e-DÖNÜŞÜM TÜRKİYE PROJESİ
BİRLİKTE ÇALIŞABİLİRLİK ESASLARI REHBERİ

Sürüm 1.0

T.C.
BAŞBAKANLIK
DEVLET PLANLAMA TEŞKİLATI MÜSTEŞARLIĞI
Bilgi Toplumu Dairesi

TEMMUZ **2005**

Bu Rehberle ilgili sorularınız ve güncelleştirme önerilerinizi lütfen;

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

veya

irtibat bilgileri aşağıda sunulan ilgiliye iletiniz.

Hakan DEMİRTEL

Tel: 312 – 294 64 11

e-posta: demirtel@dpt.gov.tr

Bu dokümanın güncel ve yürürlükte olan sürümüne http://bilgitoplumu.gov.tr/kdep/34/eDTrBirlikteCalisabilirlik.doc adresinden erişebilirsiniz.

DPT Müsteşarlığı Bilgi Toplumu Dairesi koordinasyonunda hazırlanan Rehber'e kurumları adına katkıda bulunan Sn.Ayşegül İbrişim (TSE) , Sn.Bilge Karabacak (TÜBİTAK – UEKAE) , Sn.Ersel Şengül (TCMB), Sn.Gülin Atabek (TCMB), Sn.Hakan Özfidan (Başbakanlık), Sn.Haluk Tanrıkulu (Ulaştırma Bakanlığı), Sn.Nusret Güçlü (ODTÜ Enformatik Enstitüsü), Sn.Selim Gümüş (TCMB), Sn.Tuncay Terzioğlu (TCMB), Sn.Türker Gülüm (TÜBİTAK), Sn.Umut Barış Erdoğan (TÜBİTAK – UEKAE), Sn.Z.Savaş Cengiz'e (MSB) ve görüşleri ile katkı sağlayan tüm kurum ve kuruluşlara teşekkür ederiz.

ÖNSÖZ

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

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

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

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

Bu amaçla Devlet Planlama Teşkilatı Müsteşarlığı koordinasyonunda katılımcı bir yaklaşımla hazırlanan bu Rehber'in kamu bilgi ve iletişim teknolojileri yatırımlarının etkinliği açısından büyük yarar sağlayacağı kanaatindeyim. e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (KDEP) "Birlikte çalışabilirlik esaslarının belirlenmesi ve rehber yayımlanması" eylemi çerçevesinde Devlet Planlama Teşkilatı Müsteşarlığı koordinasyonunda kamu, özel kesim ve sivil toplum kuruluşlarından katkı verebilecek tüm ilgililere ulaşılmaya azami gayret gösterilerek hazırlanan Rehber, teknik unsurlar içermesi nedeni ile zaman içinde gelişecek, genişleyecek ve sonradan gelen yeniliklere ayak uyduracak olup, bundan sonra da toplumun tüm kesimlerinin katkısına açık bir belge niteliğindedir.

Devlet Planlama Teşkilatı Müsteşarlığı, bilgi ve iletişim teknolojileri alanındaki kamu yatırımlarının ülkemiz ihtiyaç ve öncelikleri doğrultusunda planlanmasını ve yürütülmesini sağlamak açısından bu Rehber'in hayata geçirilmesine büyük önem vermektedir. Bu amaçla, ilgili idari mekanizmalar ivedilikle tanımlanacak ve harekete geçirilecektir.

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

Dr. Ahmet TIKTIK
Müsteşar

İÇİNDEKİLER

ÖNSÖZ i

BİRİNCİ BÖLÜM 2
1 GİRİŞ 2
2 GENEL ESASLAR 3
2.1 AMAÇ 3
2.2 KAPSAM 3
2.3 TANIMLAR ve KISALTMALAR 3
2.4 UYUM MEKANİZMALARI 3
2.5 YETKİ ve SORUMLULUKLAR 3
2.6 GÜNCELLEME 4
3 BİRLİKTE ÇALIŞABİLİRLİK POLİTİKASI 4
3.1 GİRİŞ 4
3.2 POLİTİKA 6
3.2.1 Avrupa Komisyonu Çalışmalarıyla Uyum 6
3.2.2 Ana İletişim Mekanizması Olarak İnternet ve www'in Kullanımı 6
3.2.3 Eşit Erişim Hakkı 6
3.2.4 Güvenlik 6
3.2.5 Kişisel Verilerin Korunması 6
3.2.6 Açık Standartların ve Uluslararası Standartların Kullanımı 6
3.2.7 Anlamsal Bütünlüğü Sağlayacak Ortak Standartların Kullanımı 7
3.2.8 Ölçeklenebilirlik 7
3.2.9 Katılımcılık Esası 7

İKİNCİ BÖLÜM 9
1 DOSYA (VERİ) SUNUMU ve DEĞİŞİMİ 9
1.1 ESASLAR 9
1.2 KULLANILACAK STANDARTLAR 9
1.2.1 Sıkıştırılmış Dosyalar 10
1.2.2 Kelime İşlem Dokümanları 10
1.2.3 Sunum Dokümanları 10
1.2.4 Elektronik Çizelge Dokümanları 11
1.2.5 Karakter Kümesi 11
1.2.6 Resim Dosyaları 11
1.2.7 Animasyonlar 12
1.2.8 Ses-Video 12
1.2.9 Gerçek Zamanlı Ses-Video Yayını 12
2 ARA BAĞLANTI 13
2.1 ESASLAR 13
2.2 KULLANILACAK STANDARTLAR 13
2.2.1 İnternet Aktarım Protokolleri 13
2.2.2 Güvenli İnternet Aktarım Protokolleri 13
2.2.3 e-Posta Protokolleri 14
2.2.4 İnternet Dosya Transfer Protokolleri 14
2.2.5 Devlet Alan Adı Protokolleri 15
2.2.6 Yerel Ağ/Geniş Alan Ağı Erişimi(Lan/Wan Interworking) 15
2.2.7 Gerçek Zamanlı Mesajlaşma (Real Time Messaging) Hizmetleri 16
2.2.8 Haber Grubu Hizmetleri 16
2.2.9 Web Servisleri (Web Services Transport) 16

3 VERİ ENTEGRASYONU VE İÇERİK YÖNETİMİ 17
3.1 ESASLAR 17
3.2 İÇERİK YÖNETİMİ 17
3.3 SÜREÇ ve VERİ ENTEGRASYONU 18
3.3.1 Kamu Hizmet ve Karar Destek Süreçlerinin Tanımlanması ve İyileştirilmesi 18
3.3.2 Süreçlerde Kullanılan Verilerin Belirlenerek Tanımlanması 20
3.3.3 Kurumların Veri Toplama/Güncelleme/Erişim Yetkilerinin Düzenlenmesi 21
3.3.4 Veri Paylaşımına İmkan Verecek Veri Entegrasyonu Altyapısının Oluşturulması 21
3.4 KULLANILACAK STANDARTLAR 21
4 GÜVENLİK 24
4.1 ESASLAR 24
4.1.1 Bilgi Güvenliği Yönetim Sistemi (BGYS) 24
4.1.2 Ortak Kriterler 25
4.1.3 Elekronik İmza 25
4.1.4 Kriptografik İşlemler 26
4.2 KULLANILACAK STANDARTLAR 26
4.2.1 Bilgi Güvenliği Yönetimi 26
4.2.2 Bilgi Güvenliği Yönetimini Destekleyen Standartlar ve Kılavuzlar 26
4.2.3 Bilgi Teknolojileri Ürünleri Güvenliği 27
4.2.4 Web Servisleri (WS) Güvenliği 27
4.2.5 E-Posta Güvenliği 28
4.2.6 Ağ Katmanı Güvenliği 28
4.2.7 Şifreleme ve İmzalama 29
4.2.8 Güvenli Doküman Alışverişi 29
5 ÇÖZÜM YAŞAM DÖNGÜSÜ 31
5.1 ESASLAR 31
5.2 KULANILACAK STANDARTLAR 31

ÜÇÜNCÜ BÖLÜM 33
1 REHBERİ TAMAMLAYICI NİTELİKTE YÜRÜTÜLECEK ÇALIŞMALAR 33
1.1 Kılavuzların Hazırlanması 33
1.2 e-Devlet Metaveri Standardı 33
1.3 Veri Entegrasyonu İçin Gerekli Çalışmalar 33
1.4 Elektronik Kayıt Yönetimi Çerçevesi 34
1.5 XML Şemalarının Çıkartılması 34
1.6 e-Hizmetlerin Geliştirilmesi ve Kolay Erişim 34

EK-A 36
AÇIKLAMALAR 36
EK-B 37
TANIMLAR 37
EK-C 46
KISALTMALAR 46

BİRİNCİ BÖLÜM

BİRİNCİ BÖLÜM

1 GİRİŞ

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

Rehber'de; 5 temel konuda esaslar ve kullanılacak standartlar belirlenmiştir. Bunlar; dosya (veri) sunumu ve değişimi, ara bağlantı, süreç ve veri entegrasyonu ve içerik yönetimi, güvenlik ve çözüm yaşam döngüsüne ilişkindir. Rehber'de kapsanan konular, elektronik devlet hizmetlerinin sunumunda kamu kurum ve kuruluşlarının birlikte çalışabilirliğinin temelini oluşturmaktadır.

