

CRC Software



**E-Devlet ve Elektronik İletişim
Sistemleri**

www.crcyazilim.com

CRC imza

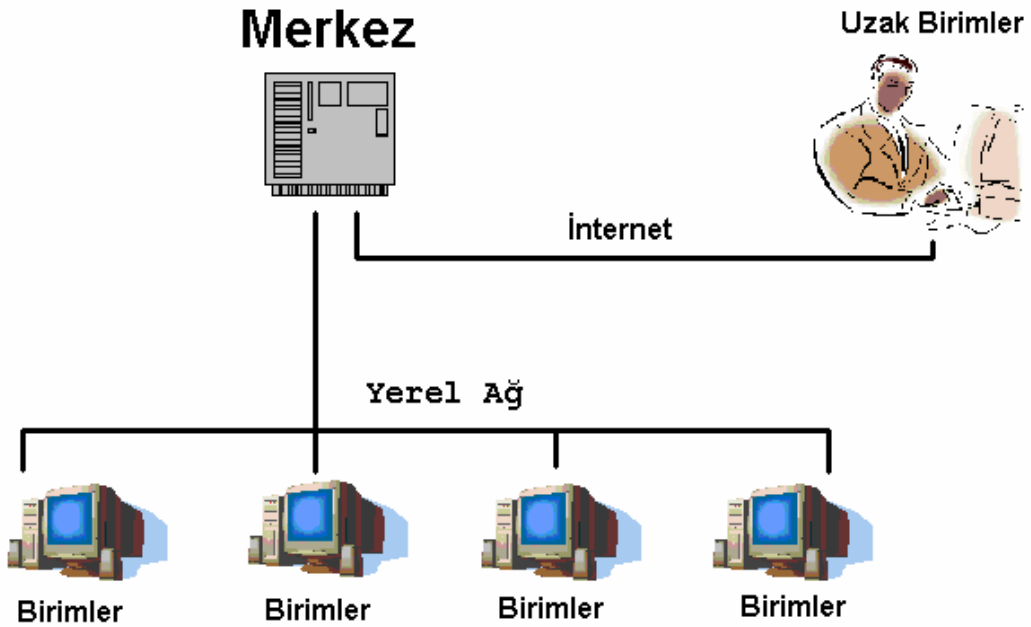
E-DEVLET PROJESİ

1. PROJENİN TANIMI.....	2
2. CRC İMZA.....	3
E-DEVLET PROJESİ'NİN GETİRDİKLERİ	3
3. ELEKTRONİK İMZA KANUNU	4
3.1 BİRİNCİ KISIM	4
3.2 İKİNCİ KISIM	5
4. CRC İMZA SİSTEMİ'NİN TEKNİK ÖZELLİKLERİ.....	7
4.1 SUNUCU PROGRAMI (MERKEZ YAZILIMI)	7
4.1.1 CRC imza Sunucu Sistem Gereksinimleri (2000 kullanıcı için).....	7
4.2 İSTEMCİ PROGRAMI (BİRİMLER İÇİN)	7
4.2.1 CRC imza İstemci Minimum Sistem Gereksinimleri.....	7
4.3 SİSTEMİN YAPISI VE ÇALIŞMA MANTIĞI.....	7
4.4 BELGE GÖNDERME VE SİSTEM	8
5. CRC İMZA SİSTEMİ'NİN GÜVENLİĞİ.....	9
5.1 SUNUCU GÜVENLİĞİ.....	9
5.1.1 Sistem Güvenliği.....	9
5.1.2 Güvenlik Temelleri.....	9
5.1.3 Açık Anahtarlı Şifreleme (Asimetrik Şifreleme).....	10
5.1.4 Anahtar Boyutları.....	11
5.1.5 Simetrik Şifreleme ve Asimetrik (Açık Anahtarlı Şifreleme) Arasındaki Farklar.....	11
5.2 İSTEMCİ GÜVENLİĞİ.....	12
5.3 SIKIŞTIRMA ALGORİTMASI	12
5.4 VERİ TABANI :	13
5.5 MYSQL VERİTABANIN DIĞER VERİTABANLARI İLE PERFORMANS KARŞILAŞTIRMASI	13
5.6 VERİ TABANI.....	14
6. VERİTABANINDA TUTULACAK KAYITLAR	15
6.1 İSTEMCİ.....	15
6.2 SUNUCU.....	15
7. BELGE ARŞİVLEME	15
7.1 ARŞİV TARIMA.....	15
7.2 KULLANICI GRUPLARI	15
8. TEKNİK ÖZELLİKLER.....	16
8.1 YAZILIMIN TEKNİK ÖZELLİKLERİ	16
8.1.1 İstemci Yazılımı (Birimler için)	16
8.1.2 Sunucu Yazılımı (Müdürlük için).....	17
8.2 VERİTABANI YÖNETİM SİSTEMİ TEKNİK ÖZELLİKLERİ	19
8.2.1 İstemci Yazılımı VTYS.....	19
8.2.2 Sunucu Yazılımı VTYS.....	19

