e-DÖNÜŞÜM TÜRKİYE PROJESİ BİRLİKTE ÇALIŞABİLİRLİK ESASLARI REHBERİ

Sürüm 2.0

BİLGİ TOPLUMU DAİRESİ

www.bilgitoplumu.gov.tr

28 Şubat 2009

DPT Müsteşarlığı Bilgi Toplumu Dairesi koordinasyonunda hazırlanan bu Rehber'e kurumları adına katkıda bulunan Sn. A.Uğur Cebeci (Maliye Bakanlığı), Sn. Aydın Nusret Güçlü (TBV), Sn. Ayşegül İbrişim (TSE), Sn. Bilge Karabacak (TÜBİTAK-UEKAE), Sn. Cafer Canbay (Telekomünikasyon Kurumu), Sn. Demet Kabasakal (Telekomünikasyon Kurumu), Sn. Erkan Tekman (TÜBİTAK-UEKAE), Sn. Erol Tetik (Tapu ve Kadastro Gn.Md.), Sn. Ersel Şengül (TCMB), Sn. Fatih Birinci (TÜBİTAK-UEKAE), Sn. Gökhan Özkan (TBD), Sn. Gülin Atabek (TCMB), Sn. Hakan Özfidan (Başbakanlık), Sn. Haluk Tanrıkulu (Ulaştırma Bakanlığı), Sn. Murat Çolak (TÜRKSAT), Sn. Mustafa Canlı (TÜRKSAT), Sn. Mustafa Musa Ülker (TÜRKSAT), Sn. Savaş Cengiz (MSB), Sn. Selim Gümüş (TCMB), Sn. Tuncay Terzioğlu (TCMB), Sn. Türker Gülüm (TBD), Sn. Umut Barış Erdoğan (TÜBİTAK-UEKAE) ve görüşleri ile katkı sağlayan tüm kurum ve kuruluşlara teşekkür ederiz.

DEVLET PLANLAMA TEŞKİLATI MÜSTEŞARLIĞI
Bilgi Toplumu Dairesi

ÖNSÖZ

Günümüzde bilgi, ya kısıtlı kaynaklar olan emek, sermaye ve doğal kaynakların doğrudan yerini almakta veya emek ve sermayenin niteliğini değiştirmek yoluyla tüm ekonomik aktivitelerde temel girdi olarak kullanılmaktadır. Bilginin üretilmesinin yanı sıra zamanında ve etkin kullanılmasında da bilgi ve iletişim teknolojilerindeki gelişmelerin büyük katkısı bulunmaktadır.

Bilginin, bilgi ve iletişim teknolojileri kullanılarak üretilmesi, iletilmesi, erişilmesi ve etkin olarak kullanılması, küresel rekabet koşullarında ülkelerin rekabet gücünü artırırken, sürdürülebilir ekonomik ve sosyal kalkınmanın vazgeçilmez bir unsuru haline gelmiştir.

1960 yılından bu yana plan, program ve proje hazırlamak konusunda çalışmalar yaparak büyük deneyim kazanmış olan Devlet Planlama Teşkilatı Müsteşarlığı, bilgi toplumu olma yolunda toplumsal bir dönüşüm projesi olarak ele aldığı e-Dönüşüm Türkiye Projesini bu deneyiminden aldığı güçle ve kararlılıkla yürütmektedir. Bahse konu projenin bir bileşeni olan e-devlet bağlamında birbiri ile entegre, etkin, şeffaf ve basitleştirilmiş iş süreçlerine sahip bir devlet yapısının oluşturulması ilkesi ile yürütülen çalışmalarda vatandaşımıza ve iş alemine daha kaliteli ve hızlı kamu hizmeti sunulması amaçlanmıştır.

Bilgi toplumuna giden yolda kamu kurum ve kuruluşlarınca yürütülmekte olan bilgi ve iletişim teknolojileri yatırımlarında temel olarak dikkat edilmesi gereken önemli unsurlardan biri, yapılan yatırımların birlikte çalışabilirlik ihtiyaçları çerçevesinde birbiri ile uyumlu yapılar oluşturması ve bunun devamında da entegrasyonu kolay ve mümkün çözümlerin üretilerek ülke yararına kullanılmasıdır. Birlikte çalışabilirliğin en vazgeçilmez unsuru standartların kullanımının sağlanmasıdır. Kamudaki birlikte çalışabilirlik ihtiyaçlarını en geniş anlamda ele alarak uyulması gereken standartları ortaya koymak doğru ve birlikte çalışabilir sistemler oluşturmanın önemli bir adımıdır.

Bu amaçla Devlet Planlama Teşkilatı Müsteşarlığı koordinasyonunda katılımcı bir yaklaşımla hazırlanan ve ilk sürümü Ağustos 2005'te yayımlanan bu Rehber'in kamu bilgi ve iletişim teknolojileri yatırımlarının etkinliği açısından büyük yarar sağladığı kanaatindeyim. e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (KDEP) "Birlikte çalışabilirlik esaslarının belirlenmesi ve rehber yayımlanması" eylemi çerçevesinde Devlet Planlama Teşkilatı Müsteşarlığı koordinasyonunda kamu, özel kesim ve sivil toplum kuruluşlarından katkı verebilecek tüm ilgililere ulaşılmaya azami gayret gösterilerek hazırlanan Rehber, teknik unsurlar içermesi nedeni ile zaman içinde sürekli gelişecek, genişleyecek ve yeniliklere uyum sağlayacak olup, toplumun tüm kesimlerinin katkısına açık bir belge niteliğindedir. Bu çerçevede, Rehber'in yeni sürümünde de bu ilkelere bağlı kalınmış ve katılımcı bir yaklaşımla güncellemeler yapılmıştır.

Devlet Planlama Teşkilatı Müsteşarlığı, bilgi ve iletişim teknolojileri alanındaki kamu yatırımlarının ülkemiz ihtiyaç ve öncelikleri doğrultusunda planlanmasını ve yürütülmesini sağlamak açısından bu Rehber'in hayata geçirilmesine büyük önem vermektedir. Bu amaçla, kamuya ait tüm bilgi ve iletişim teknolojisi yatırımlarının Rehber'e uyumlu olması zorunlu tutulmuştur.

2006-2010 yıllarını kapsayan ve bir dönüşüm stratejisi olarak hazırlanan Bilgi Toplumu Stratejisi ve Eylem Planında da Rehber'i tamamlayıcı nitelikte ve Rehberde yer alan esas ve standartların etkin olarak uygulanacağı kurumsal ve merkezi çözümlere yönelik eylemlere yer verilmiştir.

Rehber'in hazırlanmasında ve güncellenmesinde katkısı bulunan tüm kamu, özel sektör ve sivil toplum kuruluşlarına gayretlerinden ötürü teşekkür ediyor, çalışmalarında başarılar diliyorum.

Halil İbrahim AKÇA
Müsteşar V.

GENELGE

Başbakanlıktan:
Konu : Kamu Bilgi Sistemlerinde Birlikte Çalışabilirlik Esasları.

GENELGE
2009/4[1]

Bilgi toplumuna dönüşümü amaçlayan e-Dönüşüm Türkiye Projesi'nin önemli bir bileşeni olan e-devlet; birbiri ile entegre olmuş, etkin, şeffaf ve basitleştirilmiş iş süreçlerine sahip bir yapılanma gerektirmektedir. Bu çerçevede; birlikte çalışabilirliği mümkün kılmanın en temel araçlarından birisi, kurumların kullanacakları ortak norm ve standartları belirleyerek bilgi sistemlerini ve entegre e-devlet hizmetlerini bu norm ve standartlar çerçevesinde geliştirmektir.

Birlikte Çalışabilirlik Esasları Rehberi, e-Dönüşüm Türkiye Projesi kapsamında; başta kamu kurum ve kuruluşları olmak üzere, kamuya elektronik ortamda hizmet sunan tüm kuruluşlar arasında birlikte çalışılabilirliğin sağlanması ve bu çerçevede; yetki ve sorumluluklar, esas ve prensipler, yöntem ve kriterler ile teknik standartların belirlenmesine yöneliktir.

Merkezi ve yerel düzeydeki tüm kamu kurum ve kuruluşlarınca yeni kurulacak bilgi sistemlerinde, Rehber'de yer verilen esas ve standartlara uyulması zorunludur. Halihazırda kullanılan bilgi teknolojisi altyapılarının Rehber'de belirtilen standartlara uyumlu olmayan unsurları, bütçe imkanları ve öncelikler çerçevesinde en kısa zamanda bu esaslara uyumlu hale getirilecektir.

Rehber, önümüzdeki dönemde Devlet Planlama Teşkilatı Müsteşarlığı koordinasyonunda, bilgi ve desteğine ihtiyaç duyulan tüm kamu kurum ve kuruluşları tarafından gereken destek ve katkı sağlanarak "Rehber Güncelleme" başlığı altında belirtilen esaslar çerçevesinde güncellenmeye devam edilerek, www.bilgitoplumu.gov.tr adresinde yayımlanacak, uyum çalışmalarında ve yeni kurulacak bilgi sistemlerinde, belirtilen adreste yayımlanan güncel sürüm dikkate alınacaktır.

4/8/2005 tarihli ve 2005/20 sayılı Genelge ve ekinde yer alan rehber yürürlükten kaldırılmıştır.

Bilgilerini ve gereğini rica ederim.

Recep Tayyip ERDOĞAN
Başbakan

[1] 28 Şubat 2009 tarihli ve 27155 sayılı Resmi Gazete'de yayımlanmıştır.

İÇİNDEKİLER

BİRİNCİ BÖLÜM

BİRİNCİ BÖLÜM

1 GİRİŞ

e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (KDEP)'nda yer alan 34 no'lu "Birlikte çalışabilirlik esaslarının belirlenmesi ve rehber yayımlanması" eylemi çerçevesinde Devlet Planlama Teşkilatı Müsteşarlığı koordinasyonunda hazırlanan bu Rehber, kamu, özel sektör ve sivil toplum kuruluşlarının katkıları ile şekillenmiş olup, yine aynı kurum ve kuruluşların katkıları ile güncelleme ve geliştirmeye devam edilmektedir.

Rehber'de; 6 temel konuda esaslar ve kullanılacak standartlar belirlenmiştir. Bunlar; dosya (veri) sunumu ve değişimi, ara bağlantı, süreç ve veri entegrasyonu ve içerik yönetimi, güvenlik, coğrafi bilgi sistemleri ve çözüm yaşam döngüsüne ilişkindir. Rehber'de kapsanan konular, elektronik devlet hizmetlerinin sunumunda kamu kurum ve kuruluşlarının birlikte çalışabilirliğinin temelini oluşturmakta, arka ofis entegrasyonunun sağlanmasını kolaylaştırarak e-Devlet Kapısının etkinliğini artırmaktadır. Bilgi teknolojisi yatırımlarının geri dönüşü; vatandaş ya da iş dünyası odaklı hizmetlerin sunulabilmesi, devletin etkin bir şekilde işleyişinin sağlanması ve bilgiye dayalı karar verme süreçlerinin iyileştirilmesiyle sağlanacak olup tüm bu hedefler kurumlar arası bilgi paylaşımını gerektirmektedir.

Bu itibarla; Rehber'de yer alan esas ve standartlara tüm kamu kurum ve kuruluşlarının uyum göstermesi büyük önem arz etmektedir. Kamu kurum ve kuruluşlarının bilgi ve iletişim sistemlerine ilişkin donanım, yazılım ve hizmet alımlarında ve bu kapsamda yapılacak yatırım tekliflerinin hazırlanmasında Rehber'e uyumun kural haline getirilmesi için gerekli tedbirler alınmış olup bu amaçla, kamu yatırım tekliflerinin hazırlanmasına ilişkin usul ve esasların belirlendiği "Kamu Bilgi ve İletişim Teknolojisi Projeleri Hazırlama Kılavuzu"nda Rehber'e uyum zorunlu kılınmıştır.

Rehber'in hazırlanmasında, başta Pan-Avrupa e-Devlet Hizmetlerinin sunumuna yönelik olarak çıkarılmış olan Birlikte Çalışabilirlik Çerçevesi birinci sürümü[2] ve yayımlanma aşamasındaki ikinci sürümü olmak üzere bu konuda kapsamlı çalışmalar yapmış ülke örnekleri ve bu ülkelerin yayımladıkları birlikte çalışabilirlik dokümanlarından istifade edilmiştir.

[2] http://europa.eu.int/idabc/3761 adresinden erişilebilir.

2 GENEL ESASLAR

2.1 AMAÇ

Bu Rehber, e-Dönüşüm Türkiye Projesi kapsamında başta kamu kurumları olmak üzere kamuya elektronik ortamda hizmet sunan tüm kurumlar arasında birlikte çalışılabilirliği sağlamak ve bu çerçevede yetki, sorumluluk, esas, prensip, yöntem ve kriterler ile teknik standartları belirlemek amacıyla hazırlanmıştır.

Rehber üç bölümden oluşmaktadır. Birinci bölümde; genel esaslar ve birlikte çalışabilirlik politikası, ikinci bölümde; bilginin sunumu, taşınması, değişimi, entegrasyonu, güvenliği ve geliştirilen çözümlerin yaşam döngülerine ilişkin teknik standartlar belirlenmiştir. Üçüncü bölümde ise önümüzdeki dönemde yürütülecek Rehber'i tamamlayıcı nitelikteki çalışmalara yer verilmektedir.

2.2 KAPSAM

Birlikte çalışabilir e-devlet yapısı farklı gruplar için farklı birlikte çalışabilirlik ihtiyaçları taşır. Bunlardan ilki, sistemin doğrudan kullanıcısı olan ve sistemle ilişkilerden doğrudan etkilenen vatandaştır. İkinci grup iş dünyası olup, veri değişimi ihtiyaçları bir öncekine göre daha karmaşıktır.

Rehber'in odak noktası; kamunun, gerek merkezi kurum ve kuruluşları, gerekse yerel yönetimleri içerecek şekilde, kendi içinde birlikte çalışabilirliğinin sağlanması ve buna karşılık gelen ihtiyaçların belirlenmesi ve karşılanmasıdır.

2.3 TANIMLAR ve KISALTMALAR

Bu Rehber'de kullanılan terimlere ilişkin tanımlar EK-B'de verilmektedir.

Bu Rehber'de kullanılan kısaltmalar EK-C'de verilmektedir.

2.4 UYUM MEKANİZMALARI

Kamu kaynaklarıyla yürütülen tüm bilgi teknolojisi yatırımlarında, bu Rehber'de belirtilen esas ve standartlara uyum zorunludur.

Rehber'e uyumu sağlamak üzere, Yatırım Programlarında izlenen bilgi teknolojileri projeleri için e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planında yer alan "Kamu bilgi ve iletişim teknolojileri yatırım projeleri hazırlama ve değerlendirme kılavuzlarının hazırlanması ve bu projelerin izlenmesine ilişkin usul ve esasların belirlenmesi" eylemi çerçevesinde hazırlanan ve her yıl güncellenen Kamu Bilgi ve İletişim Teknolojisi Projeleri Hazırlama Kılavuzunda, Birlikte Çalışabilirlik Esasları Rehber'ine atıfta bulunularak, bu esaslara uyum zorunlu tutulmuştur.

Ayrıca, kamu ihale mevzuatında da Rehber'e atıf yapılması ve tüm kamu bilgi ve iletişim teknolojisi ihaleleri şartname ve sözleşmelerine ilişkin yol gösterici dokümanlarda bu Rehber'deki esaslara uyumun zorunlu kılınması, bu alanda yapılacak kamu yatırımlarında etkinliğin artırılması açısından kritik önem arz etmektedir.

2.5 YETKİ ve SORUMLULUKLAR

Merkezi ve yerel düzeydeki tüm kamu kurum ve kuruluşları, bu Rehber'de yer alan esaslara uymakla yükümlüdür.

Rehber'in uygulanmasına ilişkin genel koordinasyon DPT Müsteşarlığı tarafından yürütülecektir.

2.6 GÜNCELLEME

Rehber'in birinci bölümünü oluşturan genel esaslar ve birlikte çalışabilirlik politikası, mevcut sürümün yürürlükte olduğu süre içinde gelen görüş ve öneriler dikkate alınarak, ihtiyaç duyulması halinde DPT Müsteşarlığı tarafından, yılda bir kez güncellenecektir.

Dokümanın birinci bölümüne ilişkin her türlü görüş ve öneri "birliktecalis@dpt.gov.tr" adresine e-posta yolu ile ya da DPT Müsteşarlığına yazılı olarak iletilebilir.

Dokümanın ikinci bölümünü oluşturan verinin sunumu, taşınması, değişimi, entegrasyonu, güvenliği, coğrafi bilgi sistemleri ve çözüm yaşam döngüsüne ilişkin teknik standartlar, acil ihtiyaç bildirilmesi durumunda ya da yılda bir yapılacak gözden geçirmeler sonucu ihtiyaç görüldüğünde günün koşullarına uyumlu hale getirilmek üzere ilgili kurum ve kuruluşların da katkısı ile güncellenecektir. Güncellemeler bu Rehber'i hazırlayan "Birlikte Çalışabilirlik Çalışma Grubu" tarafından yapılacaktır. İhtiyaç duyulması halinde bu çalışma grubu, görüş bildiren ve önerilerde bulunan kamu kurum ve kuruluşları başta olmak üzere, ilgili tüm kesimlerin katılımıyla genişletilecektir.

Dokümanın ikinci bölümüne ilişkin her türlü öneri "birliktecalis@dpt.gov.tr" adresine e-posta yolu ile ya da DPT Müsteşarlığına yazılı olarak iletilebilir.

Gerekli görülen güncellemeleri yapma görev ve yetkisi DPT Müsteşarlığına aittir.

3 BİRLİKTE ÇALIŞABİLİRLİK POLİTİKASI

3.1 GİRİŞ

Yasal çerçevesi belirlenmiş sınırlar içerisinde, arka planda kurumlar arası etkileşimin sağlandığı ve vatandaşa dönük yüzünde tek bir organizasyonmuş gibi davranabilen modern ve bütünleşik e-devlet yapısı, birbiriyle uyumlu, birlikte çalışabilir, etkileşimli, izlenebilir, güvenli, güvenilir ve denetlenebilir bilgi sistemlerine ihtiyaç duyar. Bilginin kurumlar arasında ve bilgi sistemlerinde kullanılabilme ve transfer edilebilme yeteneği olarak açıklanabilecek birlikte çalışabilirliğin en geniş kapsamdaki tanımı, etkin bilgi paylaşımıdır.

Birlikte çalışabilirlik; "bir sistemin ya da sürecin, ortak standartlar çerçevesinde bir diğer sistemin ya da sürecin bilgisini ve/veya işlevlerini kullanabilme yeteneği" olarak da ifade edilmektedir[3].

