# UMU-PKI v6 Sistemi İçin Sertifika Yönetimi ve Doğrulama Mekanizması Tasarımı

Burak Çalışkan [1] İbrahim Soğukpınar [2]

[1,2] Bilgisayar Mühendisliği Bölümü, Gebze Yüksek Teknoloji Enstitüsü, Kocaeli
[1] e-posta: burakc@uekae.tubitak.gov.tr [2] e-posta: ispinar@bilmuh.gyte.edu.tr

## Özetçe

Açık anahtarlama altyapısı, günümüz güvenlik mimarilerinin olduğu kadar, geleceğin güvenli haberleşme teknolojilerinin ve dağıtık uygulama ortamlarının en temel sistem bileşenlerinin başında gelmektedir. IPv6 tabanlı X509 sertifika servislerinin tasarımını ve entegrasyonunu amaçlayan UMU-PKI modeli çalışmaları, geleceğin internetinin başarılı bir şekilde IPv6 tabanlı olabilmesi için büyük önem taşımaktadır. Bu çalışmada, UMU-PKI sisteminin sertifika yönetim ve doğrulama mekanizmalarının tasarım ve entegrasyonuna yönelik iyileştirme önerileri yapılmıştır.

## 1. Giriş

Açık anahtar altyapısı temelde, orta veya büyük ölçekli organizasyonel sistemler içerisinde, açık anahtar kodlama yöntemlerinin, ilgili mekanizmalar ve işlevsel birimler aracılığıyla efektif olarak kullanımını amaçlar. Bu yapı içerisindeki temel birimler, Sertifika Makamı, Kayıt Makamı ve Dizin Sunumcu olup ek olarak uygulanacak servislere göre değişen, akıllı kartlar, zamanlayıcı sunumcular ve OCSP sunumcular yer alabilir. UMU-PKI olarak adlandırılan altyapı, IPv6 destekli X509 sertifikasyon servislerinin açık anahtar altyapısına bağlı kalarak uygulanabilmesini amaçlayan bir sistem modeli oluşturur. Bu servisler aracılığıyla kullanıcılar, arayüzleri vasıtasıyla sertifika talebi, yenilenmesi, iptali veya sertifika bilgilerinin sorgulanması gibi işlevleri kolaylıkla gerçekleştirebilirler. [1] IPv6 destekli X509 sertifika işlevleri desteğinin sağlanmasındaki temel mekanizmaların başında, sistemde yer alacak sertifika tabanlı servislerin yönetimi ve sertifika yapılarının doğru bir şekilde oluşturulması gelmektedir. Bu açıdan bakıldığında, sistemde sağlanacak sertifika yönetim ve doğrulama işlevlerinin, genel kabul görmüş metodolojilere sahip olması gerekliliği, sistemin dağıtık platformlara entegrasyonunda önemlidir. Bu iki temel unsurun sistem bazında tamamlanmamış entegrasyon eksiklikleri, geliştirilmekte olan ve sertifika yaşam döngüsü içerisinde yer alan işlevleri sağlamayı hedefleyen Certificate Management Messages Over CMS (CMC) ve sertifika yolu doğrulama işlevlerine yönelik servisler sunan Server Based Certificate Validation Protocol (SCVP) protokollerinin entegrasyon çalışmalarını beraberinde getirmektedir.

Bu çalışmada, UMU-PKI alt yapısında sertifika yönetimi ve doğrulanması işlevlerinin gerçekleştirilmesine yönelik sisteme CMC ve SCVP protokollerinin entegrasyonu önerilerek tasarım ve gerçekleme yapılmıştır. Önerilen çözüm ile IPv6 için tasarlanan altyapı, daha güvenli hale getirilmiştir.

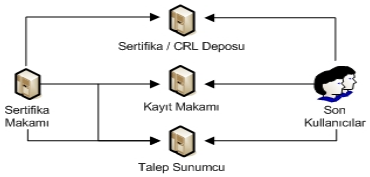
## 2. IPv6 Tabanlı PKI Sistemi : UMU-PKI v6

Bir IPv6 ağı içerisinde, açık anahtar sertifikalarını kullanarak sistemde yer alan bilgileri koruma ve sistem kullanıcılarını yetkilendirmeye yönelik HTTPS benzeri güvenli web sunumcuları içeren servisler, VPN cihazları, yetkilendirme, otorizasyon ve hesaplama servisleri yer alabilir. UMU-PKI 'ya da Java IPv6 PKI altyapısı, dağıtık organizasyonlara yönelik uygulamaların ve kişisel gizliliğe sahip bilgilerin korunması ve saklanmasında, açık anahtarlama altyapısını, IPv6 temelli teknolojileri içermek suretiyle gelişimlerini kolaylaştıracak biçimde sağlayarak, farklı işlevsel fonksiyonalitelere sahip uygulamalarla, ciddi bir gizlilik ve güvenlik platformu oluşturmaktadır. Bu servisler aracılığıyla birimler, sayısal olarak imzalanmış bilgileri kodlayabilirler.