1. PROJENİN TANIMI

CRC imza:

1. Devlet Kurumları ve bu kurumlara bağlı bulunan birimler arasında belge alışverişinin ve tüm yazışmaların bilgisayar ortamına taşınmasını sağlar.
2. Elektronik imza kanuna uygun olarak resmi evrakların birimler arasında gönderilmesini sağlar.
3. Kurum ve bağlı bulunan birimler arasında posta, faks ve telefon trafiğinin azaltılarak masrafların düşürülmesini ve süre kazancı sağlar.
4. Kurum ile bağlı bulunan birimler arasında doğrudan veri iletişimini internet üzerinden yapabilen güvenli bir sistem oluşturulmasını sağlar.
5. Kurum ve bağlı birimlerin gelişen teknolojiyi yakalaması ve e-devlet uygulamalarına ayak uydurabilmesini sağlar.



2. CRC imza

E-DEVLET PROJESİ'NİN GETİRDİKLERİ

1. Her türlü belge **transferinin** gerçekleştirilmesi.
2. Belge transferinin gerçekleşip gerçekleşmediğinin **kesin onaylanması**.
3. Göndericinin, belgenin alıcıya ulaştığından **haberdar edilmesi**.
4. **Tüm faks** ve diğer **evrak** gönderim işlemlerinin ortadan kaldırılması.
5. Gönderen ve alıcı **belge arşivinin** tutulması.
6. **Off-line** (sisteme bağlı olmama) durumunda da iletinin gönderilebilmesi.
7. Belgelerin **güvenli** olarak iletilmesi.
8. **Arşiv tarama**, sorgulama yapılabilmesi.
9. Program üzerinde, karşılıklı **eşzamanlı** olarak yazılı görüşme yapılabilmesi.
10. Elektronik imza kullanılması ve bu sayede evrağın geldiği yerin kesin olarak **onaylanabilmesi**.
11. Belge iletimi sırasında **veri kaybı olmaması** ve **orijinal** şekliyle iletilmesi.

3. ELEKTRONİK İMZA KANUNU

Kanun No. 5070

Kabul Tarihi : 15.1.2004

3.1 BİRİNCİ KISIM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1.- Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.

Kapsam

MADDE 2.- Bu Kanun, elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar.

Tanımlar

MADDE 3.- Bu Kanunda geçen;

a) Elektronik veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları,

b) Elektronik imza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,

c) İmza sahibi: Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişiyi,

d) İmza oluşturma verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri,

e) İmza oluşturma aracı: Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını,

f) İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri,

g) İmza doğrulama aracı: Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracını,

h) Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt,

ı) Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt,

j) Kurum: Telekomünikasyon Kurumunu,

İfade eder.

3.2 İKİNCİ KISIM

Güvenli Elektronik İmza ve Sertifika Hizmetleri

Güvenli Elektronik İmza, Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

Güvenli elektronik imza

MADDE 4.- Güvenli elektronik imza;

a) Münhasıran imza sahibine bağlı olan,

b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan,

Elektronik imzadır.

Güvenli elektronik imzanın hukukî sonucu ve uygulama alanı

MADDE 5.- Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur.

Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

Güvenli elektronik imza oluşturma araçları

MADDE 6.- Güvenli elektronik imza oluşturma araçları;

- a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,
- b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılmamasını ve gizliliğini,
- c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılmamasını ve elektronik imzanın sahteciliğe karşı korunmasını,
- d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini,

Sağlayan imza oluşturma araçlarıdır.

Güvenli elektronik imza doğrulama araçları

MADDE 7.- Güvenli elektronik imza doğrulama araçları;

- a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,
- b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,
- c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,
- d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,
- e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,
- f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan,

İmza doğrulama araçlarıdır.

4. CRC imza SİSTEMİ'NİN TEKNİK ÖZELLİKLERİ

4.1 Sunucu Programı (Merkez Yazılımı)

Tüm programların bağlanacağı kontrol programıdır. **CRC imza** sunucu programı merkezde bulunan sunucu bilgisayara kurulur. **Bağlantı paylaşımını ve güvenliği sağlar.**

4.1.1 CRC imza Sunucu Sistem Gereksinimleri (2000 kullanıcı için)

*Intel XEON 3 Ghz Dual CPU
4 GB Ram
4 X 80 GB 15000 rpm HDD
Raid Kartı*

4.2 İstemci Programı (Birimler için)

CRC imza istemci programı, her kullanıcının bilgisayarına kurulacak olan kısımdır. **CRC imza** İstemcisi, **CRC imza** sunucusuna bağlanarak belge paylaşımı yapan kullanıcı arabirimidir.

