E-İMZA ULUSAL KOORDİNASYON KURULU
ALTYAPI ÇALIŞMA GRUBU
İLERLEME RAPORU

1 YÖNETİCİ ÖZETİ

2 RAPORUN AMACI VE KAPSAMI

5070 sayılı Elektronik İmza Yasası kapsamında, Türkiye'nin ihtiyaçlarına cevap verebilecek açık anahtar altyapısının oluşturulmasına yönelik olarak dünyadaki mevcut uygulamaların incelenmesi ve değerlendirilmesi; ülkemizde kamu kesimindeki e-dönüşüm faaliyetleri ve özel sektör bünyesinde devam eden çalışmalar, sektörün farklı beklentileri, uluslararası entegrasyon, kaynakların etkin kullanımı, ulusal güvenlik, teknolojik gelişim ve yerli katkı gibi hususlar göz önünde bulundurularak Türkiye için alternatif açık anahtar altyapısı modelleri önerilmesi.

3 RAPORUN HAZIRLANMASINA KATKIDA BULUNANLAR

Altyapı Çalışma Grubu'nun 70'e yakın üyesi bulunmasına rağmen, raporun hazırlanmasına katkıda bulunan ve toplantıya katılan üyelerin sayısı 19 ile sınırlı kalmıştır. Aşağıda toplantıya katılan ve/veya aktif olarak katkıda bulunan üyelerin isimleri yeralmaktadır:

Muzaffer YILDIRIM (TÜBİTAK - UEKAE)
Sertaç ÇELİKYILMAZ (E-Güven)
Özgür Arzu BARBAROS (Tüm İnternet Derneği / Koç.net)
Durmuş Okan BOZKIRLI (T.C. Başbakanlık Gümrük Müsteşarlığı)
Musa BAYSAN (Uzak Mesafe Telefon ve İl. Hiz. San. Tic. A.Ş.)
Ertuğrul AĞAR
Çiğdem ÖLEKLİ (Gantek)
Hakan ÖZFİDAN (T.C. Başbakanlık Bilgi İşlem Başkanlığı)
Mustafa AFYONLUOĞLU (Türkiye Noterler Birliği (TNB))
Davut ŞAHİNEL (TPAO)
Can ORHUN (E-Güven/SBS/ VeriSign, MPKI)

Koray ÇANDIR (E-Güven/SBS/ VeriSign, MPKI)
M.Feridun AKTAŞ (Garanti Bankası)
Ayşe PEHLİVAN (Vasco Data Security)
Ömer KURTULMUŞ
Furkan CİVELEK (DPT)
Sedat BAŞMAN (EreNet A.Ş.)
Serhat ÖZEREN (TEDER)
Mete VARAS (TurSign Dijital Sertifika Hiz. A.Ş.)