### 2.1. UMU-PKI v6 Mimarisi

UMU-PKI v6 ya ait temel karakteristik fonksiyonaliteler [2] :

- Kullanıcılar sertifikaları oluşturabilir, yenileyebilir, iptal edebilir ve kullandıkları web arayüzleri üzerinden tüm sertifika işlemlerini gerçekleştirebilirler.
- LDAP v6 dizin servisleri, kullanıcıları, sertifika iptal listelerini ya da Sertifika Makamı sertifikalarını saklamayı destekler.
- Kullanıcılar, opsiyonel olarak akıllı kartlar içerisinde kendilerine ait kriptografik bilgileri saklayabilirler.
- Organizasyona ait güvenlik politikaları, sistem dahilindeki tüm PKI bileşenlerince entegre edilebilir.
- JAVA platformunda geliştirilmiştir. IETF standartlarına uygundur. Sistem içerisinde IPv6 veya IPv4 kullanılabilir
- Cihazların sertifikalanabilmesini sağlayan Simple Certificate Enrollment Protocol (SCEP) protokolünü, 6WIND yönlendiricileri ve çapraz sertifikaları destekler.




*Şekil 1*: Sistem Bileşenleri

Kayıt Makamı, taleplerin Sertifika Makamı'na iletiminden sorumludur. Sistem konfigürasyonuna bağlı olarak, birden fazla sayıda Kayıt Makamı bulunabilir. Sistem yöneticisi, sertifika, yenileme ya da iptal taleplerini ilgili politika gereğince kontrol edebilir. Kayıt Makamı, gelen talepleri, Sertifika Makamı tarafından işlenmek üzere veritabanında saklar. Talep Sunumcu, sisteme bağlı birimlerden yapılan talepleri toplayan ve kendi veritabanında saklayan birimdir.

Sertifika Makamı, Talep Sunumcu'da yer alan talepleri gerçekleştirmekten sorumludur. Sertifika taleplerinde, Sertifika Makamı tarafından oluşturulan sertifika, veritabanında kaydedilerek LDAP sunumcudan yayınlanır ve kullanıcı imzalı bir e-posta ile bilgilendirilir. Yenilemelerde, geçerli olan sertifika bilgisi, Sertifika Makamı tarafından veritabanında ve LDAP sunumcuda güncellenir. Sertifika iptallerinde, veritabanındaki sertifika bilgisi Sertifika Makamı tarafından işaretlenerek bir sonraki sertifika iptal listesinde yayınlanmak üzere kaydedilir. Burada Talep Sunumcu ile Sertifika Makamı bağlantısı tek yönlüdür. Bu sayede sistemdeki bir birim, Sertifika Makamı'na direk bağlantı kuramaz. Sistem, opsiyonel olarak kullanıcılarına Sertifika Deposu kullanımı imkanını da sağlamaktadır. LDAP v6 dizini içerisinde tüm sertifikalar ve iptal listeleri kullanıcılara açık halde saklanabilir. Sistem politikasının tanımlanması ve uygulanması, bu noktada organizasyondaki kullanıcıların, sistemde gerçekleştirecekleri işlemlerde, hangi sınırlamaların olması gerektiğini tanımlar. Sistem politikası, bir seri numarası, geçerlenme tarihleri ve bir grup birim tanımlamalarına sahip sayısal bir dokümandır. Buradaki birim tanımlamaları, politikadaki sınırlamalarının hangi birimler üzerinde uygulanacağını belirtir. Politika tanımlandıktan sonra Sertifika Makamı tarafından imzalanarak tüm birimlerce uygulanır hale gelir. [2]

### 2.2. UMU-PKI v6 Servisleri

Sertifika yaşam döngüsü olarak adlandırılan, sertifikaların talep edilmeleri, geçerlenmeleri, yayınlanmaları, iptal edilmeleri ve yenilenmeleri süreçlerini sağlayan yapılardır.

#### *2.2.1. Sertifika Talepleri*

Sertifika talepleri sistemde PKCS#10 [3] formatında olup, taleplerin gerçekleştirilmesinde farklı yöntemler izlenebilir. Örneğin kullanıcılar, Kayıt Makamı üzerinden taleplerini gerçekleştirebilirler. Kayıt Makamı, PKCS#10 nesnesini kullanarak bir talep oluştur ve SSL bağlantısı üzerinden Talep Sunumcu'ya iletir. Diğer yöntemde, kullanıcılar, web arayüzleri üzerinden taleplerini üretir ve Talep Sunumcu'ya kaydeder. Talepler Kayıt Makamı tarafından geçerlenerek Sertifika Makamı tarafından işlenmek üzere saklanır.

