

KURUMLARÜSTÜ BİLGİ GÜVENLİĞİ STRATEJİSİ

Erhan KUMAŞ

*Türksat Uydu ve Kablo TV Operatörü İşletme A.Ş.,
Bilgi Teknolojileri Direktörlüğü
Konya Yolu 40. Km. Gölbaşı/ANKARA
ekumas@turksat.com.tr*

ÖZET : Yirmibirinci yüzyıla şimdiden damgasını vuran bilgi ve iletişim teknolojileri, yeni bir toplumsal dönüşüme yani “bilgi toplumu”na da zemin oluşturmaktadır. Bilgi toplumuna dönüşümdeki en önemli konu ise bilgini üretilmesi, üretilen bilginin yönetilebilmesi ve güvenliğinin sağlanabilmesi olarak değerlendirilebilir. Bu noktada uzun vadeli projelerin desteklenmesi, ülkemizin bürokratik devletten elektronik devlete geçebilmesinin temel şartı olarak görülmektedir. Yazımıza başlık olan kurumlarüstü bilgi güvenliği stratejisi; ilgili tüm kurum ve kuruluşları bir şemsiye altında toplayabilmeyi hedeflemektedir.

ANAHTAR KELİMELER: *Bilgi Güvenliği, e-Devlet Kapısı, ISO 20000*

SUBJECT OF PAPER

Federal Information Security Strategy

ABSTRACT : Information and Communication Technologies which have already marked 21st century, pave the way for a new social transformation which can also be described as “The Information Society.” The most significant elements in this transformation process are the production of the information, management of the information and maintaining of the security. At this point, supporting long term projects is the key for our Turkey’s transformation from a bureaucratic government to an electronic government. Information security which is the theme of this essay aims to gather all the related institutions and establishments under the same roof.

KEYWORDS : *Information Security, eGovernment Gateway, ISO 20000*

1. GİRİŞ

Küreselleşme olgusunun gelişiminde önemli etkisi olan bilgi ve iletişim teknolojilerindeki yenilikler,

ekonomik ve sosyal yaşamın her alanını ve toplumun tüm kesimlerini çeşitli yönlerden etkisi altına almakta; kamu yönetimi yaklaşımlarını, iş dünyasının iş yapma usullerini ve bireylerin yaşamlarını derinden etkilemekte, bir başka ifadeyle toplumsal bir dönüşüme neden olmaktadır. Yirmibirinci yüzyıla şimdiden damgasını vuran bu teknolojiler, yeni bir toplumsal dönüşüme yani “bilgi toplumu”na da zemin oluşturmaktadır.

Türkiye içerisinde uzman olarak kabul görmüş Firmaları veya kişilerin deneyimini kullanarak Bilgi Güvenliği sürecinin değişik parçalarını tamamlayacak şekilde ve üç ayrı tecrübeyi kullanarak süreç içerisinde çapraz kontrol (cross-check) mekanizmasını da kullanarak T.C. devleti ‘nin en iyi altyapısına sahip e-Devlet Kapısı Projesi’ne güvenlik şemsiyesi giydirilebilir kanaatindeyim.

Bu konudaki uzun vadeli strateji önerimiz şekil 1’de görüldüğü üzere olacaktır. Bilgi güvenliği alanında tarafımızca en önemli dört başlık olarak öngörülen;

1. Bilgi Güvenliği,
2. Eğitim İhtiyacının Giderilmesi,
3. Kripto Sistemlerinin Oluşturulması,
4. Güvenlik Altyapısı’nın Kurulması

kavramları üzerinde yoğunlaşarak bir strateji öngörümüz bulunmaktadır. Bu dört ana başlık üzerine; Türksat’a, 28 Temmuz 2006 tarihli resmi gazetede yayımlanan Bilgi Toplum Stratejisi ve Eki Eylem Planı’nda¹ bahsedilen altı ayrı eylem’de yürütecek bir kurum olarak ortaya koyacak olursak gerek ülkemizin bilgi toplumu’na dönüşümü, gerekse altyapı eksikliğinin giderilmesine yönelik çalışmaların baş mimarı olacak olan bir kurumun vizyonu yansıtılmaya çalışılacaktır.