4.2.1 CRC imza İstemci Minimum Sistem Gereksinimleri

CRC imza istemci programının çalışabilmesi için, Microsoft Windows 98 işletim sisteminin sorunsuz olarak çalıştığı bir bilgisayar konfigürasyonu yeterlidir. Daha iyi sonuç almak için aşağıda önerilen minimum sistem tavsiye edilir.

*Pii veya Celeron tabanlı işlemci
128 MB Ram
Minimum 56K internet bağlantısı
Windows 98 ve üzeri işletim sistemi*

4.3 Sistemin Yapısı ve Çalışma Mantığı

CRC imza sunucu programı sürekli bir internet bağlantısına ve sabit bir IP Numarasına ihtiyaç duyar. **İstemci programların sabit bir internet bağlantısına ve sabit bir ip numarasına ihtiyacı yoktur.** İstemci programı sisteme bağlandığında kendisine gelen belgeleri okuyabilir.

Kullanıcı sisteme bağlanırken, kendisine daha önceden verilmiş olan kullanıcı adı ve parolasını kullanır. **CRC imza** istemci programı, **CRC imza** Sunucu

programına sabit IP Numarasını kullanarak bağlanır. Sunucu kullanıcı adı ve parolasını kontrol eder ve **doğrularsa** sisteme giriş yapılabilir. İstemci programları, sabit IP kullanmıyorsa IP Numaraları “Dinamik” olacaktır ve her bağlantıda değişecektir. Sunucu **CRC imza** programı, istemcinin Dinamik IP numarasını veritabanına kaydederek daha sonraki transferlerde kullanılmak üzere diğer kullanıcıların kullanımına açar.

Sunucu, kendisine bağlanan kullanıcılara, sisteme bağlı olan ve olmayan kullanıcıların listesini gönderir. Listede, kurumlar ve kurumların altındaki birimler de bulunur. Böylece **istemci programlar, kimlerin bağlı olduğunu ve grup şemasını bilirler.**

4.4 Belge Gönderme ve Sistem

Kullanıcının göndereceği belgeyi seçmesi ve belge hakkındaki bilgileri girmesi yeterlidir. (Belge No, Konu, Alıcı bilgisi v.s) İşin geri kalanı **sistem tarafından otomatik olarak yapılacaktır.**

CRC imza istemci programı alıcının Açık Anahtarını **CRC imza** sunucusundan talep eder ve gönderilecek belgeyi bu anahtar ile **şifreler.**

5. CRC imza SİSTEMİ'NİN GÜVENLİĞİ

5.1 Sunucu Güvenliği

5.1.1 Sistem Güvenliği

CRC imza programı, sadece kendi izin verdiği kişilerin sunucuya bağlanmasına olanak tanıyan bir sistem kullanır. Bu da kimlik kanıtlama (authentication) ile mümkün olabilmektedir. Kimlik kanıtlama sistemleri, **şifrelemeye** dayalı sistemlerdir. İstemci ile sunucu bir protokolle aralarında haberleşerek ortak bir sırrı paylaşırlar. Böylelikle, **birbirlerinin kimliklerinden emin olurlar**. Açık kanallardan giden bilginin yetkisiz insanlar tarafından öğrenilmesini engellemek için şifreleme yöntemleri kullanılır. Bu şekilde **kullanıcıların birbirlerinin kimliklerini kullanması önlenir**. Bunun dışında, iletişimde bulunan taraflar ortak bir oturum anahtarı üzerinde anlaşarak aralarında ilettikleri veriyi şifrelerler. Açık anahtar şifreleme algoritmaları yapılarından dolayı kırılmaları imkansız ve anahtar dağıtım sorunu da yoktur. **Bankacılık, elektronik alışveriş ve elektronik ödeme gibi paraya dayalı Internet uygulamalarında daha güvenli olduğu için açık anahtar tabanlı sistemler tercih edilmektedir**. Genel olarak ağ güvenliğinden bahsedildiğinde akla gelen diğer bir sorun da açık kanallarda dolaşan bilginin gizliliği ve bütünlüğüdür. **CRC imza** programı da güçlü yapısı sebebiyle açık anahtarlı şifreleme algoritmasını kullanır.

5.1.2 Güvenlik Temelleri

- **Bilgi gizliliği:** Verinin alıcısı dışında kimse tarafından okunamaması.
- **Bilgi bütünlüğü:** Verinin değişmeden alıcısına ulaşması.
- **İnkâr edememe (non-repudiation):** Kullanıcının gönderdiği belgeyi daha sonra inkâr edemez. Gönderici, karşı tarafın belgeyi aldığını üçüncü kişilere ispat edebilir.