Diğer taraftan, Rehber'de belirlenen esas ve standartlar, hazırlıkları devam eden e-devlet kapısı (portal) teknik altyapısının hayata geçirilmesi açısından da büyük önem taşımaktadır. e-Devlet kapısına ilişkin mekanizmanın işleyişinde gerekli olan arka ofis işlemlerinin, bir başka ifadeyle kamu kurumları arasında elektronik ortamda yürütülecek bilgi ve belge alışverişi, kimlik doğrulama, kimlik paylaşımı, ödeme gibi işlemlerin bu Rehber'de yer alan esas ve standartlarla uyumlu olması ve uygun hallerde Rehber'in yeni ihtiyaçlara cevap verecek şekilde geliştirilmesi gerekmektedir. e-Devlet hizmetlerinin etkin şekilde yürütülmesi ancak bu koşullarla mümkün hale gelebilecektir. Aksi takdirde, bilgi toplumuna geçiş sürecinin devam ettiği ülkemizde bilgi paylaşımından uzak, birbirinden bağımsız bilgi sistemlerinden oluşan e-kurum yapılanmasının ötesine geçilemeyecektir.

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 uyum konusunun kural haline getirilmesi için gerekli tedbirler en kısa zamanda alınacaktır. Bunun en önemli araçlarından biri kamu yatırım tekliflerinin hazırlanmasına ilişkin usul ve esaslardır.

Rehber'in hazırlanmasında, bu konuda kapsamlı çalışmalar yapmış ülke örnekleri ve bu ülkelerin yayımladıkları birlikte çalışabilirlik dokümanlarından istifade edilmiştir. Rehber'in hazırlanmasında yararlanılan dokümanların listesi aşağıda sunulmuştur.

Kaynak	**Dokümanın Adı**
AB	European Interoperability Framework for Pan-European e-Government Services
AB	Architecture Guidelines
İngiltere	eGovernment Interoperability Framework
İngiltere	Technical Standards Catalogue
Almanya	Standards and Architectures for eGovernment Applications (SAGA)
Avustralya	Interoperability Technical Framework for the Australian Government
Danimarka	National Interoperability Framework
Hong Kong	Analysis Underpinning The HKSARG Interoperability Framework Recommendations
Yeni Zelanda	New Zealand e-Government Interoperability Framework (NZ e-GIF)

2 GENEL ESASLAR

2.1 AMAÇ

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

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

2.2 KAPSAM

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

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

2.3 TANIMLAR ve KISALTMALAR

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

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

2.4 UYUM MEKANİZMALARI

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

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

Ayrıca, kamu ihale mevzuatında da Rehber'e atıf yapılması ve tüm kamu bilgi ve iletişim teknolojisi ihaleleri şartname ve sözleşmelerine ilişkin yol gösterici dokümanlarda bu Rehber'in referans olarak alınması sağlanacaktır.

2.5 YETKİ ve SORUMLULUKLAR

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

Rehber'in uygulanmasına ilişkin genel koordinasyon Devlet Planlama Teşkilatı Müsteşarlığı tarafından yürütülecektir.

2.6 GÜNCELLEME

Rehber'in birinci bölümünü oluşturan genel esaslar ve birlikte çalışabilirlik politikası, bir sürümün yürürlükte olduğu yıl boyunca gelen görüş ve öneriler doğrultusunda, Devlet Planlama Teşkilatı Müsteşarlığı tarafından katkısına gerek görülen öneri sahibi kurum ve kuruluşları da içerecek şekilde oluşturulacak "Gözden Geçirme Komisyonu"nun yapacağı çalışmalar sonucunda ihtiyaç duyulması halinde, yılda bir kez güncellenecektir.

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

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

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

Gerekli görülen güncellemeleri yapma görev ve yetkisi Devlet Planlama Teşkilatı Müsteşarlığına aittir.

3 BİRLİKTE ÇALIŞABİLİRLİK POLİTİKASI

3.1 GİRİŞ

Yasal çerçevesi belirlenmiş sınırlar içerisinde, arka planda kurumlar arası etkileşimin sağlandığı ve vatandaşa dönük yüzünde tek bir organizasyonmuş gibi davranabilen modern ve bütünleşik e-devlet yapısı, birbiriyle uyumlu, birlikte çalışabilir, etkileşimli, izlenebilir 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[1].

[1] Burada yer verilen tanım, İrlanda'nın AB Dönem Başkanlığını yürüttüğü 2004 yılında European Public Administration Network eGovernment Working Group tarafından hazırlanan "Key Principles of an Interoperability Architecture" adlı çalışmadan alınmıştır. (Kaynak: http://europa.eu.int/idabc/en/document/3591/5671).

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

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

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

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

Sunulacak ve ortak platformdan (e-Devlet Ana Kapısı Projesi, 2005 Eylem Planı 21 numaralı eylem) erişilecek kamu hizmetlerinin ve organizasyonel ihtiyaçların belirlenmesi ile bu hizmetlere ilişkin iş süreçlerinin modellenmesi ve uygulamaların geliştirilmesi çalışmaları bu Rehber'in kapsamında olmayıp, hizmet veren kurum ve kuruluşlar tarafından bu Rehber'de belirtilen politika ve standartlar esas alınarak yapılacaktır.

e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (KDEP) içerisinde ele alınan eylemler aracılığı ile anlamsal birlikte çalışabilirlik ihtiyaçları ve atılması gereken adımlar konusunda farkındalık yaratılmaya çalışılmıştır. Önümüzdeki dönemde e-Dönüşüm Türkiye Projesi kapsamında bu alanda yürütülecek eylemler Rehber'deki esaslar çerçevesinde eylemlerden sorumlu kuruluşlar tarafından üstlenilecektir.

3.2 POLİTİKA

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

3.2.1 Avrupa Komisyonu Çalışmalarıyla Uyum

Esaslar belirlenirken, Avrupa Komisyonu çalışmalarıyla uyum gözetilmiş, "İdareler Arası Veri Değişimi Programı (IDA)" kapsamında yürütülen çalışmalar ve hazırlanan raporlardan yararlanılmıştır.

3.2.2 Ana İletişim Mekanizması Olarak İnternet ve www'in Kullanımı

Hedef, küresel İnternet devriminde maliyeti ve riski düşürebilmek, İnternet'in tüm taraflarca aktif olarak kullanımını sağlamaktır. Bu amaçla geliştirilecek uygulamaların arayüz olarak İnternet tarayıcısını (browser) kullanmaları esastır.

3.2.3 Eşit Erişim Hakkı

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

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

3.2.4 Güvenlik

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

3.2.5 Kişisel Verilerin Korunması

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

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[2]:

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

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

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

iv. Standardın yeniden kullanımı konusunda hiç bir sınırlama olmamalıdır.

3.2.7 Anlamsal Bütünlüğü Sağlayacak Ortak Standartların Kullanımı

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

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

3.2.8 Ölçeklenebilirlik

Oluşturulacak yapının değişen ihtiyaçlara cevap verebilecek bir tasarıma sahip olması gereklidir.

3.2.9 Katılımcılık Esası

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

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

İKİNCİ BÖLÜM

İKİNCİ BÖLÜM

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

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

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

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

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

1 DOSYA (VERİ) SUNUMU ve DEĞİŞİMİ

1.1 ESASLAR

Bir çok 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, belirli ürünlere/firmalara bağımlılık yaratmaması ve alternatifli olması e-devlet uygulamalarından etkin şekilde faydalanabilmenin ön koşuludur.

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

1.2 KULLANILACAK STANDARTLAR

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

1.2.1 Sıkıştırılmış Dosyalar

Bu tip dosyalar için aşağıdaki tabloda yer verilen formatlardan herhangi birisi kullanılabilir.

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

1.2.2 Kelime İşlem Dokümanları

Kelime işlem dokümanlarından üzerinde işlem yapılmasına ihtiyaç duyulmayanlar için ".html" veya ".pdf" formatlarından uygun olanı kullanılmalıdır. Üzerinde işlem yapılabilmesine olanak sağlayan (".html" ve ".pdf" formatlı dokümanlar üzerinde değişiklik yapılamaz) kelime işlem dokümanlarının paylaşımı için aşağıdaki tabloda belirtilen formatlardan en az birinin kullanımı zorunludur. Bunlardan hangisinin kullanılacağına ihtiyaca göre karar verilebilir. Diğer taraftan, OASIS (Organization for the Advancement of Structured Information Standards) tarafından ofis dokümanları için standart olarak kabul edilen "Open Document Format for Office Applications - OpenDocument" formatının önümüzdeki dönemde kamu kurumlarının belge değişimi için zorunlu standart olarak kullanılması öngörülmektedir.

Bileşen	Standart/Teknoloji	Açıklama
Kelime işlem dokümanları (üzerinde işlem yapılamayan)	Hypertext File Format v4.01 (.html)	
	Portable Document Format v4 (.pdf)	Türkçe yazı tipleri gömülü olarak saklanmalıdır.
Kelime işlem dokümanları (üzerinde işlem yapılabilen)	Microsoft Word 97 (.doc)	
	Rich Text Format (.rtf)	
	Plain/Formatted Text (.txt)	
	OpenDocument (.odt)	

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

1.2.3 Sunum Dokümanları

Sunum dokümanlarından üzerinde işlem yapılmasına ihtiyaç duyulmayan dokümanlar için ".html" veya ".pdf" formatlarından uygun olanı kullanılmalıdır. Üzerinde işlem yapılabilmesine olanak sağlayan (".html" ve ".pdf" formatlı dokümanlar üzerinde değişiklik yapılamaz) sunum dokümanlarının paylaşımı için aşağıdaki tabloda belirtilen formatlardan ihtiyaca uygun olanı kullanılmalıdır. Üzerinde işlem yapılabilecek şekilde üretilecek dokümanlar için "OpenDocument" sunum formatının önümüzdeki dönemde kamu kurumlarının belge değişimi için zorunlu standart olarak kullanılması öngörülmektedir.

