YAPILANDIRILABİLİR VE DİNAMİK BİR SERTİFİKA DOĞRULAMA KÜTÜPHANESİ MODELİ

Işıl HASIRCIOĞLU, Dindar ÖZ
TÜBİTAK UEKAE
{ihasircioglu, oz}@uekae.tubitak.gov.tr

ABSTRACT

As Information technologies and information security have been becoming prevalent in every aspect of life day by day, Electronic Certificates increase their popularity in many areas. The validation and the verification of a certificate has as much importance as its functions and differs significantly from one application to another. Thus applications involving Public Key Infrastructure (PKI) should have a very flexible and reconfigurable Certificate Validation and Verification API in order to manage with the rapid changes in this area. In this paper, certificate validation and verification standards will be examined and after that our proposed model for Certificate Validation and Verification API developed by an object-oriented approach will be explained.

Key words: electronic signature, certificate verification, certificate validation standards

1. GİRİŞ

Elektronik imza, güvenli bir ortamda oluşturulan, kişilerin kimlik doğrulamasını sağlayan ve içeriği onayladıklarını gösteren imzadır. İmza, kişiye ait nitelikli sertifika ve bu sertifikaya ait özel anahtar ile güvenli bir ortamda oluşturulmaktadır. Bu imza doğrulanırken de imzayı atan özel anahtarın açık anahtarı kullanılmaktadır. Bu doğrulama işlemi; imzalama yapılan algoritmaya, açık anahtarın verilmesi ve imzalanan verinin imzalı veriyle kriptografik olarak doğrulanmasıyla gerçekleşir.

Bir elektronik imzanın doğrulanması için; imzalanan veri, bu verinin imzası, doğrulama verisi olarak tanımlanan elektronik imzayla ilgili diğer veriler sağlanmalıdır. Doğrulama verisi; imzalama yapan sertifikaları, iptal durumu bilgisini(sertifika iptal listeleri, OCSP cevapları) içerebilir.

İmzanın kriptografik olarak doğrulanması, bir algoritmanın çalıştırılmasından ibarettir. Ancak bu aşamaya geçilebilmesi için, imzayı oluşturan anahtara ait sertifikanın geçerliliği kontrol edilmelidir. Sertifika doğrulama süreçleri, CEN/ISSS Workshop on Electronic Signatures yayını olan CWA 14171[1]'de tanımlanmış ve bu dokümanın referans olarak verdiği RFC 3280[2]'de ayrıntılarıyla açıklanmıştır.

2. SERTİFİKA DOĞRULAMA STANDARTLARI

Bir sertifikanın geçerli olabilmesi için sertifikadan kök sertifikasına giden yol üzerindeki tüm sertifikaların geçerli olması gerekmektedir. Doğrulama işleminde güvenilir nokta olarak verilen kök sertifikaya kadar tüm sertifikaların geçerlilik kontrolleri yapılması neticesinde sertifikanın geçerlilik durumu tespit edilebilir. Bu yol üzerindeki son sertifika olan kök sertifika, sertifika doğrulama işlemine güvenilir sertifika olarak verilmelidir. Güvenilir sertifika olarak verilen sertifikanın kök sertifikası olmadığı durumlar da mümkün olabilmekte, sertifika zinciri üzerindeki herhangi bir sertifika güvenilir olarak belirlenmişse sertifika doğrulama işlemi bu sertifikaya gelindiği noktada son bulup kök sertifikaya kadar gitme zorunluluğu olmayabilmektedir.

RFC 3280[2]'de Internet X.509 PKI sertifika yapısı; tüm temel alanları, farklı işlevlere ait eklentileri ve bunların yapıları ayrıntılarıyla anlatılmış, bir sertifikanın bu yapıya uyması için gerekli tüm koşullar sıralanmıştır. Bir sertifikanın bu standarda göre geçerli sayılabilmesi için, bu sertifikayla birlikte güvenilir bir sertifikaya kadar olan yol üzerindeki tüm sertifikaların bu şartları sağlaması gerekmektedir.