Not: Aynı şekilde de, alıcı belgenin kendisine ulaştığını inkâr edemez. Alıcı karşı tarafın belgeyi gönderdiğini üçüncü kişilere ispat edebilir. Alıcının inkâr edememesi, şifreleme ile alakalı bir özellik olmayıp, **CRC imza** sistemlerinin özelliğidir.

5.1.3 Açık Anahtarlı Şifreleme (Asimetrik Şifreleme)

Açık anahtarlı şifreleme, yukarıda belirtilen güvenlik temellerini karşılamaktadır. İnkâr edememe ve dolayısıyla **başkasının adını kullanarak belge gönderememe özelliği**, ancak açık anahtar tabanlı şifreleme algoritmaları kullanan sayısal imzalar (digital signatures) destekli sistemler ile mümkündür. Açık anahtar tabanlı şifreleme algoritmalarında şifreleme anahtarı (açık anahtar) ve şifre çözme anahtarı (gizli anahtar) farklıdır ve şifreleme anahtarı herkese açıktır. Ancak, **şifreleme anahtarından şifreyi çözme anahtarını elde etmek imkansızdır**. Bundan başka, bu iki anahtar birbirlerinin tersi işlemler yaparlar. Birinin kodladığını diğeri çözer. Bu özelliği sayesinde **açık anahtar tabanlı sistemler hem belge gizleme, hem de sayısal imzalama yapabilmektedir**. Bir belge, alıcının açık anahtarı (public key) ile kodlandığında, ancak alıcının gizli anahtarı (secret key) ile açılacağından ve bu anahtara sadece alıcı sahip olduğundan, **esas belgeyi sadece alıcı okuyabilecektir**. O yüzden, bu kodlama bilgiyi gizleyen bir şifreleme işlemidir. Böylelikle, **bilgi gizleme ve bilgi bütünlüğü sorunları çözümlenebilir**.

Bir belge gönderenin gizli anahtarı ile kodlandığında, söz konusu gizli anahtara sadece gönderen sahip olduğundan, bu kodlama işlemi o belgeye gönderenin attığı bir **sayısal imza** olarak değerlendirilir. İmzanın kontrolü ise kodlanmış belgenin gönderenin açık anahtarı ile açılmasıdır. Açık anahtar da herkes tarafından bilindiğinden, herkes sayısal imza kontrolü yapabilmektedir. Böylelikle, **inkâr edememe, başkasının yerine belge gönderememe ve gönderenin alıcıya kimliğini kanıtlaması** sorunları çözülebilmektedir.

Tüm kullanıcılara ait açık anahtarlar sunucu üzerindedir ve herkesin kullanımına açıktır. İstemci programlar sunucu programına bağlanıp, belge gönderecekleri kişilerin açık anahtarlarını otomatik olarak alacaklardır. Belge gönderirken **CRC imza** istemci programı, belge gönderilecek kişilerin açık anahtarını kullanarak belgeyi **otomatik olarak şifreler**. Belgeyi ancak gizli anahtara sahip olan alıcı açabilecektir. Belgenin açık anahtarla şifrelenip açık anahtarla açılması **kesinlikle mümkün değildir!** Gizli anahtarlar ise, sadece sahibi olan kullanıcının bilgisayarında şifrelenip tutulacaktır. Söz konusu gizli anahtar, kullanıcının şifresi ve MD5 şifreleme algoritması ile paketlenip MySQL veri tabanında tutulur. Söz konusu veritabanına ulaşım da şifrelidir ve şifre **CRC imza** istemci programının içine gömülüdür.

Sunucu üzerinde tutulan tüm açık anahtarlarda **kefalet (certification)** mekanizmaları kullanılır. Kefalet, bir açık anahtar, açık anahtarın sahibinin kimliğinden oluşan bir veriye **CRC imza** sunucusunun koyduğu sayısal imzadır. Tüm açık anahtarlar, **CRC imza** sunucu programının gizli anahtarı

ile imzalanır. Böylece sunucu üzerinde tutulan tüm anahtarların geçerliliği sağlanmış olur ve **kötü niyetli kişilerin sahte açık anahtarlarla belgeleri kendilerine yönlendirmeleri önlenmiş olur.**

5.1.4 Anahtar Boyutları

2 Bitlik bir anahtar ile şifrelenmiş bir belgeyi açmak için olası dört farklı anahtar vardır ve çözüm kolaylıkla bulunabilir. Fakat anahtar boyutu arttıkça, olası çözüm anahtar sayısı da artmaktadır. Örneğin 10 bitlik bir anahtarı çözmek için olası 1024 (bin yirmi dört) adet anahtar denenmelidir. Aşağıda en çok kullanılan anahtar boyutları ve anahtar sayıları verilmiştir.