Bileşen	Standart/Teknoloji	Açıklama
Sunum Dokümanları (üzerinde işlem yapılamayan)	Hypertext File Format v4.01 (.html)	
	Portable Document Format v4 (.pdf)	Türkçe yazı tipleri gömülü olarak saklanmalıdır.
Sunum Dokümanları (üzerinde işlem yapılabilen)	Microsoft Powerpoint 97 (.ppt)	
	OpenDocument (.odp)	

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

1.2.4 Elektronik Çizelge Dokümanları

Elektronik çizelge dokümanı sunumunda, üzerinde işlem yapılmasına ihtiyaç duyulmayan dokümanlar için ".html" veya ".pdf" formatlarından uygun olanı kullanılmalıdır. Üzerinde işlem yapılabilmesine olanak sağlayan elektronik çizelge dokümanlarının paylaşımı için aşağıdaki tabloda belirtilen formatlardan ihtiyaca uygun olanı kullanılmalıdır. Üzerinde işlem yapılabilecek şekilde üretilecek dokümanlar için "OpenDocument" elektronik çizelge formatının önümüzdeki dönemde kamu kurumlarının belge değişimi için zorunlu standart olarak kullanılması öngörülmektedir.

Bileşen	Standart/Teknoloji	Açıklama
Elektronik Çizelge Dokümanları (üzerinde işlem yapılamayan)	Hypertext File Format v4.01 (.html)	
	Portable Document Format v4 (.pdf)	Türkçe yazı tipleri gömülü olarak saklanmalıdır.
Elektronik Çizelge Dokümanları (üzerinde işlem yapılabilen)	Comma Separated Value (.csv)	
	Microsoft Excel 97 (.xls)	
	OpenDocument (.ods)	

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

1.2.5 Karakter Kümesi

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

1.2.6 Resim Dosyaları

Kullanım amacına göre aşağıdaki standartlar arasında tercih yapılabilir.

Bileşen	Standart/Teknoloji	Açıklama
Resim Dosyaları	Tagged Image File Format (.tiff)	Veri kaybına izin verilmediği durumlarda bu standart tercih edilmelidir.
	Graphics Interchange Format (.gif)	Çizim, animasyon gibi fazla detay içermeyen görüntülerin sıkıştırılmasında kullanılmalıdır.

Bileşen	Standart/Teknoloji	Açıklama
	Joint Photographic Experts Group (.jpg) (ISO 10918)	24 bit renk derinliği destekleyen bu format renk duyarlığı gereken durumlarda kullanılmalıdır.
	Portable Network Graphics (.png)	Kullanımının mümkün olduğu durumlarda önerilmektedir.
	Enhanced Compressed Wavelet (.ecw)	Yüksek sıkıştırmaya ihtiyaç duyulan durumlarda kullanılabilir.

1.2.7 Animasyonlar

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

Bileşen	Standart/Teknoloji	Açıklama
Animasyonlar	Animated GIF	
	Apple Quicktime (.mov, .qt)	
	Macromedia Flash (.swf)	
	Macromedia Shockwave (.swf)	

1.2.8 Ses-Video

Bileşen	Standart/Teknoloji	Açıklama
Ses-Video	MPEG-1 (ISO 11172)	
	MPEG-2 (ISO 13818)	
	MPEG-4 (ISO 14496)	
	MPEG-7	
	DV	
	MP3	Bu formatta dosya oluşturmak telif ücreti ödenmesini gerektirmektedir.
	WAV	
	Quicktime	

1.2.9 Gerçek Zamanlı Ses-Video Yayını

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

Bileşen	Standart/Teknoloji	Açıklama
Gerçek Zamanlı Ses-Video Yayını	Real Audio/ Real Video	
	Macromedia Shockwave	
	Windows Media Format (.asf, .wma, .wmv)	
	Apple Quicktime	

2 ARA BAĞLANTI

2.1 ESASLAR

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

2.2 KULLANILACAK STANDARTLAR

2.2.1 İnternet Aktarım Protokolleri

Bileşen	Standart/Teknoloji	Açıklama
İnternet Protokolu	IP (DARPA Internet Program Protocol Specification) (RFC 791)	Kullanılması önerilmektedir.
Dosya iletimi	HTTP 1.1(RFC 2616)	Kullanılması önerilmektedir.
	WebDAV (RFC 2518, RFC 2291, RFC 3253, RFC 3648, RFC 3744)	Kullanılması önerilmektedir.
Taşıma (transport)	TCP (RFC 793) UDP (RFC 768)	Kullanılması önerilmektedir.
Hypertext aktarım protokolleri	RFC 2817, RFC 2818 http1.1'in içinde taşıma katmanı güvenliği (Transport Layer Security - TLS) kullanılması gerekmektedir. RFC 3546, RFC 3749	Kullanılması önerilmektedir.

2.2.2 Güvenli İnternet Aktarım Protokolleri

Daha detaylı bilgi için İkinci Bölüm, madde 4'te yer alan Güvenlik kısmına bakınız.

Bileşen	Standart/Teknoloji	Açıklama
IP güvenliği (kaynağın kimliğinin doğrulanması, kaynağın ve verinin bütünlüğü)	RFC 2402 IPSec (AH - Authentication Header)	Güvenlik kısmında belirtilmiştir. (Bkz. İkinci Bölüm, madde 4)
IP güvenliği (verinin gizliliği ve/veya bütünlüğü)	RFC 2406 RFC 2407 RFC 2451 RFC 3602 IPSec (ESP - Encapsulating Security Payload) (VPN gereksinimleri için kullanılabilir.)	Güvenlik kısmında belirtilmiştir. (Bkz. İkinci Bölüm, madde 4)

2.2.3 e-Posta Protokolleri

Bileşen	Standart/Teknoloji	Açıklama
e-Posta taşıma (e-mail transport)	e-posta SMTP/MIME'ye uygun olarak taşınmalıdır. RFC 2821, RFC 2822, RFC 2045, RFC 2046, RFC 2646, RFC 2047, RFC 2231, RFC 2048, RFC 3023, RFC 2049	
e-Posta taşıma güvenliği (e-mail transport security)	RFC 3207	Güvenlik kısmında belirtilmiştir. (Bkz. İkinci Bölüm, madde 4)
e-Posta kutusu erişimi (e-mailbox access)	e-Posta erişimi için POP3 veya IMAP kullanılması gerekmektedir. POP3 için RFC 1939, RFC 1957, RFC 2449. IMAP için RFC 3501, RFC2342, RFC 2971, RFC 3502, RFC 3503, RFC 3510.	Kullanılması önerilmektedir.
e-Posta içerik güvenliği (e-mail content security)	Uçtan-uca güvenlik gerektiğinde S/MIME v3 kullanılması gerekmektedir. S/MIME için RFC 3369, RFC 2631, RFC 2632, RFC 2633.	Güvenlik kısmında belirtilmiştir. (Bkz. İkinci Bölüm, madde 4)
Güvenli posta kutusu erişimi (secure mailbox access)	RFC 2595, IMAP, POP3 ve ACAP için TLS standartlarını vermektedir.	Güvensiz ortamlarda mail erişimini sağlamak için HTTPS kullanılması gerekmektedir. Taşıma güvenliği (transport security) standartları güvenlik kısmında belirtilmiştir. (Bkz. İkinci Bölüm, madde 4)

2.2.4 İnternet Dosya Transfer Protokolleri

Bileşen	Standart/Teknoloji	Açıklama
Dosya aktarım protokolleri (file transfer protocols)	FTP RFC 2228, RFC 2640	Kullanılması önerilmektedir. RFC 959: RFC 2640 sayılı RFC ile güncellenmiştir. Uzak oturumların güvenli olarak açılması ve bunun için bedelsiz ürün olan "openssh" kullanımı önerilmektedir.

Bileşen	Standart/Teknoloji	Açıklama
Güvenli dosya transferi protokolleri (secure file transfer protocols)	RFC 2585 (İnternet X.509 Açık Anahtar Altyapısı İşletim Protokolleri (PKI Operational Protocols): FTP ve http). RFC 2577 (FTP güvenlik hususları)	Kullanılması önerilmektedir.

2.2.5 Devlet Alan Adı Protokolleri

Bileşen	Standart/Teknoloji	Açıklama
Güvenli DNS		Güvenlik için Bkz. İkinci Bölüm, madde 4.
Alan Adı Hizmetleri	DNS RFC 1034 RFC 1035 IPv6 ile DNS işlemleri için RFC 3363, RFC 3364	Üzerinde çalışılması gereklidir. RFC 1034 : RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 2065, RFC 2181, RFC 2308, RFC 2535 sayılı RFC'ler ile güncellenmiştir. RFC 1035 : RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2181, RFC 2137, RFC 2308, RFC 2535, RFC 2845, RFC 3425, RFC 3658 sayılı RFC'lerle güncellenmiştir.

2.2.6 Yerel Ağ/Geniş Alan Ağı Erişimi (Lan/Wan Interworking)

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

Bileşen	Standart/Teknoloji	Açıklama
Yerel-ağ/geniş-alan-ağı erişimi Mobil erişim Kablosuz ağ (WLan)	RFC 1349, RFC 2474, RFC 3168, RFC 3260 IPv6 – RFC 3697, RFC 3513, RFC 3484 Mobile IPv6 – RFC 3775, RFC 3776 IEEE 802.11 serisi standartları	Kullanılması önerilmektedir. IP v4 ile kurumlar arasında ara bağlantının sağlanmasının yanı sıra IPv6 geçiş çalışmalarının da yapılması gerekmektedir.
DHCP	RFC 3633, RFC 3736 (IPv6 için DHCP)	Üzerinde çalışılması gereklidir.

