SERTİFİKA GEÇERLİLİK KONTROLÜNDEKİ SORUNLARIN GİDERİLMESİ

GÜLEN ÇELEBİ BAŞÇİ
TÜBİTAK Kamu Sertifikasyon Merkezi
gulen.basci@tubitak.gov.tr

ÖZET : Bu makalede kullanımı hızla yaygınlaşan elektronik imza için gerekli olan elektronik sertifikanın tanımı yapılmış, hangi amaçlarla kullanıldığı, sertifikayla atılan bir imzanın geçerli sayılabilmesi için, sertifika geçerlilik kontrolünün nasıl yapıldığı kısaca açıklanmıştır.Ayrıca sertifika geçerlilik kontrolü sırasında , sertifikanın iptal durumunu öğrenmek için kullanılan Sertifika İptal Listesi (SİL / CRL – Certificate Revocation List) ve Çevrim İçi Sertifika Durum Protokolleri(ÇiSDuP / OCSP – Online Certificate Status Protocol) anlatılmış, aralarındaki farklardan bahsedilmiş ve kontrol sırasında ortaya çıkabilecek güvenlik açıkları ve hatalar anlatılarak alınabilecek önlemler ve çözüm yolları açıklanmıştır.

ANAHTAR KELİMELER: Sertifika, Sertifika geçerlilik kontrolü, SİL, OCSP

PREVENTION AND CORRECTION OF PROBLEMS DURING CERTIFICATE VALIDATION

ABSTRACT : In this paper, I briefly describe digital certificate which is one of the key enablers for electronic signature. Furthermore, the usage areas of digital certificate and certificate validation process is explained. CRL (Certificate Revocation List) that lists the revoced certificates and OCSP (Online Certificate Status Protocol) is described in detail including the core differences between them, problems that may occur during validation process and solutions to prevent and correct those problems.

KEYWORDS : Certificate , Certificate validation, CRL , OCSP

Giriş

Elektronik sertifika; e-imza kanunundaki tarifiyle[1]; İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır. Başka bir deyişle ; nüfus cüzdanı, ehliyet gibi kişinin elektronik ortamda kendisini ispatlaması için kullanılan elektronik dosyalardır. Elektronik Sertifika içerisinde biri açık diğeri de gizli olmak üzere iki çeşit anahtar bulunur. Gizli anahtar, Gizli anahtarlı kriptografide kullanılan anahtardır.Açık anahtar ise, Açık anahtarlı kriptografide kullanılan, herkesin erişimine ve kullanımına açık olan anahtardır. Gizli olan anahtarla matematiksel bağlantısı vardır..[2]
Açık anahtar, gizli anahtarla atılan imzayı kontrol etmek, gizli anahtarla yapılan şifrelemeyi çözmek, ya da sadece gizli anahtarın çözebileceği şekilde metnin şifrelenmesi için kullanılır. [2]

