T.C.
KALKINMA BAKANLIĞI

e-DÖNÜŞÜM TÜRKİYE PROJESİ

BİRLİKTE ÇALIŞABİLİRLİK ESASLARI REHBERİ

Sürüm 2.1

BİLGİ TOPLUMU DAİRESİ

MAYIS 2012

e-DÖNÜŞÜM TÜRKİYE PROJESİ

BİRLİKTE ÇALIŞABİLİRLİK ESASLARI REHBERİ

Sürüm 2.1

BİLGİ TOPLUMU DAİRESİ

MAYIS 2012

Bu Rehberle ilgili sorularınız ve güncelleştirme önerilerinizi
e-posta ile lütfen birliktecalis@kalkinma.gov.tr adresine iletiniz.

Bu dokümana http://www.bilgitoplumu.gov.tr adresinden erişebilirsiniz.

Bu Rehberin önceki sürümleri ve yayınlanma tarihleri:

Sürüm 2.0 : Şubat 2009
Sürüm 1.0 : Temmuz 2005

KALKINMA BAKANLIĞI
Bilgi Toplumu Dairesi Başkanlığı

İnternet Adresi: http://www.bilgitoplumu.gov.tr
e-Posta: btd@kalkinma.gov.tr
Telefon: +90 312 294 6609
Faks: +90 312 294 6677

Bu Rehber, Kalkınma Bakanlığı Bilgi Toplumu Dairesi koordinasyonunda, Başbakanlık, Başbakanlık Devlet Arşivleri Genel Müdürlüğü, Maliye Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Çevre ve Şehircilik Bakanlığı Coğrafi Bilgi Sistemleri Genel Müdürlüğü, Türk Standardları Enstitüsü, Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu – Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (TÜBİTAK-BİLGEM), Tapu ve Kadastro Genel Müdürlüğü, Türkiye Cumhuriyet Merkez Bankası, TÜRKSAT, Türkiye Bilişim Vakfı ve Türkiye Bilişim Derneği katkılarıyla hazırlanmıştır. Rehber'in ilk sürümünden itibaren görüşleri ile katkı sağlayan tüm kurum ve kuruluşları ile temsilcilerine teşekkür ederiz.

2009/4 Sayılı Başbakanlık Genelgesi

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:

GENEL ESASLAR ve BİRLİKTE ÇALIŞABİLİRLİK POLİTİKASI

BİRİNCİ BÖLÜM

1.1 GİRİŞ

Kalkınma Bakanlığı koordinasyonunda hazırlanan bu Rehber, kamu, özel sektör ve sivil toplum kuruluşlarının katkıları ile şekillenmiş olup, yine aynı kurum ve kuruluşların katkıları ile güncellenmeye ve geliştirilmeye devam edilmektedir.

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 yürütülmesi öngörülen Rehberi tamamlayıcı nitelikteki çalışmalara yer verilmektedir.

Rehberin Teknik Standartlar bölümünde 6 temel konuda esaslar ve kullanılacak standartlar belirlenmiştir. Bu temel konular; (1) dosya sunumu ve değişimi, (2) ara bağlantı, (3) veri entegrasyonu ve içerik yönetimi, (4) güvenlik, (5) coğrafi bilgi sistemleri ve (6) bilgi sistemlerinin geliştirilmesi ve yönetimidir. 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 projesi tekliflerinin hazırlanmasına ilişkin usul ve esasların belirlendiği "Kamu Bilgi ve İletişim Teknolojileri Projeleri Hazırlama Kılavuzu"nda Rehber'e uyum zorunlu kılınmıştır.

Rehber'in hazırlanmasında, başta Pan-Avrupa e-Devlet Hizmetleri için Avrupa Birlikte Çalışabilirlik Çerçevesi (European Interoperability Framework for Pan-European e-Government Services)[2] ve Avrupa Kamu Hizmetleri için Avrupa Birlikte Çalışabilirlik Çerçevesi (European Interoperability Framework for European Public Services)[3] olmak üzere bu konuda kapsamlı çalışmalar yapmış ülke örnekleri ve bu ülkelerin yayımladıkları birlikte çalışabilirlik dokümanlarından istifade edilmiştir.

[2] http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529 adresinden erişilebilir.
[3] http://ec.europa.eu/isa/strategy/doc/annex_ii_eif_en.pdf adresinden erişilebilir.

1.2 GENEL ESASLAR

1.2.1 AMAÇ

Bu Rehber, e-Dönüşüm Türkiye Projesi kapsamında başta kamu kurum ve kuruluşları 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.

1.2.2 KAPSAM

Birlikte çalışabilir e-devlet yapısı farklı gruplar için farklı birlikte çalışabilirlik ihtiyaçları taşır. Rehber kapsamında, kamunun üç farklı grupla etkileşimine ilişkin genel esas, politika ve teknik standartlar yer almaktadır.

Söz konusu gruplardan ilki, sistemin doğrudan kullanıcısı olan ve sistemle ilişkilerden doğrudan etkilenen vatandaştır. İkinci grup iş dünyası olup, veri değişimi ihtiyaçları bir öncekine göre daha karmaşıktır. Üçüncü grup ise, Rehber'in odağını oluşturan kamu kurum ve kuruluşlarıdır. Merkezi kurum ve kuruluşlar ile yerel yönetimleri içerecek şekilde, kamunun kendi içinde birlikte çalışabilirliğinin sağlanması ve buna karşılık gelen ihtiyaçların belirlenmesi ve karşılanması etkin bir e-devlet yapısı açısından önem arz etmektedir.

1.2.3 TANIMLAR ve KISALTMALAR

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

Bu Rehber'de kullanılan kısaltmalar EK-C'de yer almaktadır.

1.2.4 UYUM MEKANİZMALARI

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

Rehber'e uyumu sağlamak üzere, Yatırım Programlarında yer alan bilgi ve iletişim teknolojileri projeleri için her yıl güncellenen Kamu Bilgi ve İletişim Teknolojileri Projeleri Hazırlama Kılavuzunda, Birlikte Çalışabilirlik Esasları Rehberi'ne atıfta bulunularak, Rehber'e uyum zorunlu tutulmuştur.

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

1.2.5 YETKİ ve SORUMLULUKLAR

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

Rehber'in uygulanmasına ilişkin genel koordinasyon Kalkınma Bakanlığı tarafından yürütülecektir.

1.2.6 REHBER 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 Kalkınma Bakanlığı tarafından güncellenecektir.

Dokümanın ikinci bölümünde yer alan teknik standartlar, acil ihtiyaç bildirilmesi durumunda ya da düzenli olarak yapılacak gözden geçirmeler sonucu ihtiyaç görüldüğünde günün koşullarına uyumlu hale getirilmek üzere güncellenecektir. Güncellemeler bu Rehber'i hazırlayan "Birlikte Çalışabilirlik Çalışma Grubu" tarafından değerlendirilecektir. İhtiyaç duyulması halinde bu çalışma grubu, görüş bildiren ve önerilerde bulunan kamu kurum ve kuruluşları başta olmak üzere, ilgili tüm kesimlerin katılımıyla genişletilecektir.

Dokümana ilişkin her türlü öneri "birliktecalis@kalkinma.gov.tr" adresine e-posta yolu ile ya da Kalkınma Bakanlığına yazılı olarak iletilebilir.

Gerekli görülen güncellemeleri yapma görev ve yetkisi Kalkınma Bakanlığına aittir.

1.3 BİRLİKTE ÇALIŞABİLİRLİK POLİTİKASI

1.3.1 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[4].

e-Devlet kapsamında birlikte çalışabilirliği sağlamaya yönelik faaliyetlerin amacı, düzenleyici rol üstlenerek, kamuda etkin bilgi paylaşımını sağlamak ve böylelikle bir yandan bilgi teknolojilerine (BT) 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

[4] Burada yer verilen tanım, European Public Administration Network eGovernment Working Group tarafından hazırlanan "Key Principles of an Interoperability Architecture" adlı çalışmadan alınmıştır.
(Kaynak: http://www.epractice.eu/files/media/media_553.pdf).

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.

Birlikte çalışabilirlik ihtiyaçları içerisinde genel olarak teknik boyutu kapsayan Rehber'in, 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 sağlaması hedeflenmektedir.

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 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. Bu çalışmalar Rehber'deki esaslar çerçevesinde sorumlu kuruluşlar tarafından üstlenilecektir.

1.3.2 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, göz önünde bulundurulan ve mevcut durumun izin verdiği ölçüde uyulan esaslar aşağıda ifade edilmektedir.

1.3.2.1 Avrupa Komisyonu Çalışmalarıyla Uyum

Esaslar belirlenirken, Avrupa Komisyonu çalışmalarıyla uyum gözetilmiş, "İdareler Arası Veri Değişimi Programı (IDA)" ve "pan-Avrupa Hizmetlerinin İdareler, İş Dünyası ve Vatandaşlara Birlikte Çalışır Sunumu Programı (IDABC)" kapsamında yürütülen çalışmalar ve hazırlanan raporlardan yararlanılmıştır. Bundan sonraki çalışmalarda da başta Avrupa

Kamu İdareleri için Birlikte Çalışabilirlik Çözümleri Programı (ISA) olmak üzere Avrupa Komisyonu bünyesinde sürdürülmekte olan çalışmalardan yararlanılacaktır.

1.3.2.2 Ana İletişim Mekanizması Olarak İnternet ve www'nin Kullanımı

Kamu hizmetlerinin sunumunda, maliyet ve riskleri düşürebilmek amacıyla, internetin tüm taraflarca aktif olarak kullanımı sağlanmalıdır. Bu amaçla geliştirilecek uygulamaların arayüz olarak W3C standartlarını sağlayan internet tarayıcılarını (browser) desteklemesi esastır. Kullanıcı tarafından herhangi bir lisans ücreti gerektirmeyecek şekilde tarayıcı vasıtasıyla indirilebilen eklenti ve aracı yazılımlardan yararlanılabilir.