2.2.7 Gerçek Zamanlı Mesajlaşma (Real Time Messaging) Hizmetleri

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

2.2.8 Haber Grubu Hizmetleri

Bileşen	Standart/Teknoloji	Açıklama
Haber grubu hizmetleri (Newsgroup services)	NNTP – RFC 977, RFC 2980	Kullanılması önerilmektedir.

2.2.9 Web Servisleri (Web Services Transport)

Bileşen	Standart/Teknoloji	Açıklama
Web servisi istemi (Web service request delivery)	SOAP v1.2, W3C tarafından tariflenmiştir. Dokümanlar için www.w3.org sitesine bakınız. RFC 3288	Bkz. İkinci Bölüm, madde 3.4
Web servisi istem kaydı (Web service request registry)	UDDI v 2.0-v3.0 (Universal Description Discovery and Integration) www.uddi.org/specification.html	Bkz. İkinci Bölüm, madde 3.4
Web servisi tanımlama (Web service description language)	WSDL 1.1 (Web Service Description Language) www.w3.org/TR/wsdl	Bkz. İkinci Bölüm, madde 3.4
Diğer web servisi standartları		Bkz. İkinci Bölüm, madde 3.4

3 VERİ ENTEGRASYONU VE İÇERİK YÖNETİMİ

3.1 ESASLAR

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

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

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

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

3.2 İÇERİK YÖNETİMİ

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

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

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

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

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

Kaynak keşfi metaverisi şu bilgileri verir:

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

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

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

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

3.3 SÜREÇ ve VERİ ENTEGRASYONU

Kurumlar arası süreç ve veri entegrasyonunun sağlanabilmesi için yapılması gereken işlemler dört adımda özetlenebilir:

- Kamu çekirdek hizmet ve destek süreçlerinin tanımlanması ve iyileştirilmesi.
- Süreçlerin herhangi bir aşamasında kullanılan verilerin belirlenerek tanımlanması.
- Tanımlanan veri ve süreçler kapsamında kurumların veri toplama/güncelleme/erişim yetkilerinin düzenlenmesi.
- Veri paylaşımına imkan verecek veri entegrasyon mekanizmalarının oluşturulması.

3.3.1 Kamu Hizmet ve Karar Destek Süreçlerinin Tanımlanması ve İyileştirilmesi

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

3.3.1.1 Süreç Modelleme

3.3.1.1.1 Süreç Tanımlama Standardının Oluşturulması

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

3.3.1.1.2 Süreçlerin Tanımlanması

Süreçler, aşağıdaki yaklaşımla çıkarılarak tanımlanacaktır.

i. Mevcut süreçlerin çıkarılması (Mevcut Model).

1. Farklı bakışlarla (organizasyonel, fonksiyonel, veri vb.) entegre süreçlerin modellenmesi,
2. Mevcut kurumsal yapının, problemlerin, yetersizliklerin belirlenmesi,
3. Performans göstergelerinin oluşturulması,
4. Varlıklar; mevcut envanterin (insan, materyal) çıkarılması,
5. Bulguların birleştirilerek mevcut modelin son haline getirilmesi,
6. Personelin değişim açısından sosyolojik ve psikolojik yapısının incelenmesi,
7. Personelin eğitim durumlarının tespiti,
8. Gözden geçirme, doğrulama ve geçerleme.

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

ii. Stratejik Plan doğrultusunda mevcut süreçlerin bilgi ve iletişim teknolojilerinin getirdiği imkanlardan da yararlanacak şekilde iyileştirilmesi ve gerekirse yeniden tasarlanması (Hedef Model).

1. Süreçlerdeki darboğazlar, tıkama noktaları ve eksikliklerin belirlenmesi,
2. Raporlama ve yönetim ihtiyacının geliştirilmesi,
3. Bilgi akış haritalarının oluşturulması,
4. Modellenen süreçlerin revize edilmesi veya yeniden tasarlanması,
5. Süreçlere uygun organizasyonel yapı, iş/görev tanımlarının oluşturulması,
6. Uluslararası standartlar ve en iyi iş yapma biçimleri temelinde değerlendirme yapılması,
7. Gözden geçirme, doğrulama ve geçerleme.

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

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

1. Organizasyonel ilişkilerdeki dönüşüm adımlarının belirlenmesi,

2. Malzeme ve insan kapasitesini arttırma çalışmaları,
3. Eleman ve eğitim gereksinimlerinin ve çözümlerinin belirlenmesi,
4. Fiziksel altyapı (ofis alanı, malzeme, vb.), yazılım, donanım gereksinimlerinin belirlenmesi,
5. Varsa pilot uygulama kapsamına alınacak süreç(ler)in saptanması (geçiş adım adım planlanmalı ve pilot çalışmalar örnek alınarak revize edilmelidir),
6. Belirlenen gereksinimler için bütçeleme yapılması ve alım stratejilerinin tanımlanması,
7. Uyumluluk çalışmalarının gerçekleştirilmesi,
8. Değişim hareketinin sosyolojik ve psikolojik etkilerinin belirlenmesi ve alternatif çözümlerin oluşturulması,
9. Yasal düzenleme ihtiyacı; taslak mevzuatın hazırlanmasına katkı verilmesi,
10. Gözden geçirme, doğrulama ve geçerleme.

Bu aşamada temel olarak organizasyonel geçiş ve hareket planı (R-AP), eleman ve eğitim ihtiyacı, eğitim müfredatı (R-SyTrP), bilgi teknolojileri stratejik planı (R-SP), yaygınlaştırma ve operasyon planları (R-SyDOP), fiziksel altyapı oluşturma, yenileme ve geliştirme gereksinimleri ile gerekiyorsa taslak mevzuatı (R-L&R) içeren sistem gereksinim belgesi (R-SyRS) oluşturulacaktır.

iv. Gerçekleştirme sürecinin bundan sonraki aşamaları ISO 15288, ISO 12207 ve TS ISO/IEC 17799 gibi standartlar temelinde yürütülecek, tedarik yönetimi, entegrasyon ve sürdürülebilirliğe özel önem verilecektir.

3.3.2 Süreçlerde Kullanılan Verilerin Belirlenerek Tanımlanması

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

3.3.2.1 Veri Tanımlama

3.3.2.1.1 Veri Sözlüğü Standardının Oluşturulması

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

3.3.2.1.2 Veri Sözlüğü Hazırlama

Kurumlar, veri sözlüklerini kurumsal stratejiler ve Kamu Kurumları Veri Sözlüğü Standardı'na göre oluşturacak ve güncel tutacaktır. Tek noktadan erişilebilecek meta sözlük Devlet Planlama Teşkilatı Müsteşarlığı sorumluluğunda hazırlanacak ve güncel tutulacaktır.

3.3.2.2 Veri Modelleme

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

3.3.2.3 Veri Yapısı Tanımlama

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

3.3.2.4 Verinin Gösterimi (Format)

Verinin gösteriminde standart olarak XSL kullanılacaktır.

3.3.3 Kurumların Veri Toplama/Güncelleme/Erişim Yetkilerinin Düzenlenmesi

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

3.3.4 Veri Paylaşımına İmkan Verecek Veri Entegrasyonu Altyapısının Oluşturulması

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

3.4 KULLANILACAK STANDARTLAR

Bileşen	**Standart/Teknoloji**	**Açıklama**
Kaynak keşfi ve elektronik kayıt yönetimi metaveri standartları	ISO 15489-1:2001, ISO 15489-2:2001, ISO 15836:2003, ISO 23950:1998	Her iki alan için geliştirilecek standartlar, birbirleriyle uyumlu olacak şekilde Dublin Core veri kümesine dayanarak geliştirilecektir. Kaynak keşfi, arşiv ve kayıt yönetim sistemi için tasarlanmış metaveri kümesinin alt kümesi olarak kullanılacak, her iki alanda geliştirilen standartların birbirleriyle uyumlu (tutarlı) olmaları sağlanacaktır. Kurumların bu standartlara uyum mekanizmaları, geliştirilecek standartlarla birlikte hazırlanacak rehber içerisinde belirtilecektir.
Metaveri sınıflama ve kayıt	ISO/IEC 11179	
Süreç modelleme	İş süreçleri, süreç zincir çizenekleri (Process Chain Diagram) kullanılarak modellenmelidir. Yazılım desteği sağlanacak süreçler daha sonra UML kullanılarak detaylandırılacaktır.	Kullanılması önerilmektedir.

Bileşen	Standart/Teknoloji	Açıklama
Süreç uygulama dili (web servisleri için)	BPEL (Business Process Execution Language) BPEL4WS (Business Process Execution Language for Web Services)	
Süreç tanımlama (web servisleri için süreç tanımı depoları)	ebXML	Üzerinde çalışılması gereklidir.
Şüreçlerin çağırılması	ASAP (Asynchronous Service Access Protocol)	Kullanılması önerilmektedir.
Veri modelleme	Nesne bağıntı çizenekleri (Entity Relationship Diagram), Veri akış çizenekleri (DFD - Data Flow Diagram)	Kullanılması önerilmektedir.
Veri modeli değişimi	XMI	Kullanılması önerilmektedir.
Veri/metaveri yapısı tanımlama	XSD	Kullanılması önerilmektedir.
Veri gösterimi	XSL	Kullanılması önerilmektedir.
Veri dönüştürme (data transformation)	XSLT (XSL Transformation)	Kullanılması önerilmektedir.
Ontoloji tabanlı bilgi değişimi	OWL	Üzerinde çalışılması gereklidir.
Veri değişimi	Web servisi, XML	Kullanılması önerilmektedir.
Web servisi istemi (Web service request delivery)	SOAP v1.2, W3C tarafından tariflenmiştir. Dokümanlar için www.w3.org sitesine bakınız. RFC 3288	
Web servisi istem kaydı (Web service request registry)	UDDI v2.0-v3.0 (Universal Description Discovery and Integration) www.uddi.org/specification.html	

Bileşen	Standart/Teknoloji	Açıklama
Web servisi tanımlama	WSDL 1.1 (Web Service Description Language) www.w3.org/TR/wsdl	
Diğer web servisi standartları		Kullanılması önerilmektedir. Diğer standartlar için web servisleri birlikte çalışabilirlik (WS-I) sitesi (www.ws-i.org) ile OASIS ve W3C web servis komitelerine bakınız.
Kamu Kurumları Veri Sözlüğü Standardı		ISO/IEC 11179 temelinde geliştirilecektir.