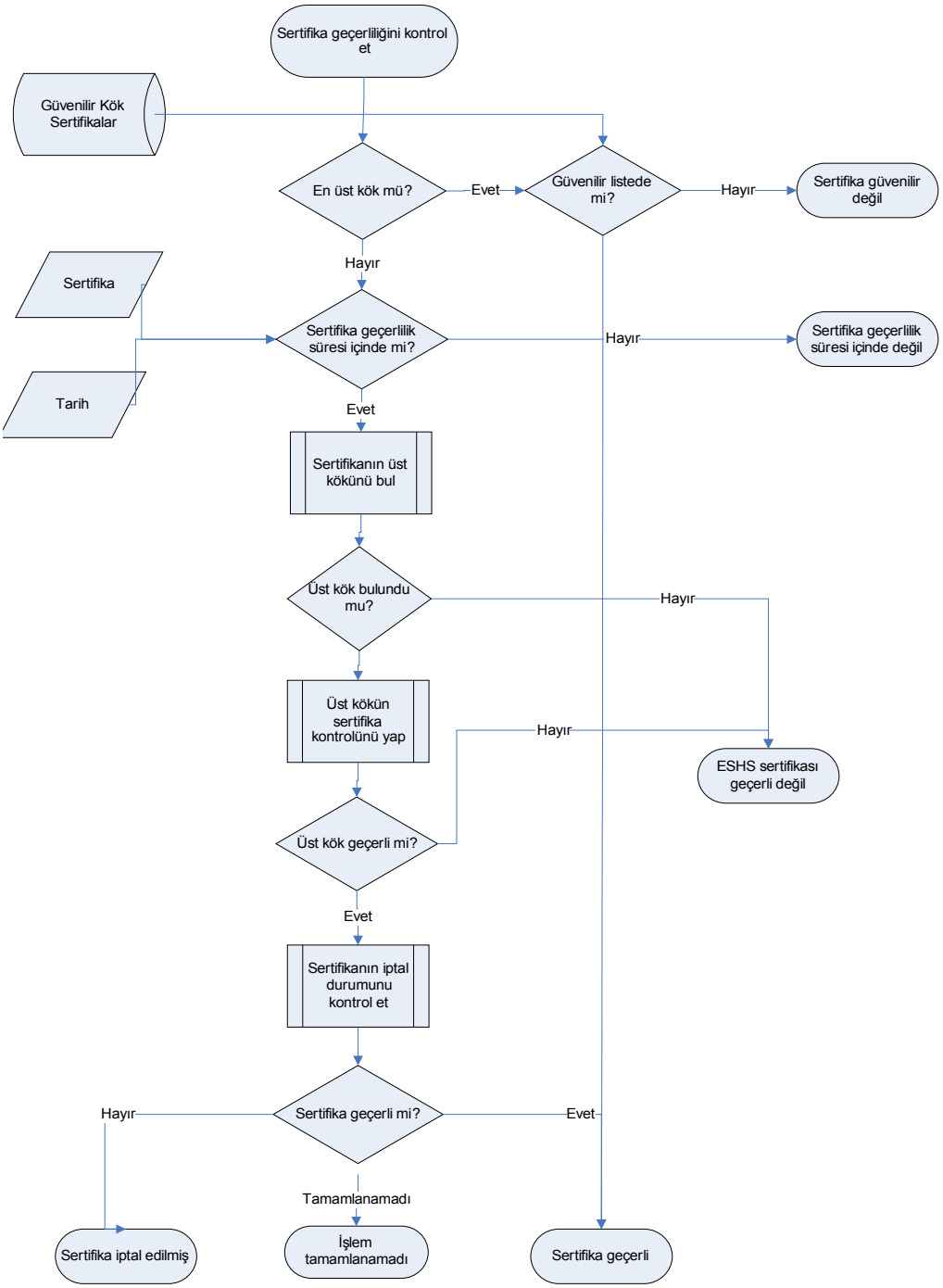
Elektronik sertifika ile atılan imzanın geçerli sayılabilmesi için belirli kriterlere göre geçerli olup olmadığı, iptal edilip edilmediğinin kontrol edilmesi gerekmektedir.Sertifikanın geçerliliği o an için kontrol edilebileceği gibi geçmiş bir zaman için de kontrol yapılabilir.

Sertifika Geçerlilik Kontrol Süreci

Bir sertifikanın geçerliliğinin kontrol edilmesi uzun ve kritik bir süreçtir. Bu süreç içerisindeki bir hata geri dönülmez sonuçlara yol açabilir. Örneğin, iptal edilmiş bir sertifika ile atılan bir imza geçerli olmayan bir verinin geçerli sayılması demektir Sertifika geçerlilik kontrolü, elektronik sertifikayla ilgili her işlem sırasında yapılmalıdır, çünkü sertifika her an iptal edilebilir, süresi dolabilir ya da yerine yeni sertifika üretilebilir. Geçerlilik kontrol süreci içerisinde sadece sertifikanın kendisi değil, sertifikayı veren Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) sertifikalarının da geçerliliği kontrol edilmelidir. Bir sertifikanın geçerli olabilmesi için:

1. Sertifikanın başlangıç ve bitiş tarihleri arasında olması gerekmektedir.
2. Sertifika güvenilir köklerden üretilmelidir. Eğer en üst kök değil ise , sertifikayı üreten köklerin(ESHSlerin sertifikalarının) bulunması ve bu kök sertifikaların da geçerliliklerinin ve imzalarının geçerliliği kontrol edilmelidir.
3. Sertifika iptal edilmemiş olmalıdır.