#### *2.2.2. Sayısal Sertifikaların Edinilmesi*

Sertifika Makamı bir sertifikayı geçerli hale getirdiğinde, ilgili kullanıcı sertifikayı alabilmelidir. Bu işlem, bir web arayüzü veya LDAP deposu aracılığıyla gerçekleştirilebilir. Oluşturulan sertifika ya da liste, web üzerinden kullanıcının arayüzüne indirilir. Eğer kullanıcı bir akıllı karta sahipse, ilgili anahtarlar kaydedilebilir. Sertifikalar, kullanıcılara açık bir depoda saklanarak LDAP istemcisi üzerinden edinilebilir.

#### *2.2.3. Sertifika Yenileme Talepleri*

Kullanıcılar, sertifikalarının geçerlilik sürelerini, sistem politikası uyarınca güncelleyebilirler. Bu işlem Kayıt Makamı veya web arayüzünden SSL vasıtasıyla sistemde sağlanabilir.

#### *2.2.4. Sertifika İptal Talepleri*

Bazı durumlarda, sertifikalar, geçerlilik süreleri dolmadan önce sistemden kaldırılabilir. Kullanıcılar, iptal işlemi için, Kayıt Makamı üzerinden bir iptal talebinde bulunma ya da aynı işlemi web üzerinden gerçekleştirme yöntemlerini kullanabilirler.

## 3. Sertifika Yönetimi ve Doğrulama : CMC ve SCVP Protokolleri Entegrasyonları Tasarımı

Bu yapı içerisinde (UMU-PKI) sertifika yönetimi ve sertifika yolu kurulumu, iki önemli unsur olarak gözükmektedir. Sertifika yönetimiyle, sertifika yaşam döngüsü içerisindeki mekanizmaların kontrolü sağlanırken, sertifika yolunun kurulması ve bir birim tarafından doğrulanması da, bu başlık altında incelenmesi gereken ikinci temel noktayı oluşturur. CMC ve SCVP protokolleri, içerdikleri servislerle sistemsel olarak bu mekanizmaları sağlayacak çözümler sunmaktadır. Güncel çalışmalar göz önünde bulundurulduğunda, sertifika yönetimi ve doğrulama süreçlerinde gereken mekanizmaların, sistemin tümünde uygulanabilir ve kolaylıkla entegre edilebilir yapıda olması zorunluluğu bulunmaktadır. Bu nedenle, bu iki temel unsurun tasarımında, uluslararası platformlarda kabul gören servislerin entegrasyonu gerekliliği açıktır. Buradaki çalışmanın da temelini teşkil eden, UMU-PKI sisteminin bu protokolleri destekleyecek servislerle entegrasyonuna yönelik tasarım modellemelerinin gerçekleştirilmesi, sisteme ait uygulama alanının genişletilmesinin yanı sıra, süreçler bazında performans katkılarına da neden olacaktır.

### 3.1. Sertifika Yönetiminde CMC Entegrasyonu

Cryptographic Message Syntax (CMS) temelli sertifika yönetim mekanizmaları sunan CMC protokolü, bir PKI sisteminde ihtiyaç duyulan açık anahtar servislerine yönelik arayüz ihtiyacını gidermek amacıyla tasarlanmıştır. Buna ek olarak, temel servisleri destekleyecek bir takım tamamlayıcı ek servisler de protokol bünyesinde sağlanabilir. Bir sertifika kayıt işlemi, genelde tek mesaj döngüsü içerisinde oluşturulmaktadır. [3] Bir kayıt talebi, istemciden sunumcuya gönderilir ve talebe karşılık yanıt, sunumcudan istemciye iletilir. Bu çevrimde iki farklı talep-yanıt çifti tanımlanabilir.

#### *3.1.1. Basit PKI Talebi*

PKCS#10 [3] tabanlı formata sahip olan bu tip taleplerin içeriğinde, sertifika talebine ait konu adı, açık anahtar bilgisi ve özellikler dizisi yer alır. Oluşan bilgi, ilgili özel anahtarla imzalanarak talep formatı oluşturulur.

#### *3.1.2. Basit PKI Yanıtı*

Bu yanıt tipi, içerik olarak SignerInfo bilgisine sahip olmayan CMS SignedData [3] nesnesini içerir. SignedData nesnesi, tanımı itibariyle birden fazla sertifika bilgisini içerebilirken, oluşturulan yanıt bilgisinin imzalanmasına gerek yoktur.

