Denetci.org

REFERANS İLKELERİ

Dijital Sertifika Yönetimi İlkeleri

Rİ-KRP-3

Sürüm 1.0 · 11.08.2026

www.denetci.org

Dijital Sertifika Yönetimi İlkeleri

Dijital sertifikalar, bir kimlik ile kriptografik anahtar arasında başkalarının güven kararlarında kullanabileceği bir ilişki kurar. Bu ilkelerin amacı belirli bir sertifika otoritesi, protokol veya sertifika yaşam süresi belirlemek değil; sertifikaya duyulan güvenin hangi kimliğe, hangi anahtara, hangi yetkiye ve hangi güven zincirine dayandığının açık ve sınırlandırılmış olmasını sağlamaktır.

İlke 1: Sertifika, temsil ettiği kimlikle doğrulanabilir bir ilişkiye dayanmalıdır.

Bir sertifikanın teknik olarak üretilebilmesi, içindeki kimlik bilgisinin doğru olduğunu göstermez. Sertifika verilmeden önce anahtar ile temsil edildiği iddia edilen kişi, sistem, hizmet, cihaz veya kuruluş arasındaki ilişki yeterli güvenle kurulmuş olmalıdır.

İlke 2: Sertifika verme yetkisi, yeni bir güven ilişkisi oluşturma yetkisidir.

Sertifika üretmek yalnızca teknik bir işlem değildir; başka sistemlerin belirli bir kimliğe güvenmesine neden olabilir. Bu nedenle sertifika verme gücü, oluşturabileceği güven alanı ve etkiyle birlikte değerlendirilmelidir.

İlke 3: Bir sertifikaya neden güvenildiği açıklanabilir olmalıdır.

Güven yalnızca son sertifikanın varlığına değil, onu destekleyen sertifika zincirine ve güven köküne dayanabilir. Bir tarafın neden güvenilir kabul edildiği gerektiğinde hangi köke ve hangi güven ilişkisine kadar uzandığıyla gösterilebilmelidir.

İlke 4: Sertifika otoritesine duyulan güven sınırsız bir kimlik kabulüne dönüşmemelidir.

Bir otoritenin güvenilir olması, verebildiği bütün sertifikaların her sistem ve her amaç için uygun olduğu anlamına gelmez. Güven, kimlik alanı, kullanım amacı ve gerektiğinde başka sınırlarla daraltılabilmelidir.

İlke 5: Sertifika otoritelerinin yetkisi taşıdıkları gerçek etkiyle orantılı olarak sınırlandırılmalıdır.

Bir kök veya ara otoritenin kaybı çok sayıda kimliğin sahte biçimde güvenilir görünmesine neden olabilir. Sertifika verme gücü gereksiz biçimde tek bir geniş ve ortak güven alanında toplanmamalıdır.

İlke 6: Sertifikanın kullanım amacı açık ve sınırlı olmalıdır.

Bir anahtar-kimlik ilişkisinin sunucu kimliği, istemci kimliği, kod imzalama veya başka bir amaç için güvenilir olması diğer amaçlar için de güvenilir olduğu anlamına gelmez. Bir güven amacı için oluşturulan sertifika ilgisiz güven kararlarında kullanılmamalıdır.

İlke 7: Sertifikanın kapsamı temsil ettiği gerçek kimlik alanını aşmamalıdır.

Çok sayıda hizmeti, sistemi veya adı aynı sertifika altında toplamak işletimi kolaylaştırabilir; ancak tek bir anahtarın kaybını daha geniş bir kimlik kaybına dönüştürebilir. Sertifika

kapsamı, sağladığı kolaylık ile oluşturduğu ortak etki alanı birlikte düşünülerek belirlenmelidir.

İlke 8: Sertifika güvenliği özel anahtarın güvenliğinden ayrı düşünülemez.

Sertifika açık biçimde dağıtılabilir; ancak ona karşılık gelen özel anahtar başka bir tarafın eline geçtiğinde sertifikanın temsil ettiği kimlik taklit edilebilir. Sertifikanın gerçek güven düzeyi, özel anahtarın kimler tarafından ve hangi koşullarda kullanılabildiğiyle sınırlıdır.

İlke 9: Aynı özel anahtarın yayılması bağımsız kimlik alanlarını birbirine bağlamamalıdır.

Bir anahtarın çok sayıda sistemde kopyalanması, bu sistemlerden herhangi birinin kaybını aynı anahtarı kullanan diğer kimliklere taşıyabilir. Ortak sertifika kullanımı gereksiz ortak güven kaybı oluşturmamalıdır.

İlke 10: Sertifika yaşamı sınırsız güven varsayımına dayanmamalıdır.

