

# Internet'te Bireysel Gizlilik ve Güvenlik

DiKEY8

Can ALPTEKİN [ca@dikey8.com](mailto:ca@dikey8.com)  
Korhan GÜRLER [kg@dikey8.com](mailto:kg@dikey8.com)

- Web Tarayıcısı Güvenliği
- Şifreler
- Sosyal Mühendislik
- Virüs, Kurtçuk, vs...
- E-Posta Güvenliği ve Gizliliği
  - PGP Uygulaması
- Paranoya

- Çoklu ortam eklentileri yeni riskler yaratıyor.
- Seyyar kodlar (ActiveX, Java) kötü niyetli kullanılabilir.
- Kullanıcılar mahremiyetlerini koruyamıyorlar.
- Çerezler bilgi sızdırabiliyor.
- SSL Sertifikaları.
- Cross-Site Scripting.
- Parola saklama seçenekleri.

# Web Tarayıcıları (önlemler -I)

---

- Yazılımın, üretici tarafından çıkarılan yamalarını derhal uygulamak ve düzenli olarak takip etmek.
- Seyyar kodları çalıştırmaktan kaçınmak.
- Anonymizer yazılımlarla mahremiyeti korumak.
- Çerez kabul ederken seçici davranmak.
- E-ticaret veya benzeri şifrelenmiş trafik kullanılan sitelerde SSL sertifikaların kontrollerini dikkatli yapmak.
- Umulmadık anlarda karşılaşılan sisteme giriş sayfasının tekrar görüntülenmesi gibi durumlarda dikkatli olmak.
- Tarayıcının parola saklama seçeneklerini kullanmamak.

- ActiveX programları spesifik fonksiyonları yerine getirmek üzere (klip göstermek ya da bir ses dosyası çalmak gibi) yazılmış kodlardır ve web sayfalarına konarak bu özelliklerin sayfada oluşması sağlanabilir.
- ActiveX kontrolleri genellikle .OCX soyadına sahiptir (Java ile yazılmış olanları hariç)
- IE böyle bir sayfa görüntülemeye çalıştığında önce kullanıcının makinasına bakarak gerekli ActiveX kontrolünün olup olmadığını kontrol eder, yoksa kendisi yüklemeye çalışır.
- ActiveX kontrolünü yüklemeden önce imzalarına bakıp geçerli bir ActiveX olup olmadığını kontrol eder, değilse kullanıcıyı uyarır.

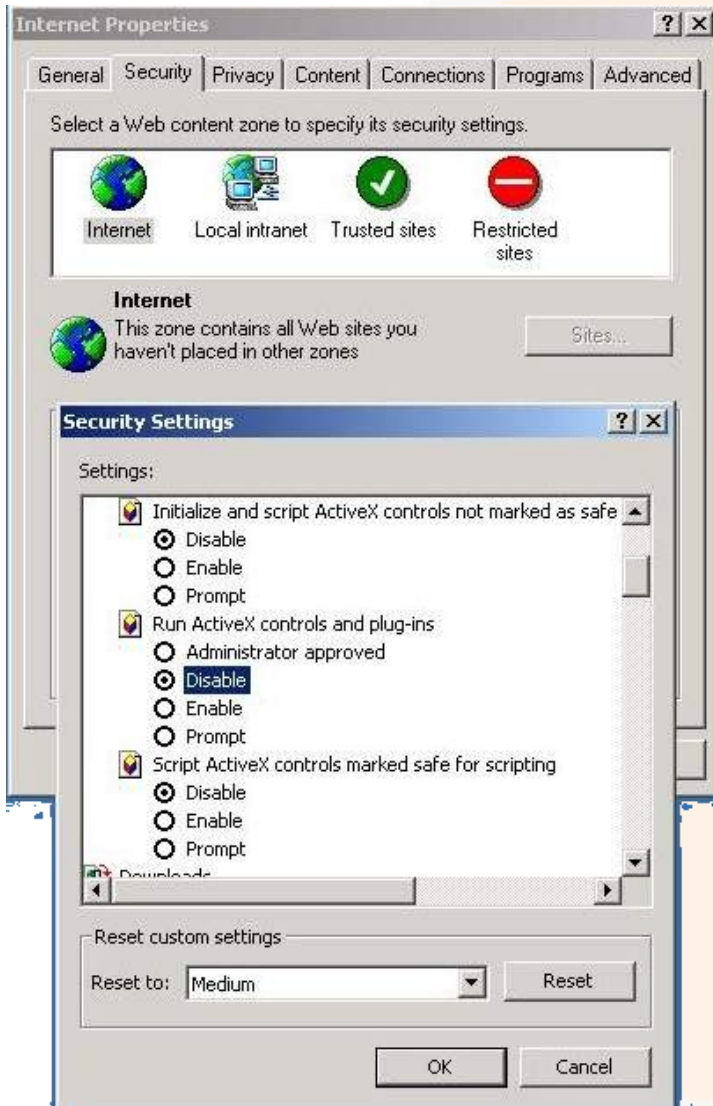
# IE Güvenliği (devam)

---

ActiveX ne gibi bir tehdit oluşturuyor?

- “Safe for Scripting” açığı : Bununla ActiveX kodu içerisinde makinanızdaki herhangi bir dosyanın üzerine yazılabilir, yeni bir dosya yaratılabilir.
- Active Setup Dosya Yükleme açığı : Bu açık ise bir DoS saldırısı olarak tanımlanabilir. Saldırgan “Active Setup” ın imzalı Microsoft .CAB dosyalarını diske yüklemesi ile ilgili bir açığı kullanarak saldırısını gerçekleştirir.