1.3.2.3 Eşit Erişim Hakkı

Bilgi ve hizmetlerin internet 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. Bu kapsamda, 12/11/2010 tarihli ve 27757 sayılı Resmi Gazetede yayımlanan "Ulaşılabilirlik Stratejisi ve Ulusal Eylem Planı (2010-2011)" esas alınacaktır.

1.3.2.4 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.

1.3.2.5 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.

1.3.2.6 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[5]:

1. 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.

2. 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.

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

4. Standardın yeniden kullanımı konusunda hiç bir sınırlama olmamalıdır.

1.3.2.7 Anlamsal Bütünlüğü Sağlayacak Ortak Standartların Kullanımı

Veri değişiminde anlam bütünlüğünü sağlamak ve veri içeriğine ilişkin farklı yorumları engellemek üzere uluslararası standartlar ve kamuda kullanımına karar verilen yapı, uygulama ve çözümler kullanılacaktır.

1.3.2.8 Ölçeklenebilirlik

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

1.3.2.9 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.

1.3.2.10 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. Rehber'in güncelleştirilmesi sürecinde Genel Esaslar'da Rehber Güncelleme başlığı altında belirtilen yöntem kullanılacaktır.

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

İKİNCİ BÖLÜM
TEKNİK STANDARTLAR

İKİNCİ BÖLÜM

Bu bölümde listelenen standart, format, belirtim (specification) ya da kılavuzlar, 4 farklı kategoride sınıflandırılmıştır:

1. **Uyulması Zorunlu:** Kamu kurumları tarafından ilgili bileşene ilişkin açıklama bölümünde belirtilen kapsamda uyulması zorunlu standart, format, belirtim ya da kılavuzları ifade eder.

2. **Takdire Bırakılan:** İhtiyaçlara bağlı olarak, ilgili bileşene ilişkin açıklama bölümünde belirtilen kapsamda uyulması zorunlu olan, ancak bu bileşen altında listelenenler arasından seçimi kurumun takdirine bırakılan standart, format, belirtim ya da kılavuzları ifade eder.

3. **Önerilen:** İhtiyaçlara bağlı olarak kullanımı önerilen standartları ifade eder.

4. **Üzerinde Çalışılan:** Rehber'de zorunlu tutulması için bir takım geliştirmeler ve incelemeler gerektiren veya henüz geliştirilmemiş, ancak geliştirilmesi gereken standartlar bu kategori altında belirtilmiştir.

Bu bölümde birlikte çalışabilirlik ihtiyaçlarını karşılamaya yönelik olarak kullanılması, uyulması veya sağlanması gereken standartlar, yukarıda yer verilen sınıflandırmaya uygun olarak 6 ana başlık altında değerlendirilmiştir.

2.1 DOSYA SUNUMU ve DEĞİŞİMİ

2.1.1 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 dosyaların 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.

2.1.2 KULLANILACAK STANDARTLAR

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

2.1.2.1 Dosya Sunumu

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Dosya sıkıştırma ve Arşivleme	ZIP (.zip)	2	Kullanım yaygınlığı itibarıyla genel amaçlı kullanımda ZIP tercih edilmelidir. GZIP, TAR ile beraber kullanıldığında, büyük boyutlu dosyalarda daha yüksek sıkıştırma oranına sahiptir. TAR, sıkıştırma amaçlı kullanılmamakta olup sadece arşivleme amacıyla kullanılmaktadır.
	GZIP (.gz)	2	
	7ZIP (.7z)	2	
	TAR (.tar)	2	
Üzerinde işlem yapılamayan kelime işlem, sunum ve elektronik çizelge belgeleri	Hypertext File Format v4.01 (.html)	2	Üzerinde işlem yapılamayan belgelerin internet üzerinden sunumunda mümkün olan durumlarda HTML tercih edilmelidir. PDF kullanılması durumunda 1.6 ve öncesi sürümler tavsiye edilmektedir.
	Portable Document Format (.pdf)	2	
Üzerinde işlem yapılabilen kelime işlem belgeleri	Microsoft Word 97 (.doc)	2	Standart/teknoloji tercihi yapılırken, kurumsal ihtiyaçlar, bu dosyaların paylaşıldığı ve belgeler üzerinde değişiklik yapması beklenen son kullanıcıya getirdiği ilave yükler ve kullanım kolaylığı dikkate alınmalıdır. Bu bölümde belirtilen formatlar ve bu formatlarda belge üretebilen araçlar konusunda daha detaylı bilgiler EK-A'da verilmiştir.
	Zengin metin biçimi (.rtf)	2	
	Düz metin (.txt)	2	
	OpenDocument (.odt), ISO/IEC 26300:2006	2	
	Office Open XML (.docx), ISO/IEC 29500:2008	2	
Üzerinde işlem yapılabilen elektronik çizelge belgeleri	Virgül ile ayrılmış değer (.csv)	2	Standart/teknoloji tercihi yapılırken, kurumsal ihtiyaçlar, bu dosyaların paylaşıldığı ve belgeler üzerinde değişiklik yapması beklenen son kullanıcıya getirdiği ilave yükler ve kullanım kolaylığı dikkate alınmalıdır. Bu bölümde belirtilen formatlar ve bu formatlarda belge üretebilen araçlar konusunda daha detaylı bilgiler EK-A'da verilmiştir.
	Microsoft Excel 97 (.xls)	2	
	OpenDocument (.ods) ISO/IEC 26300:2006	2	
	Office Open XML (.xlsx), ISO/IEC 29500:2008	2	

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Üzerinde işlem yapılabilen sunum belgeleri	Microsoft Powerpoint 97 (.ppt)	2	Standart/teknoloji tercihi yapılırken, kurumsal ihtiyaçlar, bu dosyaların paylaşıldığı ve belgeler üzerinde değişiklik yapması beklenen son kullanıcıya getirdiği ilave yükler ve kullanım kolaylığı dikkate alınmalıdır. Bu bölümde belirtilen formatlar ve bu formatlarda belge üretebilen araçlar konusunda daha detaylı bilgiler EK-A'da verilmiştir.
	OpenDocument (.odp), ISO/IEC 26300:2006	2	
	Office Open XML(.pptx), ISO/IEC 29500:2008	2	
Karakter Kümesi	UNICODE	2	Unicode standardı ile ISO/IEC 10646-1:2000 standartları birbiri ile uyumludur.
	ISO/IEC 10646-1:2000	2	
Resim Dosyaları	Tagged Image File Format (.tiff)	2	TIFF ve BMP, veri kaybına izin verilmediği durumlarda tercih edilmelidir. GIF, çizim, animasyon gibi fazla detay içermeyen görüntülerin sıkıştırılmasında kullanılmalıdır. 24 bit renk derinliği destekleyen JPEG formatı renk duyarlılığı gereken, fakat veri kaybına izin veren durumlarda kullanılmalıdır. GIF'e nazaran daha fazla sıkıştırma sağlayan PNG formatı, bazı kısımları saydam olan resimlerde daha iyi sonuç vermektedir. Daha yüksek sıkıştırmaya ihtiyaç duyulan durumlarda ise ECW formatı kullanılabilir.
	Graphics Interchange Format (.gif)	2	
	Joint Photographic Experts Group (.jpg, .jpeg), ISO 10918	2	
	Portable Network Graphics (.png), ISO/IEC 15948:2004	2	
	Enhanced Compressed Wavelet (.ecw)	2	
Animasyonlar	Hareketli GIF	2	Eklenti (plug-in) gerektirmemesi nedeniyle hareketli GIF tavsiye edilmektedir.
	Adobe Flash (.swf)	2	
	Adobe Shockwave (.swf)	2	
Ses-Video	MPEG-1, ISO 11172	2	MP3 formatı yaygın kullanılmakla birlikte, bu formatta dosya oluşturmak telif ücreti ödenmesini gerektirebilir. Veri kaybı istenmeyen durumlarda WAV formatı kullanılmalıdır. OggTheora video formatı, OggVorbis ise ses formatıdır. OggTheora ve OggVorbis veri kaybına izin verilen durumlarda kullanılmalıdır.
	MPEG-4 (.mp4) , ISO 14496	2	
	MP3 (.mp3)	2	
	WAV (.wav)	2	
	Apple Quicktime (.mov/.qt)	2	
	Adobe Flash (.swf/.flv)	2	
	OggTheora (.ogg/.ogv)	2	
	OggVorbis (.ogg/.oga)	2	
	Audio Video Interleave (.avi)	2	

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Gerçek Zamanlı Ses-Video Yayını	Real Audio / Real Video	2	Gerçek zamanlı ses ve video yayını için ITU tarafından geliştirilen H.263 veya H.264 standardını destekleyen herhangi bir format kullanılabilir. Bu formatlardan bazıları listelenmektedir.
	Adobe Flash	2	
	Microsoft Windows Media Format (.asf)	2	
	Apple Quicktime (.mov/.qt)	2	
	Ogg Media	2	

2.1.2.2 Kamu Kurum ve Kuruluşları Arasında İletilen Resmi Yazışmalar

Bu bölümde, e-Yazışma Projesi kapsamında, kamu kurum ve kuruluşları arasında iletilen resmi yazılar için belirlenen formatlar sunulmaktadır. Kurumlar, kendilerine başka kurumlar tarafından gönderilen ve aşağıda belirtilen formatlarda hazırlanmış üst yazı ve eklerini, elektronik belge sistemlerine entegre etmekle yükümlüdürler. Bu kapsamda, metin tabanlı ekler ile, ses ve resim dosyalarının paylaşımında kullanılacak müşterek standartlar ortaya konmuştur. Diğer taraftan, kamu kurum ve kuruluşları, karşılıklı olarak üzerinde anlaşmaları halinde, dokümanların değişimine sebep olan kod veya makroları içermeyecek şekilde başka formatlarda da belge alışverişi yapabilirler. Burada yer verilmeyen formatlardaki dosya paylaşımında kurumlar arası ikili anlaşmalar esastır.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Üst Yazı ve Metin Tabanlı Ekler	ISO/IEC 19005-1:2005, Portable Document Format/Archive (PDF/A) (.pdf)	1	Kamu kurum ve kuruluşları, e-Yazışma Projesi kapsamında, kendilerine gönderilen ve PDF/A formatında oluşturulmuş üst yazı ve eklerini elektronik belge sistemlerine entegre etmekle yükümlüdürler. PDF/A, dokümanların oluşturulduğu ya da görüntülendiği bilgisayara bağlı kalmayacak şekilde görüntülenmesini sağlar. Ancak bunun bir sonucu olarak, doğuracağı depolama ihtiyaçları daha fazla olacaktır. Bant genişliği ve depolama maliyetleri gözetilerek, metin fontu olarak Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelikte belirtildiği şekilde "Times New Roman" fontu kullanılması ve doküman içerisinde sadece bu fontun yer alması gereklidir. PDF/A'nın bir diğer özelliği içine ses, video ve işlenebilir dosyaların eklenememesidir. Üstyazı ve metin tabanlı eklerin içine gömülebilecek sayısal grafik, diyagramlar ve fotoğraflar için aşağıdaki ilgili kısımlara bakınız.
Sayısal Grafik ve Diyagramlar	Graphics Interchange Format (.gif)	1	Üstyazı ve metin tabanlı eklerin içine gömülebilecek sayısal grafik ve diyagramlar için bu formatın kullanılması zorunludur.
Sayısal Fotoğraflar	Joint Photographic Experts Group (.jpg, .jpeg), ISO 10918	1	Üstyazı ve metin tabanlı eklerin içine gömülebilecek sayısal fotoğraflar için bu formatın kullanılması zorunludur.