[3] Burada yer verilen tanım, 2004 yılında European Public Administration Network eGovernment Working Group tarafından hazırlanan "Key Principles of an Interoperability Architecture" adlı çalışmadan alınmıştır. (Kaynak: http://europa.eu.int/idabc/servlets/Doc?id=24117).

e-Devlet kapsamında birlikte çalışabilirliği sağlamaya yönelik faaliyetlerin amacı, düzenleyici rol üstlenerek, kamuda etkin bilgi paylaşımını sağlamak ve böylelikle bir yandan bilgi teknolojilerine yapılan yatırımların geri dönüşünü hızlandırmak, diğer yandan da vatandaşlarımıza bütünleşik kamu hizmetleri sunmak ve kullanıcı memnuniyetini artırmaktır. Çünkü, bilgi ve iletişim teknolojilerinden yararlanılarak başarılması hedeflenen iki temel konu; kamu hizmetlerinin vatandaş (daha genel tanımla "kullanıcı") ihtiyaçları gözetilerek sunumu ve gelişmiş karar destek süreçlerinin tesisidir ki, bu amaçlara ancak doğru, güncel, eksiksiz bilginin ilgili kamu kurum ve kuruluşları arasında güvenli, güvenilir ve etkin bir şekilde paylaşılması yoluyla ulaşılabilir.

Birlikte çalışabilirlik ihtiyaçları teknik, organizasyonel ve anlamsal olmak üzere üç boyutta incelenebilir. Teknik boyutta farklı uygulamalar arasında bilgi paylaşımını mümkün kılacak teknolojilere odaklanılırken, organizasyonel boyut teknolojilerden çok süreç modelleme dilleri, nesneye dayalı yazılım mühendisliği gibi mühendislik metodojilerine dayalıdır. Organizasyonel birlikte çalışabilirlik kapsamında, kurumlara ait iş süreçlerinin ilişkili diğer kurumları da içerecek şekilde modellenmesiyle ilgilenilir ve kurumların amaçları ile teknik altyapıyı şekillendiren uygulama ve sistemler arasında bütünlük, diğer bir ifadeyle, paylaşılan bilginin daha etkin olarak değişimini sağlayacak şekilde oluşturulmuş iş süreçleri ve buna uygun kurumsal yapılanma hedeflenir. Ayrıca, süreçlerin yeniden mühendisliği, kurum içi ve kurumlar arasında iş akış yönetimi, süreç ve hizmetler için ihtiyaçların belirlenmesi gibi konuları içerir. Anlamsal birlikte çalışabilirlik kapsamında ise verinin, onu üreten kurumun dışındaki kurumlar tarafından da doğru şekilde anlaşılması ve yorumlanmasına yönelik çalışmalar yer alır.

Tüm kurumların e-devlet stratejilerini uygularken benimseyecekleri temel standartları içeren ve uygulama düzeyinde birlikte çalışabilirliği hedefleyen bu Rehber, değişen teknoloji ve ihtiyaçların şekillendireceği yaşayan bir doküman olarak değerlendirilmekte olup zaman içerisinde geliştirilmeye ve güncellenmeye devam edilecektir.

Hazırlanan esaslar, üç boyutlu birlikte çalışabilirlik ihtiyaçları içerisinde teknik boyutu kapsamakta olup, kurumların uyacağı asgari müşterek standartlar vasıtasıyla uygulama düzeyinde birlikte çalışabilirliğin gerçekleştirilebilmesine imkan tanıması, daha üst katmanlarda (anlamsal ve organizasyonel) ihtiyaçların karşılanabilmesinde kullanılacak araçları ortaya koyması, yapılacak yatırımlarda uyulacak asgari müşterek standartların belirlenmesi gibi yararlar sağlamaktadır.

Kamu Kurum ve Kuruluşları tarafından elektronik ortamda sunulacak ve e-Devlet Ana Kapısı Projesi kapsamında ortak platformdan erişilecek kamu hizmetlerinin ve organizasyonel ihtiyaçların belirlenmesi ile bu hizmetlere ilişkin iş süreçlerinin modellenmesi ve uygulamaların geliştirilmesi çalışmaları bu Rehber'in kapsamında olmayıp, hizmet veren kurum ve kuruluşlar tarafından bu Rehber'de belirtilen politika ve standartlar esas alınarak yapılacaktır.

e-Dönüşüm Türkiye Projesi eylem planları içerisinde ele alınan eylemler aracılığı ile anlamsal birlikte çalışabilirlik ihtiyaçları ve atılması gereken adımlar konusunda farkındalık yaratılmaya çalışılmıştır. 2006-2010 yıllarını kapsayan Bilgi Toplumu Stratejisi ve eki Eylem Planı kapsamında özelikle kurumsal mimari önerileri ve merkezi erişim çözümleri geliştirilmesini öngören eylemlere yer verilmiştir. Önümüzdeki dönemde e-Dönüşüm Türkiye Projesi kapsamında bu alanda yürütülecek kamu hizmetleri sunumuna yönelik eylemler Rehber'deki esaslar çerçevesinde eylemlerden sorumlu kuruluşlar tarafından üstlenilecektir.

3.2 POLİTİKA

Normlar ve standartlar, farklı sistemlerin birbirleriyle anlaşabilmesini sağlayacak yöntemi ortaya koyarlar. Bu standartların, bir taraftan birlikte çalışmayı mümkün kılarken, diğer taraftan da kurumlara hareket serbestliği kazandıracak ve rekabet ortamı yaratacak şekilde belirlenmesi esastır. Standartlar belirlenirken, gözönünde bulundurulan ve mevcut durumun izin verdiği ölçüde uyulan esaslar aşağıda ifade edilmektedir.

3.2.1 Avrupa Komisyonu Çalışmalarıyla Uyum

Esaslar belirlenirken, Avrupa Komisyonu çalışmalarıyla uyum gözetilmiş, "İdareler Arası Veri Değişimi Programı (IDA)" yeni adıyla "pan-Avrupa Hizmetlerinin İdareler, İş Dünyası ve Vatandaşlara Birlikte Çalışır Sunumu Programı (IDABC)" kapsamında yürütülen çalışmalar ve hazırlanan raporlardan yararlanılmıştır. Bundaki sonraki çalışmalarda da başta Standartlar ve Belirtimler için Ortak Değerlendirme Yöntemleri (CAMSS – Common Assesment Methods for Standards and Specifications) grubu olmak üzere IDABC altında yer alan gruplar bünyesinde sürdürülmekte olan çalışmalardan yararlanılacaktır.

3.2.2 Ana İletişim Mekanizması Olarak İnternet ve www'in Kullanımı

Hedef, küresel İnternet devriminde maliyeti ve riski düşürebilmek, İnternet'in tüm taraflarca aktif olarak kullanımını sağlamaktır. Bu amaçla geliştirilecek uygulamaların arayüz olarak W3C standartlarını sağlayan İnternet tarayıcılarını (browser) desteklemesi esastır. Kullanıcı tarafından herhangi bir lisans ücreti gerektirmeyecek şekilde tarayıcı vasıtasıyla indirilebilen eklenti ve aracı yazılımlardan yararlanılabilir.

3.2.3 Eşit Erişim Hakkı

Bilgi ve hizmetlerin web sayfası ve diğer alternatif kanallardan, kullanıcılar için tespit edilen arayüzlerin toplumun tüm fertleri tarafından kolay kullanılabilecek ve kullanıcı tarafında gerekli olabilecek ek ticari yazılımları mümkün olan en alt seviyede tutacak şekilde sunumu hedeflenmektedir.

Bilgiye ve hizmetlere, yasal çerçevede hakkı olan herkesin erişebilmesi esastır. Kamu kurum ve kuruluşları sundukları hizmetlere erişimi sağlamak üzere dezavantajlı vatandaşların da ihtiyaçlarına uygun önlemleri almak konusunda sorumludur. Ayrıca, hizmetlerin sunumunda engelli ve dezavantajlı vatandaşlarımızın kolay kullanımını mümkün kılacak özel önlemler de alınmalıdır.

3.2.4 Güvenlik

Elektronik ortamda sunulan hizmetlerde başarı, güven ortamının sağlanmasına bağlıdır. Bu da, güvenlikle ilgili politika ve düzenlemelerin geliştirilmesini gerektirir. Esaslar belirlenirken, tüm katmanlarda güvenlik ihtiyaçları üzerinde durulacak, uluslararası düzeydeki gelişmelerle, e-Dönüşüm Türkiye Projesi kapsamında teknik altyapı ve bilgi güvenliği ile ilgili olarak yürütülen çalışmaların sonuçları, Rehber'in sürümlerine yansıtılacaktır.

3.2.5 Kişisel Verilerin Korunması

Kişisel verilerin, bilgiyi temin eden kurum dışında diğer kurumlarca kullanılmasında bilgiyi veren kullanıcının izni esastır. Bilgilerin korunmasından ve amacı dışında kullanılmamasından bilgiyi temin eden ve kullanan tüm kurum ve kuruluşlar ortak şekilde sorumludur. Teknoloji seçimlerinde, bu yönde mahremiyeti sağlayıcı çözümlere gidilmelidir.

Kişisel verilerin toplanmasından önce kurum ve kuruluşların, bu verilerin toplanmasının amaçlarını belli etmesi ve sonraki kullanımlarını da bu amaçlarla sınırlı tutması gerekmektedir. Toplanma amacının değişebileceği her durumda da, değişime konu olan amaçların aynı şekilde belirgin olması gereklidir. Mahremiyeti sağlayacak önlemler kullanıcının rahatlıkla okuyabileceği biçimde sunulmalı, ayrıca, mahremiyet ile ilgili kullanıcı tercihi gerektiren durumlarda, hizmet, kullanıcının tercihlerini, bilgi alımı öncesinde tam olarak belirleyebileceği şekilde tasarlanmalıdır.

3.2.6 Açık Standartların ve Uluslararası Standartların Kullanımı

Birlikte çalışabilirliği mümkün kılma ve rekabeti artırma hedefi kapsamında açık standartların kullanımı benimsenmiştir.

Bir standardın açık standart sayılabilmesi için, aşağıda yer alan asgari niteliklere sahip olması gereklidir[4]:

i. Kar amacı gütmeyen bir kuruluş tarafından kabul görmüş ve gelecekte de bu kuruluş tarafından destekleneceği belirtilmiş olmalı, zaman içinde geliştirilmesi ilgili tüm kesimlerin katılabileceği şeffaf bir karar alma sürecinde yapılmalıdır.

ii. İlgili doküman yayımlanmış olmalı ve bedelsiz ya da itibari bir bedelle temin edilebilmelidir. İsteyen herkes tarafından bedelsiz ya da itibari bir bedelle çoğaltılabilir, dağıtılabilir ve kullanılabilir olmalıdır.

iii. Standart üzerindeki fikri haklar (örneğin; patent gibi), geri alınamaz şekilde herhangi bir hak talebinden (röyalti) bağımsız olmalıdır.

iv. Standardın yeniden kullanımı konusunda hiç bir sınırlama olmamalıdır.

3.2.7 Anlamsal Bütünlüğü Sağlayacak Ortak Standartların Kullanımı

Veri değişiminde anlam bütünlüğünü sağlamak ve veri içeriğine ilişkin farklı yorumları engellemek üzere uluslararası standartlar kullanılacaktır.

Anlamsal birlikte çalışabilirlik ihtiyaçlarına uygun e-devlet metaveri standardının, ontoloji depolarının, ortak modelleme (veri, süreç, mesaj), gösterim ve erişim standartlarının kullanımı sağlanacaktır.

3.2.8 Ölçeklenebilirlik

Oluşturulacak yapının değişen ihtiyaçlara cevap verebilecek bir tasarıma sahip olması gerekliliği dikkate alınmıştır.

3.2.9 Bilginin Zaman İçinde Korunumu

Alınan karar ve prosedürleri belgeleyen kayıtların uzun dönemde erişilebilir olması gereklidir. Bu doğrultuda, elektronik belgelere ilişkin formatlar belirlenirken, belgelerde saklanan bilgilerin uzun dönemde erişilebilirliğinden emin olunmalıdır.

[4] European Interoperabilty Framework for Pan-European eGovernment Services, Version 1.0, Interchange of Data between Adminsitrations-IDA, November 2004, p.8.

3.2.10 Katılımcılık Esası

Teknik standartların belirlenmesi sırasında, bu standartlara uymak durumunda olan kurumların katılımı sağlanmalı, karar verme sürecinde şeffaflık gözetilmelidir. Bu çalışmanın temel amacı, kurumların ya da kişilerin münferit ihtiyaçlarının karşılanması yerine, bilgi paylaşımı ihtiyaçlarının karşılanarak kamunun ortak çıkarlarının korunmasıdır. Buna imkan verecek şekilde, esasların yönetiminin, geliştirilmesinin ve uygulanmasının katılımcı ve mümkün olduğunca mutabakata dayalı olması hedeflenmiştir. Bu yaklaşımla hazırlanan Rehber'in güncelleştirilmesi sürecinde de bu yaklaşım izlenmiş ve izlenecek olup, bu bölümün 2.6 başlığında belirtilen güncelleme yöntemi kullanılmaktadır.

İKİNCİ BÖLÜM

İKİNCİ BÖLÜM

Bu bölümde birlikte çalışabilirlik ihtiyaçlarını karşılamaya yönelik olarak kullanılması, uyulması veya sağlanması gereken standartlar altı ana başlık altında değerlendirilmiştir.

Bu bölümde listelenen standart, belirtim (specification) ya da kılavuzlar, aksi belirtilmedikçe "benimsenen" standartlardır. Rehber'de, aynı alanda birden fazla standardın benimsendiği durumlarda, uygun görülecek standart kurumlar tarafından ihtiyaçlar göz önüne alınarak seçilmelidir.

Benimsenen standartların yanında, kurumların tercihine bırakılmış ve kullanılması faydalı olacak standartlar da söz konusudur. Kurumların tercihine bırakılan standartlar için "**kullanılması önerilmektedir**" ifadesi kullanılmıştır.

Rehber'de benimsenmesi için bir takım geliştirmeler ve incelemeler gerektiren standartlar ise aşağıdaki listelerde "**üzerinde çalışılması gerektiği**" şeklinde ifade edilmiştir.

Henüz geliştirilmemiş, ancak geliştirilmesi gereken standartlar "**geliştirilecek**" ibaresi ile belirtilmiştir.

1 DOSYA (VERİ) SUNUMU ve DEĞİŞİMİ

1.1 ESASLAR

Birçok kamu kuruluşu elektronik ortamda kullanıcılara bilgi sunmakta, bilgi sunumu ve değişimi e-devlet uygulamalarının önemli bir bölümünü oluşturmaktadır. Bu açıdan sunulan bilgilere, ilgili tüm taraflar için en az yük getirecek şekilde, kolay erişim sağlanması, etkinliği artırmak ve e-devlet uygulamalarından beklenen faydayı elde etmek için son derece önemlidir. Birlikte çalışabilirlik standartlarının tümünde olduğu gibi, veri sunumu ve değişimi için kullanılacak standartların da belirli bir teknolojiyi öne çıkarmaması, rekabeti önleyecek biçimde belirli ürünlere ya da firmalara bağımlılık yaratmaması ve alternatifli olması e-devlet uygulamalarından etkin şekilde faydalanabilmenin ön koşuludur.

Bu bölümde, elektronik ortamdaki verilerin sunumu ve değişimi için gerekli standartlar ortaya konmuştur. Standartlar belirlenirken dikkat edilen temel noktalar; sunulan bilgilerin kullanıcı tarafında asgari derecede ek yazılım gerektirmesi, kullanılacak araçların mümkün olduğunca açık standartlara dayalı olması ve bu bilgilere farklı platformlardan ulaşılabilmesidir.

1.2 KULLANILACAK STANDARTLAR

Aşağıda veri sunumu ve değişimine ilişkin formatlar belirtilmiştir. Mümkünse, bilgilere farklı araçlarla erişimi kolaylaştırmak amacıyla, aynı dosyanın farklı formatlarda oluşturulmuş sürümlerinin de sunulması önerilmektedir.

1.2.1 Dosya Sıkıştırma ve Arşivleme

Dosya sıkıştırma ve/veya arşivleme için aşağıdaki tabloda yer verilen formatlardan herhangi birisi ya da birkaçı birlikte kullanılabilir.

Bileşen	Standart/Teknoloji	Açıklama
Dosya sıkıştırma ve arşivleme	ZIP (.zip)	
	GZIP (.gz)	
	7ZIP (.7z)	
Arşivleme	TAR (.tar)	

1.2.2 Üzerinde İşlem Yapılmasına İhtiyaç duyulmayan Kelime İşlem, Sunum ve Elektronik Çizelge Belgeleri

Bileşen	Standart/Teknoloji	Açıklama
Üzerinde işlem yapılamayan kelime işlem, sunum ve elektronik çizelge belgeleri	Hypertext File Format v4.01 (.html)	
	Portable Document Format/Archive; PDF/A (.pdf)	ISO/IEC 19005, Türkçe yazı tipleri gömülü olarak saklanmalıdır.

1.2.3 Üzerinde İşlem Yapılabilen Kelime İşlem, Sunum ve Elektronik Çizelge Belgeleri

Üzerinde işlem yapılabilmesine olanak sağlayan kelime işlem, sunum ve elektronik çizelge belgelerinin paylaşımı için aşağıdaki tabloda belirtilen formatlardan en az birinin kullanımı zorunludur. Bunlardan hangisinin kullanılacağına ihtiyaca göre karar verilebilir.

Bileşen	Standart/Teknoloji	Açıklama
Kelime işlem belgeleri	Microsoft Word 97 (.doc)	
	Zengin metin biçimi (.rtf)	
	Düz metin (.txt)	
	OpenDocument (.odt)	ISO/IEC 26300:2006
Sunum belgeleri	Microsoft Powerpoint 97 (.ppt)	
	OpenDocument (.odp)	ISO/IEC 26300:2006
Elektronik çizelge belgeleri	Virgül ile ayrılmış değer (.csv)	sadece değerlerin saklandığı, formüllerin taşınmadığı bir standarttır.
	Microsoft Excel 97 (.xls)	
	OpenDocument (.ods)	ISO/IEC 26300:2006

Bu bölümde belirtilen formatlar ve bu formatlarda belge üretebilen araçlar konusunda daha detaylı bilgiler EK-A'da verilmiştir.

1.2.4 Karakter Kümesi

Bileşen	Standart/Teknoloji	Açıklama
Karakter Kümesi	UNICODE	Unicode standardı ile ISO/IEC 10646-1:2000 standartları birbiri ile uyumludur.
	ISO/IEC 10646-1:2000	

1.2.5 Resim Dosyaları

Kullanım amacına göre aşağıdaki standartlar arasında tercih yapılabilir.

Bileşen	Standart/Teknoloji	Açıklama
Resim Dosyaları	Tagged Image File Format (.tiff)	Veri kaybına izin verilmediği durumlarda bu standart tercih edilmelidir.
	Graphics Interchange Format (.gif)	Çizim, animasyon gibi fazla detay içermeyen görüntülerin sıkıştırılmasında kullanılmalıdır.
	Joint Photographic Experts Group (.jpg) (ISO 10918)	ISO 10918, 24 bit renk derinliği destekleyen bu format renk duyarlığı gereken durumlarda kullanılmalıdır.
	Portable Network Graphics (.png)	ISO/IEC 15948:2004
	Enhanced Compressed Wavelet (.ecw)	Yüksek sıkıştırmaya ihtiyaç duyulan durumlarda kullanılabilir.

