SET Secure Electronic Transfer

SET banka kartları ve ödemeler ile ilgili bilgilerin güvenliğini sağlamak amacıyla Visa, Mastercard, Microsoft, Netscape, GTE, IBM, SAIC, Terisa Systems ve Verisign'ın katılımıyla oluşan bir konsorsiyum tarafından geliştirilmiştir. SET uyumlu ilk alışveriş, 18 Temmuz 1997'de San Francisco'da yapılan tanıtımla İspanya ve Singapur'da bulunan sanal mağazalardan gerçekleştirilmiştir. Garanti Bankası Şubat 1998'de gerçekleştirdiği SET uyumlu alışverişle, bu protokolü kullanmaya başlayan Dünya'da yedinci, Avrupa'da dördüncü ve Türkiye'de ilk kuruluş olmuştur.

SET protokolünde alışveriş, sanal cüzdan ve sertifika aracılığı ile daha güvenli bir ortamda gerçekleştirilir. SET, alışveriş işlemi sırasında ödeme bilgisi gizliliğini, kart kullanıcısının gerçek kart sahibi olduğunu ve işyerinin banka ile anlaşmalı bir işyeri olduğunu garantiler.

SET sisteminde provizyon işlemi müşteri alışveriş seçimini yaptıktan sonra müşterinin sanal cüzdanı ile mağazanın Sanal POS'unun (V-POS) birbirlerinin gerçekliklerini dijital sertifikalar aracılığıyla kontrol etmeleri ile başlar. Mağazanın Sanal POS yazılımı sipariş tutarını ve sanal cüzdanda bulunan ve alışveriş için seçilen kredi kartının sertifika bilgilerini bankaya iletmesi ile devam eder. Banka yapılan alışverişin içeriğini (malın ne olduğu, kaç tane alındığı vb.) görmeksizin provizyon verir. Müşterinin kredi kartı bilgilerini görmeyen sanal mağaza ise bankadan gelecek onayı bekler. Onayı aldıktan sonra da ürünü alıcısına gönderir.

SET sistemi (SSL'de olduğu gibi) işyeri ve banka arasındaki veri akışı sırasında bilgilerin şifrelenerek gönderilmesi esasına dayanır. Bu sistemden faydalananabilmek için kullanılmak istenen kredi kartının SET uyumlu olması gerekir. SET protokolünü kullanmak isteyen kredi kartı sahipleri iki ön koşulu yerine getirmek zorundadırlar: Öncelikle kullanmak istedikleri her bir kredi kartı için sertifikasyon kurumu (Certificate Authority) ayrı birer SET sertifikası almalıdırlar. Ardından kart sahipleri yine kredi kartı veren bir bankadan sanal cüzdan adı verilen bir programı alıp bilgisayarlarına yüklemeli ve bu yükleme sırasında SET sertifikalı kredi kartlarını programa tanıtmalıdırlar. SET uyumlu alışverişler sanal cüzdanın yüklü olduğu bilgisayar kullanılarak SET uyumlu mağazalardan yapılabilecektir. Sanal cüzdan programı en fazla üç kez yüklenmek üzere yazıldığından en fazla üç bilgisayarda kullanılabilecektir. SET protokolünün SSL'e göre çok daha yüksek denebilecek güvenliğine rağmen yeterince yaygınlaşamaması sanal cüzdanın mobilitesinin olmamasına bağlanabilir. Bu yüzden Garanti Bankası sistemi SET uyumlu olmasına karşın SET protokolünü tam olarak uygulamamaktadır. Sanal mağazalar ise Sanal POS (Point of Sale) olarak adlandırılan V-POS yazılımını yükledikten sonra bir sertifikasyon kurumundan (www.verisign.com, www.gte.com) dijital bir sertifika alarak alışverişlerin güvenliğini sağlarlar.

SET ile gerçekleşen alışveriş sırasında gerçekleşen işlemler sırasıyla aşağıdaki gibidir:

SET protokolü, kart sahibi Internet üzerinde araştırmasını tamamlayıp seçimini yaptıktan ve siparişini verdikten sonra devreye girmektedir. SET işleminin başlamasından önce kart sahibi sipariş formunu doldurmuş ve onaylamış olmalıdır. Kart sahibi ayrıca kart türünü de seçmiş olmalıdır.

1. Kart sahibinin yazılımı satıcı firmaya kullanılacak kredi kartını belirten ve ödeme altyapısını sağlayan kuruluşun sertifikalı açık anahtarının kopyasını isteyen bir mesaj gönderir.

2. Satıcı firmanın yazılımı mesajı aldığında, sadece o mesaja özel bir işlem tanımlama numarası belirler. Daha sonra bu özel tanımlama numarasıyla beraber kart sahibine satıcı firmanın açık anahtarını ve ödeme altyapısını sağlayan kuruluşun (genelde bankalar) onaylı açık anahtarını gönderir.

3. Kart sahibinin yazılımı satıcı firmanın ve ödeme altyapısını sağlayan kuruluşun sertifikalarını kontrol eder ve sipariş sürecinde kullanmak üzere bunları kaydeder. Kart sahibinin yazılımı sipariş bilgisini ve ödeme talimatlarını oluşturur. Yazılım satıcı firma tarafından belirlenen özel tanımlama numarası ile sipariş bilgisini ve ödeme talimatlarını ilişkilendirir. Bu tanımlama daha sonra satıcı firma tarafından ödeme talebi yapıldığında, ödeme altyapısını sağlayan kuruluş tarafından sipariş bilgisini ve ödeme talimatlarını ilişkilendirmede kullanılacaktır.

4. Kart sahibinin yazılımı sipariş bilgisi ve ödeme talimatları için bir dijital imza oluşturur. Yazılım daha sonra ödeme altyapısını sağlayan kuruluşun açık anahtarını kullanarak dijital olarak imzalanan ödeme talimatlarını şifreler. Son olarak yazılım imzalanmış ve şifrelenmiş sipariş bilgisini ve ödeme talimatlarını bir mesajla satıcı firmaya gönderir.

5. Satıcı firmanın yazılımı siparişi alır ve kart sahibinin açık anahtarı üzerindeki dijital sertifikayı kontrol eder. Bundan sonra gene bu açık anaharı kullanarak siparişin gerçekten kart sahibinden geldiğinden ve mesajın gönderim esnasında değiştirilmediğini teyit eder (Satıcı firma ödeme talimatları ödeme altyapısını sağlayan firmanın açık anahtarı ile şifrelendiği için deşifre edemez).

6. Bu işlemlerin ardından satıcı firmanın yazılımı ödeme onayı istenmesi de dahil olmak üzere siparişle ilgili işlemlere başlar (lütfen 9. Maddeye bakınız)

7. Sipariş bilgisi işleme alındıktan sonra, satıcı firmanın yazılımı bir cevap mesajı hazırlar ve dijital olarak imzalar (satıcı firmanın onaylı açık anahtarı ile). Kart sahibinin siparişinin alındığının ve işleme konulduğunun bildirilmesi amacıyla hazırlanan cevap mesajı kart sahibine gönderilir.

8. Kart sahibinin yazılımı satıcı firmadan cevap mesajını aldığı zaman dijital sertifikasını kontrol eder. Bunun ardından bu mesajı kullanarak kart sahibine bir teyit mesajı gösterir veya siparişin durumunu günceller.