Kurumsal olarak bakış açımıza ilaveten ülkemizin ilk ve orta öğretiminin eğitim müfredatına girdi sağlayarak, MEB ve Üniversitelerle ortak işbirliği

çerçevesinde ülke genelinde ilk ve orta öğretimden lisans ve lisansüstü düzeylere kadar bilgi güvenliği ile ilgili müfredat revizyonu ve farkındalık için girişim ve liderlik rolü üstlenmek uzun vadeli stratejimiz içerisinde yerini almaktadır. T.C. devleti'nin Bilgi Güvenliği Stratejisi genelinde ve kamu kurumları bilgi güvenliği stratejilerinin oluşturulması özelinde rehberlik sağlama

sorumluluğu alma girişimi öngörülmektedir. Bu noktada özel sektörün rekabet açısından ayakta kalmasına da destek olmak amacıyla yurtdışı örneklerinde olduğu gibi devletin vizyonunu ortaya koyabilecek ekiplerle özel sektöre bilgi güvenliği ve alt başlıkları konusunda teknik danışmanlık desteği ve yol gösterme, yönlendirme faaliyetleri yapılması hedeflerimiz içerisinde bulunmaktadır.



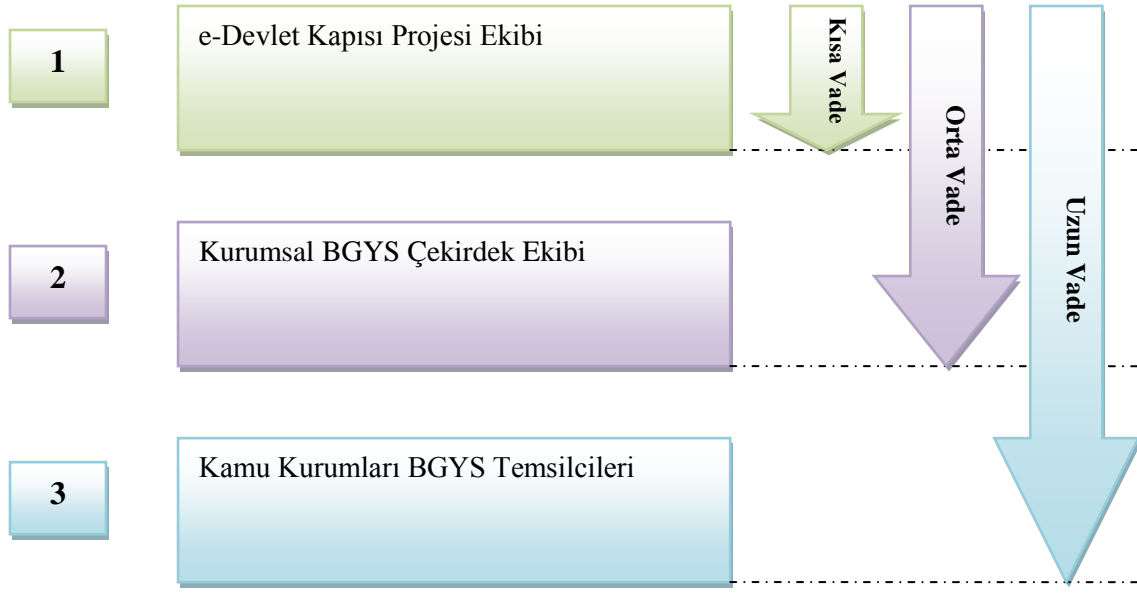
Şekil_1: Kurumlarüstü Bilgi Güvenliği Stratejisi

2. BGYS EĞİTİM STRATEJİSİ, PROJE EKİBİ VE KAMU FARKINDALIĞI

Bilgi güvenliği ve alt başlıkları konusunda gerek ve yeter şartı sağlayacak şekilde bir donanıma sahip olunabilmesinin en önemli adımının bir ekip kurmak olduğu kanaatindeyiz. Bu noktada gerek e-Devlet Kapısı projesi özelinde gerekse Türksat A.Ş.'nin bilgi güvenliği kavramı açısından tatmin edilmesi için, çalışmanın nihayetinde de kamu kurumlarının bu konudaki eksikliklerinin

giderilmesine yönelik oluşturulması gereken ekiplerle ilgili üç aşamalı yayılım önerimiz Şekil_2'deki gibidir.

e-Devlet Kapısı projesi teknik şartnamesi⁴ çerçevesinde öngörülen ve gerek şart olarak sunulan projenin ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi² şartlarına göre dizaynını, altyapı kurulumunu, sürdürülebilirliğini önce e-Devlet Kapısı özelinde sonra kamu kurumları genelinde şöyle yapmayı planlamaktayız;