2.2 ARA BAĞLANTI

2.2.1 ESASLAR

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

Aşağıda yer alan standartların büyük kısmı endüstri standardı olan ve halihazırda yaygın şekilde kullanılan standartlardır. Bununla birlikte kurumlar, karşılıklı olarak mutabık kalmak kaydıyla, kendi aralarındaki haberleşmeler için burada listelenen standartlardan başka standartlar da kullanabilirler.

2.2.2 KULLANILACAK STANDARTLAR

2.2.2.1 İnternet Aktarım Protokolleri

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
İnternet protokolü	IPv4 RFC 791	2	IPv6 kullanımıyla ilgili olarak, 08/12/2010 tarihli Resmi Gazete'de yayımlanan 2010/25 sayılı Başbakanlık Genelgesi dikkate alınmalıdır.
	IPv6 RFC 2460	2	
Taşıma (transport)	TCP RFC 793	2	İletim (transport) katmanında bağlantı yönelimli (connection-oriented) iletişime ihtiyaç duyuluyorsa TCP, bağlantısız (connectionless) iletişime ihtiyaç varsa UDP kullanılmalıdır.
	UDP RFC 768	2	

2.2.2.2 e-Posta Protokolleri

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
e-Posta taşıma (e-mail transport)	SMTP/MIME RFC 2821 (SMTP), RFC 2822, RFC 2045 ve RFC 2231 (MIME Part One), RFC 2046 (MIME Part Two), RFC 2047 ve RFC 2231 (MIME Part Three), RFC 4289 (MIME Part Four), RFC 2049 (MIME Part Five), RFC 3798, RFC 2142	1	e-Posta mesajlarının taşınmasında bu standardın kullanılması zorunludur.
e-Posta taşıma güvenliği (e-mail transport security)	RFC 3207	3	Güvenlik kısmında belirtilmiştir. (2.4.2.6 no'lu bölüme bakınız)

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
e-Posta kutusu erişimi (e-mailbox access)	POP3 RFC 1939, RFC 2449, RFC 5034	2	e-Posta kutusuna erişimin farklı terminal ve lokasyonlardan olacağı uygulamalar için IMAP kullanılmalıdır. Böyle bir ihtiyaç yoksa POP3 kullanılabilir.
	IMAP RFC 3501, RFC 4466, RFC 2971, RFC 3502, RFC 3503, RFC 2177, RFC 4469	2	
e-Posta içerik güvenliği (e-mail content security)	RFC 3850 RFC 3851 RFC 3852	3	Güvenlik kısmında belirtilmiştir. (2.4.2.6 no'lu bölüme bakınız)
Güvenli posta kutusu erişimi (secure mailbox access)	RFC 2595	3	Güvensiz ortamlarda e-posta erişimini sağlamak için HTTPS kullanılması önerilmektedir. Taşıma güvenliği (transport security) standartları güvenlik kısmında belirtilmiştir. (2.4.2.6 no'lu bölüme bakınız)

2.2.2.3 Dosya Transfer ve Dizin Erişim Protokolleri

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Dosya aktarım protokolleri (file transfer protocols)	FTP RFC 959, RFC 2640, RFC 3659	2	İnternet ortamında dosya transferi için FTP, SFTP, HTTP veya WebDAV protokollerinden biri kullanılmalıdır. Bu tür uygulamalarda güvenlik öncelikli bir ihtiyaçsa SFTP kullanılmalıdır. Farklı kullanıcıların aynı dosya üzerinde eş zamanlı olarak çalışması gerektiği durumlarda WebDAV kullanılmalıdır.
	SFTP RFC 2228, RFC 2428	2	
	HTTP 1.1 RFC 2616	2	
	WebDAV RFC 4918, RFC 2291, RFC 3253, RFC 3648, RFC 3744, RFC 4316, RFC 4331, RFC 4437, RFC 4791	2	
Güvenli dosya aktarım protokolleri (secure file transfer protocols)	RFC 2585 (İnternet X.509 Açık Anahtar Altyapısı İşletim Protokolleri: FTP ve HTTP). RFC 2577 (FTP güvenlik hususları) RFC 4217 (TLS ile FTP güvenliği)	3	

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Hipermetin aktarım protokolleri (Hypertext transfer protocols)	HTTP 1.1 RFC 2616, RFC 2817, RFC 2818	1	Hipermetin (birbirine bağlantılı nesneler kümesi) iletimi için kullanılması zorunlu olan, genellikle web içeriğinin taşınmasında kullanılan uygulama seviyesi protokolüdür.
Kablosuz Uygulama Protokolü (WAP 1.2.1/2.0)	WAP-210-WAPArch-20010712-a	3	
Dizin Erişim Protokolü	LDAP v3 RFC 4510, RFC 4511, RFC 4512, RFC 4513, RFC 4514, RFC 4515, RFC 4516, RFC 4517, RFC 4518, RFC 4519	1	Çevrimiçi dizinlere erişim hizmetleri için bu protokolün kullanılması zorunludur.

2.2.2.4 Ulusal Alan Adı Protokolleri

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Güvenli alan adı hizmetleri	Secure DNS RFC 4033, RFC 4034, RFC 4470	3	
Alan adı hizmetleri	DNS RFC 1034, RFC 1035, RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2137, RFC 2181, RFC 2308, RFC 2535, RFC 2845, RFC 3425, RFC 3658, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 4592, RFC 1912 IPv6 ile ilgili DNS işlemleri için: RFC 3363, RFC 3364, RFC 2874, RFC 3596	1	Alan adı hizmetlerinin sunumunda bu standardın kullanılması zorunludur.

2.2.2.5 Gerçek Zamanlı Mesajlaşma (Real Time Messaging) Hizmetleri

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Birleştirilmiş mesajlaşma hizmetleri (Unified messaging services)	RFC 4239	3	
Gerçek zamanlı mesajlaşma hizmetleri (Real-time messaging services, Instant messaging services)	RFC 2778, RFC 2779	3	

2.2.2.6 Haber Grubu Hizmetleri

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Haber grubu hizmetleri (Newsgroup services)	NNTP RFC 3977, RFC 2980, RFC 3977	3	

2.3 VERİ ENTEGRASYONU VE İÇERİK YÖNETİMİ

2.3.1 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.

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

2.3.2 İÇERİK YÖNETİMİ

Kamu ile vatandaşlar ve iş dünyası arasında, ana iletişim mekanizması olarak internetin kullanımı esastır. Ancak, bu hedef beraberinde yeni ihtiyaçları da getirmektedir. Bilgilerin internet sitelerinde yayımlanması, o bilgiye ulaşılabilmesini garanti etmez. 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, internetle 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. açılardan bilgi veren yapısal bilgi olarak tanımlanabilir.

İçerik yönetimi çalışmaları çerçevesinde, metaverinin iki temel alanda kullanımı öngörülmektedir. Bunlardan birincisi doküman, internet sayfası, kurumsal süreç, veritabanı ve veri sözlükleri gibi kaynakların keşfi, diğeri ise arşiv ve kayıt kayıt yönetimidir.

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

Kaynak keşfi metaverisi şu bilgileri içerir:

- Yer; belli bir kaynağın varlığı konusunda bilgi sağlar.
- Uygunluk; kaynağın kullanışlılığı ya da aranan konuyla ilgisi hakkında bilgi 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; yazar, yaratılma tarihi, tanım, anahtar kelimeler ve ilişkili konulara 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 (record keeping) 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. Bilgi ve Dokümantasyon – Elektronik Belge Yönetimi Standardı (TS 13298) kapsamında bu amaçla hazırlanmış olan metaveri kümesinin tüm kamuda kullanımı, kurumların elektronik kayıtlarını sistematik ve tutarlı şekilde tanımlamalarına ve yönetmelerine yardımcı olacaktır.

Bilginin paydaşa sunumunda mutlaka metaveri kullanılmalıdır. Kamu kurumları tarafından internet dahil herhangi bir ağ ortamında yayınlanan 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/veya bilgiye dönüştürülebilmelidir.

2.3.3 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) hizmetlere ilişkin süreçler ve bu temel süreçleri destekleyen destek süreçlerinin tanımlanması,
    - Temel 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 bilgi sistemleri kullanılarak elde etme süreçlerinin iyileştirilmesi.

2.3.3.1 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.

2.3.3.1.1 Süreç Modelleme

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.

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 yayınlama.

   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. Kurumun stratejik planı 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 yayınlama.