9. Kart sahibinden gelen siparişlerin işleme konulması esnasında (lütfen 6. maddeye bakınız) satıcı firmanın yazılımı ödenmesi talep edilen tutarı, sipariş bilgisindeki işlemi belirleyen özel tanımlama numarasını ve işlemle ilgili diğer bilgileri içeren bir ödeme onay talebini hazırlar ve bu mesajı dijital olarak imzalar. Ardından bu talep ödeme altyapısını sağlayan kuruluşun açık anahtarı kullanılarak şifrelenir. Satıcı firmanın ödeme onay talebi ve kart sahibinin şifrelenmiş ödeme talimatları ödeme altyapısını sağlayan kuruluşa gönderilir.

10. Ödeme altyapısını sağlayan kuruluş onay talebini aldığı zaman satıcı firmadan gelen onay talebini kendi gizli anahtarını kullanarak deşifre eder. Ardından satıcı firmanın açık anahtarı üzerindeki dijital sertifikayı kontrol eder ve sertifikanın geçerlilik sürerisinin dolup dolmadığını belirler.

11. Ödeme altyapısını sağlayan kuruluş kart sahibinin satıcı firmadan gelen onay talebiyle birlikte gönderilen ödeme talimatlarını kart sahibinin açık anahtarını kullanarak deşifre eder. Ardından bu açık anahtarı kullanarak kart sahibinin ödeme talimatları üzerindeki dijital imzasını kontrol eder ve böylece ödeme talimatlarının kart sahibi tarafından imzalandığından ve iletim esnasında değişikliğe uğramadığından emin olur.

12. Ödeme altyapısını sağlayan kuruluş satıcı firma tarafından gönderilen işlem tanımlayıcısı ile ile kart sahibinden gelen ödeme talimatlarındaki tanımları karşılaştırarak her ikisininde aynı olup olmadığını kontrol eder. Kontrolün ardından ödeme altyapısının sağlayan kuruluş, kredi kartını veren bankaya Internet üzerinden çalışmayan bir ödeme sistemiyle bir onay talebi gönderir.

13. Kartı veren banka onay talebini işleme alır ve ödeme altyapısını sağlayan kuruluşa güvenli ödeme sistemi aracılığıyla bir cevap gönderir.

14. Onay cevabını aldıktan sonra ödeme altyapısını sağlayan kuruluş kartı veren bankanın cevabını ve onaylı açık anahtarını içeren bir onay cevap mesajı yaratır ve dijital olarak imzalar. Cevap satıcı firmanın açık anahtarını kullanarak şifrelenir ve satıcı firmaya gönderilir.

15. Satıcı firmanın yazılımı ödeme altyapısını sağlayan kuruluştan onay cevabını aldığı zaman kendi gizli anahtarıyla deşifre eder. Ardından ödeme altyapısını sağlayan kuruluşun açık anahtarı üzerindeki dijital sertifikayı kontrol eder ve bu açık anahtarı kullanarak ödeme alyapısını sağlayan kuruluşun onay cevap mesajındaki dijital imzayı kontrol eder. Satıcı firmanın yazılımı, sipariş tamamen yerine getirildikten sonra ödeme talebinde bulunulabilmesi için (gün sonu işlemi ile) bu onay cevap mesajını kaydeder.

16. Satıcı firma onay cevabını aldıktan sonra kart sahibinin siparişi tamamlar ve ilgili ürünü sevkeder veya sözkonusu hizmeti verir.

17. Siparişi yerine getirdikten sonra satıcı firma ödeme talebinde bulunur (Siparişin tamamlanması esnasındaki gecikmeler onay talebi ile ödeme talebi mesajları arasında önemli zaman aralıkları oluşmasına yol açabilir).

18. Ödeme talebinde bulunmak için satıcı firmanın yazılımı işlemin nihai tutarını, sipariş bilgisindeki işlem tanım numarasını ve işlem hakkındaki diğer bilgileri içeren bir gün sonu işlemi oluşturur ve dijital olarak imzalar. Bu talep ödeme altyapısı sağlayan kuruluşun açık anahtarı ile şifrelenir ve ödeme sağlayan kuruluş gönderilir.

19. Ödeme altyapısını sağlayan kuruluş gün sonu işlemi talebini aldığı zaman, kendi açık anahtarını kullanarak talebi deşifre eder. Daha sonra satıcı firmanın açık anahtarını kullanarak gün sonu işlemindeki dijital imzayı kontrol eder. Satıcı firmadan gelen gün sonu işlemiyle, daha önce işleme alınan onay talebini karşılaştırır ve bir tahsilat talebi oluşturarak bunu kredi kartını veren bankaya güvenli ödeme sistemiyle gönderir.

20. Ödeme altyapısını sağlayan kuruluş kendi onaylı açık anahtarını içeren bir gün sonu cevap mesajı oluşturur ve bunu dijital olarak imzalar. Bu cevap satıcı firmanın açık anahtarı ile şifrelenerek satıcı firmaya gönderilir. Bu mesaj sayesinde gün sonu işleminin ödeme altyapısını sağlayan kuruluş tarafından alındığını ve işleme konulduğunu satıcı firmaya bildirir.

21. Satıcı firmanın yazılımı ödeme altyapısını sağlayan kuruluştan gün sonu işleminin cevabını alınca, mesajı kendi gizli anahtarını kullanarak deşifre eder. Ardından ödeme altyapısını sağlayan kuruluşun açık anahtarı üzerindeki dijital sertifikayı kontrol eder ve yine bu açık anahtarı kullanarak ödeme altyapısını sağlayan kuruluşun dijital imzasını kontrol eder. Son olarak satıcı firmanın yazılımı günsonu işlemi cevabını yapılan ödemeler için gönderilen günsonu talep mesajları ile mutabakat için kaydeder.

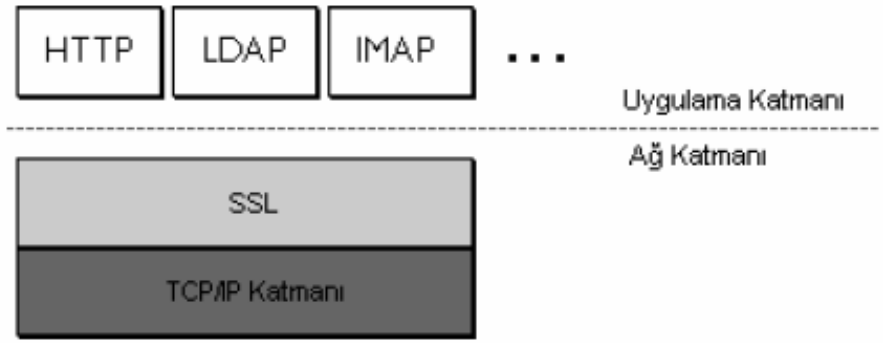
SSL'E GİRİŞ

Secure Sockets Layer (Güvenli Prizler Katmanı) protokolünü tanıtır. SSL orijinal olarak Netscape tarafından geliştirilmiştir, web de doğruluğu sınamada, istemci ve sunucular arasında şifreli iletişimi sağlamada büyük kabul görmüştür.

Aynı zamanda Transport Layer Security (Taşıma Katmanı Güvenliği) olarak adlandırılan yeni Internet Engineering Task Force (IETF-Internet Mühendislik Görev Birliği) standardı SSL üzerine kuruludur.

SSL Protokolü

TCP/IP (Transmission Control Protocol/Internet Protocol) verinin internette taşınmasını ve yönlendirilmesini idare eder. HTTP (HyperText Transport Protocol), LDAP (Lightweight Directory Access Protocol), IMAP (Internet Messaging Access Protocol) gibi diğer protokoller TCP/IP üzerinde çalışırlar ve genel kanıya göre web sayfalarının görüntülenmesi, e-posta servislerinin çalıştırılması gibi tipik uygulama programlarının sağlanması için hepsi TCP/IP 'yi kullanırlar.