Şekil_2: BGYS Eğitim ve Farkındalık Stratejisi

1. E-Devlet Kapısı Projesi Ekibi'nin farkındalık eğitimi bakımından daha önce TSE tarafından sağlanan uzmanlar tarafından bir eğitim alınmıştır. Ancak bu farkındalığı bir adım ileriye götürerek bilinçlilik düzeyine çekilmiştir. Burada yapılması gereken ilk adım; konuyla ilgili bir bilgi güvenliği ve risk yönetim ekibi, bilgi güvenliği ve risk yönetim lideri belirleyerek bu tür bir koordinasyonu sağlayabilecek ortam oluşturulmalıdır. Dünya'nın bilginin yönetilmesi ve güvenlik konusunda gittiği yöne gözattığımızda; ISO 9001:2000 (Kalite Yönetim Sistemi), ISO 27001:2005 (Bilgi Güvenliği Yönetim Sistemi), ISO/IEC 20000 (ITIL- Bilgi Teknolojileri Hizmet Yönetimi Sistemi)³ gibi standartlar global düzeyde, Proje teknik şartnamesi ve lokalde de projemizin güvenliğinin sertifikasyon ve teminat altına alınabilmesi amacıyla çalışmalarımızı bu yöne çekmeyi planlamaktayız.
2. Türksat A.Ş altında Bilgi Teknolojileri ve e-Devlet Kurumsal İletişim Direkörlükleri olarak yürüttüğümüz e-Devlet Kapısı Projesi özelinde Bilgi Güvenliği Yönetimi çalışmaları gereği belirli bir farkındalık ve bilinçlilik düzeyi sağlanması planlanmaktadır. Daha sonra da projenin çerçevesini genişleterek şirketimiz bünyesinde yürütmenin uygun olacağını düşünmekteyiz. Zira bir teknoloji şirketi

olarak ürettiğimiz tek ürünün "Bilgi" olduğunu düşünecek olursak mevcut kontrollerin yanısıra güvenliğini uluslararası sertifikalarla taçlandırmayı hedeflemekteyiz. O bakımdan şirketimizde öncelikle orta seviye yöneticiler düzeyinde bir tanıtım toplantısı yapıldıktan sonra, her direktörlükten kendilerini temsil edecek şekilde bilgi güvenliği ile ilginecek bir kişi atamaları istenecektir. Bu atamalardan sonra da bu ekibe ilk etapta kendi içimizde daha sonra da gerekirse ekstra bilinçlendirme eğitimleri ile "Türksat Bilgi Güvenlik Ekibi" nin yetkinlik düzeyinin yükseltilmesi ile sistem kurulunun ilk adımı atılmış olacaktır.