Tanımlanan sertifika temel alanları ve bu alanların sahip olması gereken yapıları şu şekilde özetlenebilir:

Sertifika seri numarası: Her bir sertifika hizmet sağlayıcı tarafından tekil olarak verilen ve sertifika hizmet sağlayıcı ismi ile birlikte sertifikayı tanımlayan bu alan, pozitif bir tam sayı olmalıdır.

Versiyon: Bu alanda v1, v2, v3 olarak tanımlanan bilgi, sertifikanın eklentiye sahip olup olmamasına göre uygun değerleri almaktadır.

İmza algoritması: Sertifikanın hangi imzalama algoritması ile imzalandığını belirten bu alandaki

algoritma bilgisi, Açık Anahtar alanındaki verinin içerdiği algoritma bilgisi ile aynı olmalıdır.

Geçerlilik tarihi: Bu alanda sertifikanın geçerli olduğu zaman aralığı, Geçerlilik Başlangıcı ve Geçerlilik Sonu alanları ile belirlenir ve sertifikanın geçerlilik kontrolünün yapılmak istendiği zaman bu aralıkta olmalıdır.

RFC 3280'de tanımlı olan bazı eklentiler ve bu eklentilerin sahip olması gereken yapı ve değerler de şunlardır:

Hizmet Sağlayıcı Anahtarı Tanımlayıcısı- Özne Anahtarı Tanımlayıcısı: Sertifikanın bir üst SM anahtarı bilgisini taşıyan Hizmet Sağlayıcı Anahtarı Tanımlayıcısı eklentisi ile sertifikanın bir üst SM sertifikasındaki, o sertifikaya ait açık anahtar bilgisini içeren Özne Anahtarı Tanımlayıcısı değerleri aynı olmalıdır.

Anahtar Kullanımı: Sertifikanın kullanım amacını(veri imzalama, veri şifreleme vb.) belirten bu eklenti, sertifikanın kullanım amacını doğrulayan bir değere sahip olmalıdır.

Temel kısıtlamalar: Doğrulama işlemi yapılacak sertifika, zincir üzerindeki ara sertifikalardan biri olarak SM sertifikasıysa bu özelliği sertifikadaki Temel Kısıtlamalar eklentisinde belirtilmelidir. Bu eklentideki Konu Türü değeri CA olarak tanımlanmış olmalıdır.
Temel Kısıtlamalar eklentisi yol uzunluğu alanında yol uzunluğu kısıtlanmaktadır. Kontrolü yapılan sertifikaya kadar geçilen yolun uzunluğu kısıtı geçmeyen bir değerde olmalıdır.

Sertifikanın geçerli sayılabilmesi için bu tanımlanan yapıya sahip olması gerekmesiyle birlikte imzasının doğrulanabilmesi ve iptal edilmemiş olduğunun kontrol edilmesi gerekmektedir:

İmza kontrolü: Sertifikanın imzası, sertifikayı imzalayan SM sertifikası açık anahtarı ile kontrol edilmelidir. Burada da imza doğrulama işlemi yapılacağı için imza değerinden önce sertifikayı imzalayan SM sertifikası geçerlilik kontrolü yapılmalıdır. Sertifika doğrulama işlemindeki zincir oluşturma adımı bu noktada başlamakta olup bir üst SM sertifikası en başından itibaren tüm adımlardan geçip doğrulanması başarıyla yapıldıktan sonra bu sertifikadaki açık anahtar ile sertifikanın imzası kontrol edilir. Tüm sertifikalar için imza doğrulama işlemi yapılması gerektiği için kök sertifikaya veya güvenilir sertifikaya kadar yol üzerindeki tüm sertifikaların doğrulanma işlemi gerçekleşmiş olur. Bir sertifikanın üst SM sertifikasına ulaşabilmek için sertifikadaki Hizmet Sağlayıcı Bilgi Erişimi eklentisindeki bilgiler kullanılabilir. Bu eklentide SM sertifikasının LDAP veya HTTP adresi verilmiştir, erişim yöntemleriyle bu uzaktaki konumlardan alınan SM sertifikası ile doğrulama işlemine devam edilir. Ayrıca üst sm sertifikası Sertifika Doğrulama sürecine dışarıdan verilebilecek yardımcı bilgiler arasında yer alabilir.

