kamu SM

GENİŞLETİLMİŞ DOĞRULAMA

SSL

SERTİFİKALARI

Genişletilmiş Doğrulama SSL Sertifikaları

SSL, internet üzerinden güvenli bağlantı kurmak için tasarlanmış bir güvenlik protokolüdür. SSL protokolünün uygulanabilmesi için SSL sertifikalarına ihtiyaç duyulur. SSL sertifikası güvenilir sertifika sağlayıcısı (CA) tarafından üretilir. SSL sertifikası temelde bir kuruluşun kurumsal kimliğini, alan adı adresiyle sahip olduğu anahtar çiftini sayısal olarak bağlar. Detayında ise kuruluş adı, konumu ve bazı durumlarda iletişim bilgilerini içerebilir.

SSL sertifikalarının tümünde verinin iletimi ve korunması için benzer yöntemler kullanılmasına rağmen, SSL sertifikaları sertifikayı talep eden kurumun kimliğinin doğrulanması açısından alan adı doğrulama (Domain Validated-DV), kuruluş doğrulama (Organization Validated-OV) ve genişletilmiş doğrulama (Extended Validated-EV) olmak üzere üç kategoriye ayrılır.

DV, OV ve EV SSL Sertifikası Nedir?

DV SSL sertifikası, belirli bir alan adı için yalnızca alan adı sahipliğinin kontrol edildiği sertifika türüdür. DV SSL sertifikası daha az doğrulama gerektirdiğinden kolayca ve hızlı bir şekilde elde edilir.

OV SSL sertifikası, DV sertifikaya ek olarak başvuru sahibinin talep edilen alan adı üzerindeki kullanım hakkı ve kurum bilgilerinin kontrol edildiği sertifika türüdür. Bu bilgiler, sertifikanın yer aldığı web sitesinin sahibi olan kurum hakkında daha fazla bilgi sağlar. Kuruma ait bilgilerin teyit edilmiş olması web sitesi ziyaretçilerine daha fazla güven verir. Bu sebeple OV sertifikaların yayımlanma süreci DV sertifikalara oranla daha uzun sürmektedir.

EV SSL sertifikalarıysa en geniş kurum kimliği doğrulama yöntemlerini içeren sertifika türüdür. Bu durum, sertifika otoritesinin kurum kimliğini doğrulamada çok daha fazla işlem gerektiren doğrulama metotlarını uygulamasını gerektirmektedir. OV sertifikalardan farklı olarak, sertifika sahibi; firmanın fiziksel, hukuki ve ticari varlığını ispat etmekle mükelleftir ve daha kapsamlı kurumsal doğrulama süreçlerine tabi olur.

EV sertifikalar, sertifika sahibinin aktif olarak hizmet verdiğini; yasalara uygun olduğunu; güvenilir ve dürüst olduğunu garanti etmez. Yalnızca, ''Özne (Subject)'' alanında yer alan kuruluşun yasal olarak var olduğunu garanti eder.

Tarayıcı ve sunucu arasında gerçekleşen bilgi trafiğinde kullanılan güvenlik mekanizmaları SSL sertifika tipinden bağımsız olarak uygulanmaktadır.

Standartlarda EV SSL Sertifikası

Sertifika otoriteleri EV SSL sertifikalarının üretiminde, ''CA/B Forum Baseline Requirements'' dokümanında yer alan kısıtların yanında, ''CA/B Forum Guidelines for Issuance and Management of Extended Validation Certificates (EVG)'' dokümanında belirtilen kısıtları da sağlamak zorundadır. EVG dokümanında yer alan kısıtlar doğrultusunda sertifika otoriteleri özel kuruluşlara, devlet kuruluşlarına, ticari kuruluşlara ve ticari olmayan varlıklara, EV için gerekli isterleri sağladıkları sürece EV SSL sertifikası verebilirler.

EV ve OV SSL Sertifika Farklılıkları

EV SSL sertifikalarının EVG dokümanına uygun olarak üretilebilmesi için sertifikanın Subject alanında

"Kuruluş (Organization)" alanında sertifika sahibinin resmi kayıtlarda belirtilen tam yasal organizasyon adının

"İş Kategorisi (Business Category)" alanında sertifika sahibinin organizasyonel yapısını belirten ifadenin (özel kuruluş, devlet kuruluşu vb.)