4 GÜVENLİK

4.1 ESASLAR

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

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

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

Kamu bilgileri güvenlik açısından üç sınıfa ayrılabilir. Bunlar; tasnif dışı, hizmete özel ve hizmete özel üstü (gizli, çok gizli) bilgilerdir. Tasnif dışı bilgi, herhangi bir gizlilik derecesi olmayan bilgidir. Hizmete özel bilgi kurum içinde serbestçe dolaşabilen ancak kurum dışına yetkisiz çıkarılmaması gereken bilgilerdir. Hizmete özel gizlilik seviyesinin üzerindeki bilgiler ise, milli koruma önlemleri gerektiren ve yetkisiz açığa çıkması durumunda sadece kurumu değil, belli bir oranda devleti de zarara uğratabilecek bilgilerdir. Rehber'in güvenlik bölümü altında verilmiş olan standart, belirtim, kılavuz ve önerilerdeki kriptografik algoritmalar tasnif dışı ve hizmete özel güvenlik seviyesindeki bilginin güvenliği için kullanılmalı, daha yüksek güvenlik seviyesindeki bilginin güvenliği için kriptoloji@uekae.tubitak.gov.tr adresine başvurulmalıdır.

4.1.1 Bilgi Güvenliği Yönetim Sistemi (BGYS)

Kurumlar için en kritik varlık bilgidir. Kurumların değerleri, sahip oldukları bilgi ile ölçülmektedir. Bilgi, sadece bilgi teknolojileriyle işlenen bir varlık olarak düşünülmemelidir. Bilgi bir kurum bünyesinde çok değişik yapılarda bulunabilmektedir.

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

Bu hedefe ulaşmak amacıyla tum kurumlarda Bilgi Güvenliği Yönetim Sistemi kurulmalıdır. İhtiyaç sahibi kurumların kendi bünyelerinde BGYS'ye sahip olmaları ve bu BGYS'lerin kurumlar arası süreçleri de kapsamaları durumunda bilginin her katmanda güvenli bir şekilde işlenmesi için gerekli altyapı sağlanmış olacaktır.

BGYS, kurum bünyesinde güvenlik ile ilgili yapılanmaları gerektiren, kurulması uzun süre alan ve sürekli izlenmesi ve iyileştirilmesi gereken doküman destekli bir süreçtir. Bu nedenle, vatandaşların bilgilerini işleyen tüm kurumların aynı anda bu sisteme geçmesi yerine öncelikle ihtiyacı olan kurumların belirlenip belli bir sıraya göre BGYS'ye geçilmesi uygun olacaktır. Kamu kurumlarında yapılacak risk analizi çalışmaları sonuçlarına göre (e-Dönüşüm Türkiye 2005 Eylem Planı, 5 No'lu eylem) BGYS'ye ihtiyacı olan kurumlar ve öncelikler belirlenmelidir.

BGYS'ni tamamlayan kurumlar, bunu, TS 17799-2:2005 veya BS 7799-2:2002 sertifikası ile belgelendirmelidir. Bu sertifika, kurum bünyesinde BGYS'nin bu standartlara uygun şekilde işletildiğini belgeler.

4.1.2 Ortak Kriterler

Ortak Kriterler bilgi teknolojileri ürün ve/veya sistemlerinin güvenlik seviyelerinin tespit edilmesi ve bağımsız laboratuarlarda test edilebilmesi için geliştirilmiş olan, temelini TCSEC ve ITSEC standartlarından alan ve Uluslararası Standartlar Organizasyonu'nun (ISO) 1999 yılında Uluslararası Bilgi Teknolojileri Güvenlik Değerlendirme Standardı olarak kabul ettiği (ISO 15408) güvenlik standardıdır. Türkiye, Eylül 2003 tarihinde bu standardı kabul eden ülkelerin imzaladığı Ortak Kriterler Tanıma Sözleşmesini imzalayarak sertifika üretici ülkelerin değerlendirmelerini kabul etmiş, bunun yanı sıra TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) bünyesinde kurulan Ortak Kriterler Test Merkezi'nde (OKTEM) gerçekleştirilen testlerle ve TSE'nin test sonuçlarını sertifikalandıracak yapısı ile de ulusal değerlendirme yapısını kurmuştur.

Kamu kurum ve kuruluşları satın alacakları veya geliştirecekleri bilgi teknolojileri sistemlerinde gizli gizlilik dereceli bilgiyi bulundurmaları veya bu sistemleri kullanarak bilgi iletmeleri durumlarında sistemlerinin güvenlik seviyelerini Ortak Kriterler standardına uygun olarak tespit etmeli ve risk analizi sonucunda tespit edilen asgari garanti düzeyini sağlayacak ürün ve/veya sistemleri kullanmalıdırlar. Bu standardın gereksinimlerini hazırlanan şartnamelerin güvenlik eklerinde bulundurmalıdırlar.

TÜBİTAK-UEKAE satın alınacak veya geliştirilecek yazılımların güvenlik gereksinimlerinin belirlenmesi, ürünün ve/veya sistemin asgari garanti düzeyinin tespit edilmesi, değerlendirmelerin Ortak Kriterler standardına uygun olarak gerçekleştirilmesi konularında hizmet vermektedir.

4.1.3 Elekronik İmza

5070 sayılı Elektronik İmza Kanunu ve ilgili ikincil mevzuat gereğince ıslak imza ile aynı hukuksal etkiye sahip e-imza kullanımı yasal bir tabana oturtulmuş ve 2004/21 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının e-imza ile ilgili sertifika ihtiyaç ve işlemlerinin TÜBİTAK-UEKAE bünyesinde kurulmuş olan Kamu Sertifikasyon Merkezi tarafından yürütülmesi kararlaştırılmıştır. Bu düzenleme ışığında hukuksal açıdan geçerliliği olan e-devlet işlemlerinde e-imza kullanma gerekliliği açıktır. Konu ile ilgili ayrıntılı bilgiye http://www.kamusm.gov.tr adresinden erişilebilir. Ayrıca, kamu kurum ve kuruluşları dışındaki kuruluşlar ve gerçek kişiler için nitelikli sertifika hizmeti Telekomünikasyon Kurumu tarafından yetkilendirilmiş özel sektör sertifika hizmet sağlayıcıları tarafından yürütülecektir.

4.1.4 Kriptografik İşlemler

Kriptografik işlemler bilginin gizliliğinin ve bütünlüğünün korunması için kullanılan temel güvenlik önlemleridir. Kriptografik işlemler ile ayrıca, kimlik doğrulama ve aslını inkar edememe prensipleri de başarıyla uygulanır.

Bir bilgi sisteminde işlenen bilgiye kriptografik işlemler uygulanmasının öncesinde, risk analizi yapılmalı ve ihtiyaçlar ortaya konmalıdır. Sistemde işlenen bilginin gizlilik seviyesine göre uygun kriptografik önlemler alınmalıdır.

"Kullanılacak standartlar" başlığı altında verilen standartlara ve kılavuzlara erişim için kullanılabilecek web siteleri aşağıda verilmiştir:

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

4.2 KULLANILACAK STANDARTLAR

4.2.1 Bilgi Güvenliği Yönetimi

Bileşen	Standart/Teknoloji	Açıklama
Bilgi güvenliği yönetimi için uygulama prensipleri	TS ISO/IEC 17799:2002	Bilgi güvenliği yönetim sistemlerinde kullanılabilecek karşı önlem önerileridir. Mümkün olan hallerde milli olarak üretilen karşı önlemlerin kullanılmasına azami özen gösterilmelidir. Standart, uluslararası ISO 17799-2:2000 standardının Türkçe çevirisidir.
Bilgi güvenliği yönetim sistemleri – Özellikler ve kullanım kılavuzu	TS 17799-2:2005	Kurumların dokümante edilmiş bir BGYS'yi tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, bakımını yapmak ve iyileştirmek için gereksinimleri kapsar. Standart, BS 7799-2:2002 standardının Türkçe çevirisidir.

4.2.2 Bilgi Güvenliği Yönetimini Destekleyen Standartlar ve Kılavuzlar

Bu tablo altındaki kılavuz ve standartlar Türkçe olarak yayımlanmamıştır.