$$2^{40} = 1.099.511.627.776$$

$$2^{64} = 18.446.744.073.709.551.616$$

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$$

$$2^{160} =$$

$$1.461.501.637.330.902.918.203.684.832.716.283.019.655.932.542.976$$

$$2^{256} =$$

$$115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936$$

$$2^{320} =$$

$$2.135.987.035.920.910.082.395.021.706.169.552.114.602.704.522.356.652.769.947.041.607.822.219.725.780.640.550.022.962.086.936.576$$

5.1.5 Simetrik Şifreleme ve Asimetrik (Açık Anahtarlı Şifreleme) Arasındaki Farklar

- Açık anahtarlı şifreleme ile, birden fazla kişiye belge gönderme çok güvenlidir. Simetrik şifrelemede ise bu doğru değildir. Çünkü şifreleme anahtarı ile şifreyi çözecek anahtar aynıdır. Bu sebepten dolayı gönderenin anahtarına sahip olan kişi, tüm alıcıların belgelerini görebilir.
- Anahtar dağıtımı Açık Anahtarlı Şifrelemede daha güvenlidir. Simetrik şifrelemede anahtar tek olduğundan dolayı, anahtar iletimi sırasında anahtar üçüncü kişilerin eline geçerse tüm belgeler okunabilir. Açık Anahtarlı Şifrelemede bu söz konusu değildir. Çünkü gönderilen anahtar sadece açık anahtardır ve üçüncü kişilerin eline geçmesinin bir sakıncası yoktur. Bununla şifrelenen bir belge **sadece sahibinde bulunan gizli anahtar ile açılabilir.**

- Simetrik şifrelemede kimlik kanıtlama yapılamaz. Çünkü anahtar tekdir ve her iki tarafta anahtara sahiptir. Açık Anahtarlı Şifrelemede yapılabilir. Çünkü gizli anahtar sadece bir kişide vardır.
- Simetrik şifrelemede inkar etme mümkündür. Açık Anahtarlı Şifreleme de ise mümkün değildir.
- Simetrik şifreleme daha hızlıdır ve sadece iki kişinin belge paylaşımı için uygundur. İnternet açık bir ortam olduğu ve anahtarları dağıtmak gerektiği için Açık Anahtar Şifreleme sistemi çoklu kullanıcı gruplarında daha uygundur.

5.2 İstemci Güvenliği

Kullanıcıların gizli anahtarları kendi makinelerinde tutulacaktır ve kendi belirleyecekleri parolalarıyla şifrelenecektir. Program minimum sekiz karakterlik parola girilecek şekilde ayarlanmıştır. Güvenliğin sağlanması açısından şifrelerin dikkatli seçilmesi gerekmektedir.

5.3 Sıkıştırma Algoritması

Gönderilen veri (belge) ilk olarak sıkıştırma işleminden geçirilir. Bu işlemin sebebi;

- Dosya boyutunu küçültmek,
- Network trafiğini azaltmak,
- Gönderim süresini düşürmek,
- Arşiv olarak saklanan belgelerin boyutunu küçültmek,
- Sistem performansını arttırmak,
- Şifreleme işleminden önce yapılarak güvenliği arttırmak.

Sıkıştırma algoritmasının test sonuçları;

Orijinal Dosya Boyutu	Sıkıştırılmış Dosya Boyutu	Sıkıştırma Oranı	Dosya Uzantısı
754 KB	149 KB	% 80	DOC
5 KB	870 Byte	% 81	DOC
74 KB	21 KB	% 72	XLS

CRC imza programının kullanmış olduğu sıkıştırma algoritması sayesinde gönderilen belgeler ortalama yüzde yetmiş beş (% 75) oranında sıkıştırılmaktadır.

5.4 Veri Tabanı :

Sistemde veri tabanı motoru olarak MySQL kullanılmıştır. MySQL tercih edilmesinin sebepleri;

- Açık kaynak olması (GPL Lisans),
- Program kodlarının değiştirilebilmesi,
- Toplam maliyetinin düşük olması,
- Güvenlik açığının olmaması,
- Diğer tüm veritabanlarına göre daha hızlı olması,
- Yüksek performanslı olması.