# IE Güvenliği (devam)



- Saldırılar sadece insanlardan direkt değil dolaştığımız web sitelerinden de gelebilir
- ActiveX kontrolleri iptal edilmeli
- Yamalar ve güncellemeler mutlaka takip edilip uygulanmalı

Şifre güvenliğini kompleks bir hale getiren durum; şifreleri başkaları tarafından tahmin edilmesi zor bir karakter dizisi olarak seçme zorunluluğu ile hatırlanması kolay bir şifre olmasının gerekliliği arasındaki tezatlıktan kaynaklanır.



**Yeterli zaman ve kaynaklar olduğu sürece  
her şifre kırılabilir!!!**

# Şifreler (devam)

---

- Yeterli uzunlukta şifreler seçilmeli (min. 6 karakterli)
- Hiç bir zaman herhangi bir sözlükte bulunabilecek bir kelime seçilmemeli
- Büyük, küçük harf ve rakamlar bir arada kullanılmalı
- Çeşitli semboller kullanılmalı (@, \$, %, ^, !, &...)
- Kitaplardaki örnek şifreler hiç bir zaman kullanılmamalı
- Klavye kalıpları kullanılmamalı
- Hiç bir zaman programlardaki “Parolayı kaydet” seçeneği kullanılmamalı
- Her hesap için ayrı bir şifre kullanılmalı
- Şifreler sık sık değiştirilmeli
- Şifreler bir yere yazılmayıp sadece ezberlenmeli
- Sosyal mühendisliğe dikkat edilmeli
- Kimseye şifrenizi vermeyin (arkadaşlarınız da dahil)

Örnek şifreler:

- K0rh@nG (akılda kalıcı)
- ^#6XsEVv%!.5T (akılda kalıcı değil)

Acı ama gerçek:

- Tüm şifrelerin %90 ila %95'i aynı 100 kelimeden oluşuyor.
- Kullanıcıların tahmin edilmesi çok basit şifreler seçtiğini gözlemledik: ya çok kısalar ya da sözlükte bulunabilecek kelimelerden seçiliyorlar.

- D. Ritchie

Şifrem çalındı ne yapmalıyım?

- Internet Servis Sağlayıcının telefonla destek hattı aranıp şifreler değiştirilmeli
- Diğer bütün hesapların şifreleri değiştirilmeli
- Üye olduğunuz listeler, haber grupları vb... kontrol edilip sizin adınıza haber gönderilip gönderilmediği kontrol edilmeli

- Kişileri inandırma yoluyla istediğini yaptırma eylemidir.
  - Albenili e-posta ekleri, web hizmetleri. (too good to be true)
  - ISP görevlisi kılığında kullanıcının şifresini öğrenmek.
  - Banka personeli kılığında kişisel ve kredi kartı bilgilerini ele geçirmek.
  - Teknisyen kılığında kurumun içine fiziksel olarak sızmak...

# Sosyal Mühendislik (çözümler)

---

- Görevli olduğunu iddia eden şahısların kimliğinden ve görev sınırları dahilinde hareket ettiğinden emin olmak.
- Albenisi fazla olan her olaya şüpheyile bakmak.
- Kişisel mahremiyeti korumak ve sahip çıkmak.

RFC 1135'e göre virüs tanımı:

“Virüs”, işletim sistemleride dahil olmak üzere, kendini bir taşıyıcıya yerleştirerek yayılan bir kod parçasıdır. Tek başına çalışamaz. Aktif hale gelebilmesi için taşıyıcı programın çalıştırılması lazımdır.



RFC 1135'e göre kurtçuk tanımı:

“Kurtçuk” taşıyıcısının kaynaklarını kullanarak tek başına çalışabilen ve çalışabilen tam bir kopyasını başka makineler üzerinde de oluşturabilen programlardır.

Klasik bir makro virüsü kelime işlemcilerin içindeki makro yazma özelliklerini suistimal ederek çalışır.

DiKEY8

- Zararsız programcıklar gibi gözükürler
- Bulaştığı program normal seyrinde çalışır
- Yapacağı işleri arka planda çalışarak kullanıcıya hissettirmez
- Sistemde farkedilmeleri çok zor olabilir

- Kullanıcının, alışkanlıklarını izleyerek merkezi bir noktaya raporlayan, kullanıcıyı kendi üye sitelere yönlendirerek hit kazandırmak gibi korsan işlevler yaratan yazılım.

DiKEY8

# Virüsler sisteme nasıl girer?

---

- Internetten çekilen programlar ile
- E-posta ekleri ile
- Ağdaki paylaşıma açık dosyalar ile
- Bilgisayarınıza taktığınız taşınabilir medya vasıtası ile

# Virüslere karşı korunma

---

- Sisteme anti-virüs programı yüklenmeli
- Internetten çekilen dosyalar konusunda dikkatli olunmalı
- Bilinmeyen kaynaktan gelen e-posta'daki ekli dosyaları açılmamalı
- Paylaşılan taşınabilir medyalar virüs kontrolünden geçirilmeli

# Virüslere karşı korunma (devam)

---

- Eğer bir programın virüslü olduğundan şüpheleniyorsanız o programı kullanmayın!
- Bir program satın aldığınızda üreticinin mühürünün yırtılmadığına emin olun