Şekil-1 SSL TCP/IP üzerinde ve yüksek seviyeli uygulama protokollerinin altında çalışır.

SSL protokolü TCP/IP üzerinde ve HTTP yada IMAP gibi yüksek seviyeli protokollerin altında çalışır. TCP/IP' yi yüksek seviyeli protokollerin lehinde kullanır ve SSL'in etkin olduğu sunucunun SSL'in etkin olduğu istemciye kendisini doğrulamasını, istemcinin de sunucuya kendisini doğrulamasını sağlar ve her iki makinanın da şifreli bağlantı kurmasını sağlar.

Bu yetenekler internet üzerinde ve diğer TCP/IP ağlarındaki iletişim hakkında köklü sorunlara hitap eder.

- **SSL sunucu doğrulaması** bir kullanıcıya bir sunucunun kimliğini onaylamasına izin verir. SSL'in etkin olduğu istemci yazılımı bir sunucunun sertifikasının ve genel kimliğinin geçerli olduğunu ve istemcinin güvenilen sertifika otoritelerinin listesinde listelenen sertifika otoritesi (CA-Certificate Authority) tarafından yayımlandığını kontrol etmek için standart genel anahtarlamalı şifreleme tekniklerini kullanır.

- **SSL istemci doğrulaması** bir sunucuya bir kullanıcının kimliğini onaylamasına izin verir. Sunucu doğrulaması için kullanılan aynı teknikler kullanılarak, SSL'in etkin olduğu sunucu yazılım, istemcinin sertifikasının ve genel kimliğinin geçerli olduğunu ve sunucunun güvenilen sertifika otoritelerinin listesinde listelenen sertifika otoritesi tarafından yayımlandığını kontrol edebilir. Örnek olarak bu onaylama eğer sunucu bir müşteriye gizli finansal bilgi gönderen bir banka ise ve alıcının kimliğini kontrol etmek istiyorsa önemli olabilir.

- **Bir şifrelenmiş SSL bağlantısı** gönderen yazılımla şifrelenmesi ve alıcı yazılımla deşifre edilmesi için bir istemci ve bir sunucu arasında gönderilen tüm bilgiyi gerektirir, böylece yüksek seviyeli bir güvenirliliği sağlamış olur. Ek olarak, şifrelenmiş SSL bağlantısı üzerinden gönderilen tüm veriler kurcalamaları bulan yani taşımada değiştirilip değiştirilmediğini otomatik olarak belirleyen bir mekanizma vasıtasıyla korunur.

SSL protokolü iki alt protokolden oluşur: SSL kayıt protokolü ve SSL el sıkışma protokolü. SSL kayıt protokolü verinin taşınmasında kullanılan biçimi tanımlar. SSL el sıkışma protokolü SSL'in etkin olduğu sunucu ile SSL'in etkin olduğu istemcinin ilk SSL bağlantısı kurduğunda aralarındaki mesajların karşılıklı taşınması için SSL kayıt protokolünün kullanımını kapsar. Bu mesajların karşılıklı taşınması aşağıdaki işlemlerin kolaylaştırılması için tasarlanmıştır.

- Sunucunun kendisini istemciye doğrulaması
- İstemci ve sunucunun her ikisinin de desteklediği şifreleme algoritmalarını yada şifrelerini seçmelerine izin vermek
- Seçimlik olarak istemcinin kendisini sunucuya doğrulaması
- Paylaşılan sırların üretilmesi için genel anahtarlamalı şifreleme tekniklerini kullanmak
- Bir şifreli SSL bağlantısını kurmak

Dijital İmza

Dijital imza hayal edilebilen tüm elektronik bilgi transferi çeşitlerinde kullanılabilen bir elektronik imzadır. Dijital imzalar matematiksel teori ve algoritmaların kullanımı üzerine kuruludurlar. İmzanın sahibinin imzalama ve doğrulama için iki anahtar sistemine sahip olmalarını gerektirir (biri özel (private) diğeri genel (public)). Doğrulanabilir ve güvenilir imzalar oluşturabilmek ve dağıtabilmek için Sertifika Otoritelerinden (Certificate Authority) yardım alınır.

Sertifika Otoritesi (Certificate Authority-CA)

Dijital imza ve genel-özel anahtar çiftlerini oluşturmak için kullanılan dijital sertifikaları yayımlayan güvenilir üçüncü şahıs organizasyon ya da şirkettir. CA'in bu işlemdeki rolü bireysel olarak tahsis edilmiş yegane sertifikanın kendisine ait olduğunu iddia eden kişiye gerçekten ait olduğunu garanti etmesidir. Bu genellikle, CA'in kredi kartı şirketi gibi bir finansal şirketle anlaşması olup, bireyin iddia ettiği kimliği finansal şirket için onaylamasıdır. CA'ler, karşılıklı bilgi alışverişinde bulunan iki şahsın iddia ettikleri şahıslar olduklarını garantilemesinden dolayı veri güvenliğinin ve elektronik ticaretin kritik bileşenleridir.

SSL Tarafından Kullanılan Cipher'lar (Şifreler)

SSL protokolü çeşitli farklı kriptografik algoritmaların yada cipher'ların kullanımını sunucuların ve istemcilerin birbirlerini doğrulamaları, sertifikaların taşınması, ve oturum anahtarlarının tahsis edilmesi gibi işlemlerde kullanmak için destekler. İstemciler ve sunucular farklı cipher takımlarını destekledikleri SSL'in sürümü, kabul edilebilir şifreleme etkinliğini gözönünde bulunduran şirket politikaları ve SSL'in etkin olduğu yazılımın dağıtımı üzerindeki hükümet sınırlamaları gibi etkenlere bağlı olarak destekleyebilirler. Diğer fonksiyonları arasında, SSL el sıkışması protokolü sertifikaların taşınması ve oturum anahtarlarının tahsis edilmesi için sunucu ve istemcinin birbirlerini doğrulamada hangi cipher takımlarını kullanacaklarını nasıl görüştüklerini belirler.

Cipher takımı açıklamaları aşağıdaki algoritmaları kapsar.

- **DES.** Data Encryption Standard (Veri Şifreleme Standardı), U.S. Hükümeti tarafından kullanılan bir şifreleme algoritması

- **DSA.** Digital Signature Algorithm (Dijital İmza Algoritması), U.S. Hükümeti tarafından kullanılan dijital doğrulama standardının bir parçası

- **KEA.** Key Exchange Algorithm (Karşılıklı Anahtar Değişimi Algoritması), U.S. Hükümeti tarafından karşılıklı anahtar değişimi için kullanılan bir algoritma
- **MD5.** Message Digest (Mesaj Sindirimi) Rivest tarafından geliştirilen bir algoritma
- **RC2 and RC4.** RSA veri güvenliği için geliştirilen Rivest şifreleme cipher'ları
- **RSA.** Hem şifreleme hem de doğrulama için bir genel anahtarlı algoritma. Rivest, Shamir ve Adleman tarafından geliştirildi.
- **RSA key exchange.** RSA algoritması üzerine kurulu SSL için bir karşılıklı anahtar değişimi algoritması
- **SHA-1.** Secure Hash Algorithm (Güvenli Hash Algoritması), U.S. Hükümeti tarafından kullanılan bir hash fonksiyonu
- **SKIPJACK.** U.S. Hükümeti tarafından kullanılan FORTEZZA-uyumlu donanımda yerine getirilmiş bir sınıflandırılmış simetrik anahtarlı algoritma
- **Triple-DES.** Üç kere etkili DES

KEA ve RSA karşılıklı anahtar değişimi gibi karşılıklı anahtar değişimi algoritmaları, sunucu ve istemcinin her ikisinin de SSL oturumunda kullandıkları simetrik anahtarları belirleme yöntemlerini idare ederler. En çok kullanılan SSL cipher takımları RSA karşılıklı anahtar değişimini kullanır.