#### *3.1.3. Tüm PKI Talebi*

Bu talepler, SignedData nesnesi içerisine paketlenmiş PKIData [3] nesnesinden oluşur. PKIData nesnesi içeriğinde kontrol özellikleri, talep bilgisi ve CMS tabanlı nesneler bulunurken, SignedData nesnesi ilgili anahtarla imzalanır.

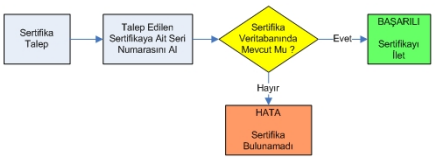
#### *3.1.4. Tüm PKI Yanıtı*

Bu format, SignedData nesnesine paketlenmiş ResponseBody [3] nesnesinden oluşur. SignedData nesnesi, Sertifika Makamı veya Kayıt Makamı tarafından imzalanır.

UMU-PKI CMC entegrasyonu, sertifika kayıt, iptal, yenileme, iptal listesi edinme ve durum sorgulama mekanizmalarının gerçekleştirilmesine yönelik servisleri sağlamalıdır. Kullanıcı, bir sertifika, iptal veya yenileme talebinde bulunduğunda talep, Sertifika Makamı tarafından geçerlenmesi için bir seri numarası üretilerek saklanır. Bu seri numarası, talep durumunun sorgulanmasına yönelik mesajlarda, durum bilgisinin edinilmesini sağlar. Sertifikaların ve iptal listelerinin edinilmesine yönelik servislerde de işleyiş benzer olmalıdır. İstemci birim, bir sertifika ya da iptal listesi talebinde bulunur. Buna karşılık sistem, istemci sertifikasını ya da iptal listesini Privacy Enhanced Mail (PEM) formatında istemciye iletebilir. [2]

### *3.1.5. Sertifika Talepleri*

Sertifika taleplerinin UMU-PKI sistemi içerisinden CMC protokolüne uygun şekilde gerçekleştirilebilmesine yönelik süreç entegrasyon modeli Şekil 3 'te gösterilmiştir.

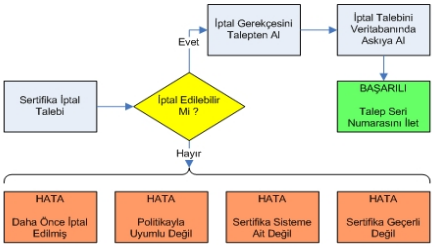



*Şekil 3*: Sertifika Talepleri Entegrasyon Modeli

Modelin uygulanmasında, Java.Security.Cert.X509Certificate sınıfına ait metodlar kullanılarak talebe ait seri numarası ve konu bilgileri alınabilir. Alınan bu bilgiler, sertifika dizisi içerisinde oluşturulacak bir kontrol döngüsü yönetiminde karşılaştırılarak sertifikayla ilgili yanıt kullanıcıya iletilebilir.

### *3.1.6. Sertifika İptal Talepleri*

İptal taleplerinin sistem içerisinden CMC protokolüne uygun şekilde gerçekleştirilebilmesine yönelik model Şekil 4 'tedir.

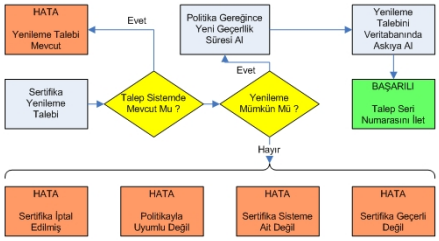



*Şekil 4*: İptal Talepleri Entegrasyon Modeli

Modelin uygulamasında, Java.Security.Cert.X509Certificate sınıfına ait metodlarla talebe ait nitelik bilgileri alınarak veritabanındaki bilgiler koşullu kontrollerle karşılaştırılabilir ve talebin iptal edilip edilemeyeceği kontrol edilebilir. Kontrol sonucunda, ilgili hata mesajı kullanıcıya iletilebilir ya da IAIK.X509.RevokedCertificate sınıfına ait metodlar kullanılarak sistemde yeni bir iptal talebi oluşturulur.

### *3.1.7. Sertifika Yenileme Talepleri*

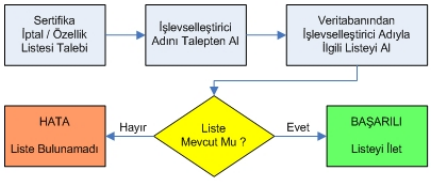
Sertifika yenileme taleplerinin CMC protokolü gereğince gerçekleştirilebilmesine yönelik model Şekil 5 'tedir. Buradaki entegrasyonda Java.Security.Cert.X509Certificate sınıfına ait metodlarla gelen talepteki sertifika bilgileri alınarak, veritabanında kontroller gerçekleştirilebilir. Sistem politikası uyarınca yenilemenin mümkün olup olmadığı kontrolü Piscis.Pki.Shared.Policy.PolicyManager sınıfına ait metodlar yardımıyla sağlanabilir. Yenileme mümkünse, geçerlilik süresi hesaplanarak yeni bir sertifika oluşturulur ve sertifika bilgileri veritabanında saklanabilir.




