**Denetci.org**

**REFERANS İLKELERİ**

# Kriptografik Anahtar Yönetimi İlkeleri

**Rİ-KRP-2**

Sürüm 1.0 · 11.08.2026

www.denetci.org

# Kriptografik Anahtar Yönetimi İlkeleri

Kriptografik anahtarlar; gizlilik, bütünlük, kimlik doğrulama, imzalama ve benzeri kriptografik güven özelliklerinin temelini oluşturan güven unsurlarıdır. Bu ilkelerin amacı belirli algoritmalar, ürünler veya anahtar yönetim teknolojileri belirlemek değil; kriptografik güvenin anahtarların gerçek yaşam döngüsü, kullanım sınırları ve kayıp durumlarıyla birlikte tasarlanmasını sağlamaktır.

**İlke 1: Kriptografik güven, anahtarın güvenilirliğinden bağımsız kabul edilmemelidir.**

Güçlü bir algoritma, onu kullanan anahtarın ele geçirilmesini veya yanlış kullanılmasını telafi etmez. Bir kriptografik mekanizmanın güvencesi, anahtarın nasıl oluşturulduğu, kimlerin kullanabildiği ve ne ölçüde korunabildiğiyle birlikte değerlendirilmelidir.

**İlke 2: Her anahtar belirli ve anlaşılabilir bir güven amacına sahip olmalıdır.**

Bir anahtarın şifreleme, imzalama, kimlik doğrulama veya başka hangi amaçla kullanıldığı belirsiz kalmamalıdır. Farklı güven sonuçlarını tek anahtarda gereksiz biçimde birleştirmek, bir kaybın etki alanını genişletebilir.

**İlke 3: Anahtar kapsamı gerçek ihtiyaçla sınırlı olmalıdır.**

Bir anahtarın tek bir hizmet veya güven alanı için yeterli olduğu durumda çok sayıda ilgisiz sistemde geçerli olması gerekmemelidir. Ortak anahtar kullanımı operasyonel kolaylık sağlasa da bağımsız alanları aynı güven kaybına bağlayabilir.

**İlke 4: Anahtar güvenilir biçimde oluşturulmadan sonraki korumalar anlamlı güvence sağlayamaz.**

Anahtarın kaynağı veya üretiminde kullanılan belirsizlik öngörülebilir ise daha sonra güçlü biçimde saklanması temel zayıflığı ortadan kaldırmaz. Üretim, anahtar yaşam döngüsünün ilk güvenlik sınırıdır.

**İlke 5: Anahtar üretildiği andan itibaren korunması gereken bir güven unsuru olmalıdır.**

Koruma yalnızca anahtar bir sisteme yüklendiğinde başlamamalıdır. Üretim, aktarım ve ilk yerleştirme sırasında oluşan kopyalar daha sonraki bütün güveni etkileyebilir.

**İlke 6: Gizli anahtar materyalinin dışarı çıkarılması olağan kullanım koşulu olmamalıdır.**

Özel veya simetrik anahtarın farklı sistemlere taşınması ve kopyalanması onun ele geçirilebileceği alanları artırır. Anahtarın sağladığı işlemin gerçekleştirilebilmesi mümkün olduğunda anahtarın kendisinin yayılmasını gerektirmemelidir.

**İlke 7: Anahtarın saklanması ile anahtarı kullanma yetkisi aynı şey olarak görülmemelidir.**

Bir bileşenin anahtar materyalini barındırması, o anahtarla her işlemi yapabilecek bütün tarafların aynı geniş erişime sahip olmasını gerektirmez. Kriptografik güç, kullanılması gereken işlem ve taraflarla sınırlandırılabilmelidir.

**İlke 8: Anahtarın korunma düzeyi oluşturabileceği güvenlik etkisiyle uyumlu olmalıdır.**

Bütün anahtarlar aynı sonuçları doğurmaz. Çok sayıda veriyi, kimliği veya sistemi etkileyebilen bir anahtarın kaybı daha dar kapsamlı bir anahtardan farklı bir güven sonucu oluşturur.

**İlke 9: Anahtar yönetimini merkezileştirmek toplam güveni de merkezileştirebilir.**

Merkezi yönetim tutarlılık ve görünürlük sağlayabilir; ancak çok sayıda kritik anahtar üzerinde tek bir yönetim veya hata alanı da oluşturabilir. Merkezileşmenin operasyonel yararı taşıdığı ortak güven kaybıyla birlikte değerlendirilmelidir.