1.2.6 Canlandırma ve Hareketli Resimler

"Hareketli GIF" eklenti (plug-in) gerektirmemesi nedeniyle tercih edilmektedir. Ancak, farklı kullanım alanları için diğer standartlar kullanılabilir.

Bileşen	Standart/Teknoloji	Açıklama
Animasyonlar	Hareketli GIF	
	Apple Quicktime (.mov, .qt)	
	Adobe Flash (.swf)	
	Adobe Shockwave (.swf)	
	Audio Video Interleave (.avi)	

1.2.7 Ses-Video

Bileşen	Standart/Teknoloji	Açıklama
Ses-Video	MPEG-1	ISO 11172
	MPEG-2	ISO 13818
	MPEG-4	ISO 14496
	MPEG-7	
	DV	
	mp3	Bu formatta dosya oluşturmak telif ücreti ödenmesini gerektirebilir.
	wav	
	Quicktime	
	Adobe Flash (.swf/.flv)	
	OggTheora	

	OggVorbis	
	Audio Video Interleave (.avi)	

1.2.8 Gerçek Zamanlı Ses-Video Yayını

Bu amaçla ITU tarafından geliştirilen H.263 veya H.264 standardını destekleyen herhangi bir format kullanılabilir. Bu formatlardan bazıları aşağıda verilmiştir.

Bileşen	**Standart/Teknoloji**	**Açıklama**
Gerçek Zamanlı Ses-Video Yayını	Real Audio/ Real Video	
	Adobe Flash	
	Microsoft Windows Media Format (.asf)	
	Apple Quicktime	
	Ogg Media	

2 ARA BAĞLANTI

2.1 ESASLAR

Bu bölümde, ara bağlantı ve ağ standartları ortaya konmuştur. Bütünlüğü bozmamak amacıyla diğer bölümlerde incelenen bazı standartlara bölüm içerisinden atıfta bulunulmuştur.

2.2 KULLANILACAK STANDARTLAR

2.2.1 İnternet Aktarım Protokolleri

Bileşen	**Standart/Teknoloji**	**Açıklama**
İnternet Protokolü	IP (DARPA Internet Program Protocol Specification) (RFC 791)	Kullanılması önerilmektedir.
Taşıma (transport)	TCP (RFC 793) UDP (RFC 768)	Kullanılması önerilmektedir.

2.2.2 e-Posta Protokolleri

Bileşen	Standart/Teknoloji	Açıklama
e-Posta taşıma (e-mail transport)	e-posta SMTP/MIME'ye uygun olarak taşınmalıdır. RFC 2821 (SMTP), RFC 2822, RFC 2231 (MIME Part One), RFC 2046 ve RFC 3676(MIME Part Two), RFC 2231 (MIME Part Three), RFC 4289 (MIME Part Four), RFC 2049 (MIME Part Five), RFC 3798, RFC 2142, RFC 3986 (URI), RFC 2183	
e-Posta taşıma güvenliği (e-mail transport security)	RFC 3207	Güvenlik kısmında belirtilmiştir. (Bkz. İkinci Bölüm, madde 4)
e-Posta kutusu erişimi (e-mailbox access)	e-Posta erişimi için POP3 veya IMAP kullanılması gerekmektedir. POP3 için; RFC 1939, RFC 1957, RFC 2449. IMAP için; RFC 3501, RFC 4466, RFC 2971, RFC 3502, RFC 3503, RFC 3510, RFC 2683, RFC 2177, RFC 4469	Kullanılması önerilmektedir. RFC 2449: RFC 5034 sayılı RFC ile güncellenmiştir.
e-Posta içerik güvenliği (e-mail content security)	RFC 3850 RFC 3851 RFC 3852	Güvenlik kısmında belirtilmiştir. (Bkz. İkinci Bölüm, madde 4)
Güvenli posta kutusu erişimi (secure mailbox access)	RFC 2595, IMAP, POP3 ve ACAP için TLS standartlarını vermektedir.	Güvensiz ortamlarda mail erişimini sağlamak için HTTPS kullanılması gerekmektedir. Taşıma güvenliği (transport security) standartları güvenlik kısmında belirtilmiştir. (Bkz. İkinci Bölüm, madde 4)

2.2.3 Dosya Transfer ve Dizin Erişim Protokolleri

Bileşen	Standart/Teknoloji	Açıklama
Dosya aktarım protokolleri (file transfer protocols)	FTP - RFC 959, RFC 2640 RFC 3659 SFTP - RFC 2228, RFC 2428	Kullanılması önerilmektedir. RFC 959: RFC 2640, 3659 sayılı RFC'ler ile güncellenmiştir. Uzak oturumların güvenli olarak açılması ve bunun için "OpenSSH" kullanımı önerilmektedir.
Güvenli dosya aktarım protokolleri (secure file transfer protocols)	RFC 2585 (İnternet X.509 Açık Anahtar Altyapısı İşletim Protokolleri (PKI Operational Protocols): FTP ve http). RFC 2577 (FTP güvenlik hususları) RFC 4217 (TLS ile FTP güvenliği)	Kullanılması önerilmektedir.
Dosya iletimi	HTTP 1.1 (RFC 2616)	Kullanılması önerilmektedir.
	WebDAV (RFC 4918, RFC 2291, RFC 3253, RFC 3648, RFC 3744, RFC 4316, RFC 4331, RFC 4437, RFC 4791)	Kullanılması önerilmektedir.
Hypertext aktarım protokolleri	RFC 2817, RFC 2818 RFC 3546, RFC 3749	Kullanılması önerilmektedir.
Kablosuz Uygulama Protokolü (WAP 1.2.1/2.0)	WAP-210-WAPArch-20010712-a	Kullanılması önerilmektedir.
Dizin Erişim Protokolü (LDAP v3)	RFC 4510 – Tanımlar RFC 4511, RFC 4512, RFC 4513, RFC 4514, RFC 4515, RFC 4516, RFC 4517, RFC 4518, RFC 4519	Kullanılması önerilmektedir.

2.2.4 Ulusal Alan Adı Protokolleri

Bileşen	Standart/Teknoloji	Açıklama
Güvenli DNS	RFC 4033, RFC 4034 RFC 4470	Güvenlik için Bkz. İkinci Bölüm, madde 4.
Alan Adı Hizmetleri	DNS RFC 920, RFC 1034, RFC 1035, RFC 1912 IPv6 ile DNS işlemleri için	Üzerinde çalışılması gereklidir. RFC 1034 : RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 2065,RFC 2181, RFC 2308, RFC 2535,

Bileşen	Standart/Teknoloji	Açıklama
	RFC 3363, RFC 3364, RFC 2874, RFC 3596	RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 4592 sayılı RFC'ler ile güncellenmiştir. RFC 1035: RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2181, RFC 2137, RFC 2308, RFC 2535, RFC 2845, RFC 3425, RFC 3658, RFC 4033, RFC 4034, RFC 4035, RFC 4343 sayılı RFC'ler ile güncellenmiştir.

2.2.5 Yerel Alan Ağı/Geniş Alan Ağı Erişimi (Lan/Wan Interworking)

Belirtilen standartlardan IPv6'ya geçiş esnasında ürün ve sistemlerin tasarımında geçiş yapısı göz önünde bulundurulmalıdır. Bu nedenle yeni temin edilecek ürünlerin hem IPv4 hem de IPv6 ağlarında çalışabilir olması gerekmektedir.

Bileşen	**Standart/Teknoloji**	**Açıklama**
Yerel-ağ/geniş-alan-ağı erişimi Mobil erişim Kablosuz ağ (WLan)	RFC 1349, RFC 2474, RFC 3168, RFC 3260 IPv6 – RFC 2460, RFC 3697, RFC 4291, RFC 3484 Mobile IPv6 – RFC 3775, RFC 3776 IEEE 802.11 serisi standartları	Kullanılması önerilmektedir. IP v4 ile kurumlar arasında ara bağlantının sağlanmasının yanı sıra IPv6 geçiş çalışmalarının da yapılması gerekmektedir. RFC 3776: RFC 4877 sayılı RFC ile güncellenmiştir.
Dinamik Host Yapılandırma Protokolü (DHCP)	RFC 3315, RFC 3633, RFC 3736 (IPv6 için DHCP)	Üzerinde çalışılması gereklidir.

2.2.6 Gerçek Zamanlı Mesajlaşma (Real Time Messaging) Hizmetleri

Bileşen	**Standart/Teknoloji**	**Açıklama**
Birleştirilmiş mesajlaşma hizmetleri (Unified messaging services)	RFC 4239	Üzerinde çalışılması gereklidir. Ses ve veri ile mesajlaşmanın birleştirilmesi.
Gerçek zamanlı mesajlaşma hizmetleri (Real-time messaging services, Instant messaging services)	Kurumlar arası görüşmelerde kullanılacak olan bu teknoloji için RFC 2778, RFC 2779 uygunluk aranmaktadır. XMPP (Extensible Messaging and Presence Protocol) ve XML ile veri akışı (streaming) konularına bakılmalıdır. RFC 3920, RFC 3921 Anında mesajlaşma (instant messaging) için SIP uyumlulukları incelenmektedir. RFC 3428, RFC 3261	Kullanılması önerilmektedir.

2.2.7 Haber Grubu Hizmetleri

Bileşen	**Standart/Teknoloji**	**Açıklama**
Haber grubu hizmetleri (Newsgroup services)	NNTP – RFC 3977(Network News Transfer Protocol (NNTP)), RFC 2980	Kullanılması önerilmektedir. RFC 2980: RFC 3977 sayılı RFC ile güncellenmiştir.

2.2.8 Web Servisleri (Web Services Transport)

Bileşen	**Standart/Teknoloji**	**Açıklama**
Web servisi istemi (Web service request delivery)	SOAP v1.2, W3C tarafından tariflenmiştir. Dokümanlar için www.w3.org sitesine bakınız. RFC 4227	Bkz. İkinci Bölüm, madde 3.4
Web servisi istem kaydı (Web service request registry)	UDDI v 2.0-v3.0 www.uddi.org/specification.html RFC 4403 (UDDIv3)	Bkz. İkinci Bölüm, madde 3.4
Web servisi tanımlama (Web service description language)	WSDL 1.1 www.w3.org/TR/wsdl	Bkz. İkinci Bölüm, madde 3.4
Diğer web servisi standartları		Bkz. İkinci Bölüm, madde 3.4

3 VERİ ENTEGRASYONU VE İÇERİK YÖNETİMİ

3.1 ESASLAR

Kurumlar arası bilgi paylaşımının mümkün olabilmesi için, kurumların sahip oldukları ve ihtiyaç duydukları bilgilerin açık ve net olarak ortaya konabilmesi gereklidir. Bu nedenle kurumların ellerindeki kaynaklar tanımlanmalı, kimin hangi bilgiye, hangi şartlar altında erişebileceğine ilişkin bilgi tutulmalıdır. Bu bölümde veri entegrasyonu ve içerik yönetimi için bir metodoloji ve bu metodoloji için gerekli araçlar belirtilmiştir.

Öncelikle metaveri standardı oluşturulacaktır. Metaveri, kaynak keşfi alanında önemli bir araç olarak kullanılmakta olup, ülkemiz bilgi envanterinin çıkarılmasında da kullanılabilecektir.

Bu Rehber'de, entegrasyon ifadesi, kamu hizmetlerinin elektronik ortamda birlikte çalışacak, ortak bir çözüm oluşturacak şekilde sunulması anlamında kullanılmaktadır. Temel olarak kamu tarafından sunulan hizmetlerin entegrasyonu, hizmetler arasındaki etkin veri paylaşımını içerir.

Hizmetlerin mevcut süreçlerle değil, vatandaş odaklı olarak sunulduğu ve kurum tercihleriyle değil vatandaşın ihtiyaç ve tercihleriyle şekillendiği vatandaş merkezli e-devlet yapısı, etkin bilgi paylaşımını ve bu da beraberinde el değiştiren bilginin içeriğinin anlam kaybına ya da değişikliğe uğramadan iletilmesi ve kullanılmasını gerektirir. Paylaşılan bilginin doğruluk, güncellik, bütünlük ve ucuzluk gibi özelliklere sahip olması, vatandaş ya da iş dünyası odaklı hizmetlerin bu niteliklerle sunulabilmesi; devletin hızlı ve etkin bir şekilde işleyişinin sağlanması, bilgiye dayalı karar verme süreçlerinin iyileştirilebilmesi hedefleri için temel ihtiyaçtır.

3.2 İÇERİK YÖNETİMİ

Kamu ile vatandaşlar ve iş dünyası arasında, ana iletişim mekanizması olarak İnternet'in kullanımı e-Dönüşüm Türkiye Projesinin temel hedeflerinden birisidir.

Ancak, bu hedef beraberinde yeni ihtiyaçları da getirmektedir. Bilgilerin İnternet sitelerinde yayımlanması, o bilgiye ulaşılabilmesini sağlamaz. Kişilere devasa bilgi kaynakları içerisinde yol gösterecek, aradıkları kaynakların yeri ve erişimi hususunda yardımcı olacak mekanizmalara ihtiyaç vardır. Kütüphane ve arşiv literatüründe, kataloglama ve arşiv kontrol sistemlerinde kullanılagelen bir kavram olan metaveri, günümüzde tüm kaynakların tanımlanabilmesi, keşfi ve aranabilmesi açısından, İnternet'le birlikte giderek daha fazla önem kazanmıştır.

Bilgi kaynaklarının tanımlanması ve yönetimi için önemli bir araç olan metaveri, sayısal olan ya da olmayan tüm kaynaklar hakkında içerik, kalite, erişim, bulunabilirlik vb. açısından bilgi veren yapısal bilgi olarak tanımlanabilir.

İçerik yönetimi çalışmaları çerçevesinde, metaverinin iki temel alanda kullanımı öngörülmektedir. Bunlardan birincisi kaynak (doküman, İnternet sayfası, kurumsal süreç, veritabanı ve veri sözlükleri) keşfi, diğeri ise elektronik kayıt yönetimidir.

Kaynak keşfi metaverisi; İnternet sayfası, doküman ve veritabanı gibi çeşitli şekillerdeki bilginin bulunmasını ve erişimini kolaylaştırarak kaynak keşfine (resource discovery) katkıda bulunur.

Kaynak keşfi metaverisi şu bilgileri verir:

- Yer; belli bir kaynağın varlığı konusunda bilgi sağlar.
- Uygunluk; kaynağın kullanışlılığı ya da aranan konuyla ilgisi hakkında fikir verir.
- Erişim; kaynağa erişimle ilgili bilgi sağlar.

Özetle, kaynak keşfi metaverisinin içeriği; kaynağın yeri, kaynağın uygunluğu ve o kaynağa erişim hakkında yapısal bilgi sunar. Bu bilgi, kaynağı tanımlayan ve kaynağın özelliklerini ortaya koyan ögelerden oluşur. Örnek olarak; işin yazarı, yaratılma tarihi, tanımı, anahtar kelimeler ve ilişkili işlere bağlantılar gibi bilgileri sağlar. Hazırlanacak metaveri kümesinin ortak tanıtıcı standart olarak tüm kamuda kullanımı, kurumların ellerinde bulundurdukları bilgilere kolay erişilebilmesi ve istenen konuda tüm kamu kaynakları arasında arama yapılabilmesi gibi yeni hizmetlerin sunumuna imkan verecektir.

Arşiv ve kayıt yönetimi metaverisi ise, kayıtların erişilebilme, taşınabilme ve doğru şekilde anlamlandırılabilmelerine yardımcı olan, kayıtların yaşam döngüleri boyunca yönetimlerini destekleyen bilgi olarak tarif edilebilir. Başka bir ifadeyle; iş aktivitelerine ilişkin olarak kimlik, doğruluk, içerik, bağlam, yapı ve yönetim ihtiyaçlarının karşılanması amacıyla ihtiyaç duyulan bilgidir. Hazırlanacak metaveri kümesinin ortak tanıtıcı standart olarak tüm kamuda kullanımı ve kayıt yönetim sorumluluklarının büyük ölçüde karşılanmasına yardımcı olacak bu standartlarla uyum sağlanması, kurumların elektronik kayıtlarını sistematik ve tutarlı şekilde tanımlamalarına, yönetmelerine ve tanıtmalarına yardımcı olacaktır.

Özetle; içerik yönetimi ve veri/bilgi paylaşımı; veri sahipliği, veri güvenliği, veri gösterimi, veri iletimi ve veri erişimi mekanizmaları üzerine kurularak veri ve metaveri sözlüğü içinde ifade edildiği şekilde kullanılacaktır.

Bilginin paydaşa sunumunda mutlaka metaveri kullanılmalıdır. Kamu kurumları tarafından İnternet dahil herhangi bir ağ ortamında yayımlanan her türlü bilgi, metaverisi ile birlikte sunulmalıdır. Sayfa tasarımları dinamik uygulamalar olarak oluşturulmalı ve sunulan veri, dinamik uygulamalar ile anlam bütünlüğüne sahip veri kümeleri ve/ya bilgiye dönüştürebilmelidir.

3.3 SÜREÇ ve VERİ ENTEGRASYONU

Kurumlar arası süreç ve veri entegrasyonunun sağlanabilmesi için yapılması gereken işlemler aşağıdaki adımlarla özetlenebilir:

- Organizasyonel çalışma
    - Kamu kurumları organizasyon yapısının en alt idari birimler de dahil olmak üzere ortaya konması,
    - Mevzuatta tariflenen görev tanımları ve mevcut iş süreçlerinin belirlenmesi.
- Süreç Çalışması
    - Kamu kurumlarının varlık nedenini oluşturan temel (çekirdek) hizmet ve temel süreçleri destekleyen destek süreçlerinin tanımlanması,
    - Çekirdek süreçlerin vatandaş odaklı olarak iyileştirilmesi; gerekirse yeniden tasarlanması.

- Veri Çalışması
    - Süreçlerin herhangi bir aşamasında kullanılan kurumsal bilgi varlıklarının (sayısal ve sözel verilerin) atomik seviyede analizi, kullanım seviyelerinin belirlenmesi (gizlilik seviyesi, stratejik önemi, paylaşılabilirlik vb.) ve tanımlanması,
    - Birden fazla kurumu ilgilendiren süreçlerde kullanılması gereken kurumlar arası bilgi varlıklarının çıkarılması,
    - Kamuda veri üretiminde kullanılan sınıflamaların ve kaynağının tespit edilmesi,
    - Süreçlerin herhangi bir aşamasında kullanılması gereken sayısal ve sözel verilerin belirlenerek tanımlanması,
    - Tanımlanan veri ve süreçler kapsamında kurumların veri toplama/güncelleme/erişim yetkilerinin, veri sahipliği dahil olmak üzere, düzenlenmesi.
    - Veri paylaşımına imkan verecek veri entegrasyon mekanizmalarının oluşturulması,
    - Bilgi varlıklarının süreç yaşam döngüsü içerisinde BT kullanılarak, elde etme süreçlerinin iyileştirilmesi.