Bileşen	Standart/Teknoloji	Açıklama
BS 7799-2 sertifikasyonu için hazırlık	PD 3001:2002	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Preparing for BS 7799-2 certification
BS 7799 risk analizi kılavuzu	PD 3002:2002	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guide to BS 7799 risk assessment

Bileşen	Standart/Teknoloji	Açıklama
BS 7799-2 denetlemesi için hazır mısınız?	PD 3003:2002	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Are you ready for a BS 7799 Part 2 audit?
BS 7799 kontrollerinin uygulaması ve denetlemesi için kılavuz	PD 3004:2002	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guide to the implementation and auditing of BS 7799 controls
BS 7799-2 kontrollerinin seçimi için kılavuz	PD 3005:2002	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guide to the selection of BS 7799 Part 2 controls
Bilgi teknolojileri ve iletişim teknolojilerinin güvenlik yönetimi için kavramlar ve modeller	ISO/IEC 13335-1:2004	ISO tarafından hazırlanmış olan standardın orijinal ismi: Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
Bilgi teknolojileri güvenliğinin yönetimi için teknikler	ISO/IEC TR 13335-3:1998	ISO tarafından hazırlanmış olan standardın orijinal ismi: Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
Karşı önlemlerin seçimi	ISO/IEC TR 13335-4:2000	ISO tarafından hazırlanmış olan standardın orijinal ismi: Guidelines for the management of IT Security -- Part 4: Selection of safeguards
Ağ güvenliği için yönetim kılavuzu	ISO/IEC TR 13335-5:2001	ISO tarafından hazırlanmış olan standardın orijinal ismi: Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security

4.2.3 Bilgi Teknolojileri Ürünleri Güvenliği

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

4.2.4 Web Servisleri (WS) Güvenliği

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

Bileşen	Standart/Teknoloji	Açıklama
Web içeriğinin güvenli iletimi (bütünlük ve gizlilik)	RFC 2246	SSL v3.0/ TLS v1.0 (İstemci SSL veya TLS'ten herhangi birisini kullanabilir. Fakat sunucu SSL ile uyumlu olan TLS'i desteklemek zorundadır.)
Web sunucusunun kimlik doğrulamasının yapılması		
Web üzerinden işlemler	OSCI transport v1.2	http://egovernment.xml.org/standards/pdf/010_osci_1_2_specification.pdf
Web servisleri mesaj seviyesi güvenliği (WS-Security)	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss	SOAP mesajlarının nasıl sayısal olarak imzalanacağını, nasıl şifreleneceğini ve sertifikaların mesaj içerisine nasıl yerleştirileceğini tanımlayan standarttır.

4.2.5 E-Posta Güvenliği

Bileşen	Standart/Teknoloji	Açıklama
e-Posta taşıma güvenliği	RFC 3207	SMTP Service Extension for Secure SMTP over TLS
e-Posta içerik güvenliği	RFC 2631 RFC 2632 RFC 2633 RFC 3369	S/MIME v3
Güvenli posta kutusu erişimi	RFC 2595	IMAPS POP3S

4.2.6 Ağ Katmanı Güvenliği

e-Devlet güvenlik ana çatısının gereksinimlerini karşılamak için kullanılacak standartlar aşağıda sıralanmıştır.

Bileşen	Standart/Teknoloji	Açıklama
IP güvenliği (kaynağın kimliğinin doğrulanması, kaynağın ve verinin bütünlüğü)	RFC 2402	IPSec (AH – Authentication Header)
IP güvenliği (verinin gizliliği ve/veya bütünlüğü)	RFC 2406 RFC 2407 RFC 2451 RFC 3602	IPSec (ESP – Encapsulating Security Payload) (VPN gereksinimleri için kullanılabilir.)

Bileşen	Standart/Teknoloji	Açıklama
Taşıma katmanı güvenliği	RFC 2246	SSL v3.0/ TLS v1.0 (İstemci SSL veya TLS'ten herhangi birisini kullanabilir. Fakat sunumcu SSL ile uyumlu olan TLS'i desteklemek zorundadır.)

4.2.7 Şifreleme ve İmzalama

Aşağıdaki algoritmalar, standart, kılavuz veya belirtim olarak belirtilen referanslar dışındaki durumlarda kullanılmak üzere önerilmektedir.

Bileşen	Standart/Teknoloji	Açıklama
Şifreleme algoritmaları (Encryption Algorithms)	FIPS 197, SP 800-38A, SP 800-38B, SP 800-38C http://csrc.nist.gov/publications/nistpubs/index.html	AES (Burada önerilen algoritma kümesini genişletmek için çalışmalar devam etmektedir.)
Sayısal imza algoritmaları (Digital Signature Algorithms)	PKCS#1, ANSI X9.31, FIPS 186-2, ANSI X9.30-1, ANSI X9.62	RSA ECDSA
Anahtar taşıma algoritmaları (Key Transport Algorithms)	RSA	RSA'da önerilen algoritma kümesini genişletmek için çalışmalar devam etmektedir.
Özetleme algoritmaları (Hash Algorithms)	FIPS 180-2, RFC 1321	SHA-1 SHA-256 SHA-384 SHA-512

4.2.8 Güvenli Doküman Alışverişi

Elektronik iş ortamında bir dokümanın birden fazla kurum arasında gidip gelmesi düşünüldüğünde sadece noktadan noktaya güvenlik sağlayan VPN, SSL, TLS tek başına yeterli gelmeyecektir. Güvenliğin bütünüyle sağlanabilmesi için mesaj seviyesinde de güvenlik ele alınmalıdır.

Bileşen	Standart/Teknoloji	Açıklama
XML sayısal imzalama	http://www.w3.org/TR/2002/REC-xmldsig-core-20020212	W3C tarafından tanımlanan XML - imza söz dizimi ve işlenmesi (XMLDsig) (XML imzalı dokümanı alan kimse, dokümanı gönderen kimseyi ve dokümanın zarar görmediğini doğrular.)
XML şifreleme	http://www.w3.org/TR/xmlenc-core/	W3C tarafından tanımlanan XML - şifreleme söz dizimi ve işlenmesi (XMLenc) (İçeriğin şifreli taşınmasını güvenli hale getirmek için kullanılır. Taşıma sonrası dokümanın şifreli kalması gereken durumlarda kullanılabilir.)

Bileşen	Standart/Teknoloji	Açıklama
XML sayısal imzalama ve şifreleme	http://www.w3.org/TR/xmlenc-decrypt	W3C tarafından tanımlanan XML imzası için şifre çözme dönüşümü
Açık Anahtar Altyapısının (PKI) kullanıldığı yerlerde XML anahtar yönetimi	http://www.w3.org/TR/xkms2/	W3C tarafından tanımlanan XML anahtar yönetimi belirtimi (XKMS 2.0)
XML tabanlı kimlik bilgisi, yetki düzeyi ve profillerin tanımlanması	http://www.oasis-open.org/committees/security/index.shtml	OASIS tarafından tanımlanan SAML
Dokümanın belirli bir tarihteki varlığının inkâr edilememesi	RFC 3161	TSP

5 ÇÖZÜM YAŞAM DÖNGÜSÜ

5.1 ESASLAR

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

5.2 KULANILACAK STANDARTLAR

Bileşen	**Standart/Teknoloji**	**Açıklama**
Yazılım süreç denetimi	ISO 15504	Kullanılması önerilmektedir.
Sistem yaşam döngüsü süreçleri	ISO 15288	Kullanılması önerilmektedir.
Yazılım yaşam döngüsü süreçleri	TS ISO/IEC 12207	Kullanılması önerilmektedir.
Güvenlik süreçleri	TS ISO/IEC 17799	Kullanılması önerilmektedir.

ÜÇÜNCÜ BÖLÜM

ÜÇÜNCÜ BÖLÜM

1 REHBERİ TAMAMLAYICI NİTELİKTE YÜRÜTÜLECEK ÇALIŞMALAR

Önümüzdeki dönemde, Birlikte Çalışabilirlik Esasları Rehberi'nin kapsamı genişleyecek, daha ayrıntılı bir kaynak halini alacaktır. Birlikte Çalışabilirlik Esasları Rehberi'nin bu sürümünde temel yapı taşlarının oluşturulmasında kullanılacak araçlar ortaya konmuştur. Bu araçlar kullanılarak geliştirilecek yapılar ve standartlar Rehber'in ileriki sürümleri içerisinde yer alacaktır. Önümüzdeki dönemdeki iş takvimini şimdiden şekillendirebilmek amacıyla yapılacak temel işler aşağıda listelenmektedir.

1.1 Kılavuzların Hazırlanması

Günümüzde birlikte çalışabilir sistemlere ilişkin çok fazla örnek yoktur. Bu nedenle bu tür projelerin geliştirilmesi için gerekli tecrübe eksikliği göze çarpmaktadır.

Bu açıdan, kurumların birlikte proje geliştirmesine ön ayak olacak yapı ve mekanizmaların geliştirilmesi, beraber geliştirilecek projelerde yol gösterecek bir kılavuz yayımlanması, ortak hizmet sunumunda risk ve maliyeti azaltıcı önlemlerin alınması büyük önem arz etmektedir.

1.2 e-Devlet Metaveri Standardı

Bilginin paylaşılabilmesi için, kurumların bilgi kaynakları envanterlerinin çıkarılmış olması gereklidir. Kurumların kendi bilgi envanterlerini çıkarırken yaşayacakları zorluklar düşünüldüğünde, diğer kurumlarda tutulan bilgilerin varlığından haberdar olmaları ve tutulan bilginin yapısını anlamaları çok daha zor olacaktır.

Metaveri, sayısal olan ya da olmayan tüm kaynaklar hakkında içerik, kalite, erişim, bulunabilirlik vb. açısından bilgi veren yapısal bilgi olarak tanımlanabilir. Kurumların bu standartlara uyarak ellerindeki verilerin haritasını çıkartması, diğer birçok katma değerli hizmete imkan vermesi yanında, bilgi paylaşımı fırsatlarının ortaya konmasında yararlı olacaktır[3].

1.3 Veri Entegrasyonu İçin Gerekli Çalışmalar

Öncelikli kamu hizmetlerine ait süreçlerin modellenmesi, bu süreçlerde ortaya konan veri ihtiyaçları ve ihtiyaç duyulan verinin paylaşılmasına yönelik olarak veri sözlüğü standardının belirlenerek bu standart doğrultusunda hazırlanacak kurumsal veri sözlükleri, veri entegrasyonu için atılacak önemli adımlar olacaktır. Bu çerçevede belirlenen veri seti üzerinde kurumsal yetki ve sorumluluklara ait işlemler yapılacak ve paylaşılacak veri için gerekli XML tabanlı altyapı işlemleri tamamlanacaktır.