İptal durumu kontrolü: Seritifikanın doğrulamasının yapılacağı zamandaki iptal durumu kontrol edilmelidir. Sertifika çeşitli sebeplerle geçerlilik zamanı dolmuş olmasa bile askıya alınmak veya iptal edilmek suretiyle geçersiz hale gelmiş olabilir. Sertifikanın iptal durumu, sil servisleri tarafından periyodik olarak yayımlanan Sertifika İptal Listeleri veya anlık sertifika durumunu verebilecek OCSP sunucuları kullanılarak öğrenilebilir. Sertifika iptal listelerinde iptal edilmiş veya askıya alınmış tüm sertifikalar listelenmektedir. OCSP sunucuları da herhangibir sertifika durum istek mesajına o sertifikanın o andaki durumunu içeren mesaj ile cevap vermektedir. Sil dosyalarının çekilebileceği LDAP veya HTTP adresleri, sertifika içinde SİL dağıtım noktaları eklentisinde yer almaktadır. OCSP sorgusu yapılabilecek servisin adresi de Hizmet Sağlayıcı Erişim Bilgisi eklentisinde verilmiş olan OCSP sunucusu adresinden edinilebilir.[3]

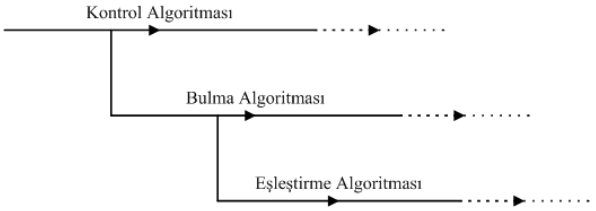
Sertifikanın tanımlanan standartlara uyumlu olarak geçerli sayılabilmesi için, sertifika tanımlanan yapıda olmalı ve sertifikanın geçerlilik kontrol adımlarından başarıyla geçmesi gerekmektedir. Ancak uygulamalardaki ihtiyaçlara göre sertifikanın geçerli sayılabilmesi için tanımlanan bu şartlardan bazıları dışarıda bırakılabilmekte veya bu şartlara yenileri eklenebilmektedir. Ayrıca bu standartta zorunlu tutulmayıp tavsiye edilen bazı koşullar da farklı uygulamalar tarafından farklı şekillerde yorumlanabilir. Örneğin 15 Ocak 2004 tarihli, T.C. 5070 sayılı Elektronik İmza Kanunu'nda tanımlanan Elektronik İmza'nın tanımlanan nitelikli sertifikalar tarafından oluşturulması gerekmekte, bu sertifikaların nitelikli sertifika olarak doğrulanması gerekmektedir. Bunun için de sertifikalar içinde tanımlanmış bir eklentinin, tanımlanmış bir değerde olması şart koşulmaktadır. Halbuki bu eklenti, RFC 3280 standardına göre sertifikada yer alabilecek ancak zorunlu olmayan bir eklenti olarak tanımlanmıştır. Ayrıca sertifikanın iptal kontrolü yapılırken kullanılacak yöntem, uygulamanın çalışma ortamı veya tercihine göre değişiklik gösterebilmektedir. Kapalı ortamlarda çalışması gereken bir uygulama, her an için OCSP sunucusuna erişemeyeceğinden geçerliliği kontrol edilmiş bir SIL dosyasının kapalı ortama alınması ve bundan sonraki tüm kontrollerin bu SIL listesi üzerinden yapılması tercih edilebilir.

