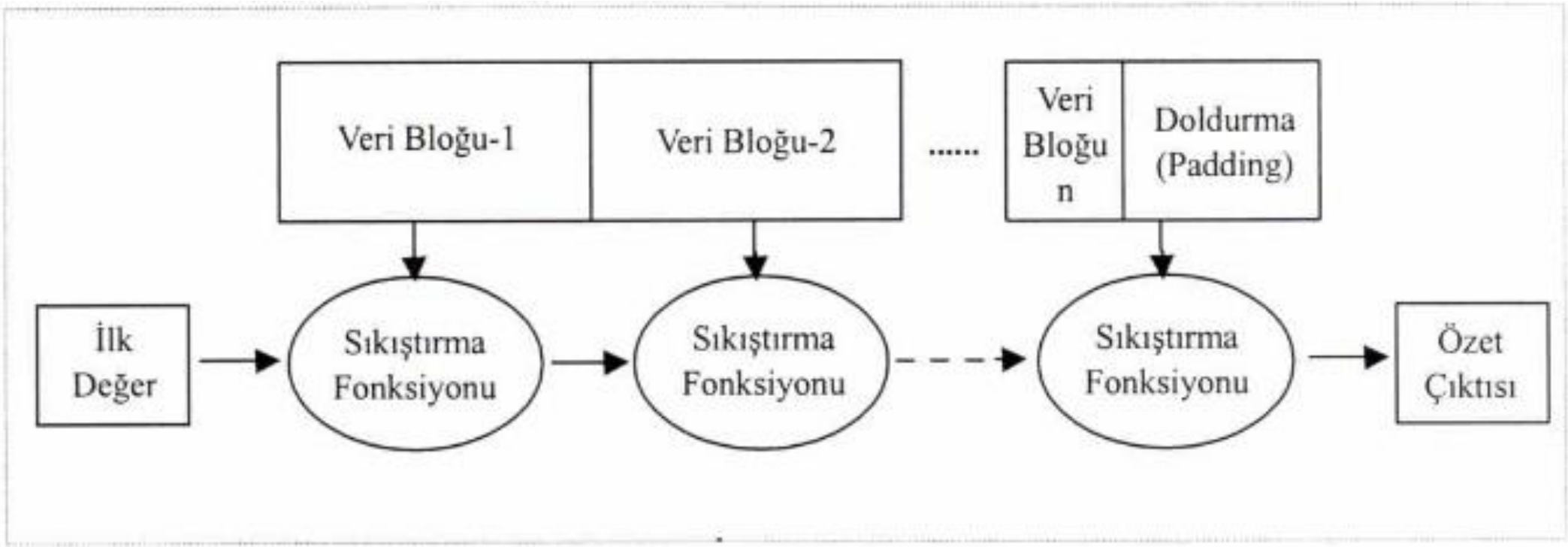
Özetleme algoritmaları güvenilirliği

- Özetleme algoritmalarının güvenliğine yönelik yapılan kriptografik saldırıların birçoğu, rastgele giriş verileri kullanılarak belirlenmiş bir çıktının elde edilmeye çalışılması işlemidir.
- Özetleme algoritmalarına yapılan saldırılardan en yaygın olanı doğum günü (Birthday Attack) saldırılarıdır.
- Özetleme algoritmalarının tek yönlülük özelliğini tehdit eden primaj(preimage) saldirılarında ise elde edilen herhangi bir özet değerinden girdiverilerine ulaşılması hedeflenmektedir.

Özetleme algoritmaları saldırıları

- Diğer bir saldırı çeşidi ise sözde çakışmalar (pseudo-collision) üzerinedir. Özetleme algoritmaları uzun girdilerin kısaltılmasında sıkıştırma algoritmaları kullanmaktadır. Zincirleme saldırıları (chaining attacks) olarak da adlandırılan bu saldırılar, sıkıştırma algoritmalarının çıktıları arasında bir çakışma tespit edilmesini amaçlar ve bu sayede özetleme algoritması ile elde edilen sonuçlara ulaşmakta kullanılır.

Özetleme algoritmaları güvenilirliği



İmzalama Algoritmaları ve Güvenilirlikleri

- İmzalama algoritmaları, girdi verilerini ve imza atacak kişinin özel anahtarını kullanarak asimetrik şifreleme yapan algoritmalardır. Esas olarak asimetrik şifreleme için geliştirilmiş bu algoritmalar, tam eşlemeli olduklarından dolayı şifreleme ve şifre çözme işlemlerinin rolleri karşılıklı olarak değiştirilerek sayısal İmzalama için de kullanılmaktadır.

İmzalama Algoritmaları

- RSA İmzalama Algoritması
- ElGamal İmzalama Algoritması
- Diffie-Hellman Anahtar Değişimi
- DSA İmzalama Algoritması
- Eliptik Eğri İmzalama Algoritmaları
- Eliptik Eğri DSA

İmzalama Algoritmaları Saldırıları

- İmzalama algoritmalarına yapılan saldırılar; orijinal şifresiz verilerin ve şifreli verilerin kullanılmasıyla gerçekleştirilir. Algoritmaların güvenilirlikleri bu saldırılara karşı gösterdikleri dirençlere göre belirlenmektedir.

- Saldırıların başarılı olması durumunda ortaya çıkabilecek sonuçlar şöyle sıralanabilir:
- Tam Kırılma (Total Break); İmza sahibinin özel anahtarının elde edilmesi,
- Evrensel Sahte İmza (Universal Forgery); Tüm mesajları imzalayabilecek etkin bir algoritma oluşturulması,
- Var olan Sahte İmza (Existential Forgery); Yeni bir mesaj - imza çifti oluşturulması.

İmza Oluşturma Sistemleri ve Araçları

- Elektronik imza oluşturma araçları; anahtar çiftini oluşturan, saklayan ve imzalama işlemini gerçekleştiren yazılım veya donanım olarak tanımlanmaktadır. Bu araçlar işlem yapabilme yeteneğine sahiptir ve bunlara kimlik denetim verisi (PIN, biyometrik veriler gibi) ile erişilebilir.

İmza Oluşturma Standartları

- CEN (Comité Européen deNormalisation - Avrupa Standardizasyon Komitesi) tarafından CWA (CENWorkshop Agreement - CEN Çalıştay Kararları) 14169 “Güvenli Elektronik imza Oluşturma Araçları EAL4+" ve CWA 14170 “imza Oluşturma Uygulamaları için Güvenlik Gereksinimleri" şeklinde iki farklı standart yayınlanmıştır.

Elektronik İmza Güvenlik Standartları

- Uluslararası Standartlar
  - TS ISO/IEC 17799 Standardı
  - TS ISO/IEC 15408 Standardı
- ETSI Standartları (European Telecommunications Standards lnstitude – Avrupa Telekomünikasyon Standartları Enstitüsü)
  - TS 101 456 Standardı
  - SR 002 176 Raporu

Elektronik İmza Güvenlik Standartları

- CEN Çalıştay Kararları
  - CWA 14167-1:2003
  - CWA 14167-2:2004
  - CWA 14169:2004
  - CWA 1417oz2oo4
  - CWA 14171 :2004

BİTTİ ☺