Sertifika geçerlilik kontrol süreci de görüntülenmektedir.



Şekil 1 – Sertifika geçerlilik kontrol süreci

Bir sertifikanın üst kökü bulunurken sertifikanın içerisindeki bilgilerden yararlanılır. Her sertifikanın içerisinde Özne Anahtar Tanımlayıcısı(SKI) ve ESHS Anahtar Tanımlayıcısı(AKI) bilgileri vardır. Özne anahtar tanımlayıcısı sertifikanın kendisini, ESHS anahtar tanımlayıcısı da sertifikayı üreten kök sertifikanın özne anahtar tanımlayıcısını gösterir. Bir sertifikanın üst kökünü bulmak için , içerisinde bulunan ESHS anahtar tanımlayıcısı bilgisi ile tüm kök sertifikaların özne anahtar tanımlayıcıları karşılaştırılır. İki değer birbirine eşit olduğunda da sertifikanın kökü bulunmuş olur. Fakat sadece sertifikayı bulmak yeterli değildir, bulunan sertifikanın da geçerliliğinin ve imzasının kontrol edilmesi gerekmektedir.

Sertifikanın iptal durumu ise; sertifikayı üreten ESHS'nin yayınladığı Sertifika İptal Listelerine(SİL) bakarak, ya da ESHS'ye ait OCSP sunucu aracılıyla olmak üzere iki şekilde öğrenilebilir.

Sertifika İptal Listesi (SİL / CRL- Certificate Revocation List)

Yetkili Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) tarafından belirlenmiş saatlerde yayınlanan (Örneğin, TÜBİTAK Kamu Sertifikasyon Merkezi tarafından 36 satte bir) elektronik imzalı bir dosyadır.İçerisinde iptal edilmiş sertifikaların seri numarasını içeren bir liste vardır. Bir sertifika için iptal kontrolü yapılacağı zaman sertifikanın seri numarası SİL içerisindeki listede aranır. Eğer seri numarası listede bulunuyorsa sertifika iptal edilmiş demektir, listede yoksa sertifika SİL'e göre geçerlidir.

Çevrimiçi Sertifika Durum Protokolü (ÇiSDuP / OCSP - Online Certificate Status Protocol)

OCSP, RFC 2560'ın içindeki Internet Engineering Task Force (IETF)' da tanımlanmış bir PKI teknolojisi standardıdır [3]. Sertifikaların geçerliliğinin kontrol edilmesinde kullanılır. İstek – cevap (Request – Response) mantığı ile çalışır. İptal edilen sertifikalar anında OCSP sunucusuna bildirilir. İstemciler, OCSP sunucularına birer istekte bulunur ve durumunu öğrenmek istedikleri sertifikayı göndererek sunucu tarafından imzalanmış bir cevap alırlar. Gelen bu cevap içerisinde de sertifikanın iptal durumu bulunmaktadır.

OCSP, SİL'in gecikme, ölçeklenebilme ve yönetim sorunlarına çözüm getirmek için SİL'e tamamlayıcı olarak geliştirilmiştir.

Sertifika Deposu

Sertifika geçerlilik kontrolünün sık yapıldığı durumlarda, SİL dosyalarının her sertifika kontrolü için yeniden indirilip içerisinden kontrol yapılması kurumlar için birçok yük getirecektir. Ortalama 1MB büyüklüğünde olan SİL dosyalarının indirilmesi hem zaman açısından çok yavaş olacaktır, hem de internet bant genişliğini tüketecektir. Bu yüzden Sertifika Deposu dediğimiz depolama yönteminin kullanılması kurumlar için çok büyük kolaylık getirecektir. Sertifika Deposunda, geçerlilik kontrolü yapılan her sertifika için kontrol sırasında gerekli olan tüm kök sertifikalar, çekilen SİLler ya da OCSP cevapları güvenliği sağlanmış bir veri tabanı gibi bir depo içerisine kaydedilir. Aynı sertifika için tekrar geçerlilik kontrolü yapılmak istendiğinde gerekli olan tüm bilgiler depoda bulunmaktadır ve bu bilgileri tekrar internetten çekmeye gerek yoktur. Sadece depoda bulunan bilgilerin güncelliği kontrol edilerek, güncel olamayan bilgiler güncellenerek geçerlilik kontrolü çok kısa bir süre içerisinde tamamlanabilmektedir.