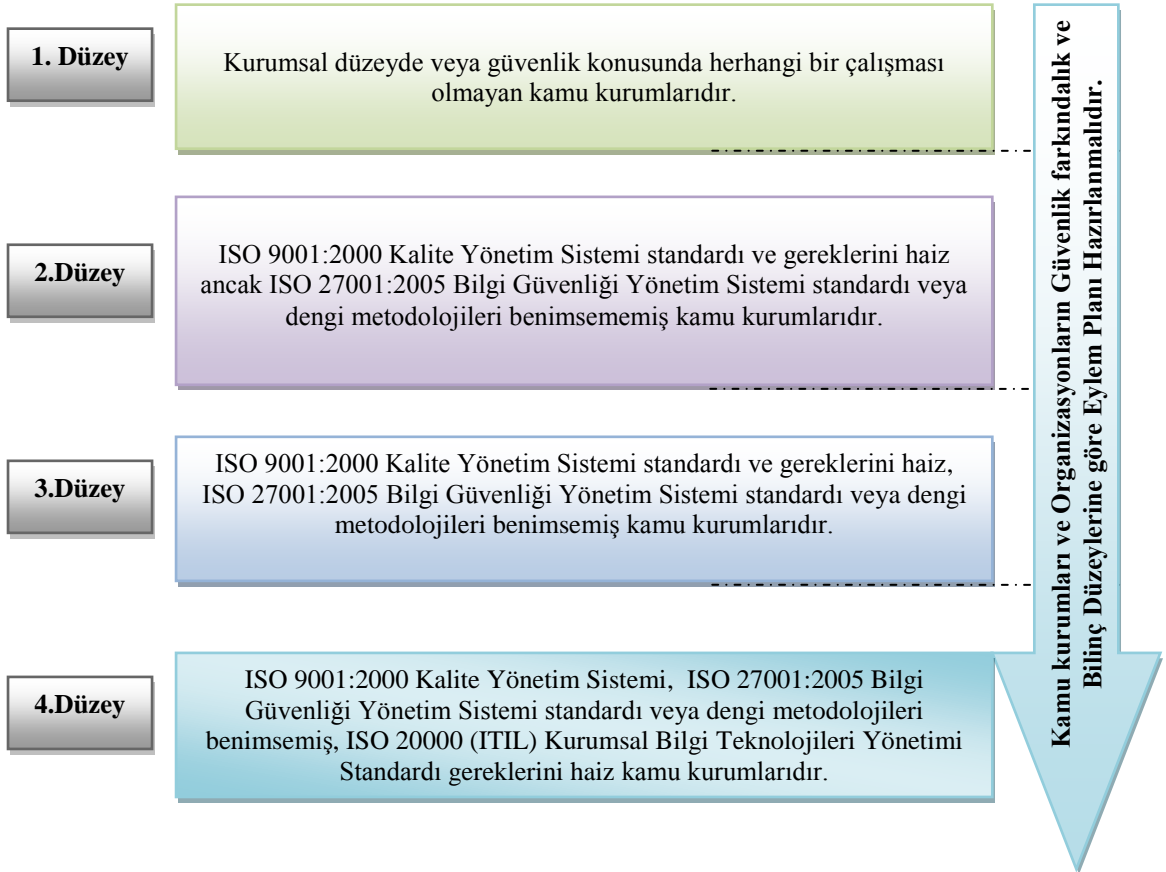
3. Buraya kadar yapılacak güvenlik çalışmalarındaki asıl hedef şirketimizin yaptığı işler gereği bilgi güvenliğinde yakalanması gereken hassasiyeti yönetirken, kamu kurumlarının da yürüttüğümüz proje gereği bu konuda bilinçlendirilmeleri gerekmektedir. İlk pilotunu kendi kurumumuzda yapacağımız güvenlik altyapısının kurulumu çalışmalarında elde edeceğimiz tecrübe ile kurumlarında bilinçlenmesini sağlamış olacağız. Bu konuda proje teknik şartnamesinde bulunan "Güvenlik Komisyonu/Grubu" nun yönlendirilmesinde kurumlara öncelikle bir farkındalık eğitimi, projenin güvenlik konusunda gidişatı ile ilgili bir bilgilendirme sağlandıktan sonra kurum temsilcilerini sağlayarak aynı yöne

koşturabileceğimiz bir strateji ortaya koymayı hedeflemekteyiz. Bu strateji çerçevesinde kurumları yönlendirilmesi ile ilgili olarak Şekil_3’de belirttiğimiz gibi bir seviyelendirmeye tabi tutulacak ve bu seviyelendirme neticesinde;

- I. Düzey : Kurumsal düzeyde veya güvenlik konusunda herhangi bir çalışması olmayan kamu kurumlarıdır.
- II. Düzey: ISO 9001:2000 Kalite Yönetim Sistemi standardı ve gereklerini haiz ancak ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi standardı veya dengi metodolojileri henüz

benimsememiş kamu kurumlarıdır.

- III. Düzey: ISO 9001:2000 Kalite Yönetim Sistemi standardı ve gereklerini haiz, ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi standardı veya dengi metodolojileri benimsemiş kamu kurumlarıdır.
- IV.Düzey: ISO 9001:2000 Kalite Yönetim Sistemi, ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi standardı veya dengi metodolojileri benimsemiş, buna ilaveten ISO 20000 ITIL Bilgi Teknolojileri Hizmet Yönetimi Standardı gereklerini haiz kamu kurumlarıdır.



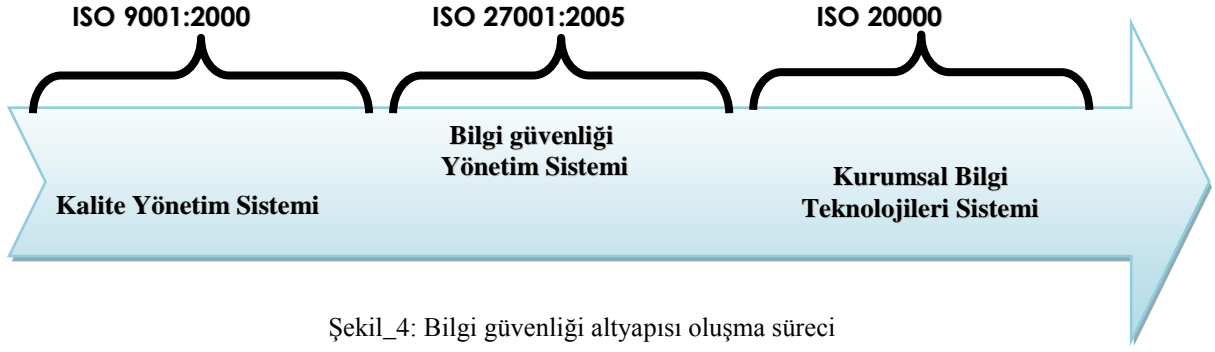
Şekil_3: Kamu Kurumları'nda Güvenlik Farkındalığı