[3] Bu amaçla e-Dönüşüm Türkiye 2005 Eylem Planı'na 35 No'lu "Birlikte Çalışabilirlik İçin Veri Paylaşımı" eylemi konmuş ve çalışmalar başlatılmıştır.

1.4 Elektronik Kayıt Yönetimi Çerçevesi

Önümüzdeki yıllarda çok daha yoğun olarak gerçekleşecek elektronik kayıt yönetimi, elektronik doküman yönetim sistemi yatırımlarının kaliteli ve birbirleriyle uyumlu gerçekleştirilebilmesi ve tüm kamu kurum ve kuruluşları arasında güvenli doküman iletimi yapılabilmesi hedefi kapsamında Elektronik Kayıt Yönetimi Çerçevesi hazırlanacaktır[4].

1.5 XML Şemalarının Çıkartılması

Kamu kurumlarının birbirleriyle anlaşabilmek için kullanacağı, XML'e dayalı kamu standartlarının oluşturulması gereklidir.

1.6 e-Hizmetlerin Geliştirilmesi ve Kolay Erişim

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

[4] Bu amaçla e-Dönüşüm Türkiye 2005 Eylem Planı'na 37 No'lu "Kamuda Elektronik Kayıt Yönetimi" eylemi konmuş ve çalışmalar başlatılmıştır.

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

EKLER

EK-A

AÇIKLAMALAR

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

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

İkinci Bölüm, madde 1.2.2'de kelime işlem dokümanları için kullanılacağı ifade edilen formatlardan MS Office 97 formatı ile doküman üretmek için MS Office-Word programının 97 ve daha sonraki sürümleri kullanılabilir. Aynı formattaki dokümanlar, www.openoffice.org İnternet adresinden, Türkçe sürümü de dahil olmak üzere, farklı diller için özelleştirilmiş sürümleri ücretsiz olarak indirilebilen açık kaynak kodlu OpenOffice programı ile de üretilebilmektedir. Söz konusu program ile aynı zamanda MS Word formatında kaydedilmiş dosyalar da işlenebilmektedir. Ancak, dosyalardaki "makrolar" gibi bazı bileşenlerin işlenmesinde problem yaşanabilmektedir. StarOffice adlı program da OpenOffice programının fonksiyonlarına benzer özellikler taşımaktadır.

İkinci Bölüm, madde 1.2.2'de belirtilen ".rtf" formatında doküman üretmek hem MS Office hem de OpenOffice programları ile mümkündür. ".txt" formatı ise düz metin formatı olup kişisel bilgisayarların hemen hepsinde bulunan metin editörleri ile oluşturulabilir.

İkinci Bölüm, madde 1.2.2'de belirtilen OpenDocument standardının kelime işlem dokümanları için kullandığı ".odt" formatı ile doküman üretmek OpenOffice programı ile mümkündür.

İkinci Bölüm, madde 1.2.3'de belirtilen ".html" formatı, web sayfalarını oluşturmak için kullanılan araçlar ile oluşturulabilir. Diğer taraftan, Microsoft Office-Powerpoint programı ile oluşturulmuş olan sunum dosyaları da ".html" uzantılı olarak kaydedilebilir. "Microsoft Powerpoint 97" formatlı dokümanlar hem Microsoft Office-Powerpoint hem de OpenOffice programı ile oluşturulabilir. OpenDocument standardının sunum dosyaları için kullandığı ".odp" formatlı dokümanlar OpenOffice programı ile oluşturulabilir.

İkinci Bölüm, madde 1.2.4'de elektronik çizelge dokümanları için kullanılabileceği belirtilen ".html" formatlı dokümanlar, elektronik çizelgeler Microsoft Office-Excel veya OpenOffice programı ile oluşturulduktan sonra ".html (web sayfası)" formatında kaydedilerek oluşturulabilir. ".csv" uzantılı dosyalar da Microsoft Office-Excel veya OpenOffice programlarında oluşturulan elektronik çizelgeler ".csv" uzantılı olarak kaydedilerek oluşturulabilir. ".csv" uzantılı dosyalar aslında düz metin dosyaları olup herhangi bir düz metin editörü (örneğin notepad) ile de görüntülenebilir. ".ods" uzantılı elektronik çizelge dokümanları ise OpenOffice programı ile oluşturulabilir.

EK-B

TANIMLAR

Doküman sıkıştırma formatları

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

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

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

Doküman formatları

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

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

PDF: Portable Document Format müseccel Adobe firma standardıdır.

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

Karakter Kümeleri

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

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

Resim-Video dosya formatları

TIF (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.

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

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

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

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

İletişim protokolleri

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

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

S/MIME (Secure MIME): S/MIME, MIME'nin üzerine tanımlanmış olup İnternet ortamından gönderilen e-postaların güvenilir şekilde iletilmesi için kullanılır. Güvenlikten

kasıt, gönderilen mesajın bütünlüğünün korunması, inkar edememezlik, şifreleme gibi elektronik haberleşme için gerekli güvenlik hizmetlerinin sağlanmasıdır. S/MIME sadece e-posta iletileri için değil, aynı zamanda MIME formatlı veri gönderen diğer iletim mekanizmalarında (HTTP) da kullanılabilir.

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

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

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

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

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

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

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

TCP (Transmission Control Protocol): Paket anahtarlamalı ağlarda veri paketlerinin hangi yolu izleyerek alıcıdan vericiye ulaşacakları ağ katmanında çalışan protokollerce

(örneğin IP) yürütülür. Her paket farklı yollardan alıcısına ulaşabileceğinden alıcıdaki paketlerin sırası gönderildiği sıradan farklı olabilir. Ayrıca bazı paketler yolda kaybolmuş olabilir. TCP, OSI referans modelinin ulaşım katmanında çalışır ve bir altındaki ağ katmanından gelen paketlerin sıralanması, kayıp paketlerin tekrar göndericiden istenmesi gibi görevleri yürütür.

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

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

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

Alan adı protokolleri

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

Erişim protokolleri

LDAP (Lightweighted Directory Access Protocol): Bu standart ile aranan kişiye ait bilgilere erişim sağlanması amaçlanmıştır. Örneğin e-posta gönderilecek kişinin e-posta

adresi gönderici tarafından bilinmiyorsa bunun için bir veri tabanından ilgili kişinin e-posta adresi sorgulanabilir. Aynı yöntem başka türlü taramalar için de geçerlidir (örneğin bir kimsenin elektronik sertifikasına ulaşmak için). Bir sunucu (bu sunucular ülke çapında bilgi içerebileceği gibi sadece bir üniversite kampüsündeki kişilerin bilgilerini de içerebilir) üzerinde bulunan veri tabanında tarama yapılarak (tarama için anahtar kelimeler kullanılabilir, sınıflandırma yapılabilir, vb.) kişilerin bilgilerine erişmek mümkün olur. LDAP bu işlerin nasıl yapılacağını belirleyen standarttır.

Genel Bilgi Güvenliği

Bilgi güvenliği, aşağıda sıralanan üç temel unsurun, ihtiyaçlara uygun kombinasyonu ile sağlanır.

- **Gizlilik:** Bilgiye, sadece o bilgiye erişmeye yetkili kişiler tarafından erişilebilmesidir.
- **Bütünlük:** Bilginin yetkisiz kişilerce yapılabilecek değiştirilme, silinme, ekleme gibi tahribatlara karşı korunmasıdır.
- **Erişilebilirlik:** Bilginin gerektiğinde yetkili kullanıcıların erişimine hazır durumda bulundurulmasıdır.

Bunlara ek olarak aşağıdaki güvenlik mekanizmaları bilgi güvenliğinin sağlanması için zaruridir.

- **Kimlik tanımlama:** Kişilerin kimliklerini sisteme tanıttıkları temel basamaktır. Bu basamak kimlik doğrulama ve erişim kontrolü için gerekli olan ilk adımdır.
- **Kimlik doğrulama:** Sisteme giriş yapan kişinin iddia ettiği kimliğin gerçekte sahip olduğu kimlik olup olmadığını garantiye alan mekanizmadır.
- **Kayıt edilebilirlik:** Kimlik doğrulaması yapılan bir kişinin faaliyetlerinin izlenmesi ve tespit edilmesi kabiliyetidir.
- **Yetkilendirme:** Kullanıcıların sistem kaynaklarına erişiminin denetlenmesi, doğru kullanıcıların, doğru kaynaklara, doğru zamanda erişiminin sağlanmasıdır.
- **Mahremiyet:** Bir sistemde çalışan bir kişiye ait bilgilere başkaları tarafından erişilmemesi olgusudur.
- **İnkar edemezlik:** Kullanıcının sistem üzerinde yapmış olduğu işlemleri inkar edememesinin sağlanmasıdır.

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

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 doğrulama ve inkar edemezlik için kullanılan temel yöntemdir. Asimetrik anahtarlı sistemler sayısal imza oluşturmak için kullanılabilir. Bunun için imza atılacak mesaj veya mesajın özet değeri, göndericinin gizli anahtarı ile şifrelenir. Uygun açık anahtara sahip olanlar imzayı doğrulayabilirler.

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.

Web Servisleri Güvenliği

SSL – Secure Socket Layer: Web üzerinde bütünlük, gizlilik ve kimlik doğrulamayı sağlayan bir kriptografik protokoldür. Bu protokol ile tek taraflı kimlik doğrulama yapılabilir. Daha açık bir ifade ile yalnızca servis sağlayıcının kimliği doğrulanır ve haberleşmenin şifreli olarak yapılması sağlanır.