*Şekil 5*: Yenileme Talepleri Entegrasyon Modeli

### *3.1.8. Sertifika İptal / Özellik Listesi Talepleri*

UMU-PKI sisteminden sertifika iptal listesi talebine yönelik CMC protokolünü destekleyen model Şekil 6 'dadır.

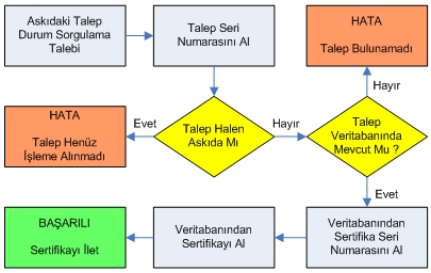



*Şekil 6*: İptal Listesi Talepleri Entegrasyon Modeli

Entegrasyonda, Java.Security.Cert.X509Certificate sınıfına ait metodlar aracılığıyla gelen talepteki sertifikaya ait bilgiler alınarak, veritabanından ilgili listenin kontrolü gerçekleştirilebilir. Java.Security.Cert.X509CRL sınıfına ait metodlar ve önceki süreçlerde gereken sertifika nesneleri yardımıyla liste oluşturularak istemciye iletilebilir.

### *3.1.9. Askıdaki Talep Durum Sorgulama Talepleri*

UMU-PKI sistemi içerisinden durum sorgulama talebine yönelik entegrasyon modeli Şekil 7 'dedir.




*Şekil 7*: Durum Sorgu Talepleri Entegrasyon Modeli

Durum sorgulama talepleri entegrasyonu, temelde gelen talepteki sertifika bilgileriyle veritabanındaki bilgiler arasındaki koşullu kontroller sonucu ortaya çıkacak durumlara özel yapılandırılan mesaj-hata iletilerinden oluşur.

### 3.2. Sertifika Doğrulamada SCVP Entegrasyonu

SCVP, sertifika yolu yapılandırma veya doğrulama işlevlerini sunumcuya devrederek, organizasyon içerisindeki doğrulama politikalarını, merkezi olarak yönetebilme ve bu sayede açık anahtar tabanlı uygulamaların entegrasyonunu kolaylaştırma imkanını sağlar. Sertifika yolu doğrulama, örneğin sertifika yolundaki sertifikaların iptal edilmiş olup olmadığı bilgisinin alınması, bir ya da birden fazla güven bağlantı noktasına sahip bir doğrulama politikasına uygun şekilde gerçekleştirilir.

Sertifika doğrulama karmaşık bir operasyondur. Eğer sertifika uygulamaları, geniş ölçekli organizasyonlar içerisinde yapılandırılacaksa, uygulamanın sertifikaları kabulü esnasında gerçekleştireceği işlevlerin sayısı asgari tutulmalıdır. Günümüzde açık anahtar altyapısını destekleyen birçok uygulama bulunmasına karşın, sertifikaların doğrulanması konusundaki yükü hafifletecek etkin çözümler yeterince geliştirilememiştir. SCVP protokolü, iki temel uygulama grubu için bu doğrultuda çözümler sunar. İlk grup uygulamaların iki amacı vardır. Sertifikanın içerisindeki kimlik bilgisinin, ilgili açık anahtara ait olup olmadığının doğrulanması ve bu anahtarın uygulamada planlanan amaca yönelik kullanılıp kullanılamayacağıdır. Bu grupta yer alan istemciler, sertifika yolu yapılandırma ve doğrulama yüklerini SCVP sunumcusuna devrederler. Bu işleme, delege edilmiş yol doğrulama adı verilir. İkinci grup uygulamalarsa, sertifika doğrulama yapabilen ancak güvenilir ve etkin bir sertifika yolu yapılandırma metoduna sahip olmayan uygulamalardır. Bu gruptaki istemciler, sertifika yolu yapılandırma görevini sunumcuya devrederken, doğrulama görevini devretmezler. Bu işleme delege edilmiş yol yapılandırma adı verilir. [4] SCVP basit bir talep-yanıt mekanizması sunar. İstemci, talep oluşturarak SCVP sunumcuya iletir, sonrasında SCVP sunumcu talebe karşılık yanıt oluşturarak istemciye gönderir.