"Kuruluş veya Tescil Yetkisi (Jurisdiction of Incorporation or Registration)" alanında ülke kodunun

''Seri Numarası (Serial Number)" alanında kuruluşa atanmış vergi kimlik numarasının

"Kuruluşun Fiziksel Adresi (Physical Address of Place of Business Field)" alanında sertifika sahibinin, fiziksel lokasyonu

bulunması zorunludur.

Ayrıca sertifika sahibi kuruluşa ait veya kuruluş tarafından yönetilen bir veya daha fazla alan adını içeren "Özne Alternatif Adı (Subject Alternative Name)" ve sertifika otoritesine ait EV OID'ini (opsiyonel olarak CA/B BR EV OID'ini) içeren "Sertifika İlkeleri (Certificate Policies)" eklentilerinin bulunması gerekmektedir.

EV SSL sertifikalarının geçerlilik süresi de OV SSL sertifikaları gibi en fazla 825 gün olabilmektedir. Ancak EVG dokümanında bu sürenin 12 ay olması önerilmektedir. **Bu durum gelecekte yapılacak güncellemelerle EV sertifika süresinin 12 aya indirilmesinin gündeme gelebileceğini düşündürmektedir.**

EV SSL sertifikalarının OV SSL sertifikalara göre avantaj sağladığı düşünülen doğrulama adımları da standartlarda belirtilmiştir. Bir kuruluş EV SSL sertifika başvurusu yaptığında sertifika otoritesi öncelikle kuruluşun yasal, fiziksel ve operasyonel varlığını doğrular. Bu süreçte devlet kaynaklı veri tabanlarından edinilen bilgilerin kullanılması gerekmektedir. Ardından başvuru sahibinin alan adı üzerindeki kontrolü doğrulanır. Başvuru sahibiyle iletişim kurulması için güvenilir bir iletişim aracı belirlendikten sonra başvuru sürecine dahil olan kişilerin yetkisi değerlendirilir. En son adım olarak ise EV SSL sertifikalarının "Özne (Subject)" alanında bulunan ekstra alanların doğrulaması yapılır.

EV SSL sertifikalarının doğrulama adımları temelde OV SSL sertifika üretim süreciyle aynıdır. EV SSL sertifikalarında bu doğrulamalara ek olarak alan adının karışık karakterler içerip içermediği kontrol edilmeli; içeriyorsa bilinen yüksek riskli alan adlarıyla karşılaştırılmalı ve benzerlik bulunması durumunda üretim durdurulmalıdır. OV SSL sertifikası üretmeden önce elde edilen doğrulama verilerinin ömrü sertifikanın ömrü (825 gün) ile aynıyken; EV SSL sertifikasında kullanılan doğrulama verilerinin ömrü 13 aydır.

Özellikle devlete bağlı sertifika otoritelerinin kamu kurumlarına SSL sertifikası sağlaması durumunda sertifika otoritesinin kurumlarla ilgili ayrıntılı bilgiye erişebilmesi sebebiyle OV ve EV SSL sertifikaları arasında önemli bir fark kalmamaktadır.

EV SSL Sertifikasının Kullanım Sıklığı

EV SSL sertifikalarının kullanım yaygınlığıyla ilgili çeşitli araştırmalar bulunmaktadır. Bu araştırmalarda dünyadaki en büyük web siteleri ve dünya çapındaki en popüler web sitelerinin yer aldığı Alexa Top 1 Million veritabanı kaynak olarak kullanılmıştır. Bu araştırma çalışmalarını incelemeden önce EV SSL sertifikalarının devlete ait sertifika otoriteleri tarafından kullanım sıklığını analiz edelim.

Mozilla Wiki sayfasında bir ülke ya da bölgenin hükümetinin sahip olduğu sertifika otoriteleri listesi yer almaktadır [1]. Bu liste incelendiğinde Mozilla güvenilir kökler listesinde 7 adet devlete ait sertifika otoritesi olduğu görülmektedir.