TLS - Transport Layer Security (iletim katmanı güvenliği): Bu protokol, SSL'in İnternet standardı sürümü olarak geliştirilmiştir. Protokolün amacı haberleşen iki uygulama arasında veri güvenliği ve bütünlüğünün sağlanmasıdır. Protokol iki katmandan oluşur. İlk katman TLS kayıt protokolü, diğeri ise TLS mutakabat (handshake) protokolüdür. TLS kayıt protokolü ile veriler simetrik kripto anahtarları ile şifrelenir. Her bağlantı için farklı bir simetrik kripto anahtarı kullanılır. Bu anahtar TLS mutabakat protokolü kullanılarak alıcı ve verici tarafından paylaşılır. TLS mutabakat protokolü ile kripto algoritmasının ve anahtarların ilgili taraflarca kararlaştırılması sağlanır. TLS mutabakat protokolü ile haberleşecek tarafların birbirlerini yetkilendirmeleri ve kripto algoritması ve anahtarların karşılıklı değişimi sağlanır. Bunun için asimetrik kriptolama kullanılır.

SSL/TSL ile güvenli hale getirilmiş web sayfaları "http://" yerine "https://" ile adreslenir.

Ağ Katmanı Güvenliği

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).

Şifreleme ve İmzalama

3DES (Triple Data Encryption Standart): Simetrik şifreleme algoritmasıdır. DES'in 56 bitlik anahtar uzunluğundan kaynaklanan güvenlik eksikliğini azaltmak için 3DES algoritması geliştirilmiştir. 3DES ile 168 (56x3) bit uzunluğunda kripto anahtarları kullanılır ve çalışma prensibi DES'e benzer. 3DES ile kriptolamada DES algoritması birden çok anahtar ile arka arkaya uygulanır. 3DES, DES'ten daha uzun kripto anahtarları kullandığından algoritma daha yavaş çalışır.

AES (Advanced Encryption Standard): Simetrik şifreleme algoritmasıdır. 128 bitlik mesaj bloğunu 128, 192 veya 256 bitlik anahtar kullanarak şifreler. Güvenlik açısından 3DES kadar güvenli, algoritmanın çalışması bakımından ise daha hızlı bir şifreleme tekniğidir.

Blowfish (simetrik kriptolama): AES'e benzer şekilde hızlı çalışmak üzere tasarlanmış bir algoritmadır. 32 bit mikro işlemciler ile 1 byte data 18 işlemci döngüsünde (clock cycle) şifrelenir. 5 KB'tan daha az bir hafızaya ihtiyaç duyar. Uygulaması son derece kolaydır ve farklı uzunlukta kripto anahtarları seçilerek farklı güvenlik seviyeleri elde edilebilir.

RSA (Rivest-Shamir-Adleman): Geliştirilen ilk asimetrik anahtarlı şifreleme algoritmalarından biridir. Bu teknikte şifreleme ve şifre çözme için farklı kripto anahtarları kullanılır. Bu iki anahtar öyle özelliklere sahiptir ki birisi ile şifrelenen mesaj ancak ve ancak eşi olan diğer anahtar ile açılabilir. Bu anahtarlar çok büyük asal sayılar kullanılarak elde edilirler. Şifreli iletişim yapmak isteyen herkesin iki tane anahtarı vardır. Bunlardan biri sadece şifre sahibi tarafından bilinir (özel anahtar) ve başkalarının eline geçmesi engellenmelidir. Bu anahtarın eşi olan diğer anahtar ise (açık anahtar) serbestçe iletişim kurulacak kişilere verilebilir. AAA kullanıldığı durumda, açık anahtar genellikle veritabanlarından yayınlanır ve isteyen herkes istediği kişinin elektronik sertifikasını okuyarak açık anahtarını öğrenebilir. Bu altyapı ile gönderilen mesajın bütünlüğünün korunması, gönderenin belirlenmesi, yetkilendirme gibi bir çok amaç gerçekleştirilebilir. Anahtarlar ne kadar uzun seçilirse şifrenin kırılması o kadar zor olur.

DSA (Digital Signature Algorithm): Asimetrik şifreleme algoritmasıdır. Bu algoritma açık anahtar altyapısı kullanılarak elektronik imzalamanın nasıl yapılacağını tanımlamaktadır.

MD5 (Message Digest Algorithm): Bu algoritma mesaj özetleri çıkarmak için kullanılır. Mesaj özeti; bir mesajın özel bir fonksiyondan geçirilerek bu mesaja özel belirli uzunlukta bir veri oluşturulması işlemidir. Mesaj özeti çıkaran fonksiyonlar öyle özellikler gösterirler ki tam olarak aynı olmayan mesajların özetlerinin aynı olma olasılığı yok denecek kadar azdır. Ayrıca, orijinal mesajın bir tek karakteri bile değişse yeni mesaj özeti orijinal mesajın özetinden çok daha farklı olur. Mesaj özeti çıkarma işlemleri, gönderilen dokümanların daha sonra göndereni tarafından inkar edilememesini sağlama açısından önemlidir.

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

SHA (Secure Hash Algorithm): FIPS tarafından onaylanmış bir özetleme algoritmasıdır. SHA-1 160 bitlik, SHA-256 256 bitlik, SHA-384 384 bitlik, SHA-512 ise 512 bitlik mesaj özeti oluşturur.

SHA-1 (Secure Hash Algorithm): MD5 gibi mesaj özeti çıkarmaya yarayan bir algoritmadır ve çalışma prensibi de MD5'e benzer. SHA-1 algoritmasının çıkardığı mesaj özeti MD5'inkinden 32 bit daha uzundur ve kırılması daha zordur. Ayrıca SHA-1 algoritmasının teorik yapısının analiz edilmesi MD5'ten daha zordur, dolayısı ile daha güvenlidir. Bunlarla birlikte SHA-1, MD5'ten daha yavaş çalışır.

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

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

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

X.509 v3 (elektronik imza): Elektronik sertifikaların yapısını tanımlayan protokoldür.

X.509 v2 (elektronik imza): Elektronik sertifika iptal listelerinin yapısını tanımlayan protokoldür.

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

Güvenli Doküman Alışverişi

XML İmzaları: XML imzaları, XML verilerini imzalamak için geliştirilmiş sayısal imzalardır. Bu yöntem, klasik imzalamadan farklı olarak bir dokümanın tamamı yerine farklı bölümlerinin farklı kişilerce imzalanabilmesine olanak sağlar.

Diğer Tanımlar

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

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

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

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

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

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

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

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

Evrensel Açıklama, Keşif ve Entegrasyon (UDDI): Web servisleri ile ilgili olarak bir adres defteri işlevi görür. Web servislerini İnternet'te tanımlamak için oluşturulmuş bir

belirtimdir. Hangi web servisinin nerede olduğunu ve ne işe yaradığını bildirmek için kullanılır.

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

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

EK-C

KISALTMALAR

3DES	**:**	Triple Data Encryption Standart (simetrik kriptolama)
AAA	**:**	Açık Anahtar Altyapısı (Bkz. PKI)
AES	**:**	Advanced Encryption Standart (simetrik kriptolama)
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
CC	**:**	Common Criteria
DAV	**:**	Distributed Authoring and Versioning
DFD	**:**	Data Flow Diagram (Veri Akış Çizeneği)
DNS	**:**	Domain Name Service
DSA	**:**	Digital Signature Algorithm (asimetrik kriptolama)
ECDSA	**:**	Elliptic Curve Digital Signature Algorithm
ESP	**:**	Encapsulation Security Protocol
FIPS	**:**	Federal Information Processing Standards
FTP	**:**	File Transfer Protocol
GIF	**:**	Graphics Interchange Format
HTTP	**:**	Hypertext Transfer Protocol
HTTPS	**:**	HTTP Secure
IEC	**:**	International Engineering Consortium
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
IT	**:**	Information Technology
JPEG	**:**	Joint Pictures Experts Group
LDAP	**:**	Lightweighted Directory Access Protocol
LZW	**:**	Lempel Ziv Welch
MD5	**:**	Message Digest Algorithm

MIME : Multi-purpose Internet Mail Extensions
NNTP : Network News Transfer Protocol
OASIS : Organization for the Advanced of Structured Information
OWL : Web Ontology Language
PD : Published Document
PKCS : Public Key Cryptography Standard
PKI : Public Key Infrastructure
(**AAA-**Açık Anahtar Altyapısı)
PNG : Portable Network Graphics
POP3 : Post Office Protocol Version 3
POP3S : Secure Post Office Protocol 3
RFC : Request For Comments
RSA : Rivest-Shamir-Adleman (asimetrik kriptolama)
S/MIME : Secure Multipurpose Internet Mail Extensions
SAML : Security Assertion Markup Language
SHA-1 : Secure Hash Algorithm – 1
SMTP : Simple Mail Transfer Protocol
SOAP : Simple Object Access Protocol
SSL : Secure Socket Layer (iletim katmanı güvenliği)
TCP : Transport Control Protocol
TIF : Tag Image File Format
TLS : Transport Layer Security (iletim katmanı güvenliği)
TS : Türk Standartları
TSP : Timestamp Protocol
UDDI : Universal Description, Discovery and Integration
UDP : User Datagram Protocol
UML : Unified Modelling Language
VPN : Virtual Private Network
W3C : World Wide Web Consortium
WS : Web Services
WSDL : Web Services Description Language
XKMS : XML Key Management Specification
XMI : XML Metadata Interchange
XMPP : Extensible Messaging and Presence Protocol
XML : eXtensible Markup Language
XSD : eXtensible Mark-up Language Schema Definition
XSL : eXtensible Stylesheet Language