Talep modelinin sisteme entegrasyonunda öncelikli olarak bellekteki geçmiş sertifika bilgileri veritabanından alınır. Bu aşamada alınan doğrulanmış sertifika referansları dizisi içerisinde oluşturulacak kontrol döngüsü yardımıyla dizideki sertifikalara ait güven bağlantı noktaları tespit edilerek taleple ilişkilendirilir. Bu işlemden alınan veriler kullanılarak ReqWantBack [4] nesnesi, protokol tanımına uygun şekilde meydana getirilir. Sonrasında Umu.Scvp.Asn1 sınıfında yer alan metodlar aracılığıyla doğrulama talebi oluşturulabilir.

#### *3.2.1. Doğrulama Talepleri*

SCVP talepleri, korumasız ve korumalı olarak adlandırılan iki farklı forma sahiptir. Korumalı talepler, istemcinin sunumcuya karşı geçerlenmesinde ya da talep-yanıt çifti üzerinde anonim istemci entegrasyonunda kullanılır. Buradaki koruma ifadesi, bir sayısal imza ya da mesaj geçerleme kodu [4] ile sağlanır. Eğer istemciye ait açık anahtar, sertifika içerisindeyse, bu durumda istemcinin geçerlenmesinde kullanılabilir. Sunumcu kendine gelen taleplerin korumalı olmasını zorunlu tutup, korumasız talepleri dikkate almayacağını belirtebilir. SCVP istemcisinden gönderilen talep, CVRequest [4] nesnesi olmak zorundadır. Korumasız talep, ContentInfo [4] nesnesi içerisine zarflanmış bir CVRequest nesnesinden oluşur. İstemciler, imzalanmış talep ve yanıtlar için SignedData [4] nesnesini kullanmak zorundadır. Aynı zamanda, mesaj geçerleme kodu kullanıldığında, AuthenticatedData nesnesi kullanılır. Eğer istemci SignedData nesnesini kullanacaksa, belirli bir özel kimliğe, bir sertifika aracılığıyla bağlı olan açık anahtara sahip olmalıdır. İstemci, SignedData nesnesi içerisine, kendine ait sertifikayı işaret eden bir belirteç koymalıdır. İstemci talebi, istemciye ait sertifika bilgisini içerebilir ancak talep boyutunu azaltmak için bu sertifika, istemci tarafından talepten çıkarılabilir. Sertifikaların doğrulanmasına yardımcı olması amacıyla, talep içerisine ek bir takım sertifikalar eklenebilir. İstemci, talebi enkapsüle eden AuthenticatedData nesnesine açık anahtarını koyabilir. Burada belirtilen nesnelere ait sözdizimi ve semantikler CMS içerisinde tanımlanmıştır.

#### *3.2.2. Doğrulama Yanıtları*

Eğer sunumcu, ilgili doğrulama politikasını kullanarak geçerli bir sertifika yolu oluşturabilirse, talebe olumlu yanıt verebilir. Aksi halde hata mesajıyla yanıtlar. Korumalı talepler ve yanıtlarda sunumcular, zorunlu olarak SignedData, opsiyonel olarak AuthenticatedData nesnelerini destekleyebilmelidir. İstemci, sunumcudan gelecek yanıtın korumalı olmasını talep ederse, sunumcular bu nesneleri kullanmak zorundadır. Sunumcu, korumalı bir talebe karşılık, korumalı bir yanıt veriyorsa, talepteki koruma mekanizmasının aynısını, vereceği yanıtta da kullanmalıdır. [4]

Doğrulama yanıtının sisteme entegrasyonunda, öncelikle Java.Text sınıfına ait metodlardan faydalanarak güncel sistem tarihi, zaman ve replyWantBack nesneleri [4] protokolün tanımında belirtilen format içerisinde oluşturularak fonksiyonun girişinde yer alan sertifika dizisi içerisinde Umu.Scvp.Asn1 sınıfına ait metodlarla yanıt nesnesine ait bilgiler tamamlanır.

#### *3.2.3. Doğrulama Servisi Tasarımı*

Sistemdeki doğrulama servisi, doğrulama kontrolüne yönelik bir SCVP talebi aldığında, şu adımları izlemelidir :

I. Gelen sertifika bellekte kontrol edilir. Bellekte rastlanırsa, talepçi birime başarılı yanıt vererek süreci sonlandırır.