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

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 sürecin/süreçlerin 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 var ise 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 aşamalarının ISO 15288, ISO 12207 ve ISO/IEC 27002, TS ISO/IEC 27001 gibi standartlar temelinde yürütülmesi ve tedarik yönetimi, entegrasyon ve sürdürülebilirliğe özel önem verilmesi

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.
2. Süreçler, Kurumun stratejik planında 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 sunmalıdır. 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.

2.3.3.2 Süreçlerde Kullanılan Verilerin Belirlenerek Tanımlanması

İş süreçlerindeki veri akışı ve veri yapılarının ortaya konmasını içerir. Bu kapsamda yapılacak çalışmalar aşağıda verilmektedir.

2.3.3.2.1 Veri Tanımlama

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.

Veri Sözlüğü Hazırlama

Kurumlar, veri sözlüklerini kurumsal stratejiler ve Kamu Kurumları Veri Sözlüğü Standardı'na göre oluşturacak ve güncel tutacaktır. Kurumsal veri sözlükleri ve ontolojilerin hazırlanmasını takiben tek noktadan erişilebilecek meta sözlük hazırlanarak güncel tutulmalıdır.

2.3.3.2.2 Veri Modelleme

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

2.3.3.2.3 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.

2.3.3.2.4 Verinin Gösterimi (Format)

Verinin gösteriminde standart olarak XSL kullanılacaktır.

2.3.3.3 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.

2.3.3.4 Veri Paylaşımına İmkan Verecek Veri Entegrasyonu Altyapısının Oluşturulması

Süreçler arasındaki etkileşimin belirlenmesi ve bu süreçler arasında paylaşılan verinin anlamlandırılmasına imkan veren veri yapıları XSD standardı kullanılarak tanımlanmalı, veri XML kullanılarak sunulmalı ve veri değişimi için Web Servisleri kullanılmalıdır. 2.3.4.2 başlığı altında listelenmeyen web servisi standartları için web servisleri birlikte çalışabilirlik (WS-I) sitesi (http://www.oasis-ws-i.org/) ile OASIS ve W3C web servis komitelerine bakılabilir.

2.3.4 KULLANILACAK STANDARTLAR

2.3.4.1 İçerik Yönetimi

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Kamu web siteleri	Kamu Kurumları İnternet Sitesi Kılavuzu (2006)	1	"Kamu Kurumları İnternet Sitesi Kılavuzu"nun Ağustos 2006 sürümüne uyum, 2007/4 tarihli ve 26416 sayılı Başbakanlık Genelgesi kapsamında zorunludur.
	Kamu İnternet Siteleri Standartları ve Önerileri Rehberi	4	www.kakis.gov.tr adresinden erişilebilecek "Kamu İnternet Siteleri Standartları ve Önerileri Rehberi" TÜRKSAT A.Ş. tarafından hazırlanmıştır. Rehberin kamu kurumlarının uyumuna imkan verecek biçimde geliştirilmesi sonrası Rehbere uyumun zorunlu hale getirilmesi öngörülmektedir.
Web sitesi erişilebilirliği	W3C Erişilebilirlik Kılavuzu 2.0 (2008)	3	Bu kılavuzun Türkçe çevirisine www.ozurluveyasli.gov.tr adresinden erişilebilir.
Elektronik Belge Yönetim Sistemi	TS 13298	1	2008/16 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının oluşturacakları elektronik belge yönetim sistemlerinde TS 13298 no'lu standarda uymaları zorunludur.
Elektronik kayıt yönetimi metaveri standardı	TS 13298	1	Bilgi ve Dokümantasyon – Elektronik Belge Yönetimi Standardı (TS 13298) kapsamında sunulmaktadır.

Kaynak keşfi metaveri standardı	-	4	Elektronik kayıt yönetimi metaveri standardı ile uyumlu olacak şekilde Dublin Core veri kümesine (ISO 15836:2009) dayanarak geliştirilecektir. Kaynak keşfi, arşiv ve kayıt yönetim sistemi için tasarlanmış metaveri kümesinin alt kümesi olarak kullanılacaktır.
Metaveri sınıflama ve kayıt	ISO/IEC 11179	3	

2.3.4.2 Süreç ve Veri Entegrasyonu

Bileşen	Standart/Teknoloji	Sınıf	2.3.4.3 Açıklama
Kurum kimlik ve haberleşme kodları	Devlet Teşkilatı Veri Tabanı (DTVT)	1	2011/1 sayılı Başbakanlık Genelgesi ile güncelleme esasları belirlenen ve kamu.basbakanlik.gov.tr adresinden erişilebilen Devlet Teşkilatı Veri Tabanı uygulaması hayata geçirilmiştir. Söz konusu Genelge kapsamında; elektronik belge yönetim sistemlerinde veya geliştirilen diğer uygulama yazılımlarında kurumların tanımlanmasında kurum kimlik kodları, hiyerarşik yapının kullanılması gereken durumlarda da haberleşme kodları kullanılacaktır.
Süreç modelleme	Süreç Zincir Çizenekleri (Process Chain Diagram) UML 2.0	3	İş süreçleri, süreç zincir çizenekleri kullanılarak modellenmelidir. Yazılım desteği sağlanacak süreçler daha sonra UML kullanılarak detaylandırılacaktır.
Süreç uygulama dili (web servisleri için)	BPEL (Business Process Execution Language)	3	
	BPEL4WS (Business Process Execution Language for Web Services)	3	
Süreç tanımlama (web servisleri için süreç tanımı depoları)	ebXML	3	
Süreçlerin çağırılması	ASAP (Aggregate Server Access Protocol)	3	

Bileşen	Standart/Teknoloji	Sınıf	2.3.4.3 Açıklama
Veri modelleme	Nesne bağıntı çizeneği (Entity Relationship Diagram) ve Veri akış çizeneği (Data Flow Diagram)	3	
Veri modeli değişimi	XMI	3	
Veri/metaveri yapısı tanımlama	XSD	1	Verinin yapısal olarak tanımlanması gerektiği durumlarda, XML kurallarının tanımlamalarının yer aldığı bu formatın kullanılması gerekmektedir. http://www.w3.org/XML/Schema
Veri gösterimi	XSL	1	XML dokümanlarının farklı formatlarda gösterimi ve işlenmesine yarayan XSL, XML dosyalarının sunucu tabanlı dinamik dönüşümü ve gösterimi gereken durumlarda kullanılmalıdır. http://www.w3.org/TR/xsl
Veri dönüştürme (data transformation)	XSLT (XSL Transformation)	3	
Ontoloji tabanlı bilgi değişimi	OWL	3	
Veri değişimi	Web servisi, XML	1	Kurumlar / servisler arası veri değişimi gereken durumlarda kullanılmalıdır.
Web servisi istemi (Web service request delivery)	SOAP RFC 4277	1	Dağıtık uygulamalarda ve web servislerinin haberleşmesinde kullanılmalıdır.
Web servisi istem kaydı (Web service request registry)	UDDI	3	Universal Description Discovery and Integration (UDDI), kuruluşların internet üzerinde listelendiği XML tabanlı ve platform bağımsız kayıt merkezi ve web servis uygulamalarının kaydı ve yerinin tespiti amacıyla kullanılan bir mekanizma sunar.
Web servisi tanımlama	WSDL 1.1	1	Web servis bileşenlerinin detaylarının yer aldığı XML dokümanıdır. Web servisinin diğer kurum ve/veya servislerin kullanımına sunulması halinde kullanılmalıdır. www.w3.org/TR/wsdl
Web servisleri arasında mesajların güvenli aktarımı	WS-Security 1.1	3	

Bileşen	Standart/Teknoloji	Sınıf	2.3.4.3 Açıklama
Kamu Kurumları Veri Sözlüğü Standardı		4	ISO/IEC 11179 temel alınarak geliştirilecektir.

2.4 GÜVENLİK

2.4.1 ESASLAR

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

Bilginin güvenli bir şekilde iletilmesi için kurumların belli başlı bilgi güvenliği standartlarına uyması ve bilgi paylaşımında bulunan tüm kurumların bu standartları dikkate alması gerekmektedir. Son yıllarda internet 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.

Güvenlik standartları tek bir başlık altında bu bölümde açıklanmış olsa da, güvenlik bundan önceki bölümlerdeki standartlar belirlenirken göz önünde bulundurulması gereken, farklı alanlar ve sistemler için farklı seviyelerde şekillenecek önemli bir parametredir. Bu bölümde belirtilen güvenlikle ilgili standartlar, belirtimler, kılavuzlar ve tavsiyeler güvenli bir e-devlet yapısı oluşturabilmek için gereklidir.

Kamu bilgileri güvenlik açısından üç sınıfa ayrılabilir. Bunlar; tasnif dışı, hizmete özel ve hizmete özel üstü (gizli, çok gizli) bilgilerdir. Rehber'in bu bölümünde verilmiş olan standart, belirtim, kılavuz ve tavsiyelerdeki kriptografik algoritmalar tasnif dışı ve hizmete özel gizlilik seviyesindeki bilginin güvenliği için kullanılmalı, daha yüksek güvenlik seviyesindeki bilginin kriptografik güvenliği için TÜBİTAK – BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi) tarafından yayınlanan rehberler dikkate alınmalıdır.

2.4.1.1 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. Bilgi teknolojilerinin yaygın şekilde kullanımı ise bilginin maruz kaldığı riskleri artırmakta ve kurumların sahip oldukları bilginin 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 kaynakları göz önünde bulundurularak etkili ve verimli bir şekilde yönetilmesi gerekmektedir. Etkili ve verimli yönetim ise BGYS ile mümkündür.

TÜBİTAK-BİLGEM tarafından, e-Dönüşüm Türkiye Projesi 2005 Eylem Planı 5 no'lu eylemi gereğince BGYS konusunda ön çalışmalar yapılmış olup; kamu kurumlarında BGYS çalışmalarının belirli bir plan ve koordinasyon dâhilinde gerçekleştirilmesi öngörülmüştür. Bu çalışmaların koordine edilmesi görevi Bilgi Toplumu Stratejisi (2006-2010) eki Eylem Planı 88 no'lu eylem ile TÜBİTAK-BİLGEM'e verilmiştir. Son olarak, 2012 Yılı Yatırım Programında yer alan "Kamu Bilgi Sistemleri Güvenliği Programı" ve "Kritik Altyapılarda Bilgi Güvenliği Yönetimi Projesi" ile, kamu kurumlarında bilgi güvenliğine ilişkin çalışmaların yürütülmesi hedeflenmektedir.