DiKEY8

- E-postanın kullandığı altyapı güvenlik ihtiyacının duyulmadığı dönemlerde belirlendiği için kötü kullanıma en açık noktalardan birisidir.
    - Kaynağının doğruluğu,
    - İçeriğinin değiştirilmediği,
    - Mahremiyeti denetlenememektedir.
  - İstenmeyen iletiler (spam, junk, chain mail) zaman ve kaynak israfına sebep olmakta.
  - İleti ekleri art niyetli kodlar için yayılma platformu sağlamakta.
  - Ücretsiz e-posta hizmetleri, erişim denetim hizmetlerinin düşük tutulması sebebiyle kolaylıkla kötü kullanımlara yol açabilmekte.
-



# E-posta (çözümler - I)

---

- E-postanın kaynağının onaylanması, içeriğinin ve mahremiyetinin korunduğundan emin olabilmek için sayısal imza ve şifreleme yazılımları kullanılmalı.
  - S/MIME
  - PGP
- İstenmeyen iletiler için e-posta yazılımının filtreleme seçenekleriyle beraber, farklı filtreleme yazılımları kullanılmalı.
- İleti ekleri mutlaka anti-virüs yazılımlarıyla taranarak virüs içermediğinden emin olunmalı. Bilinmeyen kaynaklardan gelen iletilere şüpheyile bakılmalı, talep edilmemiş ileti ekleri kesinlikle açılmamalı.

