

Duyurular

12 Haziran 2009

Garanti İnternet İubesi, VeriSign® Extended Validation (EV) SSL Sertifikalarına geiyor!

Yeni nesil Web tarayıcılarında bulunan bazı ek güvenlik özelliklerini aktif hale getirmek için İnternet İubesi sunucu sertifikaları yenilenecektir. İu anda 128 bit SSL özellikli VeriSign® Güvenlik sertifikaları kullanılmaktadır. Yakın zamanda yine 128 bit SSL özelliğine sahip olan ve buna ek olarak kullanıcılarının sahtecilik amaçlı siteleri güvenli sitelerden daha kolay ayırt etmelerini sağlayan "**VeriSign® Extended Validation (EV) SSL**" sertifikaları devreye alınacaktır.

VeriSign® Extended Validation (EV) SSL Sertifikalarının sunduğu özelliklerden faydalanabilmek için, artık çok nadiren kullanılan eski sürüm tarayıcıları kullanan mü terilerimizin de tarayıcılarını güncellemeleri gerekmektedir.

En az, Microsoft İnternet Explorer 6.0 ve 7.0, Mozilla Firefox 3.0, Apple Safari 3.2, Opera 9.6 kadar güncel bir tarayıcı kullanmıyorsanız İnternet İubesi'ne giri inizde sorunlar ile karşılaşabilirsiniz.

Böyle bir durumla karşılaşmamak için tarayıcınızı en kısa zamanda yazılımcı firma **resmi sitesinden ücretsiz olarak güncellemeniz gerekmektedir.**

Güncellemeler için:

- **Microsoft Internet Explorer** resmi sitesi için [tıklayın.](#)
- **Mozilla Firefox** resmi sitesi için [tıklayın.](#)
- **Apple Safari** resmi sitesi için [tıklayın.](#)
- **Opera** resmi sitesi için [tıklayın.](#)
- **Google Chrome** resmi sitesi için [tıklayın.](#)

Verisign'ın resmi sitesinden, VeriSign® Extended Validation(EV) SSL hakkında detaylı bilgi edinebilirsiniz. <http://www.verisign.com/>

Kullandığımız sürüm bilgisine tarayıcınızın "Yardım" menüsündeki "Hakkında" seçeneğinden ulaşabilirsiniz.

128 bit SSL Sertifikası nedir?

SSL network üzerindeki bilgi transferi sırasında güvenlik ve gizliliğinin sağlanması amacıyla Netscape tarafından geliştirilmiş bir güvenlik protokolüdür. 1996 yılında 3.0 versiyonunun çıkarılmasıyla hemen bütün İnternet tarayıcılarının desteklediği bir standart haline gelmiş ve çok geniş uygulama alanları bulmuştur.

SSL gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini sağlar. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre

edilebilir. Her iki tarafta da do rulama yapılarak i lemin ve bilginin gizlili i ve bütünlü ü korunur.

Veri akı ında kullanılan ifreleme yönteminin gücü kullanılan anahtar uzunlu una ba lıdır. Anahtar uzunlu u bilginin korunması için çok önemlidir. SSL protokolünde 40 bit ve 128 bit ifreleme kullanılmaktadır. 128 bit ifrelemede 2^{128} de i ik anahtar vardır ve bu ifrenin çözülebilmesi çok büyük bir maliyet ve yıllarla ölçülebilecek kadar zaman gerektirir.