SSL 2.0 ve SSL 3.0 protokolleri cipher takımlarının kümelerini üst üste bindirmelerini destekler. Yöneticiler hem istemciler hem de sunucular için desteklenen cipher takımlarının herhangi birini etkinleştirebilir yada etkisizleştirebilirler. SSL el sıkışması esnasında belirli bir istemci ve sunucu karşılıklı bilgi değiştirdiğinde, ortak sahip oldukları en güçlü etkinleştirilmiş cipher takımını belirlerler ve SSL oturumları için kullanırlar.

Belirli bir organizasyonun hangi cipher takımlarını etkinleştirecekleri hakkında verdikleri kararlar ilgili verinin duyarlılığı arasındaki ticari anlayışa, cipher'ın hızına ve ihracat kurallarının kabul edilebilirliğine bağlıdır. Bazı organizasyonlar zayıf şifrelerle yapılan SSL bağlantılarını engellemek için zayıf cipher'ları etkisizleştirebilirler. Bazıları da mümkün olduğunca fazla kullanıcıya hizmet verebilmek için, mümkün olduğunca geniş SSL cipher takımlarını etkinleştirmek isteyebilirler. Bununla beraber 40-bit cipher'lar çabucak kırılabildiklerinden, başkalarının dinlemesinden endişelenen ve kullanıcıları legal olarak daha etkili cipher'ları kullanabilen yöneticiler 40-bit cipher'ları etkisizleştirmelidirler.

RSA Karşılıklı Anahtar Değişimli Cipher Takımları

Tablo-1 RSA karşılıklı anahtar değişimini kullanan SSL protokolünün desteklediği cipher takımlarını listeler. Aksi belirtilmediği sürece, tablodaki tüm cipher'lar SSL 2.0 ve SSL 3.0'ın her ikisinde de desteklenmiştir. Cipher takımları en etkinden en zayıfa doğru sıralanmıştır.

Tablo – 1 RSA Karşılıklı Anahtar Değiştirme algoritmasını kullanan SSL protokolünün desteklediği Cipher takımları

Etkinlik kategorisi ve önerilen kullanımı	Cipher takımları
En etkin cipher takımı. Sadece U.S. tarafından yayılması için izin verildi. Bu cipher takımı yüksek duyarlılıklı verileri tutan bankalar ve diğer kurumlar için uygundur.	**SHA-1 mesaj doğrulamasıyla 168-bit şifrelemeyi destekleyen Triple DES.** Triple DES SSL tarafından desteklenen en etkin cipher'dır, fakat RC4 kadar hızlı değildir. Anahtar standart DES için olduğu sürece Triple DES bir anahtarı üç kez kullanır. Anahtar boyu çok büyük olduğundan dolayı, yaklaşık olarak $3.7 * 10^{50}$ kadar, diğer cipher'lardan daha fazla mümkün anahtar oluşturulabilir. SSL 2.0 ve SSL 3.0'ın her ikisi de bu cipher takımını destekler.

Etkin cipher takımları. Sadece U.S. tarafından yayılmasına izin verildi. Bu cipher takımı çoğu iş ve hükümet ihtiyaçlarına yetecek kadar etkin şifreleme desteği verir.	**128-bit şifrelemeli ve MD5 mesaj doğrulamalı RC4.** RC4 ve RC2 cipher'ları 128-bit şifrelemeye sahip olduklarından, 168-bit şifrelemeli Triple DES'ten sonra ikinci en etkin olanlardır. RC4 ve RC2 128-bit şifreleme kırılmalarını çok zorlaştırarak yaklaşık olarak $3.4 * 10^{38}$ mümkün anahtara izin verirler. RC4 cipher'lar desteklenen en hızlı cipher'lardır. SSL 2.0 ve SSL 3.0'ın her ikisi de bu cipher takımını destekler.
	SHA-1 mesaj doğrulamayla 56-bit şifrelemeyi destekleyen DES. DES 40-bit şifrelemeden daha etkindir, fakat 128-bit şifreleme kadar etkin değildir. DES 56-bit şifreleme yaklaşık olarak $7.2 * 10^{16}$ mümkün anahtar oluşturulabilmesine izin verir. SSL 2.0 ve SSL 3.0 'ın her ikisi de bu cipher takımını kullanır, fakat SSL 2.0 mesaj doğrulaması için SHA-1 yerine MD5 kullanır.

İhraç edilebilir cipher takımları. Bu cipher takımları yukarıdakiler kadar etkin değildirler, fakat çoğu ülke için ihraç edilebilir (Fransa'nın S/MIME için değil de SSL için izin verdiğini belirtmekte fayda var). İhraç edilebilir ürünler için varolan en etkin şifrelemeyi sağlarlar.	**40-bit şifrelemeli ve MD5 mesaj doğrulamalı RC4.** RC4 40-bit şifreleme yaklaşık olarak $1.1 * 10^{12}$ (bir trilyon) mümkün anahtar oluşturulabilmesine izin verir. RC4 cipher'ları desteklenen en hızlı cipher'lardır. SSL 2.0 ve SSL 3.0'ın her ikisi de bu cipher takımını destekler.
	40-bit şifrelemeli ve MD5 mesaj doğrulamalı RC2. RC2 40-bit şifreleme yaklaşık olarak $1.1 * 10^{12}$ (bir trilyon) mümkün anahtar oluşturulabilmesine izin verir. RC2 cipher'ları RC4 cipher'larından daha yavaştır. SSL 2.0 ve SSL 3.0'ın her ikisi de bu cipher takımını destekler.
En zayıf cipher takımı. Bu cipher takımı doğrulama ve kurcalama belirleme sağlar, fakat şifreleme sağlamaz. Sunucu yöneticileri bunun etkinleştirilmesinde dikkatli olmalıdırlar, çünkü bu cipher takımı kullanılarak gönderilen veri şifrelenmediğinden çalınabilir.	**Şifreleme yok, sadece MD5 mesaj doğrulama.** Bu cipher takımı MD5 mesaj doğrulamayı kurcalama belirlemede kullanır. Tipik olarak bir istemci ve sunucunun ortak olarak diğer cipher takımlarına sahip olmadıkları durumlarda kullanılır. Bu cipher takımı SSL 3.0 da desteklenmiş, fakat SSL 2.0 da desteklenmemiştir.

RC4 ve RC2 cipher'ları için "40-bit şifreleme" ifadesinde anahtarların yine de 128 bit uzunluğunda olduğunu fakat sadece 40 bitinin kriptografik anlam taşıdığını belirtmekte fayda var.

SSL El Sıkışması

SSL protokolü genel anahtarlamalı ve simetrik anahtarlamalı şifrelemenin bir karışımını kullanır. Simetrik anahtarlamalı şifreleme genel anahtarlamalı şifrelemeden çok daha hızlıdır, fakat genel anahtarlamalı şifreleme daha iyi doğrulama teknikleri sağlar. Bir SSL oturumu her zaman **SSL El Sıkışması** olarak adlandırılan mesajların karşılıklı taşınmasıyla başlar. El sıkışma sunucunun kendisini istemciye genel anahtarlamalı tekniklerle doğrulamasını sağlar, sonra istemci ve sunucunun hızlı şifreleme, deşifreleme ve takip eden oturum esnasında karışıklık bulmak için kullanılan simetrik anahtarların oluşturulmasında birlikte çalışmaya izin verir. İsteğe bağlı olarak el sıkışma ayrıca istemcinin kendisini sunucuya doğrulamasına izin verir.