# E-posta (çözümler - II)

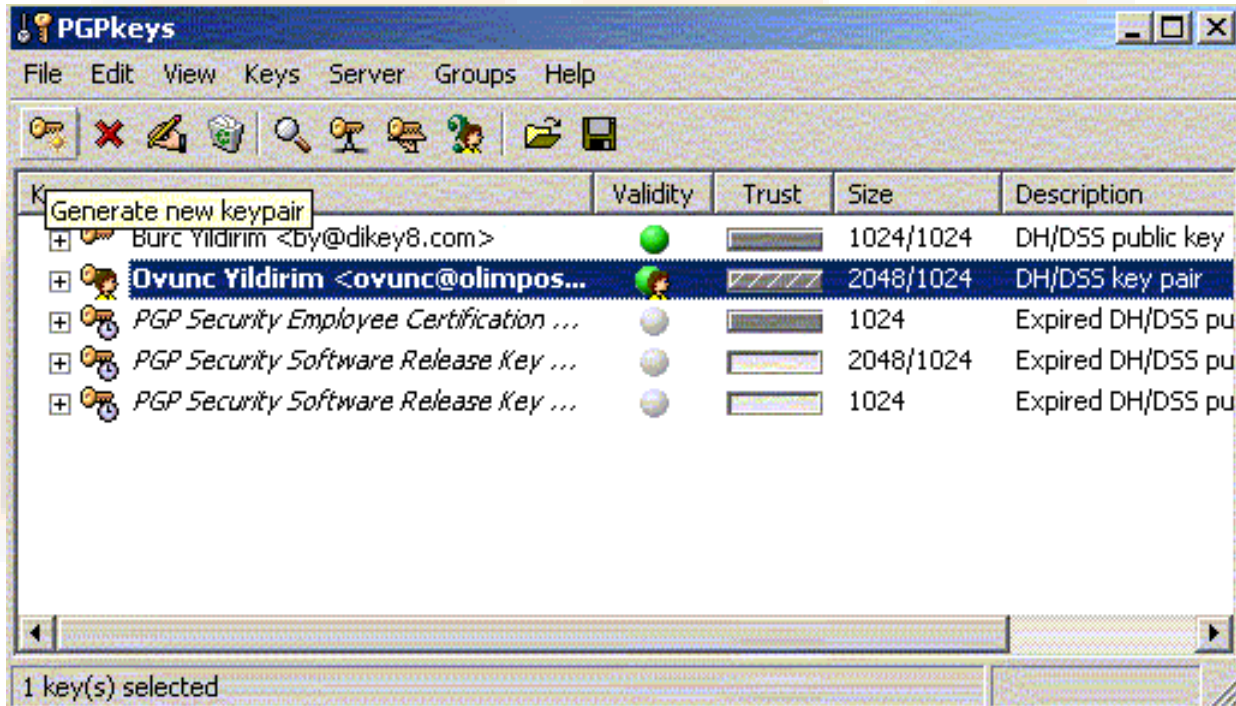
---

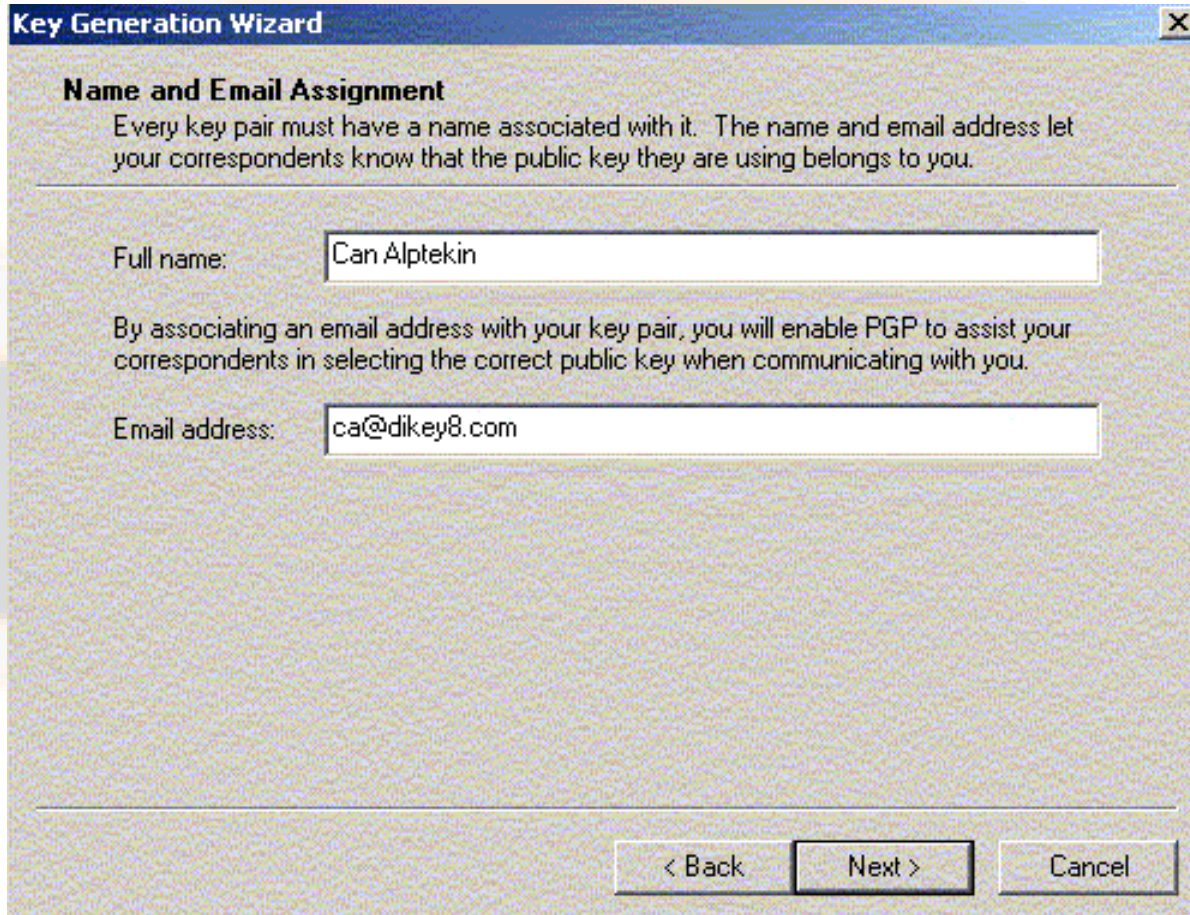
- Ücretsiz e-posta hizmetleri kesinlikle ticari amaçlı kullanılmamalı, parolalar ve parola hatırlatma mekanizmaları için seçilen kriterlerin en yakın kişilerce bile tahmin edilemeyecek kadar kişisel olmasına dikkat edilmeli. Bu tip ücretsiz e-posta hizmeti veren kuruluşların politikaları dikkatle okunmalı. (İletilerin sahibi kurumdur, vs.)
- E-posta önizlemesi iptal edilmeli, yazılımlarda çıkan açıklar önizleme durumunda bile ekli dosyaları kullanıcının izni olmadan çalıştırabilir.
- E-posta yazılımı sürekli olarak güncel tutulmalı.

# E-Posta (çözümler - III)

---

- E-posta iletileri için risksiz formatlar kullanılmalı, HTML ileti yerine, düz yazı iletisi, Word dökümanı yerine, Zengin yazı biçimi gibi.
- Çoğunluğun kullandığından farklı e-posta yazılımları tercih edilmeli, böylelikle çoğunluğu hedef alan art niyetli yazılımların saldırıları bertaraf edilebilir.
- E-posta iletilerinden birçok kişisel bilgi edinilebileceği unutulmamalı, özellikle e-posta listelerine atılan mesajların içeriklerine özen gösterilmeli.



A screenshot of a 'Key Generation Wizard' dialog box. The title bar is blue with the text 'Key Generation Wizard' and a close button. The main area has a light gray background. The first section is titled 'Name and Email Assignment' in bold. Below the title is a paragraph: 'Every key pair must have a name associated with it. The name and email address let your correspondents know that the public key they are using belongs to you.' There is a horizontal line. Below this, the label 'Full name:' is followed by a text box containing 'Can Alptekin'. Another paragraph follows: 'By associating an email address with your key pair, you will enable PGP to assist your correspondents in selecting the correct public key when communicating with you.' Below this, the label 'Email address:' is followed by a text box containing 'ca@dikey8.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Key Generation Wizard**

**Name and Email Assignment**

Every key pair must have a name associated with it. The name and email address let your correspondents know that the public key they are using belongs to you.