Örneğin bir kurum elindeki 100 sertifikanın geçerlilik bilgisini öğrenmek istemektedir. Sertifika deposu kullanılmadığı durumda bir sertifikanın geçerlilik kontrolü için hem kendisinin hem de üst köklerinin iptal durumunu sormak için SİLler çekmek zorundadır.(Bknz. Şekil 1) Şu anki ESHSlerin ürettikleri sertifikaların bir alt kök, bir de üst kök olmak üzere iki tane kökü bulunmaktadır. Bu da sertifika geçerlilik kontrolünde bakılması gereken toplamda 3 sertifika olduğunu gösterir . Kısaca her sertifika geçerlilik kontrolünde 3 ayrı SİL çekilmesi gerekmektedir. Bu da 100 sertifika için 300 SİL demektir.Fakat Sertifika Deposu kullanıldığı durumlarda kurum için alınan sertifikaların hepsinin aynı ESHSden üretildiği düşünülürse indirilecek SİL sayısı sadece 3 olacaktır. Çünkü ilk sertifika için gerekli tüm SİLler çekilip depoya kaydedilecek, diğer sertifikaların kontrollerinde de bu kaydedilen SİLlerden yararlanılacaktır ve sonuç olarak çekilen SİL sayısı 100 kat azalacaktır.Bu da kurumlara çok fazla zaman kazandıracaktır.

Tablo 1 - Sertifika Deposu kullanılarak yapılan kontrolde gerekli SİL sayıları

Sertifika sayısı	Sertifikanın kök sayısı	Çekilecek SİL sayısı	
		SD kullanılmadan	SD kullanılarak
1	2	3	3
100	200	300	3
1000	2000	3000	3

Sertifika Geçerlilik Kontrolüdeki Açıklar Ve Çözüm Yolları

Sertifikanın geçerlilik kontrolü yapılırken farkedilmesi zor hatalar oluşabilir ve bu hatalar da geri dönülemez sonuçlar doğurabilir. Bu hatalardan bazıları ve önerilen çözüm yolları aşağıda belirtilmiştir.

Sertifikanın üst kökü bulunurken:

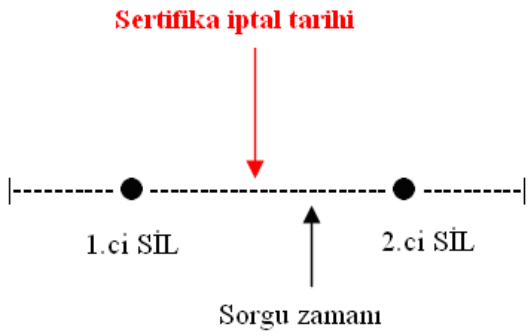
- Sertifika geçerlilik kontrolünde kullanılmak üzere tanımlı ve güvenilir kabul edilen kök sertifikalar 'Güvenilir Kök Sertifikalar Listesi'nde tutulurlar. Sertifikanın içerisindeki ESHS anahtar tanımlayıcısına bakılarak bulunan üst kökün sadece Güvenilir Kök Sertifikalar listesinde bulunması yeterli degildir. Kötü niyetli kişiler; gerçek bir kök sertifikanın sahip olduğu özne anahtar tanımlayıcısı ile sertifikanın bir kopyasını yaratarak kendi amaçları doğrultusunda kullanabilirler, bu da çok büyük ve farkedilmesi zor açıklara sebep olabilir.

  ÇÖZÜM : Sertifikanın üst kök sertifikası Güvenilir Kök Sertifikalar Listesinden bulunduktan sonra bulunan kök sertifikanın da imzasının geçerliliği kontrol edilmelidir.