3.3.1 Kamu Hizmet ve Karar Destek Süreçlerinin Tanımlanması ve İyileştirilmesi

Dönüşüm sürecinde temel hedeflerden biri, organizasyonların kendi içerisinde ve diğer kurumlarla bilgi iletişiminin önceden tanımlanmış ve kurumsallaşmış platforma çekilmesi olmalıdır. Farklı kurumlarda eş iş akışlarının bulunması olasılığına karşın, kamu kurumlarının mevcut yapısının görev ve iş süreçleri bağlamında haritasının çıkarılması dönüşüm öncesi kavram birliği açısından önem arz etmektedir. Bu yaklaşım ile dönüşüm vizyonu mevcut organizasyonel yapı üzerinde ortaya konulabilecek, sürekli değerlendirme ve iç denetim mekanizmaları ile bu yapının tutarlılığı korunabilecektir.

Bir önceki kısımda organizasyonel çalışma, süreç çalışması ve veri çalışması altında listelenen adımlar temelinde yapılacak süreç modelleme çalışmaları kapsamında, kurum ve kurumlar arası iletişimin modellenmesinde fayda görülmektedir.

Kamu hizmet süreçlerinin modellenmesi, kurum içi ve kurum dışı birimlerle etkileşimin ve süreç kapsamındaki rol ve sorumlulukların ortaya konmasını kapsamaktadır. Bu kapsamda yapılacak çalışmalar aşağıda verilmektedir.

3.3.1.1 Süreç Modelleme

3.3.1.1.1 Süreç Tanımlama Standardının Oluşturulması

İsim, amaç, hedef kitle, sürecin başlama ve bitiş koşulları, girdi ve çıktıları, süreç kapsamındaki roller, aktiviteler ve iş kuralları gibi bilgileri içerecek şekilde kurumların süreç tanımlama sırasında kullanacakları asgari standart alanlar belirlenecektir.

3.3.1.1.2 Süreçlerin Tanımlanması

Süreçler, aşağıdaki yaklaşımla çıkarılarak tanımlanacaktır.

i. Mevcut süreçlerin çıkarılması (Mevcut Durum Modeli).

1. Organizasyonel birimlerin ve rollerin yerine getirdikleri, sorumlu oldukları ve ilgili oldukları fonksiyonları, fonksiyonların girdi ve çıktılarını da içerecek şekilde temel (kurumun varlık nedenini oluşturan) süreçlerin bütünleşik bir şekilde modellenmesi,
2. Taşra yapılanması olan kurumlarda merkezin taşradan beklentileri ve taşradan raporlama süreci ve formatının irdelenmesi,
3. Varlıkların; mevcut envanterin (bilgi, bilişim altyapısı, insan kaynakları, taşınmaz, materyal) çıkarılması,
4. (Varsa) mevcut performans göstergelerinin belirlenmesi,
5. Bulguların birleştirilerek mevcut modelin son haline getirilmesi,
6. Personelin değişim açısından sosyolojik ve psikolojik yapısının incelenmesi,
7. Personelin eğitim durumlarının ve kapasite artırım gereksiniminin tespiti,
8. Gözden geçirme, doğrulama ve geçerli kılma,
9. Kurum portalında yayımlama.

Bu aşamanın temel çıktısı Mevcut Durum Model Raporu olup, süreçlerdeki, yapıdaki ve varlıklardaki değişimleri izleme mekanizması, performans göstergeleri, tıkanma noktaları, karar mekanizmaları ile personelin değişim açısından sosyolojik ve psikolojik yapılarını betimleyecektir.

ii. Stratejik Plan ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu doğrultusunda mevcut süreçlerin bilgi ve iletişim teknolojilerinin getirdiği imkanlardan da yararlanacak şekilde iyileştirilmesi ve gerekirse yeniden tasarlanması (Hedef Model).

1. Süreçlerdeki darboğazlar, tıkanma noktaları ve eksikliklerin belirlenmesi,
2. Raporlama ve yönetim ihtiyacının geliştirilmesi,
3. Bilgi akış haritalarının oluşturulması,
4. Modellenen süreçlerin revize edilmesi veya yeniden tasarlanması,
5. Mevcut kurumsal yapının, problemlerin, yetersizliklerin belirlenmesi
6. Süreçlere uygun organizasyonel yapı, iş/görev tanımlarının oluşturulması,
7. Yeni tasarlanan süreçler için gereken varlıkların (bilgi, bilişim altyapısı, insan kaynakları, taşınmaz, materyal) belirlenmesi,
8. Süreçlere ilişkin performans göstergelerinin belirlenmesi,
9. Her süreçle ilgili bir rol sahibi tanımının yapılması,
10. Gözden geçirme, doğrulama ve geçerli kılma,
11. Kurum portalında yayımlama.

Bu aşamanın temel çıktısı Hedef Model Raporu olup, hedeflenen süreçlerin tasarımını, fonksiyonel özelliklerini, insan kaynakları yönetim mimarisini (roller, yetki-sorumluluklar), yeni performans sistemini, eğitim stratejilerini, halkla ilişkiler stratejilerini, bilgi yönetimi stratejilerini, yönetim bilgi sistemi mimarisini, envanter ihtiyacını, karar süreçleri mekanizmalarını, kalite sistemini, mevzuat değişiklik gereksinimlerini, güvenlik gereksinimlerini, fiziksel altyapı gereksinimleri ile performans, kalite, karar süreçleri ve süreçlerin standartlarını içerecektir.

iii. Fark Analizi ve Geçiş Planlaması. Mevcut organizasyondan bilgiye dayalı organizasyona geçiş için stratejik planlama ve ilgili enformasyon teknolojisi, yasal çerçeve ile teknik gelişim altyapısının belirlenmesi.

1. Organizasyonel ilişkilerdeki dönüşüm adımlarının belirlenmesi,
2. Malzeme ve insan kapasitesini arttırma çalışmaları,
3. Eleman ve eğitim gereksinimlerinin ve çözümlerinin belirlenmesi,
4. Fiziksel altyapı (ofis alanı, malzeme, vb.), yazılım, donanım gereksinimlerinin belirlenmesi,
5. Varsa pilot uygulama kapsamına alınacak süreç(ler)in saptanması (geçiş adım adım planlanmalı ve pilot çalışmalar örnek alınarak revize edilmelidir),
6. Mümkünse ve süreç ile ilgili süre, maliyet, vb. bilgiler mevcut ise, uygulamaya almadan önce süreç simülasyonu yapılması,
7. Belirlenen gereksinimler için bütçeleme yapılması ve alım stratejilerinin tanımlanması,
8. Uyumluluk çalışmalarının gerçekleştirilmesi,
9. Değişim hareketinin sosyolojik ve psikolojik etkilerinin belirlenmesi ve alternatif çözümlerin oluşturulması,
10. Yasal düzenleme ihtiyacı; taslak mevzuatın hazırlanmasına katkı verilmesi,
11. Gözden geçirme, doğrulama ve geçerli kılma.

Bu aşamada temel olarak Organizasyonel Dönüşüm ve Eylem Planı, eleman ve eğitim ihtiyacı, eğitim müfredatı, Bilgi Teknolojileri Stratejik Planı, Yaygınlaştırma ve Operasyon Planları, fiziksel altyapı oluşturma, yenileme ve geliştirme gereksinimleri ile gerekiyorsa taslak mevzuatı içeren Sistem Gereksinim Belgesi oluşturulacaktır.

iv. Gerçekleştirme sürecinin bundan sonraki aşamaları ISO 15288, ISO 12207 ve ISO/IEC 27002, TS ISO/IEC 27001 gibi standartlar temelinde yürütülecek, tedarik yönetimi, entegrasyon ve sürdürülebilirliğe özel önem verilecektir.

Çalışmaların aşağıdaki temel prensiplerle uyumlu olması gerekmektedir:

1. Her kurum kendi sürecinin modellenmesinden sorumlu olduğu için, kurumsal süreç sözlükleri her kurumun kendi bünyesinde güncel tutulacaktır. DPT Müsteşarlığı kurumlar arasında kullanılacak olan üst süreç sözlüğünden sorumludur.
2. Süreçler, Stratejik Planda da ifade edilen amaç ve hedefleri gerçekleyecek şekilde tanımlanmalıdır. Stratejik Planda izlenemeyen bir temel süreç tanımlanmamalıdır.
3. Süreç modelleme çalışması amacıyla kurumlar danışmanlık hizmeti alabilir, ancak sürecin içinde yer alan tüm kurum birimlerinin seçilmiş ve yetkilendirilmiş temsilcilerinden oluşan bir çalışma grubu kurulmalıdır. Mümkünse Süreç Çalışma Grubu süreklilik arz etmeli, dönemsel olarak süreç performansını değerlendirmeli, gereken değişiklikleri yönetimin onayına sunulmalıdır. Süreç sahipleri çalışma grubu içinde temsil edilmelidir.
4. Süreç modelleme çalışmalarında Bilgi Yönetimi süreçleri de dikkate alınmalıdır.
5. Süreç modelleme ve iyileştirme çalışmaları Performans Programı içinde faaliyet ve projeler olarak ifade edilmeli, maliyetlendirilerek bütçe ile ilişkilendirilmelidir.
6. İç Kontrol sistemi tanımlı süreçler üzerinden, risk analizi sonucu, kontrol noktaları ve kuralları belirlenerek kurulmalıdır.

7. Süreç performansı operasyonel sistemler üzerinden izlenebilmelidir. Faaliyet raporunda süreç performansı verileri paylaşılmalıdır.

3.3.2 Süreçlerde Kullanılan Verilerin Belirlenerek Tanımlanması

İş süreçlerindeki veri akışı ve veri yapılarının ortaya konmasını içerir. Tüm kamu hizmet ve süreçleri sözlüğü DPT Müsteşarlığı sorumluluğu ve koordinasyonunda, hizmet sağlayan kamu kurumlarının katılımıyla oluşturulacak ve geliştirilecektir. Bu kapsamda yapılacak çalışmalar aşağıda verilmektedir.

3.3.2.1 Veri Tanımlama

3.3.2.1.1 Veri Sözlüğü Standardının Oluşturulması

Veri Sözlüğü, kurum içi veriler hakkındaki verilerin mantıksal ve merkezi bir şekilde saklandığı veri yönetimi işlevini sağlamaya yönelik standarttır. Sözlük verilerin sistematik bir şekilde organize edilmesi, sınıflandırılması ve çeşitli özelliklerinin belirtilmesiyle oluşturulur. Bu amaçla Kamu Kurumları Veri Sözlüğü Standardı geliştirilecektir.

3.3.2.1.2 Veri Sözlüğü Hazırlama

Kurumlar, veri sözlüklerini kurumsal stratejiler ve Kamu Kurumları Veri Sözlüğü Standardı'na göre oluşturacak ve güncel tutacaktır. Örneğin, Kamu Mali Yönetim Ontolojsi kapsamında Stratejik Yönetim, İç Kontrol ve Karar Alma veri grupları ile ilişkilerini belirleyerek metaveri yönetim yapısı altında sunma çalışmaları Maliye Bakanlığınca yürütülmektedir. Kurumsal veri sözlükleri ve ontolojilerin hazırlanmasını takiben tek noktadan erişilebilecek meta sözlük DPT Müsteşarlığı sorumluluğunda hazırlanacak ve güncel tutulacaktır.

3.3.2.2 Veri Modelleme

Nesne bağıntı çizenekleri (Entity relationship(E/R) diagram), veri akış çizenekleri (Data Flow Diagram (DFD)) kullanılarak veri modellemesi yapılacaktır.

3.3.2.3 Veri Yapısı Tanımlama

XML sistemler arası veri değişiminde temel standart olarak benimsenmiştir. Buna bağlı olarak XML Şema Tanımlama Dili (XSD) kullanılarak veri yapılarına ilişkin tanımlar ve açıklamalar yapılacaktır.

3.3.2.4 Verinin Gösterimi (Format)

Verinin gösteriminde standart olarak XSL kullanılacaktır.

3.3.3 Kurumların Veri Toplama/Güncelleme/Erişim Yetkilerinin Düzenlenmesi

Kurumlar arasında paylaşılan bilgi üzerinde, hangi kurumun hangi seviyede erişim yetkisi olduğu veri bazında tanımlı olmak zorundadır. Gerekli yetkilendirme tanımlarının yapılmasına altyapı oluşturacak e-devlet metaveri standardı bu ihtiyaca cevap verecek yapıda olacaktır. Bu kapsamda veri sınıflaması (önem, gizlilik seviyesi, vb.) esas alınacaktır.

3.3.4 Veri Paylaşımına İmkan Verecek Veri Entegrasyonu Altyapısının Oluşturulması

Süreçler arasındaki etkileşimin belirlenmesi ve bu süreçler arasında paylaşılan verinin anlamlandırılmasına imkan veren veri yapılarının **XSD** standardı kullanılarak tanımlanması, verinin **XML** kullanılarak sunumu ve veri değişimi için Web Servislerinin kullanılması öngörülmektedir.

3.4 KULLANILACAK STANDARTLAR

Bileşen	Standart/Teknoloji	Açıklama
Kaynak keşfi metaveri standardı	ISO 15489-1:2001, ISO 15489-2:2001, ISO 15836:2003, ISO 23950:1998	Elektronik kayıt yönetimi için geliştirilecek standart ile uyumlu olacak şekilde Dublin Core veri kümesine dayanarak geliştirilecektir. Kaynak keşfi, arşiv ve kayıt yönetim sistemi için tasarlanmış metaveri kümesinin alt kümesi olarak kullanılacaktır. Kurumların standarda uyum yöntemi, geliştirilecek standardın da yer alacağı rehberde belirtilecektir.
Elektronik kayıt yönetimi metaveri standardı	TS 13298	Bilgi ve Dokümantasyon – Elektronik Belge Yönetimi Standardı çerçevesinde geliştirilecektir.
Metaveri sınıflama ve kayıt	ISO/IEC 11179	
Süreç modelleme	İş süreçleri, süreç zincir çizenekleri (Process Chain Diagram) kullanılarak modellenmelidir. Yazılım desteği sağlanacak süreçler daha sonra UML kullanılarak detaylandırılacaktır.	Kullanılması önerilmektedir.
Süreç uygulama dili (web servisleri için)	BPEL (Business Process Execution Language) BPEL4WS (Business Process Execution Language for Web Services)	
Süreç tanımlama (web servisleri için süreç tanımı depoları)	ebXML	Kullanılması önerilmektedir.
Süreçlerin çağırılması	ASAP	

Bileşen	Standart/Teknoloji	Açıklama
Veri modelleme	Nesne bağıntı çizeneği (Entity Relationship Diagram), Veri akış çizeneği (Data Flow Diagram)	
Veri modeli değişimi	XMI	
Veri/metaveri yapısı tanımlama	XSD	
Veri gösterimi	XSL	
Veri dönüştürme (data transformation)	XSLT (XSL Transformation)	
Ontoloji tabanlı bilgi değişimi	OWL	
Veri değişimi	Web servisi, XML	
Web servisi istemi (Web service request delivery)	SOAP RFC 4277	W3C tarafından tariflenmiştir. Dokümanlar için www.w3.org sitesine bakınız.
Web servisi istem kaydı (Web service request registry)	UDDI	www.uddi.org/specification.html
Web servisi tanımlama	WSDL 1.1 ve 2.0	www.w3.org/TR/wsdl
Diğer web servisi standartları		Kullanılması önerilmektedir. Diğer standartlar için web servisleri birlikte çalışabilirlik (WS-I) sitesi (www.ws-i.org) ile OASIS ve W3C web servis komitelerine bakınız.
Kamu Kurumları Veri Sözlüğü Standardı		ISO/IEC 11179 temelinde geliştirilecektir.

4 GÜVENLİK

4.1 ESASLAR

Bilginin kurumlar arasında güvenli bir şekilde iletilmesi ve paylaşılması, işlemlerin elektronik ortamda güvenle yapılabilmesi ve yaygınlaşabilmesi açısından kritik önem taşımaktadır. Kurumların bilgi sistemleri, İnternet'e bağlı olmanın getirdiği güvenlik risklerine karşı koruma sağlayacak şekilde tasarlanmalı ve yapılandırılmalıdır. Bu sayede vatandaşlar, kamu kurumları ve iş çevreleri arasında güvenli bir etkileşim sağlanmış olacaktır.

Bilginin güvenli bir şekilde iletilmesi için kurumların da belli başlı bilgi güvenliği standartlarına uyması ve bilgi paylaşan tüm kurumların bu standartları yakalaması gerekmektedir. Son yıllarda İnternet kullanımının artmasından dolayı güvenliğin büyük önem kazanmasıyla birlikte bu alandaki standartlaşma çalışmaları da aynı oranda artmaktadır. Bunun sonucunda çok sayıda güvenlik standardı, talimatı ve tavsiyesi ortaya çıkmıştır.

Veri bütünleşmesi (integration) esnasındaki güvenlik standartları tek bir başlık altında bu bölümde açıklanmış olsa da, güvenlik bundan önceki bölümlerdeki standartlar belirlenirken göz önünde bulundurulması gereken, farklı alanlarda ve sistemlerde farklı seviyelerde şekillenecek önemli bir parametredir. Bu bölümde belirtilen güvenlikle ilgili standartlar, belirtimler (specification), kılavuzlar ve tavsiyeler güvenli bir e-devlet arabağlantı ve veri entegrasyonu çatısı (framework) oluşturabilmek için gereklidir.

Kamu bilgileri güvenlik açısından üç sınıfa ayrılabilir. Bunlar; tasnif dışı, hizmete özel ve hizmete özel üstü (gizli, çok gizli) bilgilerdir. Tasnif dışı bilgi, kurum dışına çıkması durumunda devletin varlığına ve bekasına, ülkenin ve milletin bölünmez bütünlüğüne, toplumun huzuru, genel ahlakı ve kamu çıkarlarına zarar vermeyecek bilgidir. Hizmete özel bilgi; yukarıda anılan hassasiyetler göz önüne alınarak, bilmesi gereken prensibine uygun şekilde kurum içinde serbestçe dolaşabilir, ancak kurum dışına yetkisiz çıkarılmaması gerekir. Hizmete özel gizlilik seviyesinin üzerindeki bilgiler ise milli koruma önlemleri gerektiren ve yetkisiz açığa çıkması durumunda sadece kurumu değil, belli bir oranda devleti de zarara uğratabilecek bilgilerdir. Rehber'in güvenlik bölümü altında verilmiş olan standart, belirtim, kılavuz ve önerilerdeki kriptografik algoritmalar tasnif dışı ve hizmete özel gizlilik seviyesindeki bilginin güvenliği için kullanılmalı, daha yüksek güvenlik seviyesindeki bilginin kriptografik güvenliği için TÜBİTAK – UEKAE'ye (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) başvurulmalıdır.

