SSL için SHA-2 Geçişi

SHA-2 matematiksel olarak açığı olabilecek SHA-1 algoritmasının yerine geçmek üzere NIST (Ulusal Standartlar ve Teknoloji Enstitüsü, Amerika) tarafından geliştirilen bir kriptografik özetleme algoritmasıdır. SHA-1 algoritması 2005 yılında oluşturulmuştur ve günümüz teknolojisi için zayıf bir algoritma olarak kabul edilmektedir. Günümüzde SHA-2 özetleme algoritmaları (SHA-256, SHA-384, SHA-512) halihazırda yaygın şekilde desteklenmektedir.

Google, SHA-2 geçişini hızlandırmak adına, yeni Chrome sürümlerinde SHA-1 ile üretilmiş SSL sertifikaları için farklı uyarılar vererek güvenlik bildirimleri yapmayı planlamaktadır. Google bu planını Chrome'un 39 ve üzeri sürümleri ile hayata geçirecektir. .

CA/Browser Forum (sektör standartlarını belirleyen ve önde gelen sertifika hizmet sağlayıcıları ile browser firmalarından oluşan uluslararası komite) düzenlemelerine de girmekte olan SHA-2 geçişi, aslında Google, Microsoft ve Mozilla tarayıcıları aracılığıyla Ocak 2017 tarihinde kesinleşmiş olacaktır.

SHA-1 algoritmasının tanınmayacağı önemli tarih:

1 Ocak 2017 Microsoft SHA-1 kullanan SSL sertifikalarını tanımayacak,
Mozilla SHA-1 kullanan SSL sertifikalarını tanımayacak,
Google SHA-1 kullanan SSL sertifikalarını tanımayacak,

Google, SHA-1 ile üretilen SSL sertifikalarındaki son kullanım tarihine göre, gelecek tarayıcı sürümlerinde aşağıda gösterilen görsel uyarı işaretleriyle kullanıcılara uyarı vermeyi planlamaktadır:

	Sertifikanın Son Kullanım Tarihi			
Chrome Sürümü	SHA-1 (31.12.2015)	SHA-1 (31.5.2016)	SHA-1 (31.12.2016)	SHA-1 (1.1.2017 sonrası)
Chrome 39 (Tahminen Kasım 2014)				
Chrome 40 (Tahminen Aralık 2014)				
Chrome 41 (Q1 2015)				

Not: Çoğu uygulama, sunucu ve tarayıcılar SHA-2 algoritmasıyla üretilmiş sertifikaları halihazırda desteklemekteler. Fakat Windows XP (Service Pack 3 öncesi) gibi eski sistemler ve bazı mobil cihazlar SHA-2 algoritmasını desteklemeyebilir.

TÜRKTRUST, bir sertifika hizmet sağlayıcısı olarak, SSL sertifikalarında SHA-1 yerine SHA-2 algoritmasının kullanılması gerekliliğini desteklemektedir. Bu konuda tüm müşterilerine bu geçiş döneminde gerekli desteği sağlayacaktır.