

Kampüs Ağların Elektronik İmzaya

Entegrasyonu için Optimum Çözümler

Okt. Aytuğ Boyacı, Okt. Mustafa Ulaş, Okt. Gürkan Karabatak, Okt. Erhan Akbal

Fırat Üniversitesi, Enformatik Bölümü, 23100, Elazığ

aytugboyaci@firat.edu.tr, mustafaulas@firat.edu.tr, gkarabatak@firat.edu.tr, erhanakbal@firat.edu.tr

Özet: İnternet teknolojilerinin gelişmesi ve band genişliklerinin de internet uygulamalarına imkân sağlaması ile birlikte web tabanlı bir çok uygulama yapılmakta, elektronik imzanın yasallaşması ile birlikte ıslak imza gerektiren işlemler yerlerini elektronik imza'ya bırakmaktadır. Üniversiteler de bu gelişim sürecine entegre olmalıdır. Bu amaçla üniversiteler için geliştirilen uygulamaların elektronik imzaya uyumlu olması gerekmektedir. Bununla birlikte mevcut ağ alt yapısının da geliştirilmesi, güvenli bir elektronik imza entegrasyonu yapılabilmesi için önlemlerin alınması gerekmektedir. Bu makalede üniversitelerin elektronik imzaya geçiş sürecinde yapılması gerekenler, alınması gereken güvenlik önlemleri, kurum içi ve kurum dışı elektronik imzanın dolaşımı aşamasında karşılaşılabilecek sorunlar ve çözümleri hakkında bilgi verilmeye çalışılacaktır.

Anahtar Kelimeler: Elektronik İmza, E-İmza Uygulamaları, Elektronik Sertifika

The Optimum Solution for Electronic Sign Integration to Campus Networks

Abstract: Electronic sign replace the traditional sign because of the improved internet technologies and increased bandwidth provide to build new internet applications and to become law the electronic sign. University must integrate to this development. So with this paper we try to give information about the problem in transition processes, required security precautions and the solutions.

Keywords: Electronic Sign, E-Sign Applications, Electronic Certificate

1. Giriş

İnternet teknolojilerinin gelişmesi ile birlikte bilgi teknolojileri hayatımızın vazgeçilmez bir parçası olmaktadır. İnternetin hızlı bir şekilde yayılması ve mevcut alt yapının da buna paralel olarak gelişmesi ile birlikte internet üzerindeki uygulamalar hızla gelişmekte ve kaynakların optimum kullanımına imkân sağlamaktadır. Bu süreçte üniversitelerde mevcut yazılımlarını kaynakların etkin kullanımı, verimliliğin artması, zaman ve mekân bağımlılığının ortadan kalkması için geliştirmek veya yenilemek durumundadır. Geliştirilen uygulamaların şimdiye kadar bilginin işlenmesi ve depolanması şeklindeki yasaların elektronik imza'ya imkân tanınması ile birlikte kâğıt üzerinde yapı-

labilecek ve ıslak imza gerektiren tüm işlemler artık bilgisayar ortamında yapılabilecektir. Bu bağlamda üniversiteler için geliştirilen uygulamaların da elektronik imza sürecine adaptasyonu ve yeni geliştirilecek uygulamalarında elektronik imza uyumlu olması gerekmektedir.

2. Elektronik İmza Sürecinde Kampüs Ağların Entegrasyonu

Üniversitelerde özellikle kurum içi yazışmalarda ki verimliliğin artması, kaynakların optimum kullanımı, zaman ve mekân bağımlılığının ortadan kaldırılarak kampusler arası yazışmaların hızlandırılması, yazışmaların güvenli bir şekilde arşivlenebilmesi artık bir zorunluluk haline gelmektedir. Bu bağlamda bilgi teknolojinin

gelişmesi ile birlikte bilginin kişilerin yetkileri dâhilinde ve güvenli bir şekilde kontrolü, işlenmesi ve arşivlenmesi önem kazanmaktadır. Yine aynı şekilde yazışmaların da yetkiler dâhilinde güvenli bir şekilde bilgisayar ortamında yapılması da gerekmektedir. Üniversite uygulamalarında bilginin depolanması, işlenmesi ve yazışmaların elektronik ortama taşınması tek bir çatı altında düşünülmesi geren yapılardır. Elektronik imzanın vazgeçilemez özellikleri olan kimlik doğrulama, verinin bir bütün olması, imzanın sonradan inkâr edilemeyecek bir yapıda olması için üniversitelerin bilgisayar, ağ ve uygulama alt yapılarının yeterli düzeyde olması gerekmektedir. Bu amaçla öncelikle yapılması gerekenleri sıralamak gerekirse;

- Kâğıt ortamında yapılan tüm uygulamalar ve tüm iş süreçleri için yazılım standartlarına uygun, modüler bir yapıda tasarlanmış, web tabanlı evrak takip, arşivleme ve dokümantasyon sistemi yazılımı gerçekleştirilmiş olmalıdır.
- Kullanıcıların sistemi kullanırken sorun yaşamayacakları bir yapıda kurumun büyüklüğüne ve büyüme hızına ayak uydurabilecek ağ alt yapısının tamamlanmış olması gerekmektedir.
- Geliştirilecek olan elektronik imza yazılımının kampüsler arası yazışmaları ve kurum dışı yazışmalara imkan tanıyacak bir şekilde uluslar arası belirlenmiş standartlar çerçevesinde tasarlanmalıdır.
- Geliştirilen elektronik imza alt yapısı ile imzalanmış olan evrağın arşivlenmesi için gerekli olan donanımsal alt yapı gerçekleştirilmiş olması gerekmektedir.
- Ağ alt yapısı elektronik imza uygulamasının zaman ve mekan bağımsızlığının gerçekleştirilebilmesi amacı ile sürekli çalışabilir bir yapıda tasarlanması gerekmektedir.
- Elektronik imzanın doğruluğunun takibi yazılım ile gerçekleştirilmiş olsa bile ağ içi ve ağ dışı güvenlik önlemlerinin kurumun güvenlik politikaları ile uyumlu hale getirilmesi gerekmektedir.