Kamu kurum ve kuruluşları kuracakları BGYS'leri, TSE tarafından verilen TS ISO/IEC 27001 sertifikası ile belgelendirebilirler.

2.4.1.2 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 kullanılabilir.

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; Akıllı telefon, VoIP telefon)

Yukarıda belirtilen ürünler ve sistemler için Ortak Kriterler standardında tanımlanan yedi farklı garanti seviyesi bulunmaktadır. Burada alt seviyeden (EAL 1), üst seviyeye (EAL 7) çıkıldıkça ürünün veya sistemin garanti seviyesi artmaktadır. Bu yedi 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 sistemlerin kullanılması faydalı olacaktır.

Kamu kurum ve kuruluşlarının geliştirecekleri BT ürünlerinde ve sistemlerinde ise gizlilik dereceli bilgiyi bulundurmaları ve/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 Standardları Enstitüsü (TSE), 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 TSE ve TÜBİTAK - BİLGEM 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-BİLGEM 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. Bunun yanında, bağımsız özel laboratuvarlar da bulunmaktadır.

TSE Ortak Kriterler Belgelendirme Sistemi, Türkiye adına Nisan 2010'da Uluslararası Ortak Kriterler tetkikini başarı ile geçmiş ve Türkiye, Kasım 2010'da ürün sertifikalandırma yetkisine sahip 15 ülke arasında yer almaya hak kazanmıştır.

2.4.1.3 Elekronik İmza

5070 sayılı Elektronik İmza Kanunu ve ilgili ikincil mevzuat gereğince ıslak imza ile aynı hukuki etkiye sahip güvenli elektronik imzanın (e-imza) yasal altyapısı oluşturulmuş ve 2004/21 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının nitelikli elektronik sertifika ihtiyaçlarının TÜBİTAK-BİLGEM bünyesinde kurulmuş olan Kamu Sertifikasyon Merkezi tarafından karşılanması kararlaştırılmıştır. Konu ile ilgili ayrıntılı bilgiye http://www.kamusm.gov.tr adresinden erişilebilir.

2.4.1.4 Kriptografi

Kriptografi, bilginin elektronik ortamda güvenli bir şekilde iletilmesi ve paylaşılması için gereken teknikleri içerir. Kriptografi ile ilgili bileşenler, 2.4.2 no'lu "Kullanılacak Standartlar" bölümünde farklı başlıklar altında yer almaktadır.

2.4.2 KULLANILACAK STANDARTLAR

Bu bölümde verilen standart, belirtim ve kılavuzlara erişim için kullanılabilecek internet 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

2.4.2.1 Bilgi Güvenliği Yönetimi

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Bilgi güvenliği yönetim sistemleri – Özellikler ve kullanım kılavuzu	TS ISO/IEC 27001	3	Kurumların dokümante edilmiş bir BGYS'yi kurmak, gerçekleştirmek, izlemek, gözden geçirmek, bakımını yapmak ve iyileştirmek için göz önünde bulundurulacak gereksinimleri kapsar. Ayrıca 2003/10 sayılı Başbakanlık Genelgesi uyarınca OECD Bilgi Güvenliği Politikası Rehberi dikkate alınmalıdır.
Bilgi güvenliği yönetimi için uygulama prensipleri	ISO/IEC 27002	3	Bilgi güvenliği yönetim sistemlerinde kullanılabilecek karşı önlem önerileridir. Mümkün olan hallerde milli olarak üretilen karşı önlemlerin kullanılmasına özen gösterilmelidir.

2.4.2.2 Bilgi Güvenliği Yönetimini Destekleyen Standartlar ve Kılavuzlar

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Bilgi güvenliği risk yönetimi için kılavuz	BS 7799-3:2006	3	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Information security management systems. Guidelines for information security risk management
BGYS sertifikasyonu ihtiyaçları ve hazırlığı için kılavuz	-	3	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guidelines on Requirements and Preparation for ISMS Certification Based on ISO/IEC 27001
BGYS denetimine hazırlık kılavuzu	-	3	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Are You Ready for an ISMS Audit Based on ISO/IEC 27001?

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
BGYS kontrollerinin uygulaması ve denetlemesi için kılavuz	-	3	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	-	3	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	3	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guide to the selection of BS 7799 Part 2 controls
Bilgi ve iletişim teknolojilerinin güvenlik yönetimi için kavramlar ve modeller	ISO/IEC 13335-1:2004	3	Bu standart, bilgi ve iletişim teknolojileri güvenlik yönetimine ilişkin kavramların ve modellerin genel kabul gören tanımlamalarını yapar. 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	3	Bu standart, bilgi teknolojileri güvenlik yönetimine ilişkin teknikleri tanımlar. 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	3	Bu standart, bilgi teknolojileri güvenliğinin sağlanmasına yönelik önlemlerin seçimine ilişkin süreci tanımlar. ISO tarafından hazırlanmış olan standardın orijinal ismi: Guidelines for the management of IT Security -- Part 4: Selection of safeguards

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Ağ güvenliği için yönetim kılavuzu	ISO/IEC TR 13335-5:2001	3	Bu standart, ağ güvenliğinin sağlanmasına ilişkin faktörlerin tanımlanması ve analizine kılavuzluk eder. 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	3	Bu standart, iş sürekliliği yönetimi için önerilen süreçler, prensipler ve süreçlere ilişkin bir kılavuzdur. BSI tarafından hazırlanmış olan standardın orijinal ismi: Code of practice for business continuity management

2.4.2.3 Bilgi Teknolojileri Ürünleri Güvenliği

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Bilgi teknolojileri ürünleri güvenliği	TS ISO/IEC 15408	3	Sistemlerin kritiklik düzeyine göre donanım ve hazır yazılımlar için ürün bazında bilgi güvenliğine ilişkin olarak TS ISO/IEC 15408 Ortak Kriterler (Common Criteria) standardı dikkate alınmalıdır.

2.4.2.4 Bilgi Erişimi ve Değişimi

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
XML tabanlı kimlik bilgisi, yetki düzeyi ve profillerin tanımlanması	SAML sürüm 1.1	3	Mümkün olduğu durumlarda sürüm 2.0 tercih edilmelidir.
	SAML sürüm 2.0	3	
XML tabanlı yetkilendirme	XACML sürüm 2.0	3	Erişim kontrolüne ilişkin, XML tabanlı politika, istek ve cevap dilini tanımlayan standarttır.
Kimlik bilgisi, yetki düzeyi ve profillerin değişimi	WS-Federation ID-FF v1.2	3	Kimlik bilgileri, yetki düzeyleri ve profillerin ilgili taraflar arasında elektronik olarak değişimi için kullanılan standarttır.
XML sayısal imzalama	XML Signature	3	W3C tarafından tanımlanan XML - imza söz dizimi ve işlenmesidir.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
XML şifreleme	XML Encryption	4	XML şifrelemenin, kriptografik yapısı ve hata geribildirimi nedeniyle sorunlu olduğu bilinmektedir. Bu standardın kullanılması düşünülüyorsa söz konusu sorunların giderilmesinin beklenmesi önerilmektedir.
Açık Anahtar Altyapısının (PKI) kullanıldığı yerlerde XML anahtar yönetimi	XKMS 2.0	3	W3C tarafından tanımlanan XML anahtar yönetimi belirtimidir. http://www.w3.org/TR/xkms2

2.4.2.5 Web Servisleri (WS) Güvenliği

Bir istemci bir kamu web sunucusu ile haberleşirken, haberleşmenin doğru web sunucusu ile gerçekleştiğinden emin olunması sağlanmalıdır. Gizlilik ve/veya bütünlüğün gerekli olduğu durumlarda içerik ağ üzerinde güvenli bir şekilde taşınmalıdır.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Web içeriğinin güvenli iletimi (bütünlük ve gizlilik)	TLS v1.0 (RFC 2246)	2	TLS v1.0, SSL v3.0 baz alınarak geliştirilmiş olup bu iki standart eşdeğer güvenlik özelliklerine sahiptir. TLS 1.0'ın tercih edilmesi durumunda Cipher-Block Chaining (CBC) modu kullanılmamalıdır. Mümkün olduğu durumlarda TLS v1.1 (RFC 4346) kullanılabilir. TLS v1.2 (RFC 5246) ise henüz incelenme aşamasındadır.
	SSL v3.0	2	
Web üzerinden işlemler	OSCI transport v1.2	3	Detaylı bilgi için http://egovernment.xml.org/standards/pdf/010_osci_1_2_specification.pdf adresine bakılabilir.
Web servisleri mesaj seviyesi güvenliği (WS-Security)	WS-Security 1.0	3	SOAP mesajlarının sayısal olarak nasıl imzalanacağını, nasıl şifreleneceğini ve sertifikaların mesaj içerisine nasıl yerleştirileceğini tanımlayan standarttır.