Kimlik, anahtar, kullanım amacı ve çevresel koşullar zaman içinde değişebilir. Bir sertifikanın geçmişte doğru verilmiş olması aynı güven ilişkisinin süresiz biçimde devam etmesi için yeterli değildir.

İlke 11: Yenileme geçmiş güven kararlarının otomatik olarak tekrarlanması olmamalıdır.

Sertifika yenilenirken kimlik, kapsam, kullanım amacı veya anahtar ihtiyacı değişmiş olabilir. Yenileme yalnızca sona erme tarihini ileri taşımak yerine mevcut güven ilişkisinin hâlâ geçerli olduğunu yansıtmalıdır.

İlke 12: Sertifika yenilenmesi ile anahtarın yenilenmesi ayrı güven kararlarıdır.

Yeni bir sertifika verilmesi eski özel anahtara duyulan güveni kendiliğinden yenilemez. Anahtarın ne kadar süre ve ne kadar geniş kapsamda kullanıldığı ayrıca değerlendirilebilmelidir.

İlke 13: Güvenini kaybeden sertifikanın etkisi sona erdirilebilmelidir.

Özel anahtarın ele geçirilmesi, sertifikanın yanlış verilmesi veya temsil edilen kimliğin artık geçerli olmaması gibi durumlarda yalnızca yeni sertifika oluşturmak yeterli olmayabilir. Eski güven ilişkisinin gerçek sistemler tarafından artık kabul edilmemesi mümkün olmalıdır.

İlke 14: İptal bilgisinin yayımlanması ile güvenin gerçekten sona ermesi aynı şey değildir.

Bir sertifika kayıt üzerinde iptal edilmiş olsa bile onu kullanan sistemler bu bilgiyi dikkate almıyorsa güven ilişkisi devam eder. Sertifika modelinin güvencesi, güven kaybının gerçek doğrulama davranışına yansımasına dayanmalıdır.

İlke 15: Güven depoları kabul edilen kimlik alanının bir parçasıdır.

Bir sisteme yeni bir kök veya sertifika otoritesi eklemek, o otoritenin oluşturabileceği bazı kimlikleri kabul etmeye başlamaktır. Güven deposundaki değişiklikler sıradan teknik yapılandırma değişiklikleri olarak görülmemelidir.

İlke 16: Farklı güven alanları sertifika ve anahtarlar aracılığıyla görünmez biçimde birleşmemelidir.

Üretim, geliştirme, test veya başka farklı güven düzeyindeki ortamların aynı sertifika otoritelerini, özel anahtarları veya kimlikleri paylaşması bir ortamın kaybını diğerine taşıyabilir. Ortam ayrımı sertifika güven ilişkilerinde de gerçek olmalıdır.

İlke 17: Sertifika doğrulaması sertifikanın varlığını değil iddia edilen güven ilişkisini sınamalıdır.

Bir sertifikanın imzalı ve geçerlilik süresi içinde olması tek başına yeterli değildir. Kullanılan kimlik, amaç, güven zinciri ve ilgili diğer özellikler bağlantının veya işlemin gerçekten güvenilmek istenen tarafla kurulduğunu desteklemelidir.

İlke 18: Doğrulama başarısızlığı sessizce güvene dönüştürülmemelidir.

Kimlik, zincir veya başka kritik doğrulama unsurları doğrulanamadığında sistemi çalıştırmak amacıyla doğrulamayı etkisiz hale getirmek sertifika modelinin temel anlamını ortadan kaldırabilir. Hata durumundaki davranış bilinçli bir güven kararı olmalıdır.

İlke 19: Sertifika otomasyonu güven ilişkilerini görünmez hale getirmemelidir.

Otomatik üretim ve yenileme işletim güvenilirliğini artırabilir; ancak hangi kimliklerin oluşturulduğu, hangi otoritelerin bunları verdiği ve hangi sistemlerin bunlara güvendiği bilinemez hale gelmemelidir. Otomasyon, güven kararının uygulanmasını kolaylaştırmalı; kararın kendisini gizlememelidir.

İlke 20: Dijital sertifika güvencesi çalışan güven ilişkileri üzerinden doğrulanabilmelidir.

Sertifika envanteri, PKI ürünü veya otomatik yenileme sistemi bulunması tek başına güvence oluşturmaz. Hangi sertifikaların hangi kimlikleri temsil ettiği, bunların hangi anahtarlara dayandığı, sistemlerin hangi otoritelere ve amaçlara güvendiği ve güven sona erdirildiğinde bu ilişkinin gerçek sistemlerde de sona erip ermediği gerektiğinde gösterilebilmelidir.