Şekil_4’de gösterilen her düzeye ait;

- Gerekli eğitimler,
- Gerekli kaynak yatırımları,
- Personel istihdamı ve niteliklerinin belirlenmesi,
- Yapılması gereken çalışmalar önceliklendirilmesi,

- Takip edilecek destek standartlar, metodolojilerin belirlenmesi

gibi bazı işlemler bunlarla sınırlı kalmamak kaydıyla yapılması hedeflenmektedir.



Şekil_4: Bilgi güvenliği altyapısı oluşma süreci

Yukarıdaki Şekil_4'de belirtilen süreçte yaşanan farkındalık ve yetkinlik süreci tamamlandığı takdirde bilgi güvenliği ve kurumsallaşma bakımından bir organizasyon % 80 olgunluğunu tamamlamıştır. (Kaplan İ.)⁵

E-Devlet Kapısı Projesi organizasyonunda bulunan ve projenin tüm kamu kurumlarında benimsenmesi ve layıkıyla uygulanabilmesi amacıyla kurulması öngörülen alt komisyonlar bulunmaktadır. Bunlardan “Güvenlik Grubu” nun üstlendiği görev ve sorumluluk önem arz etmektedir. E-Devlet Kapısında güvenlik bütün platforma yayılacak bir katman olacaktır. Güvenlik Grubu güvenlik katmanının tutarlı ve bütün platform için geçerli politikalarını, uygulama esaslarını belirler ve spesifik sistemlerden sorumlu personellerle birlikte uygulaması hedeflenmektedir. Bu bağlamda kamu kurumlarından resmi yollar ile bildirilen kurum temsilcileri, buldukları kurumların güvenlik liderleri olacak şekilde eğitilmeleri konusunda gerekli yönlendirmeleri yapmayı öngörmekteyiz. Yapılacak olan yönlendirmeleri genel olarak sıralayacak olursak;

- Bilgi Güvenliği Ekibinin Kurulması (Güvenlik lideri + Birimlerin temsilcileri)
- Bilgi Güvenliği Ekibinin Eğitilmesi
- Kapsamın Belirlenmesi
- Danışman Seçimi veya Önderlik Etmek
- Pilot bir birim seçilerek şablonların oluşturulması
- Dokümantasyon Çalışmaları ve Belgelendirme Sürecinin Tamamlanması

Yukarıda adım adım anlatılan kurumsal yönlendirme ve farkındalık yaratma çalışmalarına bireysel bazda kamu personellerinin kariyerlerini destekler tarzda bazı sertifikasyon hakları verilecektir. Bu sertifikalar öncelikle Türkiye Cumhuriyeti sınırları içerisinde KPSS (Kamu Personeli Seçme) sınavına ilave puan şeklinde (veya uluslararası anlaşmalar sayesinde daha geniş alanlarda tanınma şansına sahip olabilir) geçerli olacak şekilde yetkinliklerini kanıtlamalarına fırsat verecektir. Türksat A.Ş.’nin Türk Akreditasyon Kurumu ile işbirliği sonucu akredite olması ile

birlikte yurtdışında geçerli sertifikaların sınavlarını yapma ve belgeleyebilme konusunda kamu personeline şans tanınabilmesi de hedeflerimiz içerisinde bulunmaktadır.

3. GÜVENLİK ALTYAPISININ KONTROL EDİLMESİ

Kamu kurumlarının güvenlik düzeyleri Şekil 3’de bahsedildiği gibi kurumların personelleri tarafından yapılacak ilk değerlendirmeler ile belirlenecektir. Ancak buna ilaveten kurumların teknolojik güvenlik altyapısının yeterlilik düzeyi, kullandığı teknolojinin güvenlik zaafiyeti gösterip göstermediği konuları bunlarla sınırlı kalmayacak şekilde değerlendirilerek bir mevcut durum analizi yapılacaktır. Kurumun vatandaşlarına karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların devlete karşı olan hak ve yükümlülükleri karşılıklı olarak yerine getirirken olması gereken asgari güvenlik düzeyleri gözönünde bulundurularak olması gereken duruma ait bir öneri raporu ve aradaki farkı kapatmaya yönelik eylem planı sunulur.