2.4.2.6 e-Posta Güvenliği

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
e-Posta taşıma güvenliği	RFC 3207	3	SMTP Service Extension for Secure SMTP over TLS

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
e-Posta içerik güvenliği	RFC 3850 RFC 3851 RFC 3852	3	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	IMAPS POP3S (RFC 2595)	3	

2.4.2.7 Elektronik İmzalama ve Şifreleme

Burada belirtilen bileşenlerin kullanımıyla hedeflenen güvenlik düzeyine ulaşılabilmesi için gerekli anahtar boyu, uygulama koşulları vb. kriterler dikkate alınmalıdır.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Sayısal imza algoritmaları (Digital Signature Algorithms)	DSA (ISO/IEC 14888-3)	2	"Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in amacı ve kapsamı dışında kalan uygulamalarda DSA algoritması SHA-1 ile beraber kullanılmamalıdır. http://www.btk.gov.tr/mevzuat/yonetmelikler/dosyalar/e-imza-teblig.pdf
	RSA (PKCS#1 sürüm 2.1)	2	
	ECDSA (FIPS 186-3)	2	
Elektronik imza formatı	ETSI TS 101 733 (CAdEs)	2	AB'de kullanılan ve elektronik imza çeşitlerini tanımlayan standartlardır.
	ETSI TS 101 903 (XAdEs)	2	
	ETSI TS 102 778 (PAdES)	2	
Kamu kurum ve kuruluşları arasında iletilen resmi yazışmalarda kullanılacak elektronik imza formatı	ETSI TS 101 733 (CAdES-XLong)	1	e-Yazışma Teknik Rehberi uyarınca, kamu kurumları arasındaki resmi yazışmalar için elektronik imza formatı olarak kullanımı zorunludur.
Kriptografik mesaj söz dizimi (Cryptographic message syntax)	PKCS #7 sürüm 1.5 (RFC 2315)	3	
Çevrimiçi sertifika durum protokolü	RFC 2560	1	2007/DK-77/207 sayılı BTK Kurul Kararının kapsamına giren uygulamalarda kullanılması zorunludur.
Sertifikasyon isteği sözdizim belirtimi	PKCS #10 sürüm 1.7 (RFC 2986)	3	
Sertifika isteği	RFC 4211	1	Elektronik sertifika isteği mesaj formatını tanımlayan standarttır.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Sertifika profili	RFC 5280 (ITU-T Rec. X.509 V3)	1	"Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 5'inci maddesinde geçen standartlar, Tebliğ'in amacı ve kapsamı içindeki uygulamalarda kullanılmalıdır. http://www.btk.gov.tr/mevzuat/yonetmelikler/dosyalar/e-imza-teblig.pdf
Sertifika iptal listesi profili	RFC 5280 (ITU-T Rec. X.509 V2)	1	2007/DK-77/207 sayılı BTK Kurul Kararının kapsamına giren uygulamalarda kullanılması zorunludur.
Sertifika verme/alma arayüzü	PKCS #12 sürüm 1.0	1	Elektronik sertifikaları ve gizli anahtarların saklanması ve iletiminde bu standardın tanımladığı dosya yapısının kullanımı zorunludur.
Kriptografik jeton arayüzü (Cryptographic token interface)	PKCS #11 sürüm 2.20	3	MS CryptoAPI sadece Windows işletim sistemi üzerinde çalışabilmektedir. Bu alanda kullanılabilecek başka alternatif standartlar da olmakla beraber, PKCS #11 ve MS CryptoAPI en yaygın kullanılan standartlardır.
	MS CryptoAPI / CNG	3	
Kriptografik jeton bilgi sözdizimi (Cryptographic token information syntax)	PKCS #15 sürüm 1.1	3	
Zaman damgası protokolü	ETSI TS 101 861	1	"Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 10'uncu maddesinde geçen standartlar, Tebliğ'in kapsamına giren uygulamalarda kullanılmalıdır. http://www.btk.gov.tr/mevzuat/yonetmelikler/dosyalar/e-imza-teblig.pdf

Yukarıdaki bileşenler tarafından kapsanmayan uygulamalarda aşağıdaki tabloda yer alan kriptografik algoritmalar kullanılabilir.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Simetrik şifreleme	AES (FIPS 197), Çalışma Kipleri (SP 800-38A 2001 ED, SP 800-38B, SP 800-38C)	3	Blok şifreleme algoritmasıdır.
Anahtar anlaşma / anahtar taşıma	DH	3	Simetrik şifrelemede kullanılan anahtarın haberleşen taraflar tarafından ortaklaşa üretilmesini ve iletilmesini sağlar.
	ECDH (NIST SP 800-56A) (NIST SP 800-56B)	3	
Özet alma algoritmaları (hash algorithms)	RIPEMD-160	2	"Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 6'ncı maddesinde belirtilen algoritmalardan biri kullanılmalıdır.
	SHA-1	2	
	SHA-224	2	
	SHA-256	2	
	WHIRLPOOL	2	
Mesaj asıllama kodu	HMAC (FIPS PUB 198-1, RFC 2104)	3	Özet alma algoritmaları bileşeninde önerilen özet algoritmaları ile birlikte kullanılmalıdır.

2.4.2.8 Diğer Güvenlik Bileşenleri

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Ağ katmanı güvenliği	IPSec IKE (RFC 2401, RFC 2402, RFC 2406, RFC 2407, RFC 3602)	1	IPSec, IP haberleşmelerinin güvenliğini (kimlik doğruluğu, veri bütünlüğü ve gizlilik) sağlayan protokol takımlarıdır. IKE, IPSec ile yapılacak güvenli haberleşmede kullanılacak simetrik şifreleme algoritması ve anahtar gibi güvenlik parametre ve özelliklerinin (security association) oluşturulmasını sağlar. Ağ katmanı güvenliğinin sağlanmasında IPSec ve IKE kullanılması zorunludur. IPSec IKE sürüm 2.0 (RFC 4301, RFC 4302, RFC 4303, RFC 4306, RFC 4309) (güncel sürümlerin kullanılması önerilmektedir)
Taşıma katmanı güvenliği	TLS 1.0 (RFC 2246)	1	TLS, Taşıma katmanı ve/veya daha üst katmanlarda iletişim güvenliği sağlayan kriptografik protokollerdir. Taşıma katmanı güvenliğinin sağlanmasında TLS 1.0'ın kullanılması zorunludur.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
			TLS 1.1 (RFC 4346) TLS 1.2 (RFC 5246) (güncel sürümlerin kullanılması önerilmektedir)
Kişisel gizlilik politikası	P3P sürüm 1.0	3	

2.5 COĞRAFİ BİLGİ SİSTEMLERİ

2.5.1 ESASLAR

Coğrafi bilgi sistemleri (CBS); mekana/konuma dayalı çalışmalarda ve karar verme süreçlerinde kullanıcılara yardımcı olmak üzere grafik ve grafik-olmayan bilgilerin toplanması, saklanması, işlenmesi ve kullanıcıya sunumu işlevlerinin bütünlük içerisinde gerçekleştirildiği bilgi sistemleridir.

Ülkemizde farklı kurum ve kuruluşlar tarafından üretilmekte olan farklı mekansal/konumsal veriler bulunmaktadır. Ancak, veri sahipliğinde belirsizliklerin olması ve veri yapılarındaki teknik uyumsuzluklar nedeniyle disiplinler arası çalışmayı gerektiren CBS uygulamalarında sorunlar yaşanabilmektedir. Veri içerik ve değişim sorunlarının ortadan kaldırılması ve ulusal bir CBS altyapısının kurulması amacıyla Bilgi Toplumu Stratejisi (2006-2010) eki Eylem Planında 75 no'lu "Coğrafi Bilgi Sistemleri Altyapısı Kurulumu Eylemi"ne yer verilmiştir. 644 Sayılı Kanun Hükmünde Kararname ile ihdas olunan Çevre ve Şehircilik Bakanlığı bünyesinde, ulusal coğrafi bilgi sisteminin kurulmasına, kullanılmasına ve geliştirilmesine dair iş ve işlemleri yapmak ve yaptırmak, coğrafi veri ve bilginin ulusal düzeyde üretimine, kalitesine ve paylaşımına yönelik standartlar ile bunlara ilişkin temel politika ve stratejilerin belirlenmesini sağlamak ve gerekli mevzuatı hazırlamakla sorumlu olan Coğrafi Bilgi Sistemleri Genel Müdürlüğü kurulmuştur. Bu bağlamda, 75 no'lu eylemin yürütülmesi görevi de söz konusu Genel Müdürlük sorumluluğuna geçmiş olup Açık Coğrafi Bilgi Konsorsiyumu (Open Geospatial Consortium - OGC), ISO 19100 standartlar serisi ve Avrupa Birliği Coğrafi Bilgi Altyapısı (Infrastructure for Spatial Information in the European Community – INSPIRE) projesi kapsamında ortaya konan standartlar temel alınarak detay kataloglama esaslarının belirlenmesi ve metaveri profilinin oluşturulması çalışmalarına devam edilmektedir.

Avrupa coğrafi bilgi sistemleri altyapısı oluşturulmasına yönelik çalışmalara 1995 yılında başlanmış ve 14 Mart 2007'de Avrupa Birliği Parlementosu ve Konseyi'nin Avrupa Topluluğu Coğrafi Bilgi Altyapısı Kurulumu Direktifi (2007/2/EC) yayımlanarak Avrupa Birliğine üye devletler arasında coğrafi verinin toplanması, uyumlulaştırılması, düzenlenmesi ve paylaşılması amacıyla INSPIRE projesi başlatılmıştır. Söz konusu direktif, Avrupa Birliğine üye tüm ülkelere, direktif içinde yer alan teknik ve idari düzenlemelere uyma zorunluluğu getirmektedir. Proje kapsamında, Avrupa Topluluğunun çevresel politikaları ve çevre üzerinde etkisi olabilecek politikalar ya da faaliyetlere yönelik olarak, Topluluk'ta coğrafi bilgi altyapısının kurulması için genel kurallar ortaya konmuş ve üye ülkeler ilgili direktif ekinde yer alan veritabanlarını oluşturarak kullanıma açmakla yükümlü tutulmuştur.

Kılavuzun bu bölümünde kurumlar arası coğrafi bilgi paylaşımının sağlanması amacıyla web servisleri, metaveri, veriye erişim, veri değişimi ve veri yayımlama ile ilgili uluslararası kabul görmüş standart ve servislere yer verilmiştir.

Coğrafi bilgi sistemlerinde birlikte çalışabilirliği sağlamak için kullanılacak ISO, CEN, TSE ve OGC standartları aynı amaca hizmet etmekte olup bunlardan sadece OGC standartları test ve sertifikalandırma mekanizmasına sahip olduğundan; birlikte çalışabilirlik açısından Rehber'in bu bölümünün OGC standartlarına dayalı olarak düzenlenmesinin uygun olacağı değerlendirilmiştir. Standartların kullanım kategorisi belirlenirken; 75 no'lu eylem ve INSPIRE kapsamında yapılan veri içerik ve değişim standartlarına yönelik çalışmalar ile standardın kullanım düzeyi ve Türk standardı olarak kabul edilip edilmediği göz önünde bulundurulmuştur.