Sonuç olarak bir doğrulama uygulamasının hangi kontrolleri içermesi gerektiği ve bu kontrollerin yapılma yöntemleri farklı şartlara, farklı uygulamalara göre değişmekte; doğrulama uygulamasının bu değişikliklere göre dinamik olarak geçerlilik kontrolünü yapabilmesi gerekmektedir. Bu çalışmamızda, tüm bu şartları sağlayabilecek ve uygulamalara sertifika doğrulama işlemini esnek bir şekilde gerçekleştirme imkanı verecek olan bir Sertifika Doğrulama Kütüphanesi mimarisi önerimizi anlatacağız ve bileşenlerini açıklayacağız.

3. SERTİFİKA DOĞRULAMA KÜTÜPHANESİ

3.1 Genel Mimari

Sertifika Doğrulama Kütüphanesi nesne yönelimli bir modeldir ve hiyerarşik olarak tanımlanmış türetilebilir sınıflardan oluşmaktadır. Bu sınıflar kontrolcüler, bulucular ve eşleştiriciler şeklince üç temel grupta incelenebilir. Asıl doğrulama işlemini oluşturan kontrolcüler kontrol işlemleri sırasında ihtiyaç duydukları bilgilere (yayıncı sertifikası, sertifika iptal listesi SIL, çevrimiçi sertifika durum bilgisi OCSP, vb.) bulucu nesneleri aracılığıyla ulaşırlar. Bulucu nesneleri bulduğu bir bilginin aramakta olduğu bilgi olup olmadığına eşleştiriciler yardımıyla karar verirler. Doğrulama süreci kontrol, bulma ve eşleştirme süreçlerinin birbirlerini tetiklemesi ile oluşan toplam süreçtir.

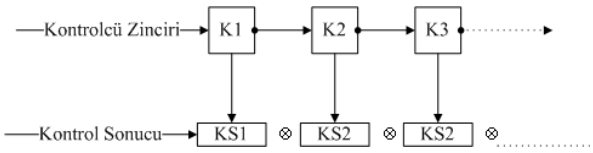


Şekil 1. Doğrulama Akışı

Kontrolcü, bulucu ve eşleştirici nesnelerinin belirli bir sırada bir araya gelmiş her bir alt kümesi bir doğrulama politikası oluşturur. Bu sayede istenilen kontrol işlemlerinin eklenilip çıkarılabildiği, kontrol sırasında ihtiyaç duyulan bilgilerin nasıl ve nereden temin edileceğinin belirtilebildiği ve bu bilgilerin birbiriyle eşleştirilmelerinin isteğe göre tanımlanabildiği dinamik ve esnek bir yapı sağlanmış olur. Bir doğrulama politikasının gerçeklenmesi bu politikayı oluşturan nesnelerin tanımlanması ve bu nesnelerin kontrolcü, bulucu ve eşleştirici adı altında üç ayrı zincir üzerinde dizilmesiyle sağlanır. Bu zincirler doğrulama politikasının bir veri yapısından (XML dosyası, ASN, vb.) okunmasıyla çalışma zamanında oluşturulabilirler.

3.2 Kontrolcüler

Sertifika Dogrulama Kütüphanesi dinamik ve değiştirilebilir bir yapı sağlamak için doğrulama işlemini bir dizi atomik kontroller şeklinde gerçekleştirir. Bu kontroller daha küçük parçalara bölünmesi makul olmayan birbirinden bağımsız modüllerdir ve bir sertifikanın geçerliliğinin kontrolünü oluşturan işlemleri içerirler. Örneğin ”Sertifika Seri Numarası pozitif bir tamsayıdır” [2] önermesinin kontrolü bir kontrol modülü olarak düşünülebilir ve sadece bu işi yapan bir kontrol sınıfı tanımlanabilir. Kontrol sınıfları atomik olarak tanımlandığı için kontrol algoritması, kontrol sınıfllarının sıralı olarak çalıştırıldığı bir algoritma olabileceği gibi bütün kontrolcülerin aynı anda çalıştığı paralel bir süreç olarak da ele alınabilir. Her bir kontrolcü sınıfı için o sınıfa ilişkin bir Kontrol Sonucu Sınıfı tanımlanmıştır ve bu sonuç sınıfında yapılan kontrolün sonucu saklanır. Dolayısıyla kontrol zincirinin çalıştırılması sonucunda ortaya bir kontrol sonucu zinciri çıkar. Kontrol sonuç sınıfları kontrolün başarılı olup olmadığını ifade eden mantıksal bir boolean değere sahip oldukları gibi eğer kontrol geçersizse bunun sebebini ifade eden bir detay bilgisi de içerirler. Sertifika doğrulama işleminin mantıksal sonucu kontrol sonuç sınıflarının mantıksal sonuçlarının VE işlemi ile toplamı sonucudur.