II. Sertifikanın güvenilir bir Sertifika Makamı tarafından işlevselleştirilip işlevselleştirilmediği kontrol edilir.

a. Sonuç olumluysa uzantıdaki AuthorityInformationAccess [4] bilgisi, Sertifika Deposu'ndan yeniden edinim işlemi için alınır, karşı Sertifika Makam'ındaki CRL listeleri ve Lokal Sertifika Makamı'ndan karşı Sertifika Makamı'na giden yolda yer alan tüm CRL listeleri alınır.

b. Tüm sertifika yolu doğrulanır. Doğrulama sonucu olumluysa, algoritma olumlu yanıt mesajı ile sonlanır ve bellekteki sertifika yolu bilgileri iletilir. Olumsuzsa, algoritma başarısız yanıt döner.

III. Hedef sertifika bilgilerinden AuthorityInformationAccess uzantısındaki bilgi alınır

a. Uzantı tanımlanmamışsa; eğer hedef sertifika bir Kök Sertifika Makamıysa VI nolu adıma gidilir, değilse, algoritma talebi işlemeye devam edemez ve başarısız mesajı iletilir

b. Uzantı tanımlanmışsa, uzantıdaki Kök Sertifika Makamı, CRL ve çapraz sertifika listesi alınır

IV. Kök Sertifika Makamı, CRL ve çapraz sertifika listesi bilgileri, talebe istinaden oluşan geçici yapı içerisine aktarılır

V. Sertifika Makamı'nın, güvenilir Sertifika Makamları listesinde olup olmadığı kontrol edilir

a. Eğer listedeyse, yola karşılık sertifika doğrulanır. Sonuç olumluysa, algoritma ilgili mesajını iletir. Yol bilgisi, bellekte saklanır. Başarısızsa, başarısız mesajı iletilir

b. Eğer listede yoksa ve Kök Sertifika Makamı'nın AuthorityInformationAccess uzantısı varsa, algoritmanın üst makama ulaşması gerektiğinden III nolu adıma dönülür

VI. Geçerli Kök Sertifika Makamı'nın herhangi bir çapraz sertifika listesine (III.b) sahip olup olmadığı kontrol edilir.

a. Eğer yoksa, algoritma başarısız yanıt döndürür.

b. Eğer varsa, listedeki çapraz sertifikaların herhangi birinin, güvenilir bir Sertifika Makamı'nca imzalanıp imzalanmadığı kontrol edilir. Sonuç olumluysa, algoritma başarılı yanıt vererek sertifika bellekte saklanır. Olumsuzsa, listedeki her bir sertifika için III nolu adıma dönülerek adımlar tekrarlanır. Herhangi bir anda, yolun geçersiz olduğu doğrulanırsa, son geçerli Kök Sertifika Makamı'na dönülür.

### 3.3. CMC ve SCVP Entegrasyonlarının Kazanımları

UMU-PKI sisteminin sertifika yönetim mekanizmalarında CMC protokolüne ait işlevlerin entegrasyonları üzerinde tasarladığımız bu modeller, protokolün henüz geliştirilmekte olan yeni eklentileriyle birlikte, günümüz teknolojilerindeki güncel yapıları kapsayabilmesi ve UMU-PKI sisteminin sertifika yaşam döngüsündeki tüm süreçleri içerecek metodlara sahip olmasının yanında, sistemin önceki sürümlerinde üzerinde çalışılan bir diğer sertifika yönetim protokolü olan Certificate Management Protocol v2 (CMP) protokolüne kıyasla daha hızlı entegre edilebilir olması, uygulama kodunun daha etkin bir şekilde geliştirilebilmesi ve bu sayede yaklaşık %10 oranında daha düşük [5] kod yükü ile entegrasyonun sağlanabilmesi gibi avantajlarla UMU-PKI sisteminin sertifika yönetim mekanizmalarının sağlanmasında, CMC protokolü üzerinde çalışmalarımızı geliştirme fikrini bize sunmuştur. UMU-PKI sisteminin sertifika doğrulama mekanizmalarının sağlanmasına yönelik olarak, günümüzde sıklıkla tercih edilen OCSP protokolü yerine SCVP protokolüne ait işlevlerin sistem mimarisi içerisine dahil edilmesi yönündeki tasarımlarımızın gerekçeleri arasında, SCVP protokolü ile gelen ve entegrasyon modellerimizde sıklıkla yer verdiğimiz güncel eklentilerden yararlanmamızın yanı sıra, SCVP protokolünün sertifikaların tüm veri bloğunun yerine, özet verisini kullanarak işlem yapmasıyla, sistemdeki mesaj boyutlarının ciddi oranda düşmesi ve paralelinde, sistemdeki talep-yanıt sürelerinin kısalması hususları ön plandadır. Ayrıca SCVP yanıtlayıcı sunumcu mimarilerinin entegrasyonuyla, sistematik olarak edinilen kazançlar şu şekilde özetlenebilir :