4.1.1 Bilgi Güvenliği Yönetim Sistemi (BGYS)

Kurumlar için en kritik varlık bilgidir. Kurumların değerleri, sahip oldukları bilgi ile ölçülmekte ve kurumun kimliğini sahip olduğu bilgi belirlemektedir. Günümüzde kamu kurumlarının sahip oldukları bilginin çok büyük bir kısmı bilgi teknolojileri vasıtası ile işlenmektedir. Bu durum bilgi teknolojilerinin önemini artırmaktadır. Bilgi teknolojilerinin yaygın şekilde kullanımı bilginin maruz kaldığı riskleri de artırmakta ve kurumların sahip oldukları bilgilerin güvenliğine ilişkin tedbirler almasını zorunlu kılmaktadır.

Kurum bünyesinde yaratılan, işlenen, depolanan, iletilen, imha edilen ve kullanılan bilgi ile kurumlar arasında iletilen bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumak güvenliğin temel hedefidir. BGYS bu temel hedefi gerçekleştirmek amacıyla tasarlanmalıdır.

Bilgi güvenliğinin sağlanması, güvenlik önlemlerinin seçilmesi ve uygulanması ile sınırlı değildir. Sürekli olarak yeni güvenlik açıkları ve saldırıların ortaya çıkması, kurum bilgi sistemlerinde teknolojik gelişmeler sonucu meydana gelen değişiklikler göz önüne alınarak güvenlik önlemlerinin düzenli olarak kontrol edilmesi, gerektiğinde iyileştirmeler ve değişiklikler yapılması gerekliliğini ortaya çıkarmaktadır.

Bilgi güvenliğinde sürekliliğin sağlanması için, tüm bu faaliyetlerin kurum ihtiyaçları ve kaynaklar göz önünde bulundurularak etkili ve verimli bir şekilde yönetilmesi gerekmektedir. Etkili ve verimli yönetim ise BGYS ile mümkün olup, bu amaçla tüm kurumlarda BGYS kuruluması gerekmektedir.

TÜBİTAK-UEKAE tarafından gerçekleştirilen e-Dönüşüm Türkiye Projesi 2005 Eylem Planı 5 no'lu eylemi gereğince ön çalışmalar yapılmış olup; kamu kurumlarında BGYS çalışmalarının belirli bir plan ve koordinasyon dahilinde gerçekleştirilmesi öngörülmüştür. Bu çalışmaların koordine edilmesi görevi Bilgi Toplumu Stratejisi eki Eylem Planı 88 no'lu eylem ile TÜBİTAK-UEKAE'ye verilmiştir.

BGYS kurulması konusunda TÜBİTAK-UEKAE tarafından kamu kurumlarına eğitimler verilmektedir. Kamu Kurum ve Kuruluşları alınan eğitimler sonrasında TÜBİTAK – UEKAE danışmanlığında yürütülen risk analizleri çalışmalarının ardından BGYS'lerini kurmaktadır.

Kamu Kurum ve Kuruluşları kurulacak BGYS'lerini, TSE tarafından verilen TS ISO/IEC 27001 sertifikası ile belgelendirebilirler.

4.1.2 Ortak Kriterler

Ortak Kriterler, (TS ISO/IEC 15408) Bilgi Teknolojileri ürünlerinin güvenlik ve garanti seviyelerinin kamuya bağlı bir belgelendirme merkezi denetiminde bağımsız bir değerlendirme laboratuvarı tarafından belirlenebilmesi ve belgelendirilebilmesi için kullanılan uluslararası güvenlik standardıdır.

BT ürünleri geliştiren veya satın alan birçok ülkenin ulusal standartlarının da yerine geçen bu standart, hem ticari sistemlerde hem de kamuya bağlı gizlilik dereceli bilgi saklayan, işleyen veya ileten sistemlerde kullanılacak BT ürünlerinde güvenlik gereksinimlerinin karşılanmasını sağlamak için kılavuz olarak kullanılmalıdır.

Ortak Kriterler standardına uygun olarak gizlilik, bütünlük, erişilebilirlik ve güvenilirlik değerlendirmesi gerçekleştirilebilecek BT ürün ve sistem portföyünde aşağıda belirtilen ürün ve sistem türleri bulunmaktadır:

- Erişim Kontrol Cihaz ve Sistemleri
- Sınır Koruma Cihaz ve Sistemleri
- Veri Tabanları
- Veri Koruma
- Saldırı Tespit Cihaz ve Sistemleri
- Entegre Devre, Akıllı Kartlar ve Akıllı Kartlarla İlgili Cihaz ve Sistemler
- Anahtar Yönetimi Cihaz ve Sistemleri
- Ağ İletişimi Cihazları
- İşletim Sistemleri

- Sayısal İmza Ürünleri
- Diğer Cihaz ve Sistemler (Örneğin; Blackberry, VoIP telefon)

Yukarıda belirtilen ürünler ve sistemler için Ortak Kriterler standardında tanımlanan yedi (7) farklı garanti seviyesi bulunmaktadır. Burada alt seviyeden (EAL 1), üst seviyeye (EAL 7) çıkıldıkça ürünün veya sistemin garanti seviyesi artmaktadır. Bu yedi (7) seviye, ürün veya sisteme özel olarak "Çok Gizli", "Gizli" ve "Hizmet Özel" gizlilik dereceleri ile eşleştirilebilir.

Kamu kurum ve kuruluşlarının satın alacakları bilgi teknolojileri ürünlerinde ve sistemlerinde gizlilik dereceli bilgiyi bulundurma veya işleme ihtiyacı varsa, bu ürün ve sistemlerin, yapılacak veya yapılmış olan risk analizi sonucunda tespit edilen garanti seviyesine göre, Ortak Kriterler değerlendirmesi tamamlanmış ve sertifikalandırılmış ürün ve sistemler kullanılmalıdır.

Kamu kurum ve kuruluşlarının geliştirecekleri bilgi teknolojileri ürünlerinde ve sistemlerinde ise gizlilik dereceli bilgiyi bulundurmaları veya işlemeleri hedefleniyorsa, bu ürün ve sistemlerin yapılacak olan risk analizi sonucunda tespit edilen Ortak Kriterler garanti seviyesine göre tasarlanması ve tasarım sonucunda Ortak Kriterler değerlendirmesinin gerçekleştirilmesi ve sertifikalandırılması bilgi güvenliği açısından önemlidir.

Türk Standartları Enstitüsü, 2003 yılında Uluslararası Ortak Kriterler Tanıma Sözleşmesini imzalayarak bu sözleşmenin tarafı olmuş ve Sertifika Üreticisi ülkeler tarafından verilen Ortak Kriterlere Uygunluk belgelerini geçerli kabul ettiğini beyan etmiştir.

Ulusal Ortak Kriterler Belgelendirme Sistemi'ni oluşturacak sertifikasyon makamı yapısı Türk Standartları Enstitüsü ve TÜBİTAK - UEKAE arasında imzalanan bir protokol ile kurulmuştur. Protokol kapsamında kurulan Ortak Kriterler Belgelendirme Sistemi, gerekli kriterleri sağlayan değerlendirme laboratuvarlarında Ortak Kriterler standardına uygun olarak değerlendirilen ürünlerde geliştiricilerin güvenlik iddialarının doğrulanması ve bilgi teknolojisi satın alıcılarının ihtiyaç duyduğu güvenlik seviyesinde ürün kullanabilmeleri için Ulusal Ortak Kriterler Belgelendirmelerini gerçekleştirmektedir. Bu değerlendirmeden başarıyla geçen ürünlere TSE tarafından Ortak Kriterlere Uygunluk belgesi verilmektedir.

TÜBİTAK-UEKAE Ortak Kriter Test Merkezi, satın alınacak veya geliştirilecek ürün ve sistemlerin güvenlik gereksinimlerinin belirlenmesi, ürünün ve sistemin asgari garanti düzeyinin tespit edilmesi ve güvenlik değerlendirmelerinin Ortak Kriterler standardına uygun olarak gerçekleştirilmesi hususunda hizmet vermektedir.

4.1.3 Elekronik İmza

5070 sayılı Elektronik İmza Kanunu ve ilgili ikincil mevzuat gereğince ıslak imza ile aynı hukuksal etkiye sahip güvenli elektronik imza (e-imza) kullanımı yasal bir tabana oturtulmuş ve 2004/21 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının nitelikli elektronik sertifika ihtiyaçlarının TÜBİTAK-UEKAE bünyesinde kurulmuş olan Kamu Sertifikasyon Merkezi tarafından yürütülmesi kararlaştırılmıştır. Bu düzenleme ışığında e-devlet işlemlerinde hukuksal geçerliliğin sağlanması için e-imza kullanma gerekliliği açıktır. Konu ile ilgili ayrıntılı bilgiye http://www.kamusm.gov.tr adresinden erişilebilir.

4.1.4 Kriptografi

Kriptoloji bilginin elektronik ortamda güvenli bir şekilde iletilmesi ve paylaşılması, için gereken teknikleri içerir. Güvenlik, tasarlanmış bir sistemin üzerine giydirilebilecek bir

bileşen olmayıp, sistem tasarımı aşamasında dikkate alınmalıdır. Bilgi güvenliği, aşağıda sıralanan dört temel unsurun, ihtiyaçlara uygun kombinasyonu ile sağlanır.

- **Gizlilik:** Bilginin açık haline, sadece yetkili kişilerin erişebilmesidir.
- **Bütünlük:** Bilgi üzerindeki yetkisiz değişikliklerin alıcı tarafında fark edilmesinin sağlanmasıdır.
- **Kimlik doğrulama:** Kişinin iddia ettiği kimliğin gerçekte sahip olduğu kimlik olup olmadığını garantiye alan mekanizmadır.
- **İnkar edemezlik:** Kullanıcının sistem üzerinde yapmış olduğu işlemleri inkar edememesinin sağlanmasıdır.

Bunlara ek olarak aşağıda güvenlik servisleri açıklanmıştır. Bu servisler, yukarıda bahsi geçen temel unsurları tamamlayıcı niteliktedir.

- **Erişilebilirlik:** Bilginin gerektiğinde yetkili kullanıcıların erişimine hazır durumda bulundurulmasıdır.
- **Erişim denetimi:** Kimlik doğrulama, yetkilendirme ve kayıt tutma mekanizmaları ile erişimin denetlenmesidir.
- **Kayıt edilebilirlik:** Kimlik doğrulaması yapılan bir kişinin faaliyetlerinin izlenmesi ve tespit edilmesi kabiliyetidir.
- **Yetkilendirme:** Kullanıcıların sistem kaynaklarına erişiminin denetlenmesi, doğru kullanıcıların, doğru kaynaklara, doğru zamanda erişiminin sağlanmasıdır.
- **Mahremiyet:** Bir sistemde çalışan bir kişiye ait bilgilere başkaları tarafından erişilmemesi olgusudur.

4.2 KULLANILACAK STANDARTLAR

Bu bölümde verilen standart, belirtim ve kılavuzlara erişim için kullanılabilecek web siteleri aşağıda verilmiştir:

TS : http://www.tse.org.tr
ISO : http://www.iso.org
IEC : http://www.iec.org
BS : http://www.bsi-global.com
RFC : http://www.ietf.org/rfc.html
FIPS : http://csrc.nist.gov/publications/fips
W3C : http://www.w3.org
OASIS: http://www.oasis-open.org

4.2.1 Bilgi Güvenliği Yönetimi

Bileşen	Standart/Teknoloji	Açıklama
Bilgi güvenliği yönetimi için uygulama prensipleri	ISO/IEC 27002	Bilgi güvenliği yönetim sistemlerinde kullanılabilecek karşı önlem önerileridir. Mümkün olan hallerde milli olarak üretilen karşı önlemlerin kullanılmasına azami özen gösterilmelidir.
Bilgi güvenliği yönetim sistemleri – Özellikler ve kullanım kılavuzu	TS ISO/IEC 27001	Kurumların dokümante edilmiş bir BGYS'yi tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, bakımını yapmak ve iyileştirmek için gereksinimleri kapsar. Standart, ISO/IEC 27001:2005 standardının Türkçe çevirisidir.

4.2.2 Bilgi Güvenliği Yönetimini Destekleyen Standartlar ve Kılavuzlar

Bu tablo altındaki kılavuz ve standartlar Türkçe olarak yayımlanmamıştır.

Bileşen	Standart/Teknoloji	Açıklama
Bilgi güvenliği risk yönetimi için kılavuz	BS 7799-3:2006	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Information security management systems. Guidelines for information security risk management
BGYS sertifikasyonu ihtiyaçları ve hazırlığı için kılavuz	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guidelines on Requirements and Preparation for ISMS Certification Based on ISO/IEC 27001
BGYS denetimine hazırlık kılavuzu	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Are You Ready for an ISMS Audit Based on ISO/IEC 27001?
BGYS kontrollerinin uygulaması ve denetlemesi için kılavuz	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi:Guide to the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001
BGYS uygulamasının etkinliğinin ölçülmesi kılavuzu	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi:Measuring the Effectiveness of your ISMS Implementations Based on ISO/IEC 27001
Karşı önlemlerin seçimi için kılavuz	PD 3005:2002	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guide to the selection of BS 7799 Part 2 controls
Bilgi teknolojileri ve iletişim teknolojilerinin güvenlik yönetimi için kavramlar ve modeller	ISO/IEC 13335-1:2004	ISO tarafından hazırlanmış olan standardın orijinal ismi: Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for

		information and communications technology security management
Bilgi teknolojileri güvenliğinin yönetimi için teknikler	ISO/IEC TR 13335-3:1998	ISO tarafından hazırlanmış olan standardın orijinal ismi: Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
Karşı önlemlerin seçimi	ISO/IEC TR 13335-4:2000	ISO tarafından hazırlanmış olan standardın orijinal ismi: Guidelines for the management of IT Security -- Part 4: Selection of safeguards
Ağ güvenliği için yönetim kılavuzu	ISO/IEC TR 13335-5:2001	ISO tarafından hazırlanmış olan standardın orijinal ismi: Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security
İş sürekliliği yönetimi için uygulama prensipleri	BS 25999–1:2006	BSI tarafından hazırlanmış olan standardın orijinal ismi: Code of practice for business continuity management

4.2.3 Bilgi Teknolojileri Ürünleri Güvenliği

Bileşen	**Standart/Teknoloji**	**Açıklama**
Bilgi teknolojileri ürünleri güvenlik değerlendirmesi	TS ISO/IEC 15408	Ortak Kriterler (Common Criteria)

4.2.4 Bilgi Erişimi ve Değişimi Alanı

Bileşen	**Standart/Teknoloji**	**Açıklama**
XML tabanlı kimlik bilgisi, yetki düzeyi ve profillerin tanımlanması	SAML sürüm 1.1 SAML sürüm 2.0	Sürüm 2.0 tavsiye edilir.
XML-tabanlı yetkilendirme	XACML	
Kimlik bilgisi, yetki düzeyi ve profillerin değişimi	WS-Federation ID-FF v1.2	Üzerinde çalışılması gereklidir.
XML sayısal imzalama	XML Signature	W3C tarafından tanımlanan XML - imza söz dizimi ve işlenmesi.
XML şifreleme	XML Encryption	W3C tarafından tanımlanan XML - şifreleme söz dizimi ve işlenmesi.

Bileşen	Standart/Teknoloji	Açıklama
Açık Anahtar Altyapısının (PKI) kullanıldığı yerlerde XML anahtar yönetimi	XKMS 2.0	W3C tarafından tanımlanan XML anahtar yönetimi belirtimi. http://www.w3.org/TR/xkms2/

4.2.5 Web Servisleri (WS) Güvenliği

Bir istemcinin, bir kamu web sunucusu ile haberleşirken, haberleşmenin doğru web sunucusu ile gerçekleştiğinden emin olmasını sağlayan tedbirler alınmalıdır (web sunucusunun kimliğinin doğrulanması). Gizlilik ve/veya bütünlüğün gerekli olduğu durumlarda içerik ağ üzerinde güvenli bir şekilde taşınmalıdır.

Bileşen	Standart/Teknoloji	Açıklama
Web içeriğinin güvenli iletimi (bütünlük ve gizlilik)	TLS v1.1 (RFC 4346) SSL v3.0	Yeni uygulamalar TLS'i desteklemelidir. Ayrıca durum elverdiği takdirde bu uygulamalar SSL 3.0'ü de desteklemelidir.
Web üzerinden işlemler	OSCI transport v1.2	http://egovernment.xml.org/standards/pdf/010_osci_1_2_specification.pdf
Web servisleri mesaj seviyesi güvenliği (WS-Security)	WS-Security 1.0	SOAP mesajlarının nasıl sayısal olarak imzalanacağını, nasıl şifreleneceğini ve sertifikaların mesaj içerisine nasıl yerleştirileceğini tanımlayan standarttır.

4.2.6 e-Posta Güvenliği

Bileşen	Standart/Teknoloji	Açıklama
e-Posta taşıma güvenliği	RFC 3207	SMTP Service Extension for Secure SMTP over TLS
e-Posta içerik güvenliği	RFC 3850 RFC 3851 RFC 3852	S/MIME sürüm 3.1 Kaynak doğruluğu, içerik bütünlüğü ve inkar edilemezlik için güvenli e-imza S/MIME v3.1 üzerinden kullanılabilir.
Güvenli posta kutusu erişimi	RFC 2595	IMAPS POP3S

4.2.7 Güvenlik Alanı

e-Devlet güvenlik ana çatısının gereksinimlerini karşılamak için kullanılacak standartlar aşağıda sıralanmıştır. Aşağıdaki kriptografik algoritmalar standart, kılavuz veya belirtim olarak verilen referanslar dışındaki durumlarda kullanılmak üzere verilmiştir. Verilen standart, kılavuz veya belirtimde aşağıdaki kriptografik algoritmalar yer alıyorsa, bu algoritmalar benimsenendir.