Bu bölümde yer alan standartlar, Çevre ve Şehircilik Bakanlığı CBS Genel Müdürlüğü'nden gelen görüşler esas alınarak şekillendirilmiştir.

2.5.2 KULLANILACAK STANDARTLAR

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Web harita servisi	OGC Web Map Service (WMS), TS EN ISO 19128	1	Bir veya birden fazla coğrafi veritabanından coğrafi referansa sahip harita görüntülerinin çağrılabilmesi için temel http arayüzünü tanımlar. Kamu kurum ve kuruluşlarının coğrafi veri yayını için kullanacakları yazılımlar, bu standardı desteklemelidir. Yazılımlar son sürümle beraber eski sürümleri de desteklemelidir.
Web detay servisi	OGC Web Feature Service (WFS), TS EN ISO 19142	1	Alttaki veritabanından bağımsız bir şekilde coğrafi detaylara erişimi ve sorgulamayı sağlayan servise ilişkin durumları tanımlar. Kamu kurum ve kuruluşlarının coğrafi veri yayını için kullanacakları yazılımlar, detay düzeyinde sorgulama veya internetten düzenleme ihtiyacının olması durumunda, bu standardı desteklemelidir. Yazılımlar son sürümle beraber eski sürümleri de desteklemelidir.
Web raster servisi	OGC Web Coverage Service (WCS), TS EN ISO 19123	3	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. Kamu kurum ve kuruluşlarının veri yayını için kullanacakları yazılımların bu standardı desteklemesi önerilmektedir.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Katalog servisi	OGC Catalogue Service (CS-W), TS EN ISO 19119	3	Mekansal veri altyapılarında mekansal verileri arama, bulma ve erişim gibi işlemleri meta veri üzerinden yapmaya yarayan servislerdir. Kamu kurum ve kuruluşlarının veri yayını için kullanacakları yazılımların bu standardı desteklemesi önerilmektedir.
Koordinat dönüşümü Hizmeti	OGC Web Coordinate Transformation Service (WCTS), TS EN ISO 19111	3	Coğrafi detayları bir koordinat sisteminden diğerine dönüştüren servisi tanımlar. Kamu kurum ve kuruluşlarının farklı kaynaklardan veri yayını için kullanacakları yazılımların bu standardı desteklemesi önerilmektedir.
Coğrafi işaretleme dili	Geography Markup Language (GML), TS EN ISO 19136	3	Kamu kurum ve kuruluşlarının üretiminden sorumlu oldukları coğrafi verinin üretimi ve yönetimi için kullanılacak yeni yazılımların, bu veriler için değişim formatı olarak tanımlanacak GML formatını desteklemesi önerilmektedir. XML Şema Dokümanları CBS Genel Müdürlüğü görüşüne sunulmalıdır.
Metaveri (Metadata)	TS EN ISO 19115	1	Metaveriler, veriler ve servisler hakkındaki tanımlayıcı bilgilerdir. Coğrafi Bilgi Sistemleri açısından bu bilgiler, konumsal veri ve servislerin detaylı tanımlamalarını içerirler. Bu standarda uyum zorunludur.
Basit Detay Servisi	OGC Simple Feature Service, TS EN ISO 19125	3	Bir detay topluluğunun SQL/CLI vasıtasıyla depolama, sorgu ve güncelleme işlemleri için standart SQL şemasını tanımlar. Kamu kurum ve kuruluşlarının üretiminden sorumlu oldukları coğrafi verinin üretimi ve yönetimi için kullanacakları yeni yazılımlarda bu standardın kullanımı önerilmektedir.

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Web Harita Karo Servisi	OGC Web Map Tile Service (WMTS)	3	Kamu kurum ve kuruluşlarının coğrafi veri yayını için kullanacakları yazılımların bu standardı desteklemesi önerilmektedir.
CityGML	City Geography Markup Language	4	CityGML, sanal 3 boyutlu kent modellerinin depolanması ve değişimi için XML tabanlı bir format ve açık bir veri modelidir. Bu standart, mekansal veri alışverişi için OGC ve ISO/TC211 tarafından yayımlanan genişletilebilir uluslararası bir standart olan coğrafi işaretleme dili (GML3) için bir uygulama şemasıdır. Standardın geliştirilmesindeki amaç, 3 boyutlu bir kent modelinin temel varlıkları, özellikleri ve ilişkilerinin ortak bir tanımına erişmektir.

2.6 BİLGİ SİSTEMLERİNİN GELİŞTİRİLMESİ VE YÖNETİMİ

2.6.1 ESASLAR

Bilgi ve iletişim teknolojilerinin yaygınlaşması ve bu teknolojilere dayalı bilgi sistemlerinin giderek karmaşık bir hal alması, hizmet sunumunda kalitenin artırılması ve sürdürülebilirliğin sağlanması için bilgi sistemlerinin bir bütün olarak yönetimini gerekli kılmaktadır. Diğer taraftan, bilgi sistemlerinin yönetimi için sadece teknik bilgi yeterli olmamakta; hizmet geliştirme ve hizmet yönetimi süreçlerinin tanımlanması ve sürekli iyileştirilmesi gerekmektedir.

Bilgi sistemleri yönetimine ilişkin standartlar, sunulacak hizmetlerin planlanmasından uygulanmasına kadar birçok alt konuda standardize edilmiş yaklaşımları ve en iyi yöntemleri tanımlamaktadır. Bilgi sistemleri yönetim sürecinin önemli bir unsuru olan bilgi sistemlerinin güvenliği konusu da bu kapsamda değerlendirilmekle birlikte, bu konuda güvenlik bölümünde yer verilen daha detaylı ve geniş kapsamlı standartlara uyum esastır.

Bilgi sistemlerinin geliştirilmesine yönelik süreçler yazılım süreç yönetimi çerçevesinde ele alınmaktadır. Yazılım süreçlerinin iyileştirilmesi ya da tedarikçi firmaların bu kapsamda değerlendirilmesi yoluyla yazılımda kalitenin sağlanması, hizmet sunumunda da kalitenin artırılmasına yardımcı olacaktır.

Ayrıca, yaygın bir şekilde kullanılmaya başlanan paket yazılımların kalitesinin ortaya konması ve belirtilen amaca hizmet edip etmediğinin doğrulanması da önem arz etmektedir. Bu kapsamda yer alan standartlar, yazılım firmalarına ürünlerinin güvenilirliğini belgelendirme fırsatı sunmaktadır.

Bu bölümde, sistemlere ve geliştirilen çözümlere ilişkin süreçlere ait olarak kullanılacak standartlar ortaya konmuştur. 2.6.2.2 no'lu Yazılım Süreç Yönetimi kısmında yer verilen bileşenler ve açıklamaları için her yıl güncellenen Yatırım Programı Hazırlama Rehberi'nin ekinde yer alan Kamu Bilgi ve İletişim Teknolojileri Projeleri Hazırlama Kılavuzu'nda belirlenen eşik değerler dikkate alınmaktadır. Söz konusu Kılavuzun güncel sürümüne http://www.bilgitoplumu.gov.tr adresinden erişilebilir.

2.6.2 KULLANILACAK STANDARTLAR

2.6.2.1 Bilgi Teknolojileri Hizmet Yönetimi

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Bilgi teknolojileri hizmet yönetim standardı	ISO/IEC 20000-1	3	Bilgi teknolojileri hizmetlerinin etkin ve verimli bir şekilde sürdürülebilmesi için göz önünde bulundurulacak gereksinimleri kapsar.
Bilgi teknolojileri hizmet yönetim standardı uygulama prensipleri	ISO/IEC 20000-2	3	Bilgi teknolojileri hizmetleri yönetim standardına ilişkin açıklama ve en iyi uygulama örneklerini kapsar.

2.6.2.2 Yazılım Süreç Yönetimi

Bileşen	Standart/Teknoloji	Sınıf	Açıklama
Yazılım süreç denetimi	SPICE (TS ISO 15504)	3	Yazılım süreçlerinin değerlendirilmesi için altyapı oluşturan bir standarttır. Kurumların sahip oldukları ve uyguladıkları süreçleri iyileştirmek, ihtiyaçlar doğrultusunda kurumun yazılım süreçlerinin ve tedarikçi firmanın gereksinimlere uygunluğunun değerlendirilmesi için kullanılmaktadır.
Yazılım süreç kalitesi	SPICE (TS ISO 15504)	2	Tahmini proje tutarı 5.000.000 TL ve üzeri olan BİT projeleri için en az SPICE seviye-2, CMMI seviye-2 veya AQAP 160 aranması zorunludur. SPICE (TS ISO 15504), yazılım süreç kalitesi belgelendirmesi hizmetleri TSE tarafından verilmektedir.
	CMMI	2	
	AQAP 160	2	
Yazılım yaşam döngüsü süreçleri	TS ISO/IEC 12207	1	Tahmini proje tutarı 5.000.000 TL'nin altında olan ve uygulama yazılımı geliştirme bileşeni içeren kamu BİT projelerinde TS ISO 12207 Yazılım Yaşam Döngüsü Standardının uygulanması zorunludur.
Sistem yaşam döngüsü süreçleri	ISO 15288	3	

2.6.2.3 Paket Yazılımların Kalitesinin Değerlendirilmesi

Bileşen	Standart/Teknoloji	Sınıf	2.6.2.1 Açıklama
Satışa sunulan yazılım ürünlerinin kalite özellikleri ve değerlendirmesi	TS ISO 25051	3	Paket yazılımların kalite gereksinimleri ve uyumluluk değerlendirmeleri için kullanılmaktadır.