- Sistem içerisindeki tüm hareketlerin loglarının tutulması, yapılan tüm işlemlerin belirli aralıklar ile arşivlenmesi son derece önemlidir.
- Gerçekleştirilen evrak takip, arşivleme ve dokümantasyon sistemleri ile elektronik imza yazılımları diğer kurumlar ile entegre olacak şekilde tasarlanmalıdır. Aksi takdirde yapılan tüm uygulamalar kampüs içinde kalacak dış dünya ile entegrasyonunda problemler ortaya çıkacaktır.

3. Elektornik İmza ve Nitelikli Elektronik Sertifika

İçerik yönetim sistemleri işler hale gelen bir üniversite elektronik imza alt yapısının büyük bir bölümünü oluşturmuş demektir. Elektronik imza uygulamasında en önemli nokta şifrelenmiş güvenli bir elektronik imzanın oluşturulması ve verinin değişikliğe uğrayıp uğramadığının tespiti yani imzanın doğruluğunun kanıtlanması durumudur.

Bir elektronik imza uygulamasında elektronik imza ile imzalanmış verinin oluşturulması için takip edilecek işlem adımlarını sıralayacak olursak;

- İmzalanacak veri içerik yönetim sisteminden belli formatlarda alınmalı,
- Alınan veri hash fonksiyonlarından geçirilmeli,
- Verinin özeti oluşturulmalı,
- Nitelikli uluslar arası standartlara uygun ve güvenilir bir elektronik sertifika ile birleştirilmeli,
- Elektronik imzalı veri oluşturulmalıdır.

Oluşturulan elektronik imzalı verinin güvenli bir elektronik imza olabilmesi gereklidir. Kim veya kimler tarafından ne zaman imzalandığı ve kadar süre boyunca imzanın geçerli olduğu sorularının cevabı imzanın geçerliliği açısından elektronik imzanın içinde mutlaka olmalıdır.

Bu amaçla geliştirilecek olan elektronik imza uygulaması gerçeklik ve doğrulama amacı ile,

bir eşinin daha olmaması, oluşturulan elektronik imzanın hiçbir şekilde benzerinin üretilmemesi ve gerektiğinde doğrulama amacı ile imzalayan kişiye gösterilmesine imkan sağlamalıdır.

Verinin güvenliği yazılım ile ve güvenlik algoritmaları ile gerçekleştirilirken, verilerin gizliliği uluslar arası standartla ile belirlenmiş olan şifreleme algoritmaları ile sağlanırken, verinin bütünlüğü ise özetleme fonksiyonları ile sağlanmalıdır.

4. Elektronik İmza Sonrası Güvenlik Önlemleri

Elektronik imza uygulamasının kampuslere entegrasyon sürecinde en önemli noktalardan biriside imzalanmış elektronik verinin güvenli bir şekilde arşivlenmesi ve gerektiği zamanda kullanılabilirliğidir.

Islak imzanın yerini elektronik imzaya bırakması ile bilgisayar ortamına taşınan evrakların güvenliğinin yanında saldırganlar içinde önemli bir saldırı kaynağıdır. Verinin güvenliği amacı ile saldırganın nereden sisteme sızacağını iyi bilmek gerekmektedir. Güvenlik önlemleri alınırken saldırganın olabilecek donanımsal ve yazılımsal imkânlarını ihmal etmemek gerekir.

Güvenlik saldırılarını donanım ve yazılım üzerinden gelebilecek saldırılar olarak gruplandırılmak mümkündür.

Donanım üzerinden gelebilecek saldırılar genellikle gizli anahtarın tutulduğu ortamdır.

Yazılım üzerinden gelebilecek saldırılar ise çeşitlilik arz edebilir. Örneğin sayısal imza için gereken ve genellikle yapısı bilinen Hash fonksiyonlarına yönelik saldırılar, Elektronik imza oluşturulurken kullanılan asal sayının veya kriptolamanın zayıflığı olarak sıralanabilir.

5. Sonuç

Bilgi teknolojilerinin hızla gelişmesinin kaçınılmaz bir sonucu olan elektronik imzaya geçiş sürecinde üniversitelerin öncü bir rol alması gerekmektedir. Bu bağlamda öncelikle üniversiteler mevcut ağ alt yapılarını hazırlamalı, tüm evrak işlem ve süreçlerini bilgisayar ortamına belli standartlar çerçevesinde geçirmeli, İçerik yönetim, arşiv ve dokümantasyon programlarının elektronik imzaya entegre olabilecek şekilde tasarlamaları gerekmektedir.

6. Kaynaklar

- [1] Elektronik İmza Kanunu, Kanun No:5070, Sayı:25355, 3 Ocak 2004 Tarihli Resmi Gazete, 2004
- [2] Landau S., "Find me a hash", Notices of the AMS, 53 (3):330-2 Mart 2006
- [3] Potter B., "Software and Network Security", Network Security, Cilt: 2004, Sayı: 10, Ekim 2004
- [4] Telekomünikasyon Kurumu, Elektronik İmza ile İlgili Kriterlere İlişkin Tebliğ, 6 Ocak 2006