Bileşen	Standart/Teknoloji	Açıklama
Ağ katmanı güvenliği	IPSec IKE sürüm 2.0 (RFC 4302, RFC 4303, RFC 4305, RFC 4306, RFC 3602)	IPSec (AH – Authentication Header) IPSec (ESP – Encapsulating Security Payload) IKE (Internet Key Exchange) Yeni uygulamalar yeni ve eski sürümleri (RFC 2402, RFC 2406, RFC 2407, RFC 4302, RFC 4303, RFC 4305, RFC 4306 RFC 3602) desteklemelidir. (VPN gereksinimleri için kullanılabilir.)
Taşıma katmanı güvenliği	TLS 1.1 (RFC 4346) SSL 3.0	Yeni uygulamalar TLS'i desteklemelidir. Durum elverdiği takdirde bu uygulamalar TLS 1.0 ve SSL 3.0'ü de desteklemelidir.
Simetrik şifreleme	AES (FIPS 197), Çalışma Kipleri (SP 800-38A 2001 ED, SP 800-38B, SP 800-38C)	
Asimetrik şifreleme	RSA (PKCS#1 sürüm 2.0)	RSA algoritması simetrik algoritmanın anahtarının şifrelenip karşı tarafa gönderilmesi için de kullanılabilir.
Sayısal imza algoritmaları (Digital Signature Algorithms)	RSA (PKCS#1 s. 2.0) DSA (ISO/IEC 14888-3) ECDSA(FIPS 186-2)	Aşağıda internet adresi verilen "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"'in amacı ve kapsamı dışında kalan uygulamalarda DSA algoritması ile SHA-1 kullanılmamalıdır. (http://www.tk.gov.tr/Duzenlemeler/Hukuki/tebligler/Tebligler.htm).
Anahtar anlaşma	DH ECDH (NIST SP 800-56A)	DH benimsenendir. ECDH değerlendirilmektedir.
Özetleme algoritmaları (Hash Algorithms)	SHA-256 SHA-384 SHA-512 (FIPS 180-2)	Bu algoritmaların dışında, aşağıda internet adresi verilen "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"'in 6. maddesinde geçen diğer algoritmalar, Tebliğ'in amacı ve kapsamı dışında kalan uygulamalarda kullanılmamalıdır (http://www.tk.gov.tr/Duzenlemeler/Hukuki/tebligler/Tebligler.htm).
Elektronik imza formatı	ETSI TS 101733(CAdEs) ETSI TS 101903(XAdEs)	AB'nde kullanılan ve elektronik imza çeşitlerini tanımlayan standartlardır.
Kriptografik mesaj söz dizimi (Cryptographic message syntax)	PKCS #7 sürüm 1.5 (RFC 2315) RFC 3852	PKCS #7 sürüm 1.5 benimsenendir. RFC 3852 değerlendirilmektedir.
Çevrimiçi sertifika durum protokolü	RFC 2560	

Bileşen	**Standart/Teknoloji**	**Açıklama**
Sertifikasyon isteği sözdizim belirtimi	PKCS #10 sürüm 1.7 (RFC 2986)	
Sertifika isteği	RFC 4211	
Sertifika profili	RFC 3280 (X.509 v3) RFC 5280	RFC 3280 benimsenendir. RFC 5280 değerlendirilmektedir.
Sertifika iptal listesi profili	RFC 3280 (X.509 v2) RFC 5280	RFC 3280 benimsenendir. RFC 5280 değerlendirilmektedir.
Sertifika verme/alma arayüzü	PKCS #12 sürüm 1.0	
Kriptografik jeton arayüzü (Cryptographic token interface)	PKCS #11 sürüm 2.11	
Kriptografik jeton bilgi sözdizimi (Cryptographic token information syntax)	PKCS #15 sürüm 1.1	
Kişisel gizlilik politikası	P3P sürüm 1.0	
Kimlik doğrulama ve yetkilendirme bilgilerinin değişimi	SAML sürüm 2.0	
Zaman damgası protokolü	RFC 3161	

5 COĞRAFİ BİLGİ SİSTEMLERİ (CBS)

5.1 ESASLAR

Coğrafi Bilgi Sistemleri; mekana/konuma dayalı çalışmalarda ve karar verme süreçlerinde kullanıcılara yardımcı olmak üzere grafik ve grafik-olmayan bilgilerin toplanması, saklanması, işlenmesi ve kullanıcıya sunulması işlevlerinin bütünlük içerisinde gerçekleştirildiği bilgi sistemidir.

Ülkemizde farklı kurum ve kuruluşlar tarafından üretilmekte olan çok farklı mekansal/konumsal veri bulunmaktadır. Bu alanda, ulusal düzeyde eşgüdüm (koordinasyon) sağlayacak idari bir mekanizmanın olmaması, veri sahipliğinde belirsizliklerin olması ve veri yapılarındaki teknik uyumsuzluklar nedeniyle disiplinler arası çalışmayı gerektiren coğrafi bilgi sistemi uygulamalarında olumsuzluklar yaşanmaktadır. Bu nedenle Bilgi Toplumu Stratejisi eki Eylem Planında 75 numaralı "Coğrafi Bilgi Altyapısı kurulumu eylemine yer verilmiş, bu kapsamda verilerin paylaşımı amacıyla bir portalin kurulması, veri sahipliği ile içerik ve değişim standartlarının belirlenmesi, ayrıca ulusal düzeyde koordinasyon sağlayacak idari ve yasal düzenlemeye ilişkin önerilerin geliştirilmesi amaçlanmıştır.

Kılavuzun bu bölümünde kurumlar arası coğrafi bilgi paylaşımının sağlanması amacıyla web servisleri, metaveri, veriye erişim, veri değişimi ve yayımlama ile ilgili uluslararası kabul görmüş standart ve servislere yer verilmiştir. Ancak, kurumlar arası birlikte çalışabilirliği tam anlamıyla sağlamak amacıyla, öncelikle ülkemize özgü bir metaveri profilinin oluşturulması gerekmektedir. Ayrıca, temel (altlık) veriler konusunda ortak kavramsal model ve kodlama modeli oluşturmak üzere ISO 19110, 19135 ve 19136 standartlarına uygun detay-öznitelik kataloğu ile GML profili oluşturulması çalışmaları yapılmalıdır.

5.2 KULLANILACAK STANDARTLAR

Bileşen	**Standart/Teknoloji**	**Açıklama**
Web harita servisi	OGC Web Map Service (WMS) ISO 19128 Geographic information -- Web map server interface	Dokümanlar için www.opengeospatial.org www.isotc211.org/ sitelerine bakınız.
Web detay servisi	OGC Web Feature Service (WFS)	Dokümanlar için www.opengeospatial.org sitesine bakınız.
Web raster servisi	OGC Web Coverage Service (WCS)	Kullanımının mümkün olduğu durumlarda önerilmektedir. Dokümanlar için www.opengeospatial.org sitesine bakınız.
Katalog servisi	OGC Catalogue Service	Dokümanlar için www.opengeospatial.org sitesine bakınız.
Koordinat dönüşüm servisi	Coordinate Transformation Service	Kullanımının mümkün olduğu durumlarda önerilmektedir. Dokümanlar için www.opengeospatial.org sitesine bakınız.

Bileşen	Standart/Teknoloji	Açıklama
Metaveri	Geographic information – Metadata (ISO 19115:2003 içerik) Metadata (ISO 19139:2007 XML uygulama şeması)	Üzerinde çalışılması gereklidir. www.isotc211.org/
Detay öznitelik kodlama kataloğu	Feature attribute coding catalogue FACC	Üzerinde çalışılması gereklidir. Dokümanlar için www.isotc211.org/ ve www.bilgitoplumu.gov.tr/kdep/rapor/kdep_47_rapor.pdf adreslerine bakınız.

6 ÇÖZÜM YAŞAM DÖNGÜSÜ

6.1 ESASLAR

Bu bölümde, sistemlere, geliştirilen çözümlere ve güvenliğe ilişkin süreçlere ait olarak kullanılacak standartlar ortaya konmuştur.

6.2 YAZILIM SÜREÇ YÖNETİMİ

TS ISO 15504 (SPICE), yazılım süreçlerinin değerlendirilmesi için bir altyapı standardıdır. Bu standart, kurumların sahip oldukları ve şu an itibariyle uyguladıkları yöntemleri iyileştirmek, ihtiyaçlar doğrultusunda kurumun yazılım süreçlerinin değerlendirilmesini sağlamak ve belirli bir sözleşme doğrultusunda tedarikçi firmanın gereksinimlere uygunluğunu değerlendirmek için kullanılmaktadır.

SPICE, gerçekleştirilen değerlendirmelerin tekrarlanabilir, kendi içerisinde tutarlı ve yeterli olduğunu garanti altına almak için değerlendirme modeli, yöntemi ve değerlendiricilerin uyması gereken kriterleri tanımlar.

TS ISO 15504; genel olarak; yazılım satın alma, yazılım geliştirme, işletim, bakım ve destek süreçleri için planlama, yönetim, gerçekleştirme, denetim ve iyileştirme aracıdır.

Yazılım Süreç Yönetimi eğitimleri ve belgelendirmesi hizmetleri Türk Standardları Enstitüsü'nden alınabilir.

CMMi (Entegre Yetenek Olgunluk Modeli); SPICE'dan farklı olarak yazılım geliştiren firmalar ve birimler için belirli seviyelerde yazılım üretim yeteneğini garanti eden ve yazılım mühendisliği ve sistem mühendisliğine ilişkin temel ilkeleri içeren bir kalite modelidir.

AQAP 160, Milli Savunma Bakanlığı tarafından verilen ve NATO askeri yazılım projeleri için CMMi 2-3, SPICE 3'ncü seviyeye karşılık gelen yazılım süreç kalitesi modelidir.

6.3 KULANILACAK STANDARTLAR

Bileşen	**Standart/Teknoloji**	**Açıklama**
Yazılım süreç denetimi	ISO 15504	Kullanılması önerilmektedir.
Yazılım süreç kalitesi	ISO 15504	Kullanılması önerilmektedir.
	CMMi	Kullanılması önerilmektedir.
	AQAP 160	Kullanılması önerilmektedir.
Sistem yaşam döngüsü süreçleri	ISO 15288	
Yazılım yaşam döngüsü süreçleri	TS ISO/IEC 12207	
Güvenlik süreçleri	TS ISO/IEC 27001, ISO/IEC 27002	
Servis sunum ve yönetimi	ISO/IEC 20000	Kullanılması önerilmektedir.

ÜÇÜNCÜ BÖLÜM

ÜÇÜNCÜ BÖLÜM

1 REHBERİ TAMAMLAYICI NİTELİKTE YÜRÜTÜLECEK ÇALIŞMALAR

Önümüzdeki dönemde kurumsal ve merkezi çalışmalar yürütülecek, örnek uygulamalar geliştirilecektir. Kurumsal uygulamalar kapsamında, kurumların birlikte çalışabilirlik ihtiyaçları çerçevesinde yürütmeleri gereken süreç çıkarma ve iyileştirme, veri şemaları hazırlama ve paylaşma çalışmalarına ilişkin model ve metodoloji hazırlanacaktır.

Çıkarılacak süreç ve hazırlanan veri şemalarının kurumlar arasında paylaşımına imkan verecek şekilde merkezi çalışmalar yapılacak, oluşturulan modelin hayata geçirilmesine yönelik pilot nitelikte örnek uygulamalar gerçekleştirilecektir.

1.1 Kurumsal Mimari Çalışmaları

Kamu kurumlarının birlikte çalışabilirlik ihtiyaçları çerçevesinde yürütmeleri gereken süreç çıkarma ve iyileştirme, veri şemaları hazırlama ve paylaşma çalışmalarına ilişkin model ve metodoloji oluşturulacaktır. Bu kapsamda, bünyesinde strateji, iş mimarisi, bilgi mimarisi, uygulama mimarisi ve teknoloji mimarisi alanlarını bulunduran, standartlaştırılabilecek bir Kurumsal Mimari Referans Modeli hazırlanacaktır.

1.2 Süreç Paylaşımı ve e-Devlet Veri Sözlüğü

Kamu kurumlarının süreç paylaşımını gerçekleştirebileceği ve merkezi bir yapıda diğer kurumların veri sözlüklerine erişebileceği merkezi kayıt depoları oluşturulacaktır.

1.3 Veri Paylaşımı

Kurumsal Mimari Çalışmaları ile yakından ilişkili olacaktır. Kamunun kamu ve iş dünyasıyla olan bilgi alış verişinde kullanacağı temel standartlar bu çalışmalarla belirlenecektir. Amaç, kamu kurumları arasında veri paylaşım standartlarının geliştirilmesi, veri şema parçalarının tekrar kullanımını destekleyerek standartlara dayalı bir şekilde gerçekleştirilebilmesini sağlamak olacaktır.

1.4 Örnek Uygulamalar

Kurumsal ve merkezi çalışmalarla oluşturulan modelin hayata geçirilmesine yönelik pilot nitelikte örnek uygulamalar gerçekleştirilecektir.

1.5 e-Hizmetlerin Geliştirilmesi ve Kolay Erişim

Geliştirilen e-hizmetlere kolay erişimi sağlamak üzere bu hizmetlere toplu halde ve kolay erişimi sağlayacak mekanizmaların oluşturulması gerekmektedir.[5]

[5] Bu amaca yönelik olarak 25 Ocak 2005 tarih ve 2005/8409 sayılı Bakanlar Kurulu Kararı ile "e-Devlet Ana Kapısı" kurulması çalışmaları başlatılmıştır.

EKLER

EK-A

AÇIKLAMALAR

Kelime İşlem, Sunum ve Elektronik Çizelge Formatları–Kullanılabilecek Bazı Araçlar :

Aşağıda belirtilen araçlar çokça bilinen ve diğerlerine oranla daha yaygın olarak kullanılan araçlar olup bu amaçlara hizmet eden farklı ürünler de mevcuttur.

Üzerinde değişiklik yapılabilen kelime işlem, sunum ve elektronik çizelge belgeleri için kullanılacağı ifade edilen formatlardan MS Office 97 formatı ile belge üretmek için MS Office programının 97 ve daha sonraki sürümleri kullanılabilir. MS Office 97 formatında (.doc, .xls ve .ppt) kaydedilmiş dosyaları görüntülemek için www.microsoft.com adresinden erişilebilecek MS Word Viewer, MS Excel Viewer ve MS Powerpoint Viewer ürünleri, Türkçe sürümlerini de kapsayacak şekilde ücretsiz olarak temin edilebilir. Aynı formattaki belgeler, www.openoffice.org İnternet adresinden, Türkçe sürümü de dahil olmak üzere, farklı diller için özelleştirilmiş sürümleri ücretsiz olarak indirilebilen açık kaynak kodlu OpenOffice programı ile de üretilebilmektedir. Söz konusu program ile aynı zamanda MS Office 97 formatında kaydedilmiş dosyalar da işlenebilmektedir. Ancak, dosyalardaki "makrolar" gibi bazı bileşenlerin işlenmesinde problem yaşanabilmektedir. StarOffice adlı program da OpenOffice programının fonksiyonlarına benzer özellikler taşımaktadır. Belirtilen ".rtf" formatında doküman üretmek hem MS Office hem de OpenOffice programları ile mümkündür. ".txt" formatı ise düz metin formatı olup kişisel bilgisayarların hemen hepsinde bulunan metin editörleri ile oluşturulabilir. OpenDocument standardının kelime işlem dokümanları için kullandığı ".odt" formatı, sunum için kullandığı ".odp" formatı ve elektronik çizelge belgeleri için ".ods" formatı ile belge üretmek OpenOffice programı ile mümkündür.

".csv" uzantılı dosyalar, Microsoft Office-Excel veya OpenOffice programlarında oluşturulan elektronik çizelgeler ".csv" uzantılı olarak kaydedilerek oluşturulabilir. ".csv" uzantılı dosyalar aslında düz metin dosyaları olup herhangi bir düz metin editörü (örneğin notepad) ile de görüntülenebilir.

Üzerinde işlem yapılmasına ihtiyaç duyulmayan kelime işlem, sunum ve elektronik çizelge belgeleri için kullanılabileceği belirtilen ".html" formatlı belgeler, Microsoft Office veya OpenOffice programı ile oluşturulduktan sonra ".html (web sayfası)" formatında kaydedilerek ya da web sayfalarını oluşturmak için kullanılan araçlar ile oluşturulabilir.

".pdf" uzantılı dosyalar ise www.adobe.com adresinden indirilebilecek "adobe reader" programı kullanılarak görüntülenebilir.

EK-B

TANIMLAR

Doküman sıkıştırma formatları

ZIP: Popüler bir dosya arşiv formatıdır. Birçok platform için yazılım alternatifleri bulunmaktadır. Bu formatı kullanan bazı şirket çözümlerinin sıkıştırma ve şifreleme metotlarının dokümantasyonunun yapılmaması nedeniyle, bazı uyum problemleri olabilmektedir. Ancak bu problemler, daha çok şifreleme ve güvenli zip standardı üzerinde olmakta olup, sıkıştırma amaçlı kullanımda sorun görünmemektedir.

TAR ve GZIP: Unix sistemlerinde kullanımları oldukça yaygındır. TAR sıkıştırmayı desteklemez. Bu nedenle, arşiv boyutunun düşürülmesi için genelde GZIP ile birlikte kullanılır. Sıkıştırılmamış dosya ve metaverilerin tek bir dosyada arşivlenmesi için TAR, bu arşivin sıkıştırılması için GZIP kullanılabilir.

7ZIP : http://www.7-zip.org/ İnternet adresinden ücretsiz olarak temin edilebilen açık kaynak kodlu bir sıkıştırma aracıdır. Bu aracın ürettiği çıktı formatı ".7z"dir.

Belge formatları

DOC: Microsoft ".doc" formatı müseccel Microsoft standardıdır.

RTF: Microsoft tarafından 1980'li yılların ortalarında birörnek metin değişimi yapabilmek üzere oluşturulmuştur. MS Word'un her yeni sürümüyle birlikte yenilenegelmiştir. Microsoft'un XML Referans Şeması son dönemde, gelecek MS Office sürümleri için ".rtf"nin yerini almıştır. ".rtf"de makrolar saklanamaz, şifre koruması ya da şifreleme desteklenmez, gömülü resimler sıkıştırılmaz.

PDF/A: PDF Referans Sürüm 1.4'ü temel alan PDF/A, ISO 19005-1:2005 ile ISO standardı olarak belirlenmiştir.

HTML: Web sayfalarının oluşturulması için kullanılan bir dizi komutlar - kodlar bütünüdür.

Karakter Kümeleri

Unicode: Unicode Standardı platform, program ve dilden bağımsız olarak her karakter için tek bir numara tanımlar. Unicode standardı bilgisayarların metin dosyalarını işlemesi için kullanılan evrensel karakter kodlama standardıdır. Unicode Standardı'nın versiyonları, karşılık gelen ISO/IEC 10646 versiyonları ile tam olarak uyumludur. Unicode'un tasarımı ASCII'nin basitliği ve uyumu üzerine inşa edilmiştir. Ancak, ASCII'nin sadece Latin alfabesini kodlama yeteneğinden daha gelişmiş yetenekleri vardır. Unicode standardı dünyadaki dillerde kullanılan tüm karakterleri kodlayabilir. Karakter kodlamasını basit ve etkin kılmak için Unicode Standardı tüm karakterlere tek bir sayısal değer ve isim atar.

ISO/IEC 10646-1:2000: Evrensel Karakter Seti uluslararası standart ISO/IEC 10646 ile tanımlanan karakter kodlama tekniğidir. Her biri sarih isimleri ile tanımlanan binlerce karakteri sayısal kodlara dönüştürür. Unicode Konsorsiyumu Unicode Standardı ve ISO/IEC 10646'yı birlikte geliştirmek için 1991 yılından bu yana ISO ile birlikte çalışmaktadır. Unicode Standardı Sürüm 2.0'ın karakter isimleri ve kodları ISO/IEC 10646-1:1993'ünküler ile aynıdır. Unicode 3.0'ın Şubat 2000'de ortaya çıkmasından sonra yeni ve güncellenmiş karakterler ISO/IEC 10646-1:2000 ile Unicode Standardı'na getirilmiştir.