Devlete Bağlı Sertifika Otoriteleri, Ocak 2019

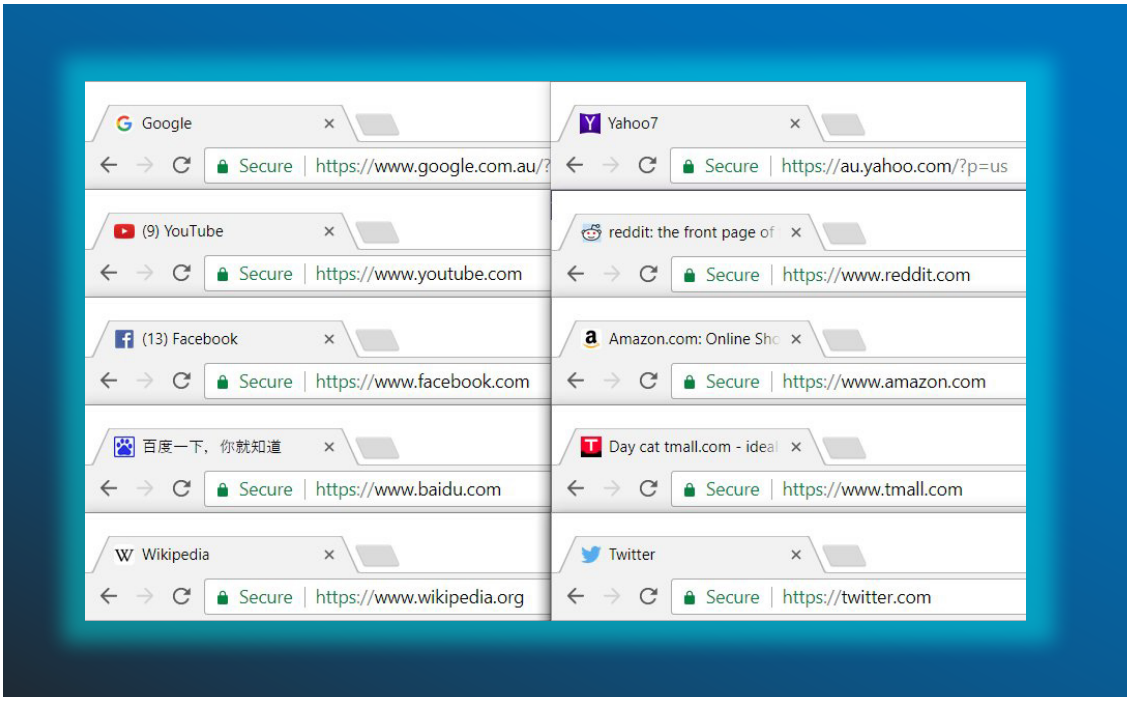
- Government of Hong Kong (SAR), Hongkong Post, Certizen
- Government of Spain, Autoritat de Certificació de la Comunitat Valenciana (ACCV)
- Government of Spain, Fábrica Nacional de Moneda y Timbre (FNMT)
- Government of Taiwan, Government Root Certification Authority (GRCA)
- Government of The Netherlands, PKIoverheid (Logius)
- Government of The Netherlands, PKIoverheid (Logius)
- Government of Turkey, Kamu Sertifikasyon Merkezi (Kamu SM)

Bu sertifika otoritelerinden Government of Hong Kong (SAR), Hongkong Post sertifika otoritesi yakın zamanda EV SSL sertifikaları yayımlamayı planladığını web sitesinde duyurmuş ve Sertifika Uygulama Esasları (SUE) dokümanını kamuoyu incelemesi için erişilebilir hale getirmiştir [2].

Government of The Netherlands, PKIoverheid sertifika otoritesi EV SSL köküne sahiptir ve bu kökün ayrı bir SUE dokümanı mevcuttur [3]. EV kök sertifika hiyerarşisi incelendiğinde sertifika otoritesinin müşteri profilinin hem kamu kurumları hem de özel şirketleri içerdiği görülmektedir [4].