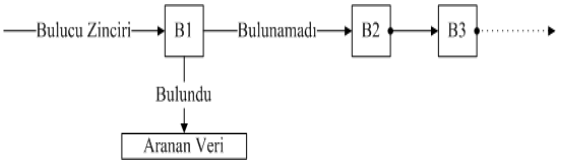


Şekil 2. Kontrol Algoritması

3.3 Bulucular

Kontrol sınıfları kontrol işlemlerini gerçekleştirirken sertifika dışında bazı bilgilere ihtiyaç duyabilirler. Bunlar o sertifikanın yayıncısının sertifikası, sertifika iptal listesi (SIL), çevrimiçi sertifika durum bilgisi (OCSP) gibi veriler olabilir. Bu bilgiler yerel olarak hazır bir kaynaktan edinilebileceği gibi (örn.: yerel makinede bir dosya), ağ üzerinden bir dizin sunucusundan edinilebilecek bir sorgu sonucu da olabilir. Bu

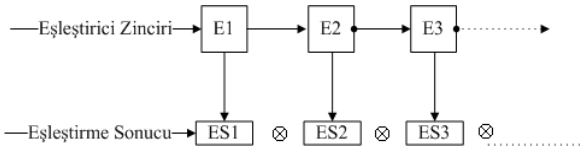
yardımcı bilgilerin kendileri ve kaynakları çeşitlilik gösterdiği ve zamanla değişime tabi oldukları için Sertifika Doğrulama Kütüphanesi bu bilgileri bulmayı sağlayan esnek ve dinamik bir arayüze sahiptir. Bulucu sınıfları herhangi bir bilginin nereden ve nasıl bulunacağını bilen bir çeşit arayüz sınıflarıdır. Genel olarak üç ayrı gruba ayrılır ve bu gruplar ihtiyaç duyulan bilginin çeşidine göre ileride arttırılabilir. Bir sertifikanın yayıncı kuruluşunun sertifikasını bulan sertifika bulucular, yayıncı kuruluşların yayınladığı sertifika iptal listelerini (SIL) bulan SIL bulucular ve bir sertifika için OCSP cevabı bulan OCSP Cevabı bulucular bulucular kümesinin temel gruplarıdır. Bu gruplar altında aranan verinin kaynağına göre bulucu sınıfları türetilmiştir. Örneğin dizinden bir yayıncı sertifikası bulmak için DizinSertifikaBulucu sınıfı tanımlıdır ve bu sınıf kendisine verilen bir yerel ya da genel ağ adresine LDAP protokolü ile bağlanıp aradığı sertifikaya nasıl ulaşacağını bilir. Kontrolcüler, bulucu zincirinde tanımlı olan bulucu sınıflarını kullanarak kendilerine gerekli olan yardımcı bilgilere ulaşırlar ve kontrol işlemlerini tamamlarlar.