5.5 MySQL Veritabanının diğer veritabanları ile performans karşılaştırması

2.000.000 kaydı indekse göre okuma

Veri Tabanı	Saniye	Saniye
mysql	367	249
mysql odbc	464	
db2 odbc	1.206	
informix odbc	121	126
ms-sql odbc	1.634	
oracle odbc	20.800	
solid odbc	877	
sybase odbc	17.614	

350.768 adet Kayıt Giriş

5.6 Veri Tabanı

	Saniye	Saniye
mysql	381	206
mysql odbc	619	
db2 odbc	3.460	
informix odbc	2.692	
ms-sql odbc	4.012	
oracle odbc	11.291	
solid odbc	1.801	
sybase odbc	4.802	

Not : Test Sonuçları MySQL resmi web sitesinden alınmıştır. www.mysql.com

6. VERİTABANINDA TUTULACAK KAYITLAR

6.1 İstemci

- Kullanıcının gizli anahtarı,
- Belge gönderilen kişilerin açık anahtarı,
- Gönderilen belgeler,
- Alınan belgeler,
- Gönderilen ve Alınan belgelerin listesi.

6.2 Sunucu

- Şifrelenmiş olarak **CRC imza** sunucusunun Gizli Anahtarı,
- **CRC imza** sunucusunun açık anahtarı,
- Tüm kullanıcıların açık anahtarı,
- On-line olmayan kullanıcıların belgeleri,
- Gönderilen ve Alınan belgelerin Listesi,
- Kullanıcıların alındı belgelerinin tarih ve saatleri.

7. BELGE ARŞİVLEME

Belgeler gönderilirken, belirtilen konu, sayı, makam, tarih v.b bilgilere göre gruplanır ve ay, yıl bilgilerine göre arşivlenir.

7.1 Arşiv Tarama

Tüm belgeler;

- Tarih Aralığına,
- Belge Sayısına,
- Konu Bilgisine,
- Gönderici Bilgisine,
- Alıcı Bilgisine göre

Arama yapılabilir ve listesi çıktı alınabilir.

7.2 Kullanıcı Grupları

Belge ve mesaj gönderirken kullanıcı grupları büyük kolaylık sağlar. **Her merkez bir gruptur.** Ve merkezlerin içinde bulunan **alt birimler de alt grupları** oluştururlar. Kullanıcı grupları sayesinde belgeler tek bir tıklama ile istenilen birimlere gönderilebilir.

8. TEKNİK ÖZELLİKLER

8.1 Yazılımın Teknik Özellikleri

CRC imza, aşağıda belirtilen teknik özelliklere sahiptir.

8.1.1 İstemci Yazılımı (Birimler için)

1. **CRC imza**, Windows 98, Me, 2000, XP işletim sistemleriyle uyumludur.
2. **CRC imza**, kullanışlı bir arabirime sahiptir.
3. **CRC imza**, bilgisayar ortamında bulunan her türlü belgeyi (ayrıt etmeksizin) diğer kullanıcılara internet ortamında gönderebilmektedir.
4. **CRC imza**, sürükle bırak (Drag&Drop) mantığını desteklemekte ve belgeler sürüklenerek programın dosya gönderme penceresine taşınabilmektedir.
5. **CRC imza**, belgeyi gönderirken bant genişliğinden tasarruf edebilmek için sıkıştırma algoritmalarını (veri boyutu küçültme) desteklemekte ve belge göndermeden önce belgeyi sıkıştırabilmektedir. Aynı şekilde alınan belgeyi de kullanıcı müdahalesi gerektirmeden sıkıştırılmış halinden eski haline çevirebilmektedir.
6. **CRC imza**, sunucu yazılımına bağlanırken, Müdürlüğün kullanıcılara önceden belirlediği kullanıcı adı ve şifresiyle bağlanabilmektedir.
7. **CRC imza**, Asimetrik ve Simetrik şifreleme yapabilmektedir.
8. **CRC imza**, ECB, CBC, MD5, SHA1 algoritmalarını desteklemektedir.
9. **CRC imza**, asimetrik şifrelemede RSA algoritmasını kullanabilmektedir.
10. **CRC imza**, Sayısal İmzayı (Digital Signature) desteklemektedir.
11. **CRC imza**, asimetrik şifrelemede gerektiği takdirde sunucu programından kullanıcıların açık anahtarlarını (Public Key) alabilmektedir.
12. **CRC imza**, aldığı açık anahtarların sunucu yazılımı tarafından imzalandığını doğrulayabilmektedir.
13. **CRC imza**, şifreleme ve şifre çözme işleri yaparken farklı bir uygulama yazılımına, plug-in, script ve benzeri bir programcıya gerek duymamaktadır. Şifreleme, şifre çözme ve imzalamada kullanılan tüm algoritmalar programın içerisinde ve başka yazılımlara ihtiyaç duymamaktadır.
14. **CRC imza**, belgeyi birden fazla kullanıcıya, tek kullanıcıya gönderirken yaptığı işlemi tekrarlamadan, aynı pencereden gönderebilmesine olanak sağlamaktadır.
15. **CRC imza**, kullanıcının gizli anahtarının (Private Key) kendi bilgisayarında ve şifreli bir tabloda (table) tutulmasını sağlamaktadır.
16. **CRC imza**, alıcı off-line durumunda olsa dahi belgeyi gönderebilmektedir.