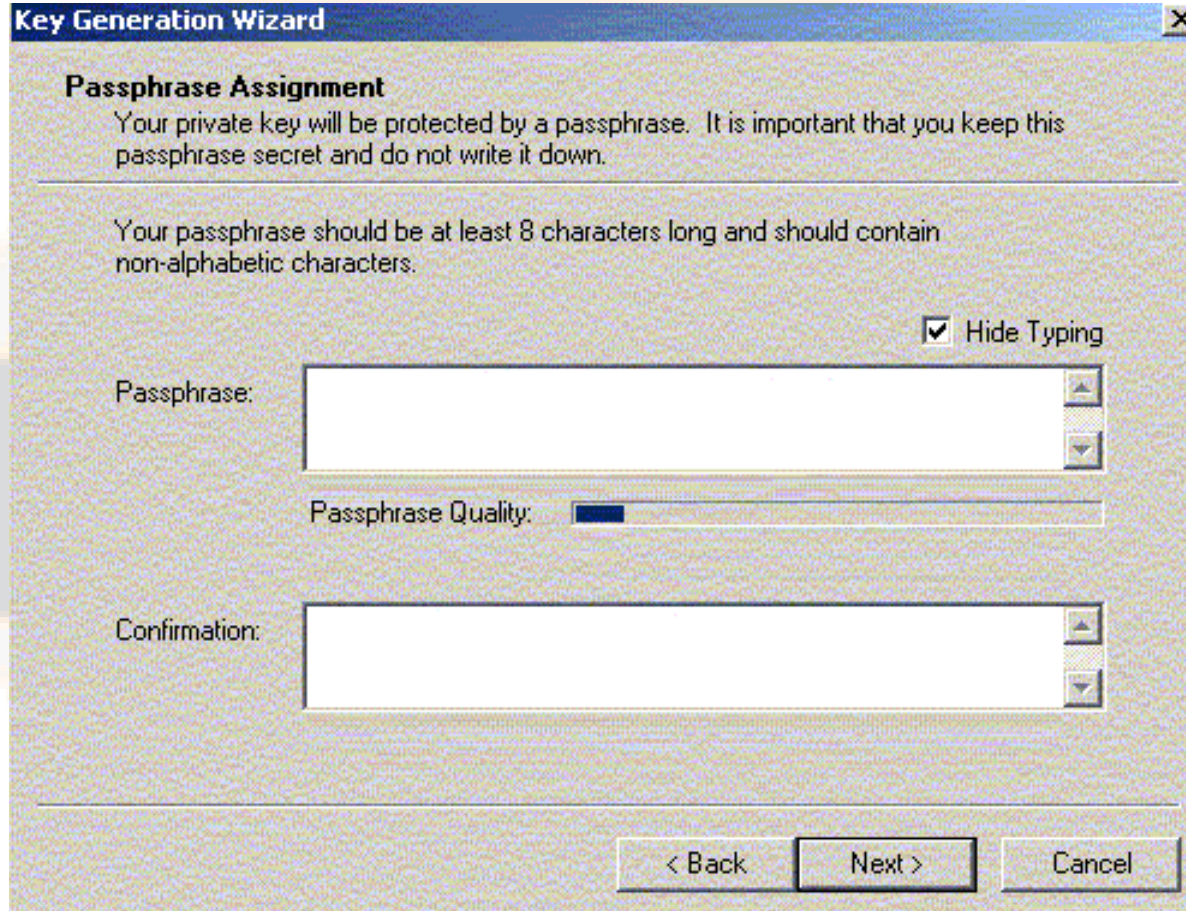
Full name:

By associating an email address with your key pair, you will enable PGP to assist your correspondents in selecting the correct public key when communicating with you.

Email address:

< Back   Next >   Cancel



A screenshot of the 'Key Generation Wizard' dialog box. The title bar says 'Key Generation Wizard'. The main heading is 'Passphrase Assignment'. Below it, a text block says: 'Your private key will be protected by a passphrase. It is important that you keep this passphrase secret and do not write it down.' Another text block below that says: 'Your passphrase should be at least 8 characters long and should contain non-alphabetic characters.' To the right of the first text block is a checkbox labeled 'Hide Typing' which is checked. Below the first text block is a text input field labeled 'Passphrase:'. Below the 'Passphrase:' field is a 'Passphrase Quality:' label followed by a progress bar that is partially filled with blue. Below the progress bar is a text input field labeled 'Confirmation:'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

**Key Generation Wizard**

**Passphrase Assignment**

Your private key will be protected by a passphrase. It is important that you keep this passphrase secret and do not write it down.

Your passphrase should be at least 8 characters long and should contain non-alphabetic characters.