- **Sistem Performansı :** Doğrulama işlevleri sunumcular tarafından gerçekleştirildiğinde, sistemdeki istemcilerin yükü hafifler ve işlem yükü fazla ortamlar içerisinde paylaşımcı ya da yedekli tasarlanan sunumcu ağlarıyla doğrulama mekanizmalarında performans yükselir.
- **Sistem Devamlılığı :** Sunumcu donanım konfigurasyonlarının düşük olmasıyla, ihtiyaç duyulan ortamlarda sunumcu sayılarının arttırılması ile sertifika mekanizmalarının sürekliliği ve sistem güvenilirliği artar.
- **Artan Ölçeklenebilirlik :** İstemci sunumcu mimarisinde, organizasyon yapısının konfigurasyonuna bağlı olarak, sistem yükü, istemci sayısı ya da diğer şartlar düşünülerek sertifika doğrulama mekanizmalarına ait birimler daha esnek bir sistem tasarımı içerisinde modellenebilir.
- **Artan Güvenlik :** İstemciler tarafından iletilen talepler, makamlar yerine direk olarak güvenilir sunumculara iletilir. Bu sayede makamlar, bağlantısız durumda dış tehditlere karşı daha rahat muhafaza edilirler. Sistem, yedekli ve performans ölçekli bir sunumcu ağıyla yapılandırıldığında, dış tehditlere yönelik daha güçlü bir ortam sağlar. Güvenlik, birden fazla sayıda noktaya bağlı olduğundan, sistem başarısızlık riski de asgariye iner.

## 4. Sonuç ve Öneriler

IPv6 tabanlı açık anahtar altyapısı, günümüz güvenlik teknolojilerinin olduğu kadar, geleceğin IPv6 haberleşme ve gizlilik altyapılarının da temel mimarisini oluşturmaktadır. UMU-PKI sistemi kullanıcılarına, IPv6 teknolojisiyle birlikte gelen yenilikleri, açık anahtar altyapısına ait bileşenlerle bütünleştirerek sunan bir mimari ortaya koyar. Bu mimari içerisindeki temel mekanizmalardan olan, sertifika yönetim ve doğrulama yapılarının oluşturduğu süreçsel ve operasyonel işlevlerin, altyapıya ve sistem bileşenlerine entegrasyonunda, dağıtık organizasyonlara yönelik, genel kabul görmüş platformların ve protokollerin araştırılması ve incelenmesine yönelik bu çalışma, sertifika yaşam döngüsü tanımı içerisinde CMC protokolünün içerdiği yönetimsel işlevlerin ve protokolün tanımı itibariyle sağladığı yeniliklerin UMU-PKI sistemine entegrasyonu, sistem süreçleriyle protokol mantığının bütünleştirilmesine yönelik uygulama temelli tasarımlar ve entegrasyon modellerini içermekte olup, yazılım tabanlı entegrasyonun geliştirilmesinde araştırıcıların faydalanabileceği mimariler ve metodlar geliştirilmiştir. Benzer şekilde UMU-PKI sistemine ait sertifika doğrulama süreçlerinin geliştirilmesine yönelik SCVP protokolü detaylandırılarak, protokolün UMU-PKI sistemi içerisindeki tasarımı modellenmiş, protokolde tanımlı istemci sunumcu yapısında, sistem içerisindeki haberleşme ve mesajlaşma öğelerinin özelliklerini ve gerçekleştirilmelerini öngören fonksiyonel tasarım modelleri sunulmuştur. SCVP tabanlı bir doğrulama servisinin, UMU-PKI sistemine ait süreçler göz önünde bulundurulduğunda, içermesi gereken akış modeli tasarlanmış olup, oluşturulan modelden yola çıkılarak protokolün entegrasyonuna yönelik çözüm önerilmiştir. Çalışma içerisinde tasarlanan teknik süreç modelleri, CMC ve SCVP protokolleriyle gelen avantajların, sistem bileşenlerine entegrasyonu ve bu protokollerin UMU-PKI mimarisine dahil edilmesiyle edinilecek operasyonel, süreç bazlı ve performansa dayalı kazançlarla ilgili saptamalar sunulmuştur.

## 5. Kaynakça


[1] Antonio F. Gómez, Mart'inez G, Cánovas Ó "New security services based on PKI", Future Generation Computer Systems 19 (2003), page 251–262, 2003

[2] UMU-PKI v6 Description Guide v6.3.4 (draft-v0.1) December 2002

[3] M. Mayers, X. Liu, J. Schaad, J. Weinstein "Certificate Management Messages over CMS", Internet Engineering Task Force, RFC 2797, April 2000

[4] A. Malpani, S. Turner, "Simple Certificate Validation Protocol" Internet Engineering Task Force, Jul. 2000

[5] SSH Communications Security Discussion "CMP and CMC Comparison" May 2002 Helsinki, Finland