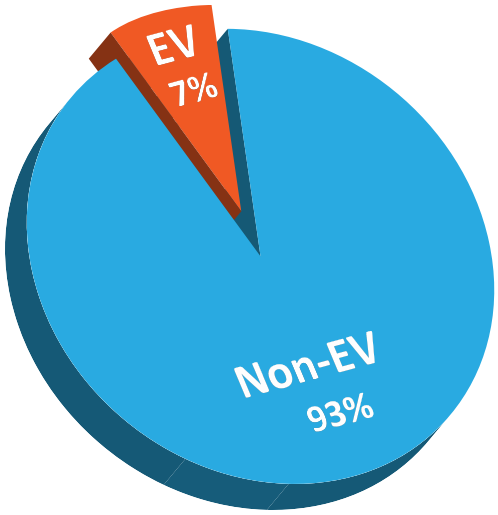
Bu iki sertifika otoritesi dışında diğer devlete bağlı sertifika otoritelerinde EV SSL sertifikasının kullanımına rastlanmamıştır. **PKIoverheid sertifika otoritesinin müşteri profilinin özel şirketleri içermesi kurumsal kimliğinin ayrıntılı olarak doğrulanmasını gerektirdiğinden EV SSL sertifikası üretimi mevcuttur.**

EV sertifikaların kullanımı, sertifika başvuru sürecinin uzunluğu ve kriptografik anlamda ekstra güvenlik sağlamaması sebebiyle git gide azalmaktadır. **Dünyadaki en büyük 10 web sitesine bakıldığında EV SSL sertifika yerine OV SSL sertifikasını tercih ettikleri görülmektedir.**

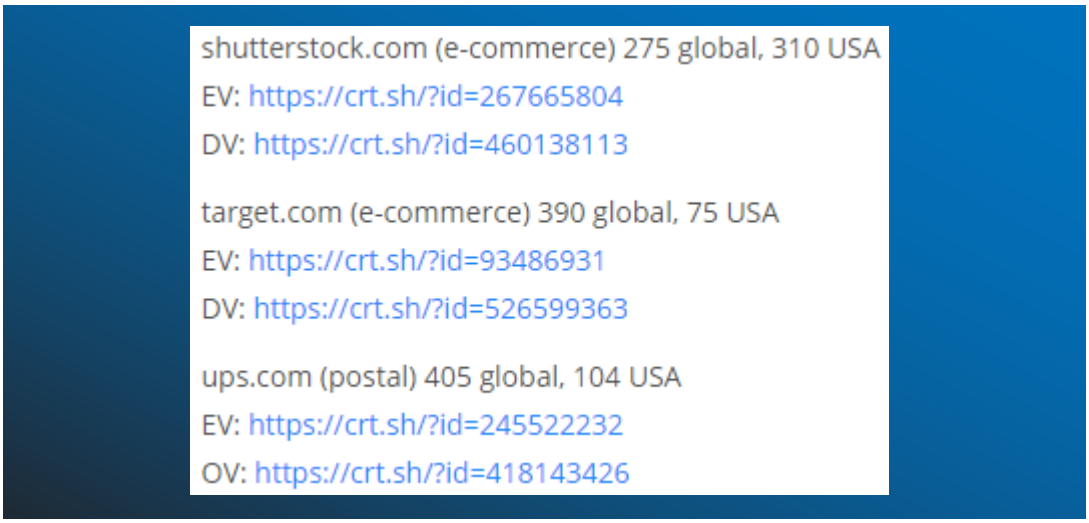


Alexa Top Million sertifika veri tabanında Ağustos 2018 tarihinde çıkarılan EV sertifika kullanım istatistiğine göre sertifikaların yalnızca yüzde 7'sinin EV SSL sertifikasına sahip olduğu görülmektedir.