17. **CRC imza**, off-line durumundayken kendisine gönderilen belgeleri, on-line konumuna geçince alabilmektedir.
18. **CRC imza**, 128, 256, 512 Bitlik şifreleme anahtarlarını desteklemektedir.
19. **CRC imza**, gelen ve giden belgeler, kullanıcının bilgisayarında şifreli tablolarda saklanmaktadır. Şifreli tablolara program ulaşırken, tabloların şifreleri programda saklı olup kullanıcıya tablo şifresi sormamaktadır.
20. **CRC imza**, gelen ve giden belgelerde arşiv taraması yapabilmektedir. Sorgu işlemi;
 - i. İki tarih arası,
 - ii. Dosya no,
 - iii. Belge sayısına göre yapabilmektedir.
21. **CRC imza**, gelen ve giden evrakların listesini tutabilmekte ve yazıcıdan çıktı olarak verebilmektedir.
22. **CRC imza**, veri gönderirken ve alırken POP3 veya SMTP gibi mail sunucuları, istemcileri, bunlara ait portları ve protokolleri kesinlikle kullanmamaktadır.
23. **CRC imza**, sunucu bilgisayarında bulunan veri tabanı yönetim sistemine güvenlik nedeniyle doğrudan erişmemektedir. VTYS'ye sunucu programı aracılığı ile ulaşabilmektedir.
24. **CRC imza**, belgeyi aldıktan sonra belgenin, gönderen kişinin bilgisayarından çıktığı andan alındığı ana kadar geçen sürede değişmediğini doğrulamaktadır.
25. **CRC imza**, oluşan hataları log dosyası olarak kaydedebilmektedir.

8.1.2 Sunucu Yazılımı (Müdürlük için)

1. **CRC imza**, Windows 2000, Windows XP, Windows 2003 işletim sistemleriyle uyumludur.
2. **CRC imza**, kullanıcı arabirimine sahiptir.
3. **CRC imza**, sistem performansının artması için kendine bağlanan her bir kullanıcı için kanal (Thread) açabilmekte ve kullanıcılardan gelen talepleri, kullanıcılar için açılan kendi kanalında karşılayabilmektedir.
4. **CRC imza**'ya bağlantı için, birden fazla port tanımlanabilmektedir.
5. **CRC imza**, kullanıcılar sisteme bağlanırken kullanıcı adı ve parolası doğrulaması yapabilen ve hatalı kullanıcı adı ve parolası ile sisteme girişi engelleyebilir bir yapıya sahiptir.
6. **CRC imza**, güvenlik nedeniyle kullanıcıların doğrudan Veri Tabanı Yönetim Sistemine ulaşmasına izin vermemektedir.
7. **CRC imza**, Veri Tabanı Yönetim Sistemi ile aynı bilgisayar veya fiziksel ortam üzerinde bulunmasa dahi çalışabilmektedir. Bu özellik sayesinde sistem genişlemeye ve çok daha fazla kullanıcının sisteme bağlanabilmesine olanak tanımaktadır.

8. **CRC imza**, güvenliğin artırılması için Veri Tabanı Yönetim Sistemine root ve admin gibi tam yetkiyle donatılmış yönetici hakları ile değil, hakları sınırlanmış kullanıcı ve parolası ile bağlanmaktadır. Ayrıca tanımlanan kullanıcı hakkı, sadece programın kurulu olduğu bilgisayara verilmektedir. Başka bir bilgisayar ve ip adresiyle, aynı kullanıcı adı ve parolası kullanarak VTYS'ne ulaşılammaktadır. Bu da güvenlik seviyesini arttırmaktadır.
9. **CRC imza**, VTYS'de kayıtlı olan açık anahtarları imzayabilmektedir.
10. **CRC imza**, kullanıcıların açık anahtarlarını imzalayabilmekte ve 512 Bitlik açık ve gizli anahtar çiftine sahiptir.
11. **CRC imza** ile, birimlerin sunucu yazılımına bağlanmak için kullanacakları kullanıcı adı ve şifreleri tanımlanabilmektedir.
12. **CRC imza**, sisteme bağlanan kullanıcılar için grup ve alt gruplar oluşturabilmekte ve kullanıcılar bu gruplara atanabilmektedir.
13. **CRC imza**, VTYS'de bulunan açık anahtarların güvenlik nedeni ile belli bir kullanım süresi vardır.
14. **CRC imza**, açık anahtarların kullanım süresini tarih olarak gösterebilmektedir.
15. **CRC imza**, hataları log dosyasında tutabilmektedir.
16. **CRC imza**, gelişmeye, genişlemeye uygundur.
17. **CRC imza**, aynı anda sistemde online olan binlerce kullanıcı yükünü kaldırabilmelidir.
18. **CRC imza**, sistem yükünü azaltmak için gerek duyulduğu takdirde program fiziksel olarak farklı bir konumda bulunan başka bir sunucuya kurulabilir ve yük dağıtılabilir.