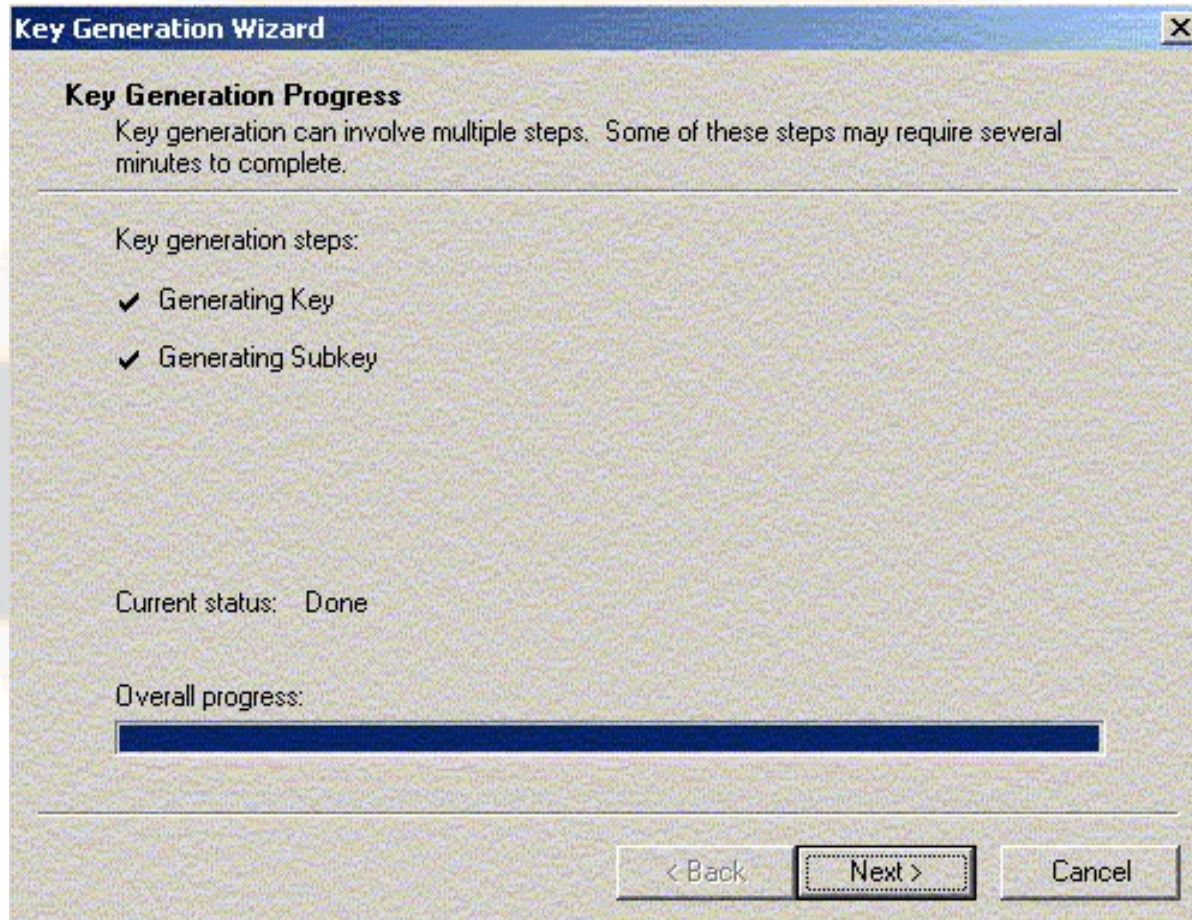
☒ Hide Typing

Passphrase:

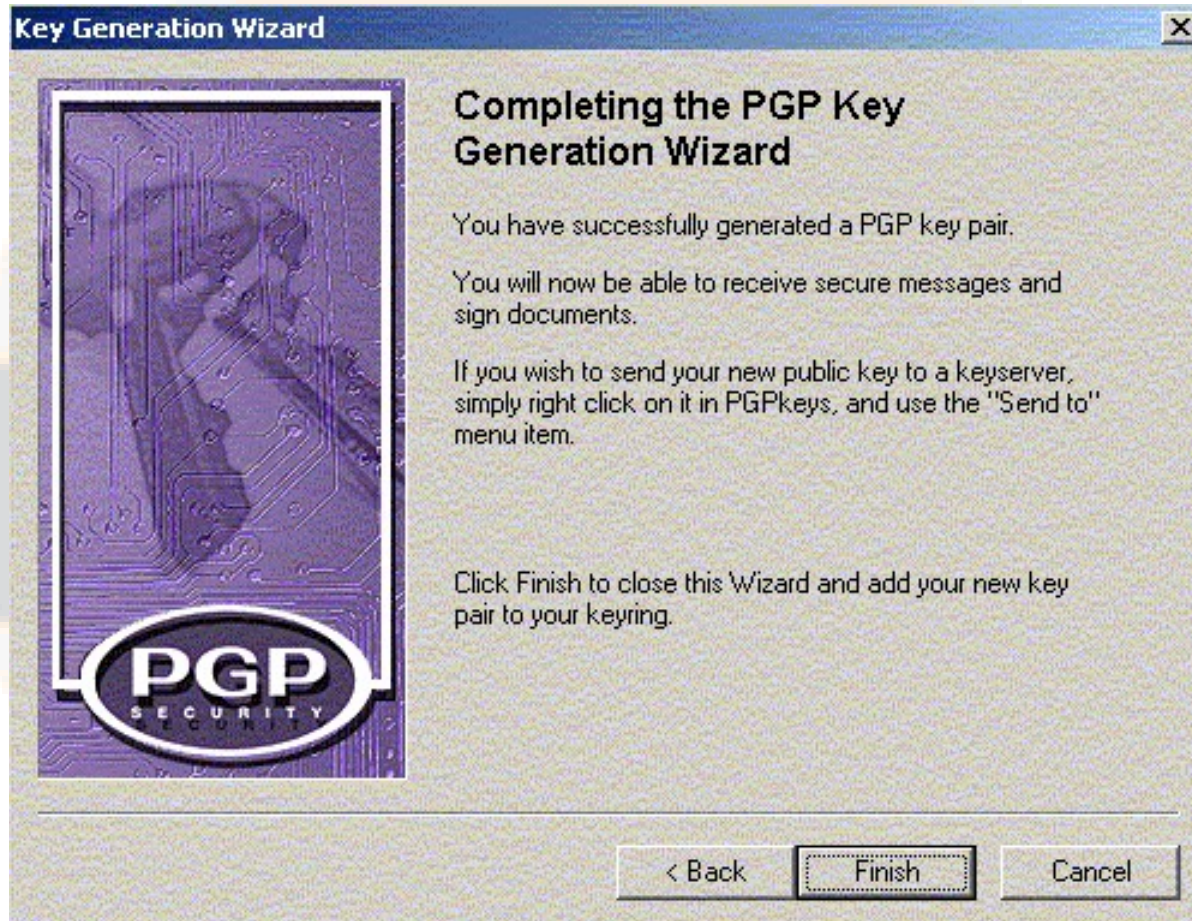
Passphrase Quality:

Confirmation:

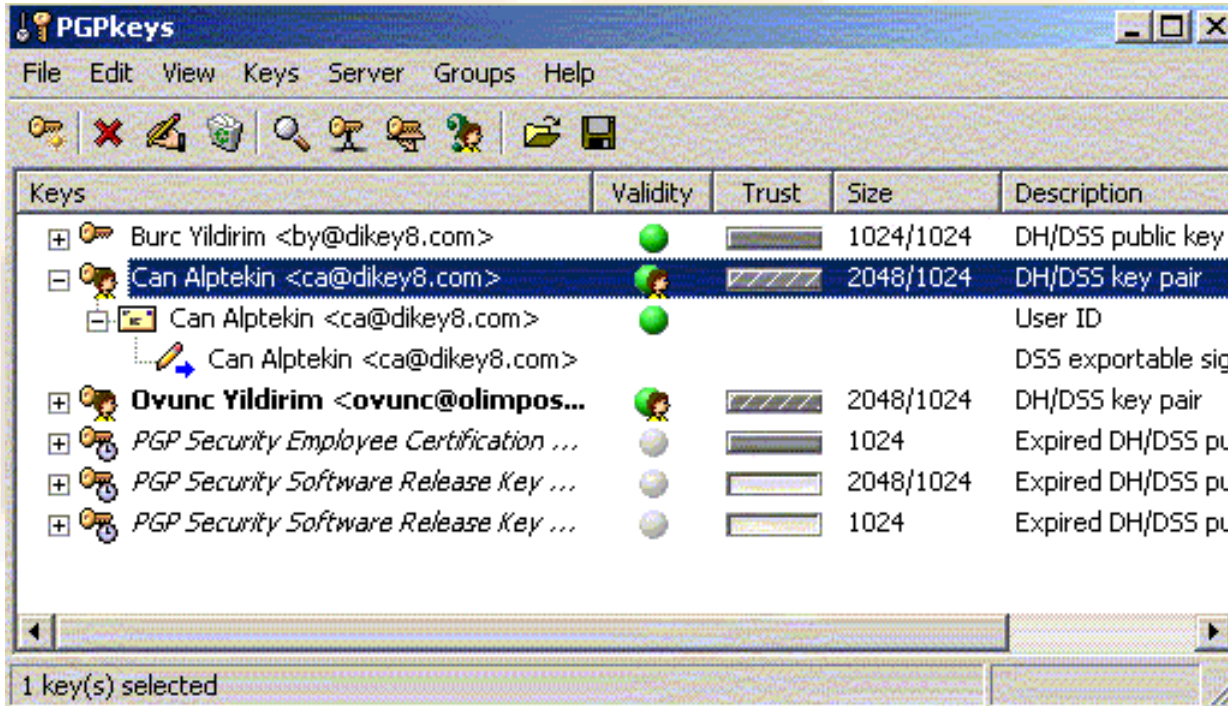
< Back   Next >   Cancel





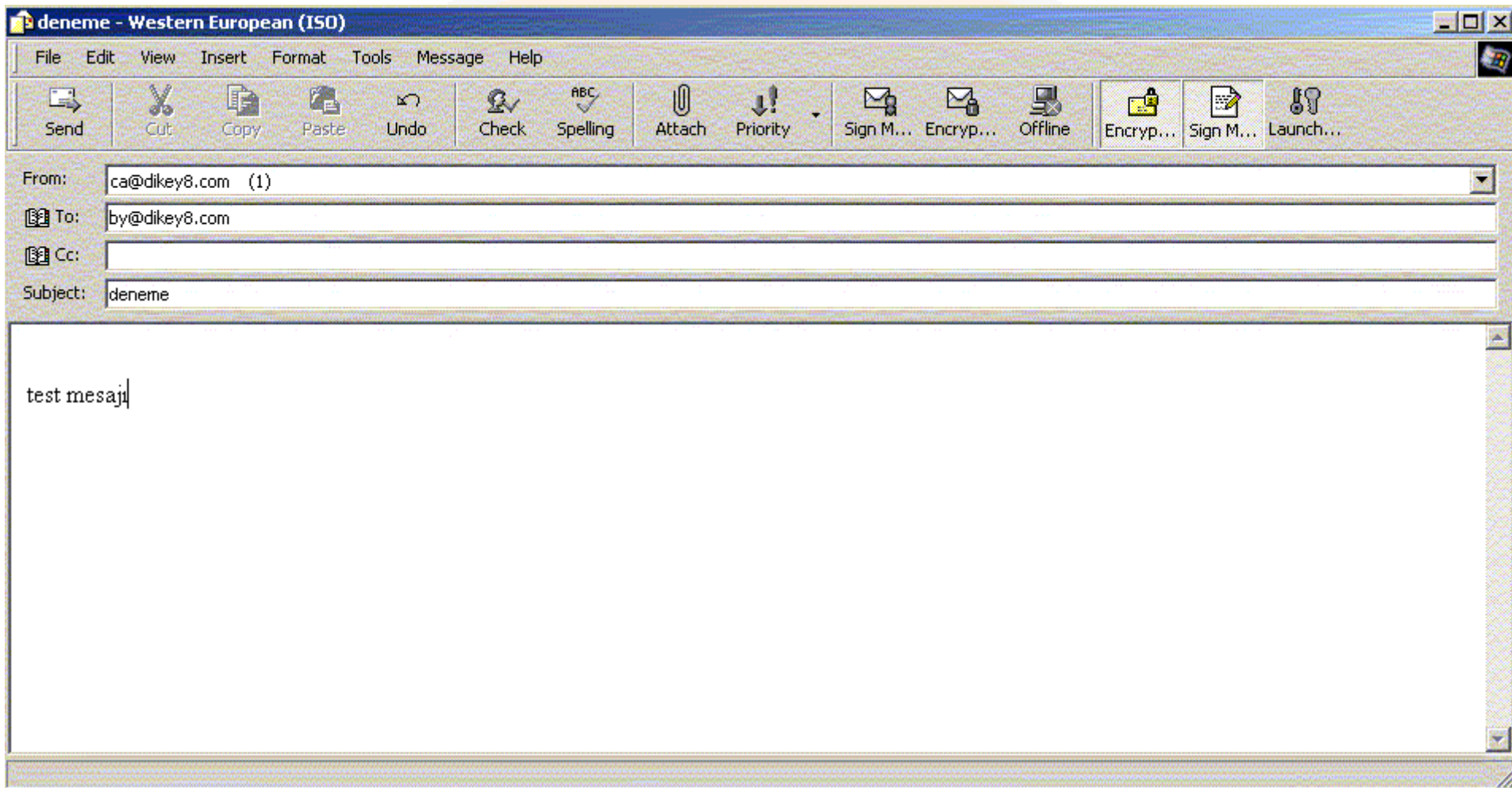


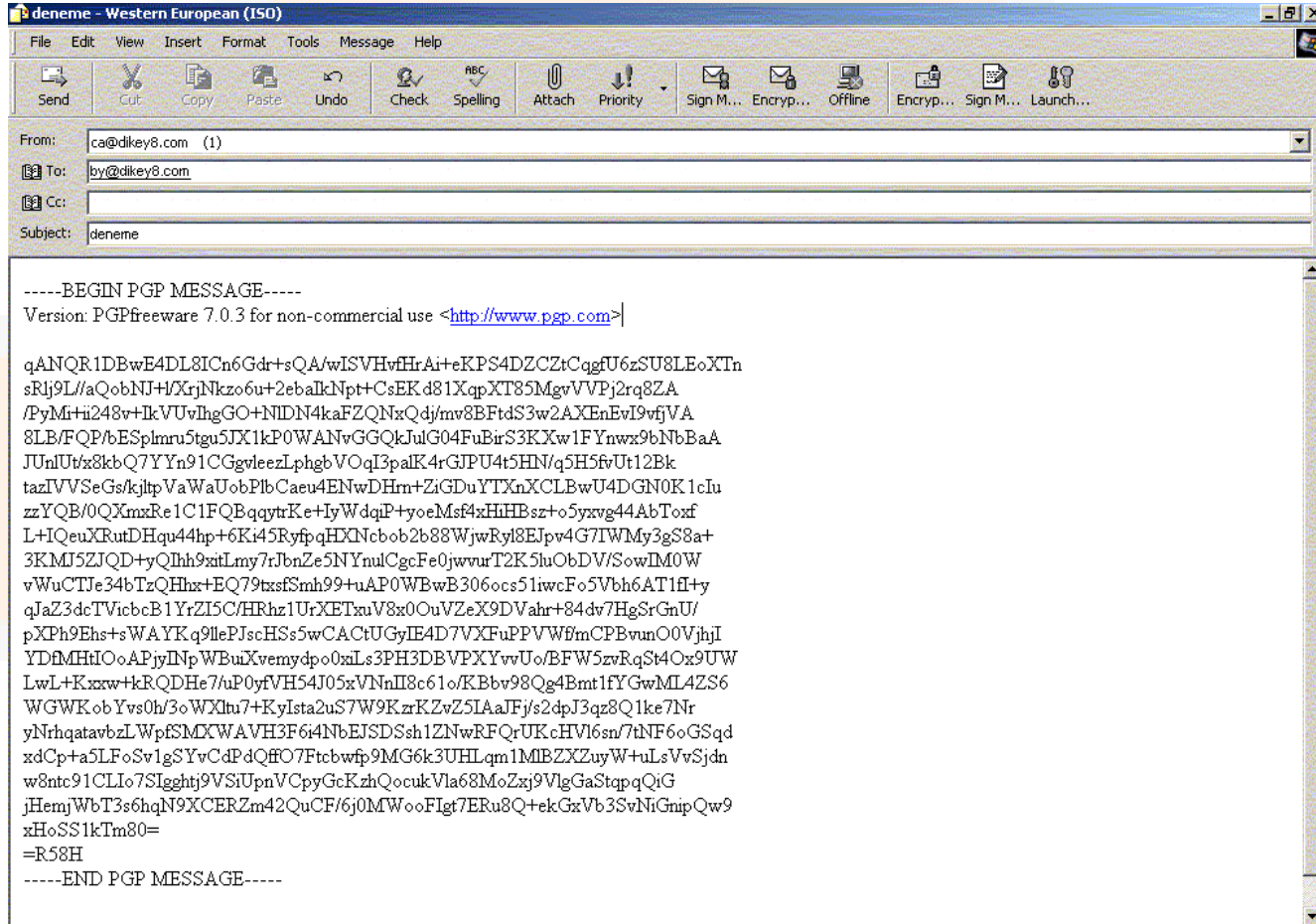






# PGP Uygulaması





**Paranoyak olmak zorundasınız çünkü sizi almaya geliyorlar...**

# PARANOYA (devam)

---

- Sürekli antivirüs programınızı çalıştırın. Eğer sürekli çalıştırma imkanınız yoksa çektiğiniz dosyaları karantinaya alıp, dosyaları çalıştırmadan önce antivirüs programı ile kontrol edin
- Bilmediğiniz dosyalara maksimum şüphe ile yaklaşın
- Makro virüslerine çok dikkat edin
- İnternette dolaşırken çok hassas olun. Bir web ya da FTP sitesi gerçek olamayacak kadar güzel şeyler vaad ediyorsa mutlaka şüphelenin



- “Bilinen Türdeki Dosya Uzantılarını Gizle” seçeneğini iptal edin





A large, faint, light orange watermark of the Dikey8 logo is centered in the background of the slide.

**Teşekkürler**