



UŞAK ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI
KRİPTOGRAFİK KONTROLLER
POLİTİKASI

Doküman No	PLT-025
İlk Yayın Tarihi	01.12.2018
Revizyon Tarihi	
Revizyon No	00
Sayfa No	1 / 2

1. AMAÇ

Bu politikanın amacı bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunmasıdır.

2. KAPSAM

Bu politika, **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı'** nın tüm bilgi varlıklarını kapsar ve uygulanmasından bilgi varlıklarını kullanmakta olan tüm personel sorumludur.

3. SORUMLULUKLAR

Uşak Üniversitesi Sistem ve Ağ Birimi sorumludur.

4. UYGULAMA

Gizlilik: Bilgi, istenmeyen kişiler tarafından anlaşılmalıdır.

Bütünlük: Bir iletinin alıcısı bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir; davetsiz bir misafir doğru iletinin yerine yanlış bir ileti koyma şansına erişmemelidir. Saklanan veya iletilmek istenen bilgi farkına varılmadan değiştirilememeli.

Reddedilemezlik: Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkar edememeli. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu yanlışlıkla reddetmemelidir.

Kimlik Belirleme: Gönderen ve alıcı, birbirlerinin kimliklerini doğrulayabilirler. Davetsiz bir misafir başkasının kimliğine bürünme şansına erişmemelidir.

Kriptografik Yöntemlere Güven: Kriptografik yöntemler, bilgi ve iletişim sistemlerinin kullanılması için güven oluşturmaktadır.

Özgür Seçim: Kullanılacak kriptografik ürünler, yasalar çerçevesinde özgürce seçilebilmelidir.

Gereksinime Bağlı Gelişme: Kriptografik yöntemler, birey, kurum ve hükümetlerin gereksinim, istem ve sorumluluklarına bağlı olarak gelişmelidirler.

Standartlar: Açık anahtar altyapısı ve şifreleme standartları ulusal ve uluslararası düzeylerde geliştirilmeli ve yaygınlaştırılmalıdır.

Bireysel Gizlilik Hakkı: Ulusal politikalar, bireysel iletişimin gizliliğine ve kişisel bilgilerin korunması gereğine saygı göstermelidir.

Yasal Erişim: Ulusal politikalar, bu kılavuzdaki diğer ilkelerle çelişmemek koşuluyla, şifreli mesajlara ve kişilerin gizli anahtarlarına yasal erişimi öngörebilir.

Yasal Sorumluluk: Kriptografi hizmeti veren ve açık/ gizli anahtarları dağıtma yetkisi taşıyan kuruluşların yasal sorumlulukları açıkça belirlenmelidir.

Uluslararası Eşgüdüm: Ulusal ve uluslararası politikalar, birbirleriyle eşgüdüm içinde oluşturulmalıdır.

Hazırlayan	Kontrol	Onay
Ali AKBULUT	Merter KARACAN	Dr. Veli ÇAPALI



UŞAK ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI
KRİPTOGRAFİK KONTROLLER
POLİTİKASI

Doküman No	PLT-025
İlk Yayın Tarihi	01.12.2018
Revizyon Tarihi	
Revizyon No	00
Sayfa No	2 / 2

Şifreleme/deşifreleme (encryption-decryption) bir bilgisayar ağında veya kişisel bilgisayarlarda haberleşme ya da dosya güvenliğini sağlamak için kullanılır. Bu nedenle günümüzde bilgisayarlarda ya da bilgisayar ağlarında şifrelemenin önemi gün geçtikçe artmaktadır.

E- İmza Kullanımı

Dijital imza, elektronik dokümanları (E-posta, Ms Excel dosyası, Ms Word dosyası gibi) imzalamak için kullanılan ve bu elektronik dokümanı alan kişinin de, gönderen kişinin kim olduğuna emin olmasını ve güvenmesini sağlayan bir elektronik koddur.

Doğal olarak dijital imza güvenilirliği şifrelenmiş olmasından kaynaklanır. Bu sistem, şifrelenmiş verileri gönderen bilgisayar ile bu şifrelemeyi çözebilen alıcı bilgisayar arasında çalışır. Gönderenin şifreleme işlemi ile alıcının doğrulama işlemi verinin güvenli bir kaynaktan geldiğini gösterir. Bu iki taraflı işlem dijital imzayı tamamlar. Dijital imza diğer adıyla elektronik imza ülkemizde 23.01.2004 yılında Resmi Gazetede yayınlanmış ve 23.07.2004'te yürürlüğe girmiş 5070 sayılı Elektronik İmza Kanunu ile de tanımlanmıştır.

Elektronik imza, elle atılan ıslak imza gibi kullanılabilirdiği için, internette her türlü resmi işlemin, hem zamandan hem de kağıt israfından tasarruf edilerek ve elektronik ortamda arşivlenerek yürütülmesini sağlar. Elektronik imza, kamu kuruluşlarıyla yapılan işlemlerde, bankacılık ve sigortacılık işlemlerinde, e-devlet, e-iş ve e-ticaret uygulamalarında, elektronik posta ve kanun kapsamındaki hukuki işlemlerde kullanılabilir. Elektronik imza ile imzalanmış herhangi bir belge bilgisayar ortamında arşivlendiğinden bulunması için zaman harcanmayacaktır. Böylece depolama maliyetleri de yok denecek kadar az olacaktır.

5. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.

Hazırlayan	Kontrol	Onay
Ali AKBULUT	Merter KARACAN	Dr. Veli ÇAPALI