8.2 Veritabanı Yönetim Sistemi Teknik Özellikleri

Kurulacak olan yazılımın alt yapısında kullanılacak veritabanı yönetim sistemi yazılımı aşağıda belirtilen özelliklere sahiptir.

8.2.1 İstemci Yazılımı VTYS

1. Veritabanı yönetim sistemi Windows 98, ME, 2000, XP işletim sistemi üzerinde sorunsuz çalışmaktadır.
2. Tablolara, **CRC imza** tarafından şifre tanımlanabilmektedir.

8.2.2 Sunucu Yazılımı VTYS

1. Veritabanı yönetim sistemi, Windows NT, Windows 2000, Windows XP, Windows 2003, Linux, Solaris, FreeBSD, HP-UX, IBM AIX işletim sistemleri üzerinde sorunsuz çalışabilmektedir.
2. Veri tabanı yönetim sistemi üzerinde çalıştığı sistemin bütün kaynaklarını optimum şekilde kullanabilmektedir. (işlemcilerin tamamı, ana bellek, veri depolama üniteleri gibi).
3. VTYS client/server yapıda çalışabilmektedir.
4. Bir sistem üzerine yüklenmiş VTYS üzerinde birden fazla veritabanı (Database) oluşturulabilme özelliğine sahiptir.
5. Her bir table büyüklüğü 2 GB a kadar çıkabilmektedir.
6. Bir database büyüklüğü 200GB a kadar çıkabilmektedir.
7. Tablo başına en az 1 clustered index tanımlanabilme özelliğine sahiptir.
8. VTYS üzerinde tanımlanmış olan bütün veritabanları aynı anda açıp kullanıcıların erişebilmesine izin verebilmektedir.
9. VTYS gerçek multithreaded server mimarisine sahiptir.
10. Veritabanı yönetim sistemiyle birlikte sunucu yönetim yazılımına sahiptir ve sisteme bağlı bütün veritabanları bir konsoldan rahatlıkla yönetilebilmektedir. Yerel bilgisayarda bulunan veritabanı üzerinde yapılan bütün işlemler, hiçbir fark olmaksızın uzaktaki VTYS'leri için de aynen yapılabilmektedir. Kullanılacak sunucu yönetim yazılımı tamamıyla gui ortamını desteklemekte ve bu ortamdan kullanılabilir. VTYS ile ilgili bütün işlemler bu sunucu yönetim yazılımı vasıtasıyla yapılabilmektedir. Sunucu yönetim yazılımı, Windows 98, Windows Me, Windows 2000, Windows XP, Windows 2003, Linux üzerinde çalışabilmektedir.
11. VTYS üzerinde dinamik locking mekanizması bulunmakta ve kilitleme işlemini VTYS kendisi otomatik olarak yapmaktadır. Veri tabanı yönetim sistemi üzerinde sayfa kilitleme özelliği bulunmaktadır.
12. VTYS üzerinde veri bütünlüğünü sağlamak üzere; referential integrity tanımları, kolon seviyesi sınırlamalar, default değer atamaları ve kural tanımlamaları yapılabilmeye izin vermektedir.
13. VTYS kullanıcı tanımlı veri tipleri oluşturulabilmesine izin vermektedir.
14. VTYS'nin tablolar, tablo içindeki columns'lar ve sql komutları üzerinde user ve host seviyesinde yetki tanımları yapılabilmeye olanak vermektedir.

15. Veritabanı yönetim sistemi üzerinde yapılan tüm işlemler, hatalar, uyarılar bir log dosyasında tutulabilmekte ve bunlar rahatlıkla izlenebilmektedir.
19. VTYS farklı uygulama geliştirme ve modelleme araçlarını desteklemektedir.
20. Veritabanı yönetim sistemi, iş yükünü otomatik dengeleyebilmek için işlemciler üzerinde tamamen simetrik çalışabilmektedir. Network işlemleri dahil olmak üzere tüm işlemler, işlemciler arasında iş yüküne bağlı olarak otomatik dağıtılabilmekte, birden fazla cpu devreye sokulabilmektedir.
21. Sadece log veya datanın backup işlemini gerçekleştirmek mümkündür.
22. Veri tabanları ve bunlara ait logları ayrı device'larda tutabilmektedir.