SİL'den iptal kontrolü yaparken;

- SİL'ler ESHSler tarafından belirlenen saatlerde yayınlandığı için, bir SİL'in yayınlanmasından diğer SİL'in yayınlanmasına kadar olan süre içerisinde iptal edilen sertifikaların geçerliliği bir sonraki SİL yayın tarihinden önce kontrol edildiğinde sertifikaların geçerlilik bilgisi doğru olarak görüntülenemeyecektir. Kısaca iptal edilmiş olan bir sertifika geçerli görünecektir. (Bu sorun geçmiş zamana yönelik olmayan o anki sorgular için geçerlidir, geçmişe yönelik sorgu yapılıyorsa böyle bir sorun yaşanmayacaktır.)

  ÇÖZÜM : Eğer o andaki geçerlilik kontrolü yapılacaksa geçerlilik kontrolünde OCSP kullanılması önerilmektedir.



Şekil 2 – Bir sertifika iptal durumu

Şekil 2 – Bir sertifika iptal durumu' ye göre 1.ci SİL'in yayınlanmasından 2.ci SİL'in yayınlanmasına kadar olan süre içinde bir sertifika iptal edilmiştir. Hemen sonrasında bir sorgu yapılmış ve bu arada henüz yeni sil yayınlanmadığı için sertifika geçerli sayılmıştır. Bu durumda OCSP kullanılmış olsaydı sertifikanın iptal edildiği anlaşılacak ve hatalar önlenmiş olacaktı.

Sertifikadaki adreslerden iptal kontrolü yaparken;

- Sertifikanın içerisindeki adreslerden indirilen Sertifika İptal Listelerinin doğruluğu da kontrol edilmelidir. Çünkü verilen adres 3.cü kişiler tarafından başka bir adrese yönlendirilerek farklı bir SİL indirilmesine sebep olabilir. Bu da yine iptal edilmiş bir sertifikanın geçerli gösterilmesine sebep olabilir.

  ÇÖZÜM : Adresten alınan iptal listesinin de tarihi ve imzasının geçerliliği kontrol edilmelidir.

OCSP'den iptal kontrolü yaparken;

- Sertifikanın içerisindeki OCSP adresinden yapılan geçerlilik kontrolünde de OCSP sunucusundan gelen cevap da kontrol edilmelidir. Çünkü verilen adres 3.cü kişiler tarafından başka bir adrese yönlendirilebilir ya da farklı bir sertifikanın durumu cevap olarak döndürülebilir.

  ÇÖZÜM : Sunucudan gelen cevabın tarihi ve imzasının geçerliliği kontrol edilmeli ayrıca gelen cevabın, durumunu öğrenmek istediğimiz sertifikaya ait olup olmadığına da bakılmalıdır.

Ek SİL listesi yayınlandığında;

- Her SİL içerisinde bir sonraki SİL'in yayınlanma tarihi bulunmaktadır. Fakat bazı durumlarda ek SİLler yayınlanabilmektedir. SİLlerin depolanarak kontrol yapıldığı durumlarda bir sonraki SİL'in yayınlanmasına daha vakit olduğu için tekrar bir SİL yayınlanıp yayınlanmadığına bakılmaz ve arada yayınlanmış olan listeler kaçırılabilir. Böylelikle yanlış sonuçlar elde edilmiş olur.

  ÇÖZÜM : Anlık kontroller yapılacaksa OCSP kullanılmalıdır.

SİL ve OCSP Karşılaştırması

Sertifika geçerlilik kontrolünde kullanılan SİL ve OCSP'lerin farklı durumlara göre birbirlerine üstünlükleri vardır. SİL'ler belirli aralıklarla yayınlandıkları için bazı kontrollerde bazı sertifikaların geçerlilik durumları doğru anlaşılamamaktadır.(Örnek : Şekil 2 – Bir sertifika iptal durumu) Bu yüzden eğer bir internet bağlantısı varsa OCSP kullanılacak ilk yöntem olmalıdır.