Usage of EV Certificates in the Alexa Top 1 Million

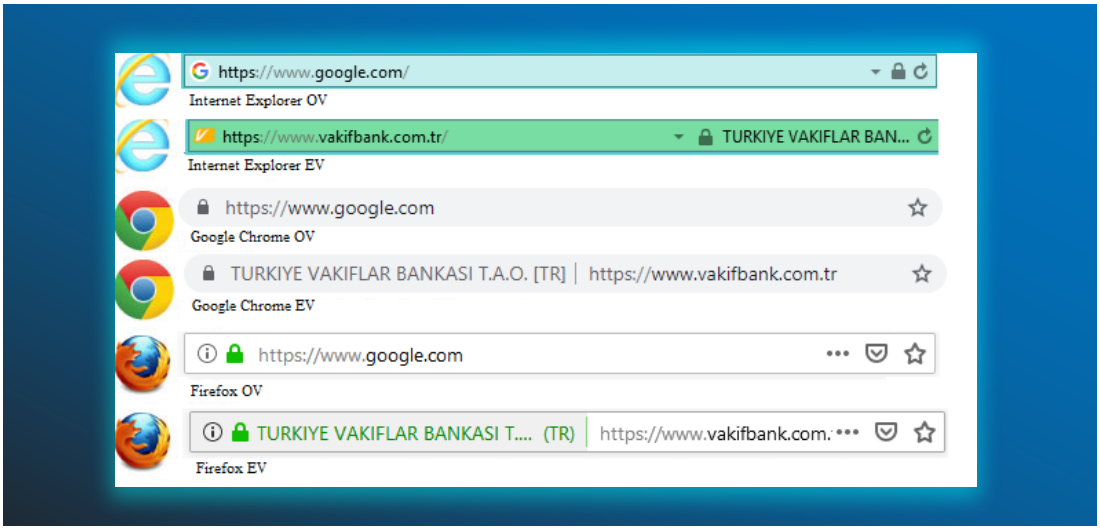


Daha önce EV SSL sertifikasına sahip olan ancak mevcut durumda sertifikalarını DV/OV SSL'e çeviren popüler siteler hakkında yapılan araştırma sonucunda sertifika kullanımlarının OV SSL sertifikalarına doğru kaydığı görülmektedir [5].



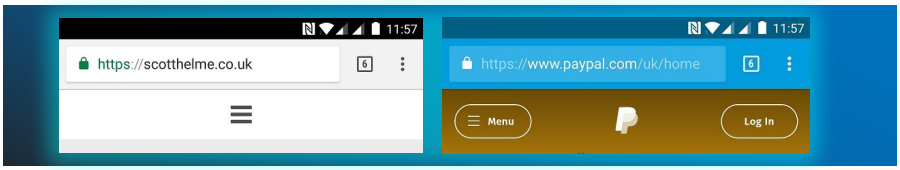
SSL Sertifikalarının Tarayıcılarda Gösterimi

Tarayıcıların SSL sertifika türleri karşısındaki görsel davranışları farklılık göstermektedir. OV SSL sertifikasına sahip bir web sayfasına web tarayıcılar aracılığıyla bağlanıldığında yalnızca asma kilit etkinleşirken; tarayıcılar genellikle sertifikanın EV olduğunu belirtmek için şirketin adını içeren yeşil adres çubuğunu da etkinleştirirler.

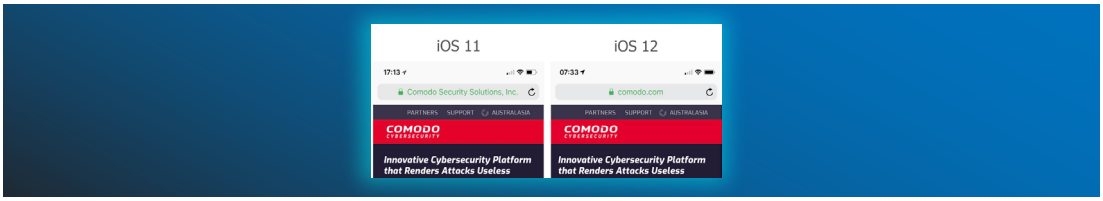


Chrome mobil platformlarda EV SSL sertifikalar için kurum adını göstermemektedir.