ÜÇÜNCÜ BÖLÜM:

REHBERİ TAMAMLAYICI NİTELİKTE YÜRÜTÜLECEK ÇALIŞMALAR

ÜÇÜNCÜ BÖLÜM

Bu bölüm, Rehberi tamamlayıcı nitelikteki çalışmalara işaret etmek üzere hazırlanmış olup birlikte çalışabilir bir e-Devlet yapısının oluşturulmasına yönelik genel iş adımlarını ortaya koymaktadır. Bu çalışmalar 2006-2010 döneminde, Bilgi Toplumu Stratejisi Eylem Planı 29 numaralı "Kamu Hizmet Envanteri", 30 numaralı "Hizmet Dönüşümü Fizibilite Çalışması", 71 numaralı "e-Devlet Kapısı Hizmetlerinin Yaygınlaştırılması" ve 78 numaralı "Birlikte Çalışabilirlik Standartları ve Veri Paylaşımı Altyapısı" eylemleri altında kısmen ele alınabilmiştir. Bu çalışmaların mevcut durum ve ihtiyaçlar çerçevesinde yeniden ele alınıp, belirlenecek eylemler çerçevesinde, uzun soluklu ve kapsayıcı çalışmalar ile yürütülmesi gerekmektedir.

Kurumsal ve merkezi çalışmalar yürütülmeli, örnek uygulamalar geliştirilmelidir. Kurumsal uygulamalar kapsamında, kurumların birlikte çalışabilirlik ihtiyaçları çerçevesinde yürütmeleri gereken süreç çıkarma ve iyileştirme, veri şemaları hazırlama ve paylaşma çalışmalarına ilişkin model ve metodolojinin hazırlanması gereklidir.

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

3.1 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 oluşturulmalıdır. Bu kapsamda, bünyesinde strateji, iş mimarisi, bilgi mimarisi, uygulama mimarisi ve teknoloji mimarisi alanlarını bulunduran, standartlaştırılabilecek bir Kurumsal Mimari Referans Modeli hazırlanmalıdır.

3.2 Süreç Paylaşımı ve e-Devlet Veri Sözlüğü

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

3.3 Veri Paylaşımı

Kurumsal Mimari Çalışmaları ile yakından ilişkilidir. Kamunun kamu ve iş dünyasıyla olan bilgi alış verişinde kullanacağı temel standartlar bu çalışmalardan yararlanarak belirlenmelidir. Kamu kurumları arasında veri paylaşım standartlarının geliştirilmesi, veri şema parçalarının tekrar kullanımını destekleyerek standartlara dayalı bir şekilde gerçekleştirilebilmesi sağlanmalıdır.

3.4 Örnek Uygulamalar

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

3.5 e-Hizmetlerin Geliştirilmesi ve Kolay Erişim

Geliştirilen e-hizmetlere kolay erişimi sağlamak üzere bu hizmetlere toplu halde ve kolay erişimi sağlayacak mekanizmalar oluşturulmalıdır. Bu amaca yönelik olarak 25 Ocak 2005 tarihli 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 kullanılabileceği LibreOffice (http://www.libreoffice.org) gibi açık kaynak kodlu ücretsiz ofis yazılım paketleri de kullanılabilir. MS Office 97 formatında (.doc, .xls ve .ppt) kaydedilmiş dosyaları üzerinde düzenleme yapma imkanı olmaksızın sadece görüntülemek için www.microsoft.com adresinden erişilebilecek MS Word Viewer, MS Excel Viewer ve MS Powerpoint Viewer ürünleri, Türkçe sürümlerini de kapsayacak şekilde ücretsiz temin edilebilir. ".rtf" formatında yukarda bahsedilen Ofis uygulamaları kullanılarak belge üretilebilir. ".txt" formatı ise basit metin formatı olup kişisel bilgisayarların hemen hepsinde bulunan metin editörleri ile oluşturulabilmektedir.

OpenDocument standardının kelime işlem dökümanları için kullandığı ".odt", sunum için kullandığı ".odp" ve elektronik çizelge belgeleri için kullandığı ".ods" formatları ile belge üretimi için yukarıda belirtilen açık kaynak kodlu ofis yazılımları yanında, Microsoft Office 2007 (service pack 2 eklentisiyle) ve sonraki sürümleri kullanılabilir. Aynı araçlar Office Open XML formatlarını da desteklemektedir.

".csv" uzantılı dosyalar, yukarda bahsedilen tüm ofis uygulamalarıyla oluşturulan elektronik çizelgeler ".csv" uzantılı olarak kaydedilerek oluşturulabilir. Bu formattaki dosyalar aslında düz metin dosyaları olup herhangi bir 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, ofis uygulamalarıyla oluşturulduktan sonra ".html (web sayfası)" formatında kaydedilerek ya da web sayfalarını oluşturmak için kullanılan araçlar ile oluşturulabilir.

".pdf" uzantılı dosyalar ise ücretsiz olarak edinilebilen Adobe Reader, Sumatra PDF Viewer, PDF-XChange Viewer veya Foxit Reader gibi programlar kullanılarak görüntülenebilmektedir.

Bilgisayar üzerinde yüklü bir programa sahip olmaksızın, internet üzerinden hizmet sunan ofis paketlerinin belge işleme amacıyla kullanımı da mümkündür. Bu amaçla Google Docs veya Microsoft Office Web Apps ücretsiz olarak kullanılabilir. Bu yöntemin, sadece gizliliğe haiz olmayan belgeler için tercih edilmesi uygundur. Microsoft Office Web Apps, Office Open XML formatlarının oluşturulmasına izin verirken, Google Docs ile bunun dışında Rehber'de yer verilen diğer tüm formatlarda belge oluşturulabilmektedir.

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 görülebilmekte 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/ internet adresinden ücretsiz olarak temin edilebilen açık kaynak kodlu bir sıkıştırma aracıdır. Bu aracın ürettiği çıktı formatı ".7z"dir.

Belge formatları

DOC, XLS, PPT: Microsoft ".doc", ".xls" ve ".ppt" formatları müseccel Microsoft standartlarıdır.

ODF: Elektronik çizelge, grafik, sunum ve metin işleme uygulamaları için geliştirilmiş, XML tabanlı bir dosya türüdür.

Office Open XML: Elektronik çizelge, grafik, sunum ve metin işleme uygulamaları için geliştirilmiş, XML tabanlı bir dosya türüdür.

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 standardının 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 standardına 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 internet üzerinden e-posta iletimi için kullanılır. Mesajlar e-posta yazılımı vasıtası ile 25 numaralı port üzerinden SMTP sunucusuna gönderilir. SMTP sunucusu mesajın iletileceği SMTP sunucusunun IP adresini DNS sunucusundan alıp mesajı alıcı SMTP sunucusuna gönderir. Alıcı SMTP sunucusu 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 çoklu ortam (multimedia) e-postaları iletebilmek için tasarlanmış bir belirtimdir. MIME, SMTP'nin bir uzantısıdır ve çoklu ortam içeriğine (ses dosyaları, görüntü-video dosyaları, ofis dokümanları vb.) sahip mesajların iletilmesinde kullanılır.

S/MIME (Secure MIME): S/MIME, MIME'nin üzerine tanımlanmış olup internet 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 internet üzerindeki bilgisayarlar arasında dosya transferine ilişkin kurallar tanımlanmıştır. HTTP ile web sayfalarının veya SMTP ile 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 (internet mail, MIME) benzer.

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) belirlenir. 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 (internet 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 birçok 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.). IPv4 protokolünde adresler 32 bit uzunluğundadır.

IPv6 (Internet Protocol Version 6): IPv6 protokolünün temel görevi IPv4 ile aynıdır. Ancak zaman içerisinde internetin 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 internet 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 gerçek zamanlı 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, 212.175.33.3 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 Kalkınma Bakanlığı için : www.kalkinma.gov.tr). Ancak, bu adres internet 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 sunucusu, kendisine sorulan internet adresine karşılık gelen IP numarasını veren makine/yazılımdır. Tek bir DNS sunucusu tüm dünyadaki internet

adreslerine karşılık gelen IP adreslerini bilemez. Dolayısı ile internet adresi-IP numarası eşleştirmesi için birçok DNS sunucusunun 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 (gizli 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 getirir. 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) değişimi 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 internet 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.

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.

Web Harita Karo Servisi (Web Map Tile Service - WMTS): Bir WMTS servisinin amacı bireysel karolara bölünmüş haritaları sunmaktır. Bir Web Harita Karo Servisi doğrudan verinin kendisine değil bu yer referanslı verinin kartoğrafik haritalarına erişim sağlar. Diğer bir ifadeyle veriler karolar halinde tutulur ve hangi karoya tıklanırsa ekranda sadece o karonun görüntülenmesi sağlanır, diğer veriler ise ön bellekte tutulur. Böylece hızlı bir harita görüntülenme hizmeti sunulur.

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 koordinat 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 arayüz 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 veritabanı için farklı bir arama kriteri belirlenmesinin önüne geçilebilmesi amacıyla 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 modellenmesini 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 modelinden 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 (eXtensible Markup Language): Bağımsız bir kuruluş olan W3C (World Wide Web Consortium) organizasyonu tarafından tasarlanan ve herhangi bir kurumun tekelinde bulunmayan XML, 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 internet 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 internette 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
AES	**:**	Advanced Encryption Standard
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
CEN	**:**	European Committee for Standardization
CS/W	**:**	Catalogue Service for the Web
DAV	**:**	Distributed Authoring and Versioning
DFD	**:**	Data Flow Diagram
DH	**:**	Diffie-Hellman
DNS	**:**	Domain Name Service
DSA	**:**	Digital Signature Algorithm
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
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
TCP	**:**	Transmission Control Protocol
TIFF	**:**	Tag Image File Format
TLS	**:**	Transport Layer Security
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 Markup Language Schema Definition
XSL	**:**	eXtensible Stylesheet Language

www.bilgitoplumu.gov.tr

T.C.
KALKINMA BAKANLIĞI
KÜTÜPHANE, YAYIN VE ARŞİV DAİRESİ BAŞKANLIĞI

Mayıs 2012

Necatibey Cad. No: 110/A 06100 Yücetepe - ANKARA
Tel: +90 (312) 294 50 00 • Faks: +90 (312) 294 69 77