**İlke 10: Anahtar hiyerarşileri güveni gereksiz biçimde yaymak yerine sınırlandırmalıdır.**

Kök, ana veya türetilmiş anahtarlar farklı güven alanları oluşturabilir. Üst düzey bir anahtarın günlük işlemlerde gereksiz kullanılması veya bağlamların aynı türetim ilişkisine bağlanması daha geniş bir kaybın önünü açmamalıdır.

**İlke 11: Anahtar kurtarma yeteneği olağan güven sınırlarının gizli alternatifi olmamalıdır.**

Bir anahtarın yedekten veya başka bir yöntemle geri getirilebilmesi süreklilik açısından gerekli olabilir; ancak bu yetenek ana anahtardan daha zayıf korunan ikinci bir erişim yolu oluşturmamalıdır.

**İlke 12: Her anahtarın kurtarılabilir olması güvenlik hedefi değildir.**

Bazı anahtarların kaybı veri veya hizmet kaybına yol açabilirken bazılarında anahtarın yeniden oluşturulması daha güvenli olabilir. Yedekleme ve kurtarma kararı, anahtarın amacı ve kaybının gerçek sonucu üzerinden verilmelidir.

**İlke 13: Anahtar yedekleri ana anahtarla aynı güven kaybına bütünüyle bağlı olmamalıdır.**

Yedekleme süreklilik sağlarken ek anahtar kopyaları ve yeni erişim yolları da oluşturabilir. Yedek, asıl anahtarın maruz kaldığı aynı olayda kolaylıkla ele geçirilecek veya yok olacak biçimde tasarlanmamalıdır.

**İlke 14: Anahtarın yaşam süresi sınırsız güven varsayımına dönüşmemelidir.**

Anahtar ne kadar uzun süre ve ne kadar geniş kapsamda kullanılırsa maruz kaldığı olaylar ve koruduğu değerler de birikebilir. Bununla birlikte anahtarı sırf takvim nedeniyle değiştirmek

değil, kullanım amacı, risk ve kriptografik bağlamla uyumlu bir yaşam döngüsü kurmak esastır.

**İlke 15: Anahtar değişimi eski anahtarın güvenini kendiliğinden sona erdirmez.**

Eski anahtar sistemlerde, yedeklerde veya geçmiş verinin doğrulanması ve çözülmesi için kullanılmaya devam edebilir. Rotasyon, yeni anahtar üretmenin yanında eski anahtarın hangi güven ilişkilerinde hâlâ anlam taşıdığını da hesaba katmalıdır.

**İlke 16: Anahtar güvenini kaybettiğinde gerçek kriptografik ilişki değişebilmelidir.**

Ele geçirilmiş bir anahtarın envanter durumunun değiştirilmesi yeterli değildir. Anahtarın şifreleme, imzalama veya kimlik doğrulama açısından sağladığı güç mümkün olduğu ölçüde sona erdirilebilmeli ve ondan etkilenmiş güven ilişkileri değerlendirilmelidir.

**İlke 17: Anahtarın kaybı ile ele geçirilmesi aynı olay olarak görülmemelidir.**

Kaybolan bir anahtar erişilebilirliğin veya verinin kaybına; ele geçirilen bir anahtar ise yetkisiz erişim, taklit veya sahte güven kanıtı oluşturulmasına neden olabilir. Anahtar yaşam döngüsü bu farklı sonuçları ayırt edebilmelidir.

**İlke 18: Kriptografik çevrenin değişmesi anahtarın güven anlamını değiştirebilir.**

Algoritmalar, anahtar boyutları, uygulamalar ve saldırı yetenekleri zaman içinde değişebilir. Uzun süre korunması gereken veri ve güven ilişkileri yalnızca anahtarın bugünkü güvenliğine dayanarak sınırsız kabul edilmemelidir.

**İlke 19: Kriptografik anahtar yönetiminin güvencesi gerçek kullanım ilişkileri üzerinden doğrulanabilmelidir.**

Bir anahtar yönetim ürünü, donanımsal koruma veya kriptografik sertifikasyon tek başına güvence oluşturmaz. Hangi anahtarın hangi amaçla kullanıldığı, kimlerin onunla hangi işlemleri yapabildiği, nerelerde kopyasının bulunduğu, güven kaybında neyin etkilendiği ve anahtarın kullanımdan kaldırılmasının gerçek sistem davranışına yansıyıp yansımadığı gerektiğinde gösterilebilmelidir.