Resim-Video dosya formatları

TIFF (Tagged Image File Format): Bir resim sıkıştırma formatıdır. Sıkıştırma için bir kayıpsız kodlama tekniği olan LZW metodunu kullanır. Bu metot ile resim dosyasının ikilik düzende karşılığı olan dizide bulunan belirli uzunlukta ve belirli bir yapıya sahip alt diziler kendileri ile birebir eşleştirilebilen daha küçük dizilerle temsil edilirler. Örneğin 10101 dizisi 101 ile temsil edilir. Böylece orijinalinden daha az yer kaplayan ve orijinal görüntünün hatasız olarak tekrar elde edilebileceği sıkıştırılmış bir dosya elde edilir. Bu format genellikle görüntü kalitesinin önemli olduğu (örneğin tıbbi uygulamalarda) kullanılır. Sıkıştırma çok etkin değildir. TIFF formatı müseccel Adobe standardıdır. Bununla birlikte TIF spesifikasyonu açıktır ve ücretsiz temin edilebilir.

GIF (Graphics Interchange Format): Bu formatta da sıkıştırma kayıpsızdır ve TIFF gibi LZW tekniğini kullanır, ancak renk sayısı 256'dır. Bu yüzden fotoğraf gibi resim dosyalarından ziyade çizim, animasyon gibi fazla detay gerektirmeyen görüntülerin sıkıştırılmasında kullanılır.

JPEG (Joint Pictures Experts Group): Kayıplı bir resim sıkıştırma tekniğidir. Sıkıştırılan resim tekrar açıldığında orjinalinin aynısı değil fakat ona yakındır. Bu yakınlık miktarı ayarlanabilir. JPEG ile yapılan, en genel manada, gözün algılayamayacağı veya düşük seviyede algılayabileceği frekans bileşenlerinin resim sinyalinden kaldırılmasıdır. Bu sayede görüntüde çok fazla bozulmaya meydan vermeden yüksek oranda sıkıştırma yapılabilir.

PNG (Portable Network Graphics): Kayıpsız bir kodlama tekniğidir. GIF formatında kullanılan patentli LZW'den farklı olarak patentsiz bir algoritma kullanır.

MPEG (Moving Picture Experts Group): MPEG-1 standardı 1992'de, MPEG-2 standardı ise 1994 yılında geliştirilmiştir. MPEG-1 video CD'lerinde kullanılan sıkıştırma teknolojisidir. MPEG-2 ise sayısal yayıncılık (DAB, DVB) gibi alanlarda kullanılan teknolojidir. 1999 yılında tamamlanan MPEG-4 standardı çoklu ortam içerik ile kullanıcı arasında etkileşimi ve yapay-doğal içeriği destekler. Bu standart ile içerik, nesnelerin kombinasyonu olarak tanımlanır ve kullanıcının nesneler üzerinde işlem yapmasına olanak sağlanır. Özellikle etkileşimli çoklu ortam ve mobil çoklu ortam uygulamalarında kullanılır. MPEG-7 standardı ile sayısal içeriğe ilişkin tanımlamayıcı veriler kodlanabilmekte, böylece elektronik içerik üzerinde tarama ve filtreleme gibi işlemler mümkün kılınmaktadır. Bunun da ötesinde, MPEG-7 standardı ile içerik üzerindeki fikri haklara ilişkin veri de sayısal içeriğe eklenmektedir.

İletişim protokolleri

SMTP (Simple Mail Transfer Protocol): Bu protokol İnternet üzerinden e-posta iletimi için kullanılır. Mesajlar e-posta yazılımı vasıtası ile 25 numaralı port üzerinden SMTP sunucuya gönderilir. SMTP sunucu mesajın iletileceği SMTP sunucunun IP adresini DNS sunucusundan alıp mesajı alıcı SMTP sunucuya gönderir. Alıcı SMTP sunucu da aldığı mesajı alıcının POP3 sunucusuna gönderir ve mesaj alıcının mesaj kutusuna kaydedilir.

MIME (Multi-purpose Internet Mail Extensions): Farklı karakter kümelerine sahip diller ile hazırlanmış mesajları ve çokluortam (multimedia) e-postaları iletebilmek için tasarlanmış bir belirtimdir. MIME, SMTP'nin bir uzantısıdır ve çokluortam içeriğine (ses dosyaları, görüntü-video dosyaları, ofis dokümanları vb.) sahip mesajların iletilmesinde kullanılır.

S/MIME (Secure MIME): S/MIME, MIME'nin üzerine tanımlanmış olup İnternet ortamından gönderilen e-postaların güvenilir şekilde iletilmesi için kullanılır. Güvenlikten kasıt, gönderilen mesajın bütünlüğünün korunması, inkar edememezlik, şifreleme gibi elektronik haberleşme için gerekli güvenlik hizmetlerinin sağlanmasıdır. S/MIME sadece e-posta iletileri için değil, aynı zamanda MIME formatlı veri gönderen diğer iletim mekanizmalarında (HTTP) da kullanılabilir.

POP3 (Post Office Protocol Version 3): Bu protokol ile e-posta sunucuların kayıtlı kullanıcılarına gelen mesajların alınmasına yönelik belirtimler tanımlanmıştır. Kullanıcılar e-posta kutularına gelen iletileri okumak için e-posta yazılımları ile 110 numaralı porttan POP3 sunucularına bağlanırlar. İlgili mesaj kutusuna erişebilmek için yetkilendirme gereklidir (kullanıcı adı + şifre gibi). Yetkilendirme yapıldıktan sonra kullanıcılar mesaj kutularına ulaşıp ilgili işlemleri yapabilirler. İşlemler tamamlandıktan sonra POP3 sunucusu ile bağlantı kesilir. POP3 protokolü bu işlemler için kuralları tanımlar.

HTTPS (HTTP Secure): HTTP'nin güvenli biçimidir. Bağlantı için SSL kullanılır. Güvenliğin sağlanması için güvenlik sertifikaları kullanılır ve veriler şifrelenerek gönderilir.

IMAP (Internet Message Access Protocol): POP3 gibi e-posta sunucusundan postaları okumak için kullanılan bir protokoldür. Ancak, POP3'ten farklı olarak okunan e-postalar sunucuda saklanmaya devam edilebilir ve sunucu üzerinde klasörler oluşturularak e-postalar organize edilebilir. Bu sayede e-posta sunucusuna farklı bilgisayarlar ile bağlanarak tüm e-postalara erişmek mümkün olur.

RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security): SMTP sunucuları arasındaki trafiğin güvenliğini sağlamak, gerektiğinde sunucuların birbirini yetkilendirmesine izin vermek için geliştirilmiş bir standarttır.

FTP (File Transfer Protocol): Bu protokol ile İnternet üzerindeki bilgisayarlar arasında dosya transferine ilişkin kurallar tanımlanmıştır. HTTP'nin web sayfalarının veya SMTP'nin e-posta iletilerinin iletimine benzer şekilde çalışır. Örneğin bir sunucudan dosya transfer etmek istenildiğinde veya bir sunucuya dosya yüklenmek istendiğinde (örneğin web sunucusuna web sayfalarının yüklenmesi) bu protokol kullanılır. İletişim kurulurken alıcı ile verici arasında önce bir kontrol kanalı oluşturulur. Kontrol kanalından ayrı olarak bir de veri iletim kanalı oluşturulur ve gönderilecek dosyalar bu kanal üzerinden gönderilir.

HTTP (Hypertext Transfer Protocol): HTTP, WEB'in ağ protokolüdür. OSI referans modelinin uygulama katmanında çalışır. Bu protokol ile HTML dosyaları, resimler, ses dosyaları ve diğer veriler Web üzerinden gönderilebilir. Protokol talep-cevap prensibine göre çalışır. Talep istemci bir uygulamadan gelir ve örneğin bir web sayfasının veya başka bir kaynağın transferini bir sunucudan ister. Sunucu da istenen veriyi gönderir. Veri değişiminde HTTP kullanılır. Yani veri HTTP ile tanımlanan kurallara göre iletilir ve alınır. HTTP'de veri formatları e-posta iletilerinde kullanılan formatlara benzer (İnternet mail, MIME).

NNTP (Network News Transfer Protocol): Bu protokol ile bir ağa bağlı kullanıcıların yeni haberlere/yazılara erişebilmeleri ve bu haber/yazıların NNTP sunucuları arasında iletilmesi sağlanır. Örneğin bir LAN'a bağlı kullanıcı ilgili NNTP sunucuya bağlanarak ilgilendiği haber gruplarında yeni haber/yazılar olup olmadığını inceleyerek istediklerini kendi bilgisayarına transfer edebilir. Daha büyük ağlarda ise birden fazla NNTP sunucusu bulunabilir. NNTP ile bu bilgisayarlar arasında bilgi transferinin gerçekleştirilmesine ilişkin kurallar belirlenmiştir.

TCP (Transmission Control Protocol): Paket anahtarlamalı ağlarda veri paketlerinin hangi yolu izleyerek alıcıdan vericiye ulaşacakları ağ katmanında çalışan protokollerce (örneğin IP) yürütülür. Her paket farklı yollardan alıcısına ulaşabileceğinden alıcıdaki paketlerin sırası gönderildiği sıradan farklı olabilir. Ayrıca bazı paketler yolda kaybolmuş olabilir. TCP, OSI referans modelinin ulaşım katmanında çalışır ve bir altındaki ağ katmanından gelen paketlerin sıralanması, kayıp paketlerin tekrar göndericiden istenmesi gibi görevleri yürütür.

UDP (User Datagram Protocol): UDP de TCP gibi ulaşım katmanında çalışan bir protokoldür. Ancak, TCP'nin sağladığı kalitede veri iletişimini garanti etmez. Örneğin kayıp paketlerin yeniden istenmesi veya paketleri sıralama fonksiyonları yoktur. Esasında tek yaptığı veri kontrolü (header checksum) ve verilerin portlara dağıtılmasıdır.

IPv4 (Internet Protocol Version 4): Paket anahtarlamalı ağlar (İnternet bunlardan biridir) üzerinde veri akışı paketler halinde gerçekleşir. Bir gönderici, göndereceği veriyi önce paketlere böler, ardından da sırasıyla iletişim kanalına koyar. Her paketin içerisinde üst katmanlardan gelen esas verinin yanı sıra göndericinin ve alıcının IP adreslerinin (ağ üzerindeki tüm cihazlar kendilerine has IP adresleri ile tanımlanırlar) bulunduğu bir başlık kısmı vardır. Paket, göndericisinden alıcısına ulaşana kadar ağın üzerindeki bir çok düğümden (örneğin yönlendirici) geçer. Her paket, alıcısına gönderilmesi esnasında ağın üzerindeki düğümlerin yoğunluğuna göre farklı bir rota izler. Örneğin 1. paket alıcısına on düğümden geçerek ulaşıyorsa 2. paket alıcısına üç düğümden geçerek ulaşabilir. IP, paketlerin göndericisinden alıcısına kadar izleyeceği yol boyunca iletilmesini sağlayan protokoldür (rota belirleme, zaman aşımı problemleri vb.). IP protokolünde adresler 32 bit uzunluğundadır.

IPv6 (Internet Protocol Version 6): IPv6 protokolünün temel görevi IPv4 ile aynıdır. Ancak zaman içerisinde İnternet'in yaygınlaşması ve kullanımının artması ile 32 bit olan IPv4 adreslerinin yeterli olmayacağı görülmeye başlanmış (IPv4 ile 2^{32} farklı adres elde edilebilmektedir) ve bu amaçla IPv6 geliştirilmiştir. IPv6 protokolünde adresler 128 bittir. Dolayısı ile 2^{128} farklı terminal adreslenebilir. Özellikle önümüzdeki dönemde İnternet protokolünün mobil hizmetlerde de kullanılmaya başlanması ile bu cihazlar için de IP adreslerine ihtiyaç duyulacaktır. IPv6 ile IPv4'ün adresleme kapasitesi artırılmış olmaktadır. Diğer yandan IPv6 ile bazı yeni olanaklar da getirilmiştir. Örneğin güvenlik ve kimlik tespiti, farklı hizmet tipleri (gerçek zamanlı veya olmayan uygulamalar) gibi konularda IPv4'e göre üstün özellikler eklenmiştir.

Alan adı protokolleri

DNS (Domain Name Service): İnternet üzerindeki makineler sayısal IP adresleri ile tanımlanırlar. Örneğin, 193.10.15.21 gibi. Kullanıcılar açısından bir IP adresini hatırda tutarak ilgili kaynağa (örneğin web sunucusuna) ulaşmak güçtür. Bunun önüne geçebilmek için kaynaklara hatırda tutması kolay isimler verilir (örneğin DPT Müsteşarlığı için : www.dpt.gov.tr). Ancak, bu adres İnternet ortamındaki makineler tarafından tanınmaz, bu yüzden bu adresin tanımladığı kaynağa ulaşabilmek için adresin karşılık geldiği IP numarasının bulunması gerekir. Bu işlem DNS sunucuları tarafından yapılır. Bir DNS sunucu, kendisine sorulan İnternet adresine karşılık gelen IP numarasını veren makine/yazılımdır. Tek bir DNS sunucusu tüm dünyadaki İnternet adreslerine karşılık gelen IP adreslerini bilemez. Dolayısı ile İnternet adresi-IP numarası eşleştirmesi için bir çok DNS sunucunun devreye girmesi gerekebilir. DNS protokolü bu işlemlerin nasıl yapılacağını tanımlar.

Erişim protokolleri

LDAP (Lightweighted Directory Access Protocol): Bu standart ile aranan kişiye ait bilgilere erişim sağlanması amaçlanmıştır. Örneğin e-posta gönderilecek kişinin e-posta adresi gönderici tarafından bilinmiyorsa bunun için bir veri tabanından ilgili kişinin e-posta adresi sorgulanabilir. Aynı yöntem başka türlü taramalar için de geçerlidir (örneğin bir kimsenin elektronik sertifikasına ulaşmak için). Bir sunucu (bu sunucular ülke çapında bilgi içerebileceği gibi sadece bir üniversite kampüsündeki kişilerin bilgilerini de içerebilir) üzerinde bulunan veri tabanında tarama yapılarak (tarama için anahtar kelimeler kullanılabilir, sınıflandırma yapılabilir, vb.) kişilerin bilgilerine erişmek mümkün olur. LDAP bu işlerin nasıl yapılacağını belirleyen standarttır.

Güvenlik Alanı

Kriptografi: Bilgi güvenliği temel unsurlarının oluşturulmasını sağlayan matematiksel teknikleri içeren bilim dalıdır.

Şifreleme algoritmaları: Gizliliği sağlamak amacıyla kullanılan kriptografik bir tekniktir. Bu algoritmalar, temel olarak, anahtar olarak adlandırılan bir parametreye bağlı matematiksel fonksiyonlardır. Günümüzde simetrik veya asimetrik anahtarlı şifreleme algoritmaları kullanılmaktadır. Simetrik anahtarlı algoritmalarda, üzerinde önceden anlaşılmış ve gizli tutulan tek bir anahtar kullanılırken asimetrik sistemlerde biri açık, diğeri gizli olan iki anahtar kullanılır. Asimetrik anahtarlı algoritmalarda, gizliliği sağlamak için mesaj, alıcının açık anahtarı ile şifrelenir ve ancak uygun alıcının gizli anahtarı ile açılabilir.

Özetleme algoritmaları: Bütünlüğü sağlamak üzere kullanılan bir tekniktir. Bu algoritmalar, sabit uzunlukta mesaj özetleri çıkarmak için kullanılır ve farklı mesajların özetlerinin aynı olma olasılığı çok düşük olacak şekilde tasarlanırlar. Ayrıca, orijinal mesajda yapılan ufak değişikliklerin özet değerlerinde istenen derecede farklılaşmaya yol açması beklenir.

Sayısal imza algoritmaları: Kimlik ve kaynak doğrulama ile inkar edemezlik için kullanılan temel yöntemdir. Asimetrik anahtarlı sistemler sayısal imza oluşturmak için kullanılabilir. Bunun için imza atılacak mesaj (genellikle standartlarda belirtilen bazı işlemlerden sonra mesajın özet değeri kullanılır) göndericinin özel anahtarı kullanılarak imzalanır. Uygun açık anahtara sahip olanlar imzayı doğrulayabilirler.

IPSec (IP Security): Ağ katmanı seviyesinde paketlerin güvenli iletimi ve alımı için tasarlanmış protokoller kümesidir. Özellikle VPN (virtual private network) uygulamalarında kullanılır. IPSec ile güvenliği sağlayabilmek için alıcı ve vericinin açık anahtarları kullanılır (asimetrik kriptolama).

SSL (Secure Socket Layer): Netscape tarafından web üzerinde dinleme, değiştirme ve sahteciliği önlemek için geliştirilmiş bir protokoldür. İnternet gibi güvensiz ağlarda uç noktaların kimlik doğrulaması ve iletişim güvenliği kriptografik mekanizmalar kullanarak sağlanır. Genellikle sunucu tarafın kimliği elektronik sertifikalar ile doğrulanırken istemci tarafın kimliği daha zayıf olan parola ile doğrulanır. Protokol, her iki tarafın kimliğinin kriptografik olarak güçlü mekanizmalarla (örn. elektronik sertifikalar) doğrulanmasını da sağlayabilmektedir.

TLS (Transport Layer Security): IETF tarafından SSL temel alınarak tasarlanmıştır. Aralarında bazı farklılıklar olmakla beraber büyük ölçüde SSL ile aynıdır. Her bağlantı için farklı bir simetrik kripto anahtarı kullanılır. SSL/TSL ile güvenli hale getirilmiş web sayfaları “http://” yerine “https://” ile adreslenir.

AES (Advanced Encryption Standard): Blok şifreleme algoritmasıdır. 128 bitlik mesaj bloklarını 128, 192 veya 256 bitlik simetrik anahtar kullanarak şifreler. Rijndael ismi ile de bilinen algoritma, NIST tarafından düzenlenen beş yıllık bir çalışmanın ardından, güvenlik ve farklı platformlardaki yazılım/donanım gerçeklemesinin kolaylığı ve etkinliği dikkate alınarak AES olarak seçilmiştir. Rijndael'in, 128 bitten büyük, 256 bitten küçük olmak üzere 32 bitin katları olarak seçilebilen blok ve anahtar boyları, AES olarak seçilmesinin ardından yukarıda ifade edilen şekilde sabitlenmiştir. AES, DES (ve 3DES) algoritmasının yerine 2002 yılından tarihinden itibaren standart blok şifreleme algoritması olarak kullanılmaya başlanmıştır.

RSA (Rivest-Shamir-Adleman): Hem şifreleme hem de imzalama yapmaya uygun ilk asimetrik anahtarlı kripto algoritmasıdır. Şifreleme/İmzalama ve şifre-çözme/imza kontrolü için farklı anahtarlar kullanılır. Bu anahtarlar çok büyük asal sayılar kullanılarak elde edilirler. Anahtarlardan biri sadece şifreleme/imzalama yapan tarafından bilinir (özel anahtar) ve başkalarının eline geçmemelidir. Bu anahtarın eşi olan diğer anahtar ise (açık anahtar) serbestçe iletişim kurulacak kişilere verilebilir.