Ayrıca SİL ve OCSP arasında büyük bir hız farkı da vardır. SİL listelerinin ortalama büyüklüğü 1MB civarındadır(üretilmiş olan 100000 sertifika için ortalama değer), OCSP'lerin ise 4KBdır. Aradaki bu fark ciddi bir hız farkına yol açar. Sil ve OCSP'ler arasındaki cevap alma süreleri 1, 100 ve 10000 sertifika için, Sertifika Deposu kullanılarak ve kullanılmadan incelenmiştir. (Bknz : Tablo3, Tablo6)

İncelemeyi kalitatif olarak yapabilmek amacıyla bir sorgunun toplam maliyetini (zaman olarak) Formül 1 ve Formül 2'deki gibi ifade edebiliriz. Formüllerdeki kısaltmaların anlamlarını aşağıdaki gibi özetleyebiliriz.

tss : toplam sorgu süresi
is : istek sayısı
ss : sorgu sayısı
pys : paket yolculuk süresi
pb : paket büyüklüğü
bg : bant genişliği
es : ESHS sayısı

$$tss_{ocsp} = \sum_{n=0}^{is} (pys + pb/bg)$$

Formül 1

$$tss_{sil} = \sum_{n=0}^{es} (pys + pb/bg)$$

Formül 2

Bu formüllere dayanarak 2, Tablo 3, 4, 5 ve Tablo 6 oluşturulmuştur.

Tablolar incelendiğinde ortaya çıkan sonuca göre; Sertifika Deposu kullanılmadığı durumda OCSP ile yapılan sorgulama SİL ile yapılan sorgudan yaklaşık 6 kat daha hızlıdır, bağlantı hızı arttıkça bu fark giderek azalmakta ve birbirine yaklaşmaktadır. Fakat herzaman sürekli hızlı bağlantı yakalamak pek mümkün olmadığından aradaki bu fark bizim için önemlidir.

Sertifika Deposu kulanılarak yapılan sorgulamalarda ise, yapılan ilk sorguda gerekli tüm SİL'ler bir kez çekilir ve Sertifika Deposuna kaydedilir. Depo kullanılarak yapılan ilk sorgulamanın depo kullanılmadan yapılan sorgudan çok fazla bir farkı yoktur, fakat ikinci sorgudan itibaren sorguya cevap alma hızı artacaktır. Çünkü durumu sorulan her sertifika için gerekli olan SİL depoda mevcuttur ve yeni bir SİL çekmeye gerek olmayacaktır. (yeni SİLlerin yayınlanmasına daha zaman olduğu durumlar için geçerlidir, yeni SİL yayınlanmışsa onun da çekilmesi gerekmektedir.)

Depo kullanıldıgı durumlardaki tablolar incelendiğinde ocsp sabit kalırken SİL ile ilgili süre giderek azalmakta ve SİL avantajlı duruma gelmektedir.

Tablo 2 – Bir Sertifika için sertifika geçerlilik kontrol sorgusu

bant genişliği (bit/saniye)	OCSP transfer süresi	OCSP paket yolculuk süresi	OCSP toplam süre	SİL transfer süresi	SİL paket yolculuk süresi	SİL toplam süre	SİL/OCSP
56K	1,0000	2,0000	3,0000	256,0000	2,0000	258,0000	86
512K	0,1250	2,0000	2,1250	128,0000	2,0000	130,0000	61,17647
1024K	0,0625	2,0000	2,0625	64,0000	2,0000	66,0000	32
2048K	0,0313	2,0000	2,0313	32,0000	2,0000	34,0000	16,73846
sonsuz	0,0000	2,0000	2,0000	0,0000	2,0000	2,0000	1

Tablo 3 - 100 Sertifika için sertifika geçerlilik kontrol sorgusu

bant genişliği (bit/saniye)	OCSP transfer süresi	OCSP paket yolculuk süresi	OCSP toplam süre	SİL transfer süresi	SİL paket yolculuk süresi	SİL toplam süre	SİL/OCSP
56K	1,0000	2,0000	300,0000	256,0000	2,0000	25800,0000	86
512K	0,1250	2,0000	212,5000	128,0000	2,0000	13000,0000	61,17647
1024K	0,0625	2,0000	206,2500	64,0000	2,0000	6600,0000	32
2048K	0,0313	2,0000	203,1250	32,0000	2,0000	3400,0000	16,73846
sonsuz	0,0000	2,0000	200,0000	0,0000	2,0000	200,0000	1

Tablo 4 - 100 Sertifika için Sertifika Deposu kullanılarak ve 3 ayrı ESHS'nın olduğu durumda yapılan ilk geçerlilik kontrol sorgusu

bant genişliği (bit/saniye)	OCSP transfer süresi	OCSP paket yolculuk süresi	OCSP toplam süre	SİL transfer süresi	SİL paket yolculuk süresi	SİL toplam süre	SİL/OCSP
56K	1,0000	2,0000	300,0000	256,0000	2,0000	774,0000	2,58
512K	0,1250	2,0000	212,5000	128,0000	2,0000	390,0000	1,835294
1024K	0,0625	2,0000	206,2500	64,0000	2,0000	198,0000	0,96
2048K	0,0313	2,0000	203,1250	32,0000	2,0000	102,0000	0,502154
sonsuz	0,0000	2,0000	200,0000	0,0000	2,0000	6,0000	0,03

Tablo 5 - 10000 Sertifika için Sertifika Deposu kullanılarak ve 3 ayrı ESHS'nın olduğu durumda yapılan geçerlilik kontrol sorgusu

bant genişliği (bit/saniye)	OCSP transfer süresi	OCSP paket yolculuk süresi	OCSP toplam süre	SİL transfer süresi	SİL paket yolculuk süresi	SİL toplam süre	SİL/OCSP
56K	1,0000	2,0000	30000,0000	256,0000	2,0000	774,0000	0,0258
512K	0,1250	2,0000	21250,0000	128,0000	2,0000	390,0000	0,018353
1024K	0,0625	2,0000	20625,0000	64,0000	2,0000	198,0000	0,0096
2048K	0,0313	2,0000	20312,5000	32,0000	2,0000	102,0000	0,005022
sonsuz	0,0000	2,0000	20000,0000	0,0000	2,0000	6,0000	0,0003

Tablo 6 - 100 Sertifika için Sertifika Deposu kullanılarak ve 3 ayrı ESHS'nın olduğu durumda yapılan 2.ci geçerlilik kontrol sorgusu

bant genişliği (bit/saniye)	OCSP transfer süresi	OCSP paket yolculuk süresi	OCSP toplam süre	SİL transfer süresi	SİL paket yolculuk süresi	SİL toplam süre	SİL/OCSP
56K	1,0000	2,0000	300,0000	0	0	0	0
512K	0,1250	2,0000	212,5000	0	0	0	0
1024K	0,0625	2,0000	206,2500	0	0	0	0
2048K	0,0313	2,0000	203,1250	0	0	0	0

* Tablolarda ortalama OCSP büyüklüğü 4KB ve SİL büyüklüğü 1024KB olarak hesaplanmıştır.

** Tablolardaki sürelerin tamamı saniye cinsinden verilmiştir.

Sonuç

Yapılan çalışmalarda sertifika geçerlilik kontrolünde farklı durumlarda farklı sorunlar ya da sıkıntılarla karşılaşıldığını gördük Bu sorunları çözmek için uygulanacak yöntem titizlikle seçilmeli ve önlemler ona göre alınmalıdır. Geçerlilik kontrolünde ne zaman OCSP kullanılacak, ne zaman SİL kullanılacak ya da Sertifika Deposu oluşturulacak mı? cevabı bulunması gereken en önemli sorulardır. Bu soruların yanıtları aranırken sorgulanacak sertifika sayısı, internet bağlantı hızı, Sertifika Deposu oluşturma maliyeti, aynı sertifika için geçerlilik kontrolü tekrarlanma oranı en önemli unsurlar olarak öne çıkmaktadır.

Teşekkür

Bu çalışmayı okuyan Sayın Dr. Kıvanç Dinçer, Sayın Faysal Başçi ve Sayın Fatih Buğan'a teşekkürlerimi sunarım.

Kaynaklar

[1] 5070 sayılı Elektronik İmza Kanunu, 23 Ocak 2004 Tarih ve 25355 sayılı Resmi Gazete, Kanun kabul tarihi 15 Ocak 2004.

[2] www.kamusm.gov.tr , Kasım 2006

[3] https://kap.bilten.tubitak.gov.tr/CA , Kasım 2006