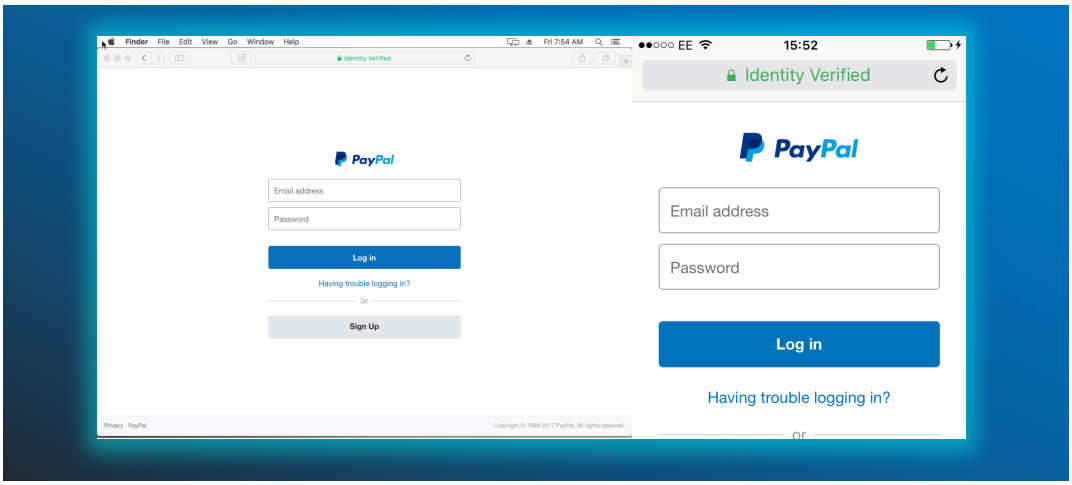
Bu durumda EV SSL sertifikaları DV sertifika ile aynı göstergelere sahiptir.



iOS yeni sürümüyle birlikte EV göstergelerini devre dışı bırakmıştır. Böylece DV, OV ve EV SSL sertifikaları arasında göstergeler temelinde herhangi bir farklılık görülmemektedir. Mac OS'da da aynı güncellemenin mevcut olduğu belirtilmiştir.



EV sertifikalardaki gösterim farkı her ne kadar güven vermesi için tasarlanmış olsa da 2017 yılında yapılan bir araştırmada, kurum adı “Identity Verified” olacak şekilde kısa bir süre içerisinde özel şirket kurulmuş; Comodo ve Symantec’e EV SSL sertifikası talebinde bulunulmuştur. Comodo, sertifika üretmeyi reddederken; Symantec, bu şirket için EV SSL sertifikası üretmiştir. Çalışmayı yapan taraf, kimlik avının ne kadar kolay olabileceğini ispatlamak adına kendi kontrolündeki web sitesinin ara yüzünü Google’nin ve Paypal’ın giriş sayfalarının bir kopyası olarak tasarlamıştır [6]. Safari tarayıcı EV SSL sertifikaları için adres çubuğunda URL göstermeksizin yalnızca sertifikadaki kurum adını göstermektedir. Normal bir web kullanıcısı için yeşil adres çubuğunda “Identity Verified” yazması güvenli ve yasal bir siteye girdiği izlenimini uyandırmaktadır ve oltalama saldırısını güçlendirmektedir.



EV SSL Sertifikasının Tarayıcıların İptal Kontrolünde Etkisi

Görsel işaretçilere ek olarak web tarayıcıları, SSL sertifikasının iptal durum bilgisini doğrulamaktadır. Sertifikaların iptal durum kontrolleri önemlidir, aksi halde çalınmış ve yanlış üretilmiş sertifikalar süresi dolana kadar kötüye kullanılabilir.

İnternet ortamında sıklıkla kullanılan web tarayıcıların iptal kontrol mekanizmaları incelendiğinde yalnızca Google Chrome ve Mozilla Firefox'un EV SSL sertifikaları için özelleşmiş iptal kontrol mekanizmaları bulunduğu görülmektedir.

Google Chrome, CRLSets adını verdiği kendi iptal kontrolü mekanizmasını kullanmaktadır. Google, anlaştığı/katılan sertifika otoritelerinden tüm Sertifika İptal Listelerini (SİL) toplar, listeyi önemli olduğunu düşündükleri sertifikaları içerecek şekilde düzenler ve tarayıcıya gönderir. Chrome'un iptal bilgilerini dâhil etmeye ilişkin kriterleri arasında EV sertifikalarını kapsayan SİL'lerin öncelikli olduğu belirtilmiştir [7]. Ancak CRLSets iptal kontrol mekanizmasında DV ve OV SSL sertifikalarını içeren iptal listeleri de yer almaktadır.