DSA (Digital Signature Algorithm): NIST tarafından standartlaştırılmış (FIPS 186-2) bir asimetrik imzalama algoritmasıdır. Sadece asimetrik imza üretmek (ve kontrolü) için kullanılabilir.

ECDSA (Elliptic Curve Digital Signature Algorithm): FIPS tarafından onaylanmış sayısal imza üretimi ve doğrulamasında kullanılan bir algoritmadır.

DH (Diffie-Hellman anahtar anlaşma algoritması): Tarafların önceden bir gizem paylaşmış olmasına gerek olmadan güvensiz iletişim kanalı üzerinden anahtar oluşturmalarını sağlayan bir kriptografik algoritmadır (protokol olarak da adlandırılmaktadır). Oluşturulan anahtar üzerinde iki tarafın katkısı vardır. Oluşturulan bu anahtar simetrik şifreleme amacı ile kullanılabilmektedir. Güvenli kullanılabilmesi için tarafların kimlik doğruluğunun sağlanması gerekmektedir.

Açık Anahtar Altyapısı (AAA veya PKI): Açık anahtarın kime ait olduğunu ve geçerliliğini sorgulamada kullanılan bir altyapıdır. Bu amaçla güvenilir üçüncü taraflar, sertifika depoları ve iptal listeleri kullanılır. Güvenilir üçüncü taraflar açık anahtar ve sahibinin bilgilerini birbirine güvenli bir şekilde bağlayarak sertifika haline getirilir. Sertifikalar ve geçerlilikleri hakkında bilgiler güvenilir üçüncü taraflarca yayınlanır.

PKCS #7 (Cryptographic Message Syntax Standard): Sayısal imzalar gibi kriptolama uygulanmış veri için genel söz dizimi kurallarını tanımlayan bir standarttır.

PKCS #10 (Certification Request Syntax Standard): Bir açık anahtarın, ismin ve diğer bazı özelliklerin sertifikasyonu için söz dizimini tanımlayan standarttır.

X.509 v3 sertifika formatı: Elektronik sertifikaların yapısını tanımlayan protokoldür.

X.509 v2 sertifika iptal listesi: Açık anahtar altyapısında iptal edilen ve güvenilmemesi gereken sertifikaları (seri numaralarını) içeren ve yayınlayıcı sertifika otoritesi tarafından imzalanmış listelerdir. Sertifikaların iptal nedeni "iptal" (geri dönülemez) veya "askıda" (geri dönülebilir) olabilmektedir.

On-line certificate status protocol (elektronik imza): Sertifika iptal listelerine çevrim içi olarak başvurup sertifikaların geçerliliğini kontrol eden protokoldür.

PKCS #11 (Cryptographic Token Interface Standard): Cryptoki olarak da adlandırılan standart kriptografik bilgiyi muhafaza eden ve kriptografik fonksiyonları işleyen API'yi tanımlamaktadır.

PKCS #12 (Personal Information Exchange Syntax Standard): Kullanıcıların özel anahtarlarının, sertifikalarının ve diğer önemli bilgilerinin ne şekilde saklanıp iletileceğini tanımlayan bir protokoldür.

PKCS #15 (Cryptographic Token Information Format Standard): Kullanıcıların API sağlayıcısından bağımsız olarak kriptografik jetonlarını (token) kullanarak birden fazla uygulamaya (standarda uygun) kendilerini tanıtmalarını sağlar.

P3P (Platform for Privacy Preferences Project): P3P, web sitelerinin gizlilik politikalarını standart bir biçimde, otomatik olarak geri alınabilen ve kolayca kullanıcı ajanları (user agent) tarafından yorumlanabilen bir şekilde ifade etmesini sağlar.

(Güvenilir) Zaman Damgası: Bir dokümanın zaman damgasında belirtilen zamandan önce oluşturulduğunu ve değiştirilmediğini güvence altına almak için kullanılır.

SAML (Security Assertion Markup Language): Kimlik doğrulama ve yetkilendirme verilerinin değişik güvenlik alanları arasında (kimlik sağlayıcı ve servis sağlayıcı) değişimini ile "single sign-on" sağlamayı hedefleyen XML tabanlı bir standarttır.

Bilgi Teknoloji Ürünlerinin Güvenliği

Ortak Kriterler: 1999 yılında ISO tarafından uluslararası bilgi güvenliği standardı olarak kabul edilen ve bilgi teknolojileri ürünlerinin güvenliğini değerlendiren bir standarttır.

Bilgi Erişimi ve Değişimi

XML İmzaları: Sayısal imzalar için XML sözdizimi tanımlamak üzere W3C tarafından geliştirilmiştir. Fonksiyonel olarak PKCS#7 ile çok benzer olmakla beraber daha fazla genişletilebilir ve XML dokümanları dahil herhangi bir sayısal veri objesini imzalamaya yöneliktir. Bu teknoloji, klasik imzalamadan farklı olarak bir dokümanın farklı bölümlerinin farklı kişilerce imzalanabilmesine olanak sağlar. SOAP, SAML gibi web teknolojileri tarafından kullanılmaktadır.

Coğrafi Bilgi Sistemleri

Web Harita Servisi (Web Map Service - WMS): Harita istekleri ve görselleştirmelerini HTTP yoluyla yapmaya yarayan, sonuçları istemciye raster formatlarda (jpeg, png gibi) gönderebilen servistir. ISO 19128:2005 standardında OGC'nin Web Harita Servisi temel alınmıştır.

Vektör ve raster veri kümelerinden web tabanlı harita çıktıları oluşturulmasını ve bu haritaların yaygın bir web tarayıcısı tarafından gösterilmesini sağlar. Aynı coğrafi parametreler ve çıktı boyutu ile üretilen iki veya daha fazla harita üstüste tam çakıştırılabilir ve böylece karma/bileşik haritalar elde edilebilir.

Bu servis ISO tarafından onaylanmıştır.

Web Detay Servisi (Web Feature Service - WFS): Sunucularda farklı formatlarda tutulan vektör verileri, istemciye GML formatında göndermeyi sağlayan servistir. Vektör veriye erişme, yeni veri oluşturma, veri sorgulama, basit mekansal analizler, veri silme ve veri güncelleme özelliklerini içerir.

Web Raster Servisi (Web Coverage Service - WCS): Web Raster Servisi mevcut veriyi detaylı tanımlamaları ile birlikte sağlar. Bu verilere karşılık gelen karmaşık sorgulamalar yapılmasına olanak verir ve sadece resmedilmiş değil yorumlanabilir ve sonuç çıkartılabilir bir veriyi orjinal anlamıyla geri gönderir. Bu haliyle, gelen bir isteme karşılık olarak gerçek vektör veriyi döndüren Web Detay Servisi ve sayısal bir görüntü dosyası üreten Web Harita Servisinden farklıdır.

Katalog Servisi (Catalogue Service): Mekansal veri altyapılarında mekansal verileri arama, bulma ve erişim gibi işlemleri meta veri üzerinden yapmaya yarayan servislerdir. Bu servisler OGC dokümanında Z39.50 ve Katalog Web Servisi (OGC Catalogue Service for the Web (CS/W) protokol ve teknik belirtimleri ile tanımlanmıştır.

Metaveri genellikle bir katalog içerisinde tutulur ve katalog arayüzleri yoluyla servis ve uygulamalara erişilir. Bu servisle, istenen kriterlere uygun mekansal verinin mevcut olup olmadığı, mevcut ise hangi kurum ya da kuruluşun veri tabanında tutulduğu bilgisine ulaşılır.

Koordinat Dönüşüm Servisi (Coordinate Transformation Service): Koordinat sistemlerinin tanımlanması ve doğru hesaplamayı destekleyen koordinat dönüşüm sistemlerine erişim için standart bir yol sunar. Böylelikle mekansal yazılım sağlayıcılarına mekansal yazılımlar için birlikte çalışabilir koordinat dönüşüm bileşenleri geliştirme imkanı verir. Bu şekilde geliştirilen yazılımlarda veri almak kolaylaşır ve kullanıcılar hangi koodinat sisteminden veri aldıklarını bilmek zorunda olmadan kendi sistemlerine verileri alabilirler. Eğer uygulama, tanımlı bir koordinat sistemindeki veriyi alamaz ise, sunucu bu koordinatları yerel koordinat sistemine dönüştürür. Bu hizmet konumlama, koordinat sistemleri ve koordinat dönüşümleri konusunda bir ara yüz sağlar.

Metaveri Standardı (Metadata Standard): Metaveriler, veriler ve servisler hakkındaki tanımlayıcı bilgilerdir. Coğrafi Bilgi Sistemleri açısından bu bilgiler, konumsal veri ve servislerin detaylı tanımlamalarını içerirler. Böylece kullanıcılar, veriyi kullanmadan önce verinin amaçları için uygun olup olmadığına karar verebilir, kullanım esnasında veri hakkında bilgi sahibi olur, kullanım sonrasında ise bu verilere dayalı olarak verdikleri kararların doğruluğu ve güvenirliği konusunda tahmin yapabilirler.

Katalog servisleri üzerinden istenen verinin bulunabilmesi ve her veri tabanı için farklı bir arama kriteri belirlenmesinin önüne geçilebilmesi için metaveri şemasının uluslararası standartlara uygun olması gerekmektedir.

Detay Öznitelik Kodlama Kataloğu (Feature Attribute Coding Catalogue - FACC): Hakkında bilgi toplanacak gerçek dünya varlıkları, bunlara ilişkin tutulacak bilgilerin ve bilgi toplamada uyulacak kuralların tanımlanarak modellendirilmesini anlatan standarttır. Aşağıdaki bilgileri içerir:

- Detaylar (kodları, isimleri ve tanımları),
- Öznitelikler (kodları, isimleri ve tanımları),
- Öznitelik değerleri (kodları, isimleri ve tanımları),
- Her detaya ilişkin öznitelikler ve alabileceği değerler,
- Her özniteliğin ilişkili olduğu detaylar

Diğer Tanımlar

Bütünleştirilmiş Modelleme Dili (UML): Tasarım, tanımlama, görselleştirme, yapılandırma ve dokümantasyon gibi işlevlerin yerine getirilmesine imkan veren sistem modelleme dilidir. Yazılım sistemleri başta olmak üzere, gerçek hayattaki sistemlerin modellemesinde kullanılan bu araçtan birlikte çalışabilirlik, yeniden kullanılabilirlik, platform bağımsızlığı gibi temel hedeflere ulaşmada yararlanılabilmektedir.

Akış Şeması (Flowchart): Belli bir süreçteki adımları grafik sembollerle gösteren şemaya akış şeması denir. Akış şeması sembolleri ANSI (American National Standards Institute) standardı olarak belirlenmiştir. Akış şemaları; süreçlerin, mevcut süreçlere nasıl entegre edileceği ve hangi alanlarda iyileştirmeye gerek olduğunun belirlenmesine yardımcı olmaktadır.

Nesne Bağıntı Çizeneği (E/R Diagram): E-R veri modeli gerçek dünyanın nesneler ve bu nesneler arasındaki ilişkiler kümesi olarak ifade edilmesinde yararlanılır. Özellikle veri tabanı tasarımında, veri tabanının kavramsal yapısını ortaya koymak için kullanılır.

Veri Akış Çizeneği (DFD): Yapısal analiz ve tasarım için kullanılan, verinin sisteme girişi ve süreçler arasındaki akışını, mantıksal depolanmasıyla birlikte gösteren çizeneklerdir.

XML Şema Tanımlama Dili (XSD): XML Şema Tanımlama Dili, XML dokümanlarının yapısı ile ilgili bilgi içeren XML tabanlı dokümanlardır. XML dokümanlarının yapısı ve veri tipinin tanımlamasında kullanılır.

XSL: XML dokümanında format ve gösterime ilişkin komutları sağlayan metin dosyası oluşturma dilidir. Aynı XML dokümanı, farklı donanımlarda farklı şekillerde sunulabilir. Bu amaçla, sunum yapılacak elektronik ortamın özelliklerine uygun şekilde dönüştürme işlemi yapılır.

XML: Bağımsız bir kuruluş olan W3C (World Wide Web Consortium) organizasyonu tarafından tasarlanan ve herhangi bir kurumun tekelinde bulunmayan XML (eXtensible Markup Language), kişilerin kendi sistemlerini oluşturabilecekleri, kendi etiketlerini tanımlayarak çok daha rahat ve etkin programlama yapabilecekleri ve belirlenen bu etiketleri kendi yapıları içerisinde standartlaştırabilecekleri esnek, genişleyebilir ve kolay uygulanabilir bir meta dildir.

Basit Nesne Erişim İletişim Kuralı (SOAP): Dağıtık uygulamalarda ve web servislerinin haberleşmesinde kullanılmak üzere tasarlanan, uygulamaların birbirlerine çağrı yapabilmeleri için oluşturulmuş bir standarttır. Uygulamaların İnternet aracılığıyla birbirlerinden nasıl bir istekte bulunacağını, bir isteğe nasıl karşılık verileceğini tanımlar.

Evrensel Açıklama, Keşif ve Entegrasyon (UDDI): Web servisleri ile ilgili olarak bir adres defteri işlevi görür. Web servislerini İnternet'te tanımlamak için oluşturulmuş bir belirtimdir. Hangi web servisinin nerede olduğunu ve ne işe yaradığını bildirmek için kullanılır.

Web Servisleri Tanımlama Dili (WSDL): Bir XML web servisinden hangi işlevlerin sağlanabileceğini, bu işlevleri çağırmak için hangi parametrelerin girilmesi gerektiğini ve servisten dönecek olan verinin tipinin ne olduğunu tanımlamaya yönelik bir standarttır.

Dublin Core Öge Kümesi: Yaygın olarak bilinen ve sıkça uyarlanarak kullanılan Kaynak Keşfi Metaverisi öge kümesidir. Dublin Core'un bu derece yaygın olarak kullanılmasının nedeni, oluşturulması ve yönetimindeki basitlik, ortak anlamlandırmaya verdiği imkan, uluslararası yaygınlığı ve geliştirilebilirliğidir.

EK-C

KISALTMALAR

AAA	**:**	Açık Anahtar Altyapısı (Bkz. PKI)
AES	**:**	Advanced Encryption Standard (simetrik şifreleme algoritması)
ANSI	**:**	American National Standards Institute
ASAP	**:**	Asynchronous Service Access Protocol
ASCII	**:**	American Standard Code for Information Interchange
BGYS	**:**	Bilgi Güvenliği Yönetim Sistemi
BPMN	**:**	Business Process Modeling Notation
BS	**:**	British Standards
BSI	**:**	British Standards Institution
CBS	**:**	Coğrafi Bilgi Sistemleri
CC	**:**	Common Criteria
CS/W	**:**	Catalogue Service for the Web
DAV	**:**	Distributed Authoring and Versioning
DFD	**:**	Data Flow Diagram (Veri Akış Çizeneği)
DH	**:**	Diffie-Hellman
DNS	**:**	Domain Name Service
DSA	**:**	Digital Signature Algorithm (asimetrik kriptolama)
ECDSA	**:**	Elliptic Curve Digital Signature Algorithm
ESP	**:**	Encapsulation Security Payload
ETSI	**:**	European Telecommunications Standards Institute
FACC	**:**	Feature Attribute Coding Catalogue
FIPS	**:**	Federal Information Processing Standards
FTP	**:**	File Transfer Protocol
GIF	**:**	Graphics Interchange Format
GML	**:**	Geography Markup Language
HTTP	**:**	Hypertext Transfer Protocol
HTTPS	**:**	HTTP Secure
IEC	**:**	International Engineering Consortium
IETF	**:**	Internet Engineering Task Force
IKE	**:**	Internet Key Exchange
IMAP	**:**	Internet Message Access Protocol
IMAPS	**:**	Secure Internet Message Access Protocol
IP	**:**	Internet Protocol
IPv4	**:**	Internet Protocol Version 4
IPv6	**:**	Internet Protocol Version 6
IPSec	**:**	IP Security Protocol Charter
ISO	**:**	International Organization for Standardization

ISO/TC 211	**:**	Geographic information/Geomatics standards technical committee
IT	**:**	Information Technology
JPEG	**:**	Joint Pictures Experts Group
LDAP	**:**	Lightweighted Directory Access Protocol
LZW	**:**	Lempel Ziv Welch
MIME	**:**	Multi-purpose Internet Mail Extensions
NAT	**:**	Network Address Translation
NIST	**:**	National Institute of Standards and Technology
NNTP	**:**	Network News Transfer Protocol
OASIS	**:**	Organization for the Advanced of Structured Information
OGC	**:**	Open Geospatial Consortium
OWL	**:**	Web Ontology Language
PD	**:**	Published Document
PDF/A		Portable Document Format/Archive
PKCS	**:**	Public Key Cryptography Standard
PKI	**:**	Public Key Infrastructure (**AAA-**Açık Anahtar Altyapısı)
PNG	**:**	Portable Network Graphics
P3P	**:**	Platform for Privacy Preferences Project
POP3	**:**	Post Office Protocol Version 3
POP3S	**:**	Secure Post Office Protocol 3
RFC	**:**	Request For Comments
RSA	**:**	Rivest-Shamir-Adleman
S/MIME	**:**	Secure Multipurpose Internet Mail Extensions
SAML	**:**	Security Assertion Markup Language
SHA-1	**:**	Secure Hash Algorithm – 1
SIP	**:**	Session Initiation Protocol
SMTP	**:**	Simple Mail Transfer Protocol
SOAP	**:**	Simple Object Access Protocol
SSL	**:**	Secure Socket Layer (iletim katmanı güvenliği)
TCP	**:**	Transmission Control Protocol
TIFF	**:**	Tag Image File Format
TLS	**:**	Transport Layer Security (taşıma katmanı güvenliği)
TS	**:**	Türk Standartları
TSP	**:**	Timestamp Protocol
UDDI	**:**	Universal Description, Discovery and Integration
UDP	**:**	User Datagram Protocol
UML	**:**	Unified Modelling Language
URI		Uniform Resource Identifier

VPN	**:**	Virtual Private Network
W3C	**:**	World Wide Web Consortium
WCS	**:**	Web Coverage Service
WebDAV	**:**	Web Distributed Authoring and Versioning
WFS	**:**	Web Feature Service
WMS	**:**	Web Map Service
WS	**:**	Web Services
WSDL	**:**	Web Services Description Language
XKMS	**:**	XML Key Management Specification
XMI	**:**	XML Metadata Interchange
XMPP	**:**	Extensible Messaging and Presence Protocol
XML	**:**	eXtensible Markup Language
XSD	:	eXtensible Mark-up Language Schema Definition
XSL	:	eXtensible Stylesheet Language

Bu Rehberle ilgili sorularınız ve güncelleştirme önerilerinizi lütfen;

e-posta ile birliktecalis@dpt.gov.tr adresine iletiniz.

Bu dokümanın güncel ve yürürlükte olan sürümüne http://bilgitoplumu.gov.tr/yayin/eDTrBirlikteCalisabilirlik.pdf adresinden erişebilirsiniz.