4. KRİPTO SİSTEMLERİ

Kripto sistemlerinin gerek e-Devlet Kapısı projesinde, gerek yukarıda detaylı olarak aktarılan Türksat A.Ş.’nin iş süreçlerinde ve gerekse kamu kurumlarının bilgi güvenliği ve şifreleme açısından ilgili uzmanlar tarafından ortaya konulacak bir metodoloji çerçevesinde geliştirilecek algoritmalarla ülkemize katma değer sağlamayı hedeflemekteyiz.

5. BİLGİ GÜVENLİĞİ

Bilgi, bir kurumun en önemli değerlerinden birisidir ve sürekli korunması gerekir. Bilgi güvenliği sistemi ve yetkili kullanıcıyı yetkisiz erişimlere, bilginin değiştirilmesine ve saldırılara karşı korumak, koruma sırasında gerekli olan kontroller ve ölçümlerin tespiti, dokümantasyon oluşturulması

ve karşı tedbirlerin alınmasını sağlamak hedeflenmektedir.

ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi

- Gizlilik (*Confidentiality*)
 - “Yetkisiz kişilere, süreçlere ve benzeri vb. açıklanmaması yada teslim edilmemesi gerekli veri ya da programların özelliği...” [Bilişim Sözlüğü, Bülent Sankur]⁶
- Bozulmamışlık (*Integrity*)
 - “Programların sistemin ve verilerin kötü niyetli olsun olmasın değiştirilmesi ve bozulmasına karşı korunması ya da korunmuş olması...” [Bilişim Sözlüğü, Bülent Sankur]
- Kullanılabilirlik (*Availability*)
 - “Bir sistem yada özkaynağın gereksinildiğinde kullanıma elverişli olma derecesi...” [Bilişim Sözlüğü, Bülent Sankur]

şeklinde belirtilen üç ana konu üzerinde yükselen bir gerekler bütünüdür.

6. SONUÇ

Ülkemiz gerek bilgi teknolojileri alanında, gerekse bilgi güvenliği alanında elle tutulur bir gelişim sürecinin içerisinde yükselen bir ivme ile hareket etmektedir. Bilgi toplumu stratejisi ve eki eylem planı hepimizin takip ettiği üzere 28 Temmuz 2006 tarihinde resmi gazetede yayımlanarak yürürlüğe girmiştir. Bu noktada Türksat A.Ş.’nin sorumluluğuna 6 eylem verilmiştir. Bu eylemler ile birlikte başlangıçta belirtmiş olduğumuz artan ivme trendinin katma değerini artıran yönde hızlandırarak ülkemizi özlenen ve beklenen; teknoloji üreten günlere taşıyacaktır.

7. TEŞEKKÜR

Bu çalışmayı hazırlamama yardımcı olan Dr. Ahmet KAPLAN, Doç.Dr. Asım BALCI, Mustafa CANLI, Ömer KILIÇ ve tüm e-devlet kapısı projesi çalışanlarına teşekkürlerimi sunarım.

8. KAYNAKLAR

1. Bilgi Toplum Stratejisi ve Eki Eylem Planı, <http://mevzuat.dpt.gov.tr/ypk/2006/38.htm>
2. Türk Standartları Enstitüsü, “Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-

Gereksinimler”, TS ISO / IEC 27001:2005, Mart 2006.

3. Bilgi Teknolojileri Hizmet Yönetimi Sistemi, ISO/IEC 20000 (ITIL)
4. e-Devlet Kapısı Projesi Teknik Şartnamesi.
5. Dr. İbrahim KAPLAN, Dr.kaplan@de.ibm.com
6. Bilişim Sözlüğü, Bülent Sankur
7. Türkiye Bilişim Derneği, TBD Kamu-BİB, “Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0”, Türkiye Bilişim Derneği Yayınları, Mayıs 2006.
8. Türk Standartları Enstitüsü, “Bilgi Teknolojisi- Bilgi Güvenliği Yönetimi için Uygulama Prensipleri”, TS ISO / IEC 17799, 2000.