Firefox, tüm SSL tiplerine ait sertifikalar ve alt kökler için varsayılan olarak Çevrimiçi Sertifika Durum Protokol (Online Certificate Status Protocol-OCSP)'den iptal kontrolü yapmaktadır. Firefox tarayıcısında diğer sertifika tiplerinden farklı olarak EV SSL sertifikaları için OCSP kontrolü aktif değilse veya gerçekleştirilemezse, EV adres çubuğu aktif olmayacaktır [8].

Diğer popüler tarayıcılardan olan Internet Explorer ve Safari EV sertifikalarına özel bir kontrol mekanizması sunmamaktadır. Windows işletim sistemi, varsayılan olarak SİL ve OCSP bilgisini önbellekte depolar. Yalnızca Windows işletim sistemi için desteği bulunan Internet Explorer, iptal bilgilerinin tutulması için Windows ön belleğini kullanmaktadır.

Popüler tarayıcıların iptal kontrol mekanizmaları göz önüne alındığından EV SSL sertifikalarının iptal kontrolünün daha sıkı bir şekilde gerçekleştirilmesine rağmen, tarayıcıların büyük bir çoğunluğunun DV ve OV SSL sertifikaları için de iptal kontrolünü gerçekleştirdiği görülmektedir.

EV SSL Sertifikalarının Kamu Kurumlarında Kullanımının Artıları ve Eksileri

Artılar

- EV SSL sertifikaları diğer sertifika türleriyle karşılaştırıldığında sertifika sahibinin tüzel kişiliği hakkında daha fazla bilgi içermektedir. Sertifika için başvuran şirketlere ekstra kimlik doğrulama adımları uygulanmakta, şirketlerin gerçekten var oldukları garanti altına alınmaktadır. Bu durum kullanıcıların şirketlerin varlığı konusunda emin olmasına sebep olmaktadır.

- Popüler tarayıcıların iptal kontrol mekanizmalarında EV SSL sertifikaları için özelleşmiş kontroller mevcuttur. Ancak tarayıcıların büyük kısmı tüm SSL tipleri için iptal kontrolü sağlamaktadır.

Eksiler

- Joker SSL desteği bulunmamaktadır. Kurumların sertifikayı aldıktan sonra geliştirdiği web sayfalarında (Örn: *.abc.gov.tr) EV SSL sertifikasını kullanmasını imkansız kılmaktadır.

- Mozilla Kök Sertifika Deposunda ekli diğer devlet sertifika otoriteleri incelendiğinde EV SSL'in yalnızca tek bir sertifika otoritesinde tercih edildiği görülmüştür. Bu sertifika otoritesinin EV kök sertifika hiyerarşisi incelendiğinde müşteri profilinin hem kamu kurumları hem de şirketleri içerdiği ve özel şirketler için EV SSL sertifikası üretimi gerçekleştirdiği görülmektedir.

- EV SSL sertifikası kullanımıyla ilgili son yıllarda yapılan araştırma sonuçları incelendiğinde EV SSL sertifikasının git gide tercih edilen sertifika türü olmaktan çıktığı görülmektedir.

- Tarayıcıların EV SSL sertifikalarına olan yaklaşımları EV'nin gösterimde sağladığı avantajı ortadan kaldıracak niteliktedir.
- EV SSL sertifikalarda kurum kimliğinin doğrulanması ve onaylanması için çok daha fazla işlem yapıldığından sertifikanın yayımlanma süresi DV ve OV SSL sertifikalarına oranla çok daha uzundur.
- EV SSL sertifikaları, DV ve OV SSL sertifikalarına karşı kriptografik açıdan üstünlük sağlamamaktadır.

REFERANSLAR

[1]https://wiki.mozilla.org/CA:GovernmentCAs

[2]https://www.hongkongpost.gov.hk/product/ecert/type/server/index.html

[3]https://cps.pkioverheid.nl/CPS_PA_PKIoverheid_EV_Root_v1.7.pdf

[4]https://censys.io/certificates?q=parsed.issuer.common_name%3A+%22KPN+PKIoverheid+EV+CA%22

[5]https://scotthelme.co.uk/sites-that-used-to-have-ev/

[6]https://0.me.uk/ev-phishing/

[7]https://www.imperialviolet.org/2012/02/05/crlsets.html

[8]https://bugzilla.mozilla.org/show_bug.cgi?id=1366100