Şekil 3. Bulma Algoritması

3.4 Eşleştiriciler

Bulucu sınıfları aramakta olduğu veriye ulaşınca bunun gerçekten aradığı veri olup olmadığını doğrulamalıdırlar. Örneğin bir yayıncı sertifika bulucusu bulduğu yayıncı sertifikasının kendisine verilen sertifikanın yayıncısının sertikası olup olmadığını kontrol etmelidir. Bu kontrol işlemi bir takım kurallara tabidir. Her bir eşleştirici bu kurallardan birini kontrol eder ve kontrol başarılı olursa eşleştirme sonucunu başarılı olarak döner. Uygulama geliştirici bu eşleştirme kurallarının hangisinin ya da hangilerinin sağlanmasının yeterli olduğuna kendi karar verebilir ve buna uygun bir eşleştirici alt kümesinden eşleştirici zinciri oluşturur. Bir veri ikilisinin (örn. sertifika ve yayıncı sertifikası ikilisi) eşleştirilebilmesi için eşleştirici zinciri üzerindeki bütün eşleştiricilerin başarılı olarak dönmesi gerekir.



Şekil 4. Eşleştirme Algoritması

3.5 Doğrulama Politikası

Elektronik sertifikaların kullanımları günden güne yaygınlaştığı ve kullanım alanları çeşitlilik gösterdiği için bir sertifikanın geçerliliğinin tespiti için sağlaması gereken kriterler de kullanım alanlarına ve uygulama geliştiricilerin güvenlik seviyesi tercihlerine göre bir o kadar çeşitlik gösterirler. Gerek kontrol edilecek özellikler gerek bu kontroller sırasında ihtiyaç duyulacak bilgilerin nerelerden ve nasıl edinileceği ve gerekse de bu bilgilerin aradığımız veri olup olmadığının nasıl eşleştirileceği uygulamadan uygulamaya ve zamandan zamana değişebilen dinamik bir doğrulama modeli gerektirir. Sertifika Doğrulama Kütüphanemiz doğrulama sırasındaki bu işlemleri (kontrol, bulma ve eşleştirme) atomik alt parçacıklara ayırarak ve bunları dinamik birer zincir üzerinde modelleyip doğrulamayı bu zincirlerin işlenmesi şeklinde ele alarak oldukça esnek bir Doğrulama Politikası modeli oluşturmuştur. Sertifika doğrulama işleminin bütün aşamaları bu politika yapısında şekillendirilebilir. Uygulama geliştiriciler Sertifika Doğrulama Politikasını herhangi bir ortak veri temsil dili formatında (XML, ASN. vb.) oluşturarak politikalarını çalışma zamanında güncelleyebildikleri, zaman içerisinde değişen ihtiyaç ve teknolojiler doğrultusunda yeni kontrol, bulma ve eşleştirme yöntemleri ekleyebildikleri bir sertifika doğrulama arayüzüne sahip olabilirler.

4. SONUÇLAR

Bilişim teknolojilerinin hayatın her alanında yer almaya başladığı ve bilgi güvenliğinin giderek önem kazandığı günümüzde elektronik sertifikaların sayısı ve kullanım alanları her geçen gün artmaktadır. Bir sertifikanın geçerliliğinin tespiti en az o sertifikanın yerine getirdiği iş kadar önemlidir. Bir sertifika ancak doğrulanabildiği zaman taşımakta olduğu güven değerine ulaşır. Kullanım alanlarının çokluğu ve zaman içerisinde standartlarda ve mevzuatlarda meydana gelen değişikler dolayısıyla sertifika doğrulama çok değişken bir süreçtir. Bu yüzden

uygulama geliştiricilerin esnek ve dinamik bir sertifika doğrulama kütüphanesine sahip olmaları gerekir. Sertifika Doğrulama kütüphanemiz kontrolcü, bulucu ve eşleştirici ata sınıflarının alt kümelerinin bir araya gelerek oluşturduğu Doğrulama Politikası modeliyle bu ihtiyaçları karşılamaktadır.

KAYNAKLAR

[1] CEN Workshop Agreement CWA 14171, July 2001

[2] IETF RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[3] Hasırcıoğlu I., Elektronik İmza Oluşturma Ve Doğrulama Standartları, *Ulusal Elektronik İmza Sempozyumu, 2006*.

[4] 5070 Sayılı Elektronik İmza Kanunu, 23.01.2004 tarih ve 25355 sayılı Resmi Gazete.