SSL el sıkışması esnasında karşılıklı taşınan mesajların kesin programatik detayları bu dokümanın sahası içindedir. Bununla beraber, bu içerilen adımlar aşağıdaki maddeler halinde özetlenebilir

1. İstemci sunucuya istemcinin SSL sürüm numarasını, cipher ayarlarını, rasgele üretilmiş veriyi ve SSL kullanarak istemciyle haberleşmek için sunucuya gereken diğer bilgileri gönderir.

2. Sunucu istemciye sunucunun SSL sürüm numarasını, cipher ayarlarını, rasgele üretilmiş veriyi ve SSL üzerinden sunucu ile haberleşmek için istemcinin ihtiyaç duyduğu diğer bilgileri gönderir.

3. İstemci sunucunun doğrulanması için sunucu tarafından gönderilen bilginin bir kısmını kullanır. Eğer sunucu doğrulanmazsa kullanıcı sorun hakkında uyarılır, şifrelenmiş ve doğrulanmış bağlantının kurulamayacağı hakkında bilgilendirilir. Eğer sunucu başarılı olarak doğrulanmazsa istemci Adım 4 'e gider.

4. El sıkışmada üretilen tüm veri kullanılarak, istemci (sunucuyla beraber çalışarak, kullanılan cipher'a bağlı olarak) oturum için **öncül sahip sırrını** (premaster secret) oluşturur, sunucunun genel anahtarı ile şifreler (sunucunun sertifikasından elde edilen, Adım 2 de gönderilen), şifrelenmiş öncül sahip sırrını sunucuya gönderir.

5. Eğer sunucu istemci doğrulamasını (el sıkışmada isteğe bağlı bir adım) istemiş ise, istemci ayrıca bu el sıkışmada yegane olan ve hem istemci hem de sunucu tarafından bilinen verinin diğer parçasını imzalar. Bu durumda istemci hem imzalı veriyi hem de istemcinin kendi sertifikasını şifrelenmiş öncül sahip sırrıyla sunucu boyunca gönderir.

6. Eğer sunucu istemci doğrulaması istemiş ise, sunucu istemciyi doğrulama teşebbüsünde bulunur (Detaylar için **İstemci Doğrulanması**'na bakınız). Eğer istemci doğrulanamaz ise oturum sonlandırılır. Eğer istemci başarılı bir şekilde doğrulanırsa, sunucu kendi özel anahtarını öncül sahip sırrını deşifre etmek için kullanır, sonra bir adımlar serisini (istemcinin de gerçekleştirdiği, aynı öncül sahip sırrından başlayarak) **sahip sırrını** (master secret) üretmek için gerçekleştirir.

7. Hem istemci hem de sunucu sahip sırrını **oturum anahtarları** (session keys) üretmek için kullanır, ki bunlar SSL oturumu esnasında karşılıklı taşınan bilginin şifrelenmesinde ve deşifre edilmesinde kullanılan simetrik anahtarlardır. Yani, SSL bağlantısı üzerinde gönderildiği zamandan alındığı zamana kadar geçen süre içinde verideki değişikliklerin bulunmasında kullanılan simetrik anahtarlardır.

8. İstemci sunucuya gelecekteki mesajların istemciden oturum anahtarı ile şifreleneceğini bildiren bir mesajı gönderir. Daha sonra el sıkışmanın istemci tarafında bittiğini belirten ayrı (şifreli) bir mesajı gönderir.

9. Sunucu istemciye gelecekteki mesajların sunucudan oturum anahtarı ile şifreleneceğini bildiren bir mesajı gönderir. Daha sonra el sıkışmanın sunucu tarafında bittiğini belirten ayrı (şifreli) bir mesajı gönderir.

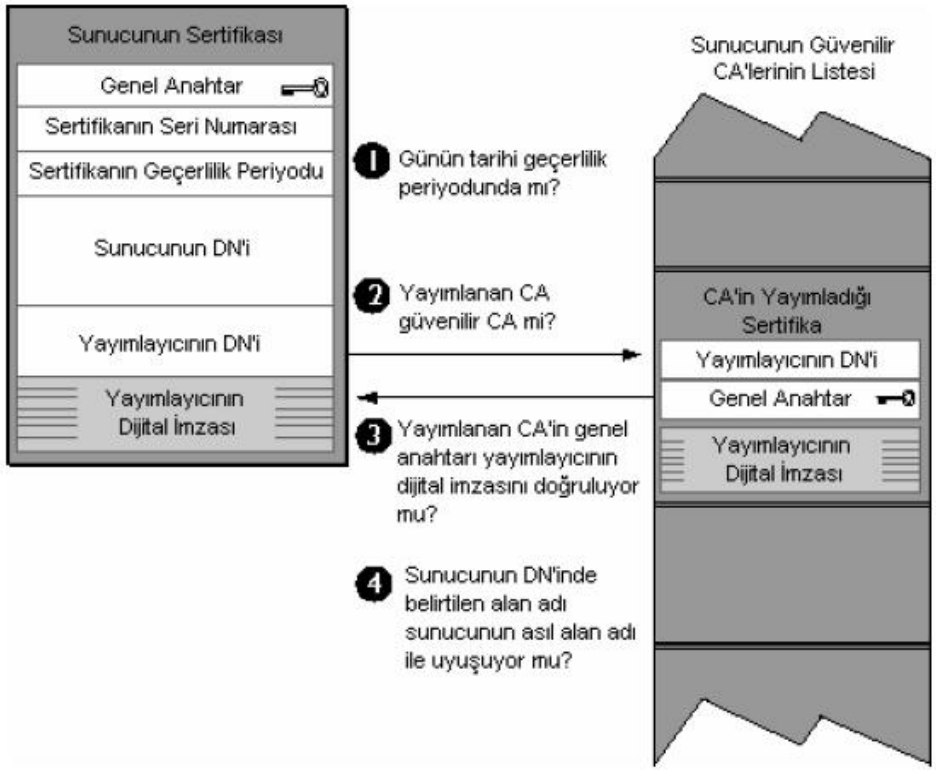
10. SSL el sıkışması artık tamamlandı, ve SSL oturumu başladı. İstemci ve sunucu birbirlerine gönderdikleri verileri şifrelemek ve deşifrelemek için ve bütünlüğü doğrulamak için oturum anahtarlarını kullanır.

Sunucu Doğrulanması

Netscape'in SSL'in etkin olduğu istemci yazılımı her zaman sunucu doğrulaması veya sunucunun kimliğinin istemcisi tarafından kriptografik doğrulanmasını gerektirir. Adım 2'de SSL El Sıkışmasında anlatıldığı üzere sunucu istemciye kendisini doğrulaması için bir sertifika gönderir. İstemci bu sertifikayı sertifikanın göstermek için iddia ettiği kimliğin doğrulanması için Adım 3'te kullanır.

Bir genel anahtarla ve genel anahtar içeren bir sertifika tarafından tanımlanan sunucu arasındaki bağın doğrulanması için SSL'in etkin olduğu istemcinin Şekil 2 de gösterilen dört sorudan "evet" cevabı almalıdır. Bu dördüncü soru SSL protokolünün teknik olarak bir parçası olmamasına rağmen bunu gerektirmenin desteklenmesi istemcinin sorumluluğudur. Böylece sunucunun kimliğinin biraz garantilenmesi sağlanır ve bu "ortadaki adam" (man in the middle) olarak bilinen bir güvenlik saldırısı biçimine karşı koruma sağlar.

Şekil – 2 Bir Netscape sunucusu bir istemci sertifikasının doğrulanmasını nasıl sağlar.



SSL'in etkin olduğu bir istemci sunucunun kimliğini doğrulanması için aşağıdaki adımlardan geçer:

1. **Günün tarihi geçerlilik periyodunda mı?** İstemci sunucunun sertifikasının geçerlilik periyodunu kontrol eder. Eğer o anki tarih ve zaman sınırın dışındaysa, doğrulama işlemi daha fazla devam etmeyecektir. Eğer o anki tarih ve zaman sertifikanın geçerlilik periyodundaysa istemci Adım 2'ye geçer.

2. **Yayımlanan CA güvenilir CA mi?** SSL'in etkin olduğu her istemci şekil-2'nin sağ tarafında koyu olarak gösterilen güvenilir CA sertifikalarının bir listesinin bakımını yapar. Liste istemcinin hangi sunucu sertifikalarını kabul edeceğini belirtir. Eğer yayımlanan CA'in DN'i (distinguished name - seçkin isim) istemcinin güvenilir CA'ler listesindeki bir CA'in DN'i ile uyuşursa, bu soruya "evet" cevabı verilir, ve istemci Adım 3'e geçer. Eğer yayımlanan CA listede değilse, listede olan bir CA'in zincir sonundaki bir sertifikayı istemci doğrulayamadıysa sunucu doğrulanmayacaktır.

3. **Yayımlanan CA'in genel anahtarı yayımlayıcının dijital imzasını doğruluyor mu?** İstemci CA'in sertifikasından (Adım 2 de güvenilir CA'lerin listesinde bulduğu) genel anahtarı gösterilen sunucu sertifikasında CA'in dijital imzasını doğrulamak için kullanır. Sunucu sertifikasındaki bilgi CA tarafından imzalandığından bu yana değiştirildiyse ve ya CA'in sertifikasındaki genel anahtar CA tarafından sunucu sertifikasını imzalamakta kullandığı özel anahtar ile uyuşmuyorsa, istemci sunucunun kimliğini doğrulamayacaktır. Eğer CA'in dijital imzası doğrulanabilirse, sunucu kullanıcının sertifikasını bu CA'den geçerli bir "tanıtımın mektubu" olarak ele alır ve işleme koyar. Bu noktada, istemci sunucu sertifikasının geçerli olduğunu belirledi. Adım 4'e Adım 5'ten önce geçilmesi istemcinin sorumluluğudur.

4. **Sunucunun DN'inde belirtilen alan adı sunucunun asıl alan adı ile uyuşuyor mu?** Bu adım sunucunun gerçekten sunucu sertifikasındaki alan adıyla belirtilen aynı ağ adresinde bulunduğunu onaylar. Adım 4'ün teknik olarak SSL protokolünün bir parçası olmamasına rağmen, bu sadece ortadaki adam (**Man in the Middle**) olarak bilinen bir güvenlik saldırısına karşı koruma sağlar. Eğer alan adları (**domain names**) uyuşmuyorsa istemci bu adımı gerçekleştirmelidir ve sunucunun doğrulanmasını ve ya bir bağlantı kurulmasını reddetmelidir. Eğer sunucunun asıl alan adı ile sunucu sertifikasındaki alan adı uyuşuyor ise, istemci Adım 5'e geçer.

5. **Sunucu doğrulandı.** İstemci SSL el sıkışması ile devam eder. Eğer istemci herhangi bir nedenden dolayı Adım 5'e geçmez ise, sertifika tarafından tanımlanan sunucu doğrulanmaz ve kullanıcı sorundan dolayı uyarılır ve şifreli ve doğrulanmış bir bağlantının kurulamayacağı hakkında bilgilendirilir. Eğer sunucu istemci doğrulanması isterse, sunucu **İstemci Doğrulanması**'nda anlatılan adımları gerçekleştirir.

Burada anlatılan adımlardan sonra, sunucu kendi özel anahtarını SSL el sıkışmasında Adım 4'te istemcinin gönderdiği öncül sahip sırrını deşifre etmek için kullanır. Aksi takdirde, SSL oturumu sonlandırılacaktır. Bu, sunucunun sertifikasındaki özel anahtarla ilişkilendirilmiş kimlik sayesinde istemcinin bağlantı kurduğu sunucunun ek garantisini sağlar.

Ortadaki Adam (Man in the Middle) Saldırısı

Yukarıda Adım 4'te önerildiği üzere, istemci uygulaması istemcinin bağlanmaya teşebbüste bulunduğu sunucunun asıl alan adına karşı sunucunun sertifikasında belirtilen sunucu alan adı ile kontrol etmelidir. Bu adım aşağıda anlatılan şekilde çalışan ortadaki adam saldırısına karşı korunmak için gereklidir.

Ortadaki adam istemci ve istemcinin SSL aracılığıyla haberleşmeye teşebbüs ettiği sunucu arasındaki tüm haberleşmenin yolunu kesen bir hilekar bir programdır. Bu hilekar program SSL el sıkışması sırasında ileri ve geri iletilen geçerli anahtarların yolunu keser, kendisininkileri yerine koyar ve istemciye kendisinin sunucu olduğunu, sunucuya da kendisinin istemci olduğunu zannetmelerini sağlar.

SSL el sıkışmasının başlangıcında karşılıklı taşınan şifreli bilgi istemci ya da sunucunun asıl anahtarları yerine hilekar programın genel anahtarı ve özel anahtarı ile şifrelenir. Bu hilekar program asıl sunucu ile kullanmak için oturum anahtarlarının bir kısmının ve istemci ile kullanmak için kalan oturum anahtarlarının doğrulanmasını tamamlar. Bu işlem hilekar programın istemci ve asıl sunucu arasında akan verilerin sadece okunmasını sağlamakla kalmaz, aynı zamanda anlaşılmadan değiştirebilmesini de sağlar. Bu yüzden, istemcinin sunucu sertifikasındaki alan adının istemcinin bağlanmaya teşebbüs ettiği sunucunun alan adıyla uyuştuğunu ve ek olarak Sunucu Doğrulanmasındaki diğer adımların işletilerek sertifikanın geçerliliğini kontrol etmesi son derece önemlidir.

İstemci Doğrulanması

SSL'in etkin olduğu sunucuların istemci doğrulaması yada istemcinin kimliğinin sunucusu tarafında kriptografik doğrulamanın gerektirilmesi ayarlanabilir. Sunucu bu şekilde ayarlandığında istemci doğrulaması gerektirir (SSL El Sıkışmasının 6. Adımına bakınız), istemci kendisini doğrulamak için hem sertifikayı hem de dijital olarak imzalanmış verilerin ayrı bir parçasını sunucuya gönderir. Sunucu sertifikadaki genel anahtarı ve sertifikanın göstermeyi iddia ettiği kimliği doğrulamak için dijital olarak imzalanmış verileri kullanır.

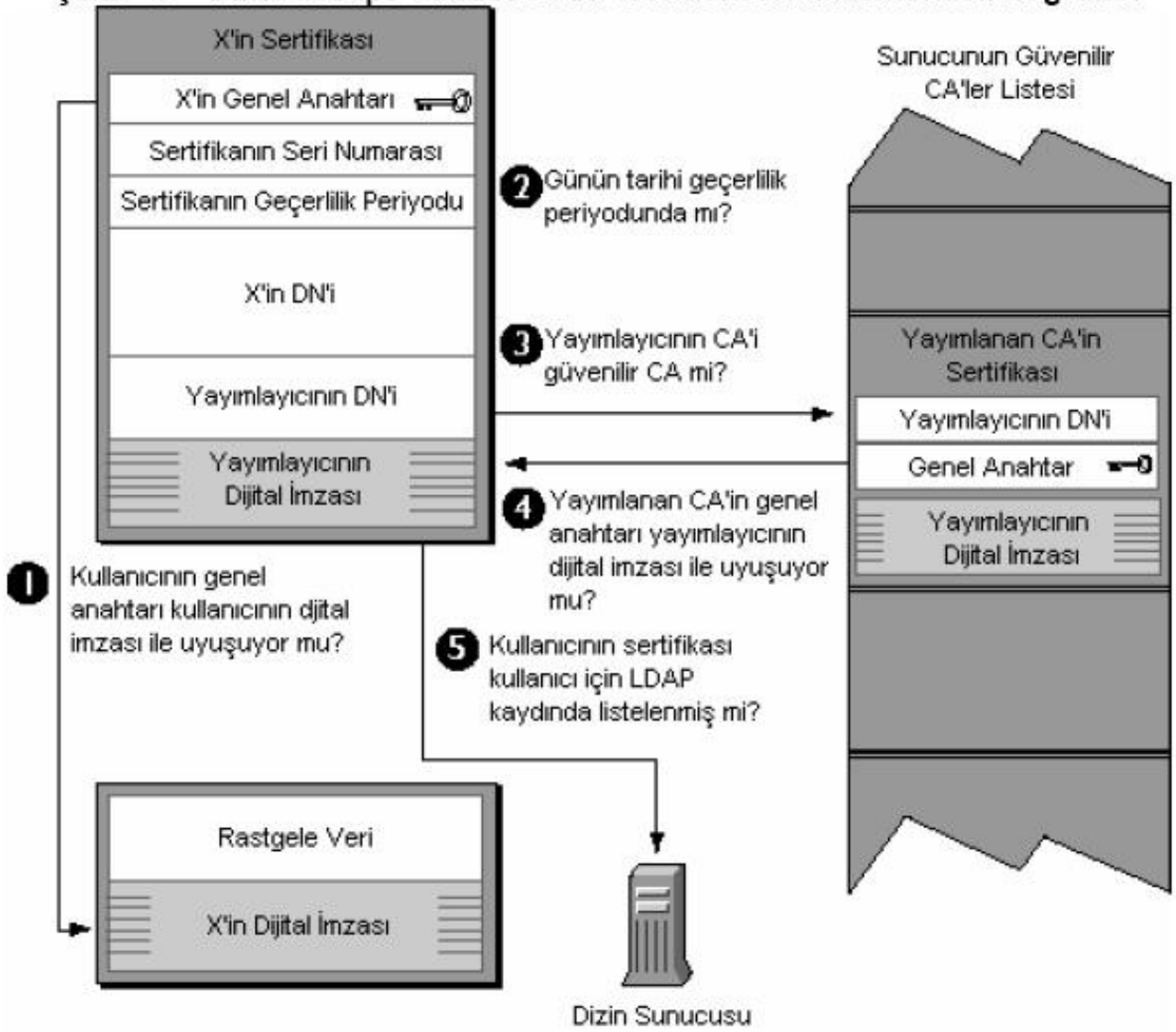
SSL protokolü istemcinin el sıkışması sırasında rasgele üretilen verilerden bir yönlü karmaşıklık oluşturarak ve sadece istemci ve sunucunun bildiği bir dijital imza oluşturmayı gerektirir. Sonra karmaşık veriler sunucuya gösterilmiş olan sertifikadaki genel anahtarla uyuşan genel anahtar ile şifrelenir.

Genel anahtar ile kişinin ya da genel anahtarı içeren sertifika tarafından tanımlanan varlığın arasındaki bağın doğrulanması için, SSL'in etkin olduğu bir sunucu Şekil-3'te gösterilen ilk dört soruya "evet" cevabını almalıdır. Beşinci soru SSL protokolünün bir parçası olmamasına rağmen Netscape sunucuları bir LDAP dizinindeki kullanıcının girişinin doğrulama işleminin bir parçası olarak alınması için bu gereksinimi desteklenmesi ayarlanabilir.

SSL'in etkin olduğu bir sunucu bir kullanıcının kimliğini doğrulamak için aşağıdaki adımlardan geçer:

1. **Kullanıcının genel anahtarı kullanıcının dijital imzası ile uyuşuyor mu?** Sunucu, kullanıcının dijital imzasının sertifikadaki genel anahtarla doğrulanabilirliğini kontrol eder. Edilebiliyorsa, Sunucu X'e ait olduğu iddia edilen genel anahtarın imzanın oluşturulmasında kullanılan genel anahtarla uyuştuğunun ve verinin imzalandığından beri kurcalanmadığının doğruluğunu ortaya koyar.

Şekil - 3 Bir Netscape sunucusu bir istemci sertifikasını nasıl doğrular.



2. **Günün tarihi geçerlilik periyodunda mı?** Sunucu sertifikanın geçerlilik periyodunu kontrol eder. Eğer o anki tarih ve zaman sınırın dışındaysa, doğrulama işlemi daha fazla devam etmeyecektir. Eğer o anki tarih ve zaman sertifikanın geçerlilik periyodunda ise sunucu Adım 3'e geçer.

3. **Yayımlayıcının CA'i güvenilir CA mi?** Şekil 3'ün sağında koyu alan ile gösterildiği üzere, her SSL'in etkin olduğu sunucu güvenilir CA sertifikalarının bir listesini idare eder. Liste sunucunun hangi sertifikaları kabul edeceğini belirler. Yayımlanan CA'in DN'i sunucunun güvenilir CA'ler listesindeki bir CA'in DN'i ile uyuşursa, bu soruya "evet" cevabı verilir, ve sunucu Adım 4'e geçer. Eğer yayımlanan CA listede değilse, sunucu listede olan bir CA'in zincir sonundaki sertifikayla doğrulayamadığı sürece istemci doğrulanmayacaktır. Yöneticiler organizasyonlarıyla hangi sertifikaların güvenilir hangi sertifikaların güvenilir olmadığını istemci ve sunucular tarafından idare edilen CA sertifikalarının listesini kontrol ederek anlayabilirler.

4. **Yayımlanan CA'in genel anahtarı yayımlayıcının dijital imzası ile uyuşuyor mu?** Sunucu CA'in sertifikasındaki (Adım 3'te güvenilir CA'lerin listesinde bulunan) genel anahtarı sertifikada gösterilen CA'in dijital imzasını doğrulamada kullanır. Eğer sertifikadaki bilgi CA tarafından imzalandığından bu yana değişmişse yada CA sertifikasındaki genel anahtar sertifikayı imzalamak icin CA tarafından kullanılan özel anahtar ile uvusmuvorsa. sunucu kullanıcının kimliğini doğrulamayacaktır. Eğer CA'in dijital imzası doğrulanabilirse, sunucu kullanıcının sertifikasını CA'den geçerli bir "tanıtım mektubu" olarak ele alır ve işleme koyar. Bu noktada, SSL protokolü sunucuya istemcinin doğrulandığını düşünmesini ve Adım 6'da açıklandığı gibi bağlantıyla devam etmesini sağlar. Netscape sunucuları Adım 5'in Adım 6'dan önce yapılmasını isteğe bağlı olarak ayarlayabilirler.

5. **Kullanıcının sertifikası kullanıcı için LDAP kaydında listelenmiş mi?** Bu seçime bağlı adım bir sistem yöneticisi için kullanıcının sertifikasını diğer tüm adımlardan geçmiş olsa bile feshedebilmesi için bir yol sağlar. Bu adımı yürütmeye ayarlanmış tüm sunucular böyle bir sertifikanın doğrulanmasını yada bir bağlantı kurulmasını reddedecektir. Eğer dizindeki kullanıcının sertifikası SSL el sıkışmasında gösterilen kullanıcının sertifikasıyla aynı ise, sunucu Adım 6'ya geçer.

6. **Doğrulanmış istemcinin istenen kaynaklara erişmeye izin verildi mi?** Sunucu erişim kontrol listesine bağlı olarak (ACL-Access Control List) istemcinin hangi kaynaklara erişimine izin verildiğini kontrol eder ve uygun erişim ile bir bağlantı kurar. Eğer sunucu herhangi bir sebepten dolayı Adım 6'ya geçmezse, sertifika tarafından tanımlanan kullanıcı doğrulanamaz ve kullanıcının doğrulama gerektiren herhangi bir sunucu kaynağına erişimine izin verilmez.

CREN şirketinin genel anahtarını içeren bir dijital sertifika örneği :

Content-Description: filename="cren.txt"
Content-Disposition: inline; filename="cren.txt"
Content-Type: text/plain; name ="cren.txt"

Certificate:
Data:
Version: 1 (0x0)
Serial Number:
04:60:00:00:02
Signature Algorithm: md2WithRSAEncryption
Issuer: C=US, O=CREN/Corp for Research and Educational
Networking, OU=Education and Research Client CA
Validity
Not Before: Nov 17 00:00:00 1999 GMT
Not After : Nov 17 00:00:00 2003 GMT
Subject: C=US, O=CREN/Corp for Research and Educational
Networking, OU=Education and Research Client CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):

00:96:f8:ea:aa:de:bc:33:74:ce:02:54:ef:1a:c7:9d:0b:93:28:f3:59:e5:36:9b:a4:05:df:79:fd:99:71:66:2c:90:1d:9c:d9:44:df:b9:ca:d9:e5:d
d:f1:69:03:dc:4a:e3:ba:ea:7d:68:84:7a:78:e8:b6:b7:8e:94:ac:af:93:1e:05:81:0b:25:a0:72:ff:9e:0c:24:9f:e3:bb:95:d4:40:82:c0:ff:d6:80:
f2:ff:a4:d6:20:be:09:bd:ec:44:59:74:ff:6f:5d:7a:69:3d:d0:38:1e:33:17:be:d2:f7:ec:a7:e8:a9:05:ae:ba:0b:98:85:3e:25:7e:92:e0:6f:25:3
2:a1:05:1f:7b:54:01:3c:28:09:58:d8:7a:83:ed:aa:18:33:5a:14:df:da:d5:d0:fe:d8:c2:17:16:fc:a7:16:af:de:c7:06:f0:07:62:de:26:7b:bb:44
:c8:02:ad:99:e4:d7:f4:ff:1a:9f:51:d2:cd:9f:91:82:88:ae:f5:93:18:5e:ec:37:1a:06:5c:62:1e:cf:9c:dd:5a:3f:23:8e:e8:c3:59:05:5a:09:0e:9
c:8c:08:c5:ad:55:fc:13:b3:bb:38:08:45:f2:36:8e:f8:5a:3c:ba:96:45:38:82:da:95:87:35:f8:2a:9a:75:1f:de:34:3d:27:0c:6c:39
Exponent: 65537 (0x10001)
Signature Algorithm: md2WithRSAEncryption
1e:50:cf:82:d0:27:fc:a2:86:f1:c6:dd:b2:d1:f2:56:dc:e9:a8:4f:cc:8b:18:5c:25:c7:fc:25:68:ab:86:3d:55:44:3e:97:bb:62:8c:33:f6:80:c4:0d
:72:41:47:ea:dc:e2:bf:d9:3e:83:c4:07:ac:25:b0:86:f5:d5:0f:63:fc:8b:0e:de:89:d5:c3:31:9f:cb:ba:71:9b:00:1d:67:64:94:2d:5f:93:59:93:
27:d0:d2:8a:10:f2:83:c0:b6:00:f6:36:5f:67:86:3f:b8:cf:55:d6:44:41:01:fc:5c:66:5a:fa:64:b6:6f:9e:c5:c1:86:31:3f:37:53:fa:fc:57:01:94:0
2:bd:2d:4d:90:49:00:14:06:54:c3:75:d3:53:14:a2:10:c6:12:37:ce:bb:97:32:ff:ad:e5:b3:58:25:5d:40:9b:ed:3e:5c:79:f3:15:3f:d1:a7:bb:8
7:68:6a:0b:70:c3:19:54:46:84:d7:d7:76:9e:b3:79:92:a8:25:63:70:dc:ea:b5:b7:1b:96:34:c8:12:52:cb:fa:a6:16:c4:a6:0f:98:51:2f:44:90:
5f:ea:74:4c:97:5a:82:33:84:20:51:70:04:bd:65:ae:97:8f:f8:c0:fa:91:08:07:e1:ec:2f:d9:bc:7c:f3:3a:02:ca:27:56:ec:67:22
-----BEGIN CERTIFICATE-----
MIIDYDCCAkgCBQRgAAACMA0GCSqGSIb3DQEBAgUAMHQxCzAJBgNVBAYTAlVTMTowOAYDVQQKEzFDUkVOL0NvcnAgZm
9yIFJlc2VhcmNoIGFuZCBFZHVjYXRpb25hbCBOZXR3b3JraW5nMSkwJwYDVQQLEyBFZHVjYXRpb24gYW5kIFJlc2VhcmNoIENs
aWVudCBDQTAeFw05OTExMTcwMDAwMDBaFw0wMzExMTcwMDAwMDBaMHQxCzAJBgNVBAYTAlVTMTowOAYDVQQKEzFD
UkVOL0NvcnAgZm9yIFJlc2VhcmNoIGFuZCBFZHVjYXRpb25hbCBOZXR3b3JraW5nMSkwJwYDVQQLEyBFZHVjYXRpb24gYW5k
IFJlc2VhcmNoIENsaWVudCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJb46qrevDN0zgJU7xrHnQuTKPN
Z5TabpAXfef2ZcWYskB2c2UTfucrZ5d3xaQPcSuO66n1ohHp46La3jpSsr5MeBYELJaBy/54MJJ/ju5XUQILA/9aA8v+k1iC+Cb3sRFl0
/29demk90DgeMxe+0vfsp+ipBa66C5iFPiV+kuBvJTKhBR97VAE8KAIY2HqD7aoYM1oU39rV0P7YwhcW/KcWr97HBvAHYt4me7tEy
AKtmeTX9P8an1HSzZ+Rgoiu9ZMYXuw3GgZcYh7PnN1aPyOO6MNZBVoJDpyMCMWtVfwTs7s4CEXyNo74Wjy6lkU4gtqVhzX4
Kpp1H940PScMbDkCAwEAATANBgkqhkiG9w0BAQIFAAOCAQEAHlDPgtAn/KKG8cbdstHyVtzpqE/MixhcJcf8JWirhj1VRD6Xu2KM
M/aAxA1yQUfq3OK/2T6DxAesJbCG9dUPY/yLDt6J1cMxn8u6cZsAHWdklC1fk1mTJ9DSihDyg8C2APY2X2eGP7jPVdZEQQH8XGZ
a+mS2b57FwYYxPzdT+vxXAZQCvS1NkEkAFAZUw3XTUxSiEMYSN867lzL/reWzWCVdQJvtPlx58xU/0ae7h2hqC3DDGVRGhNfXd
p6zeZKoJWNw3Oq1txuWNMgSUsv6phbEpg+YUS9EkF/qdEyXWolzhCBRcAS9Za6Xj/jA+pEIB+HsL9m8fPM6AsonVuxnIg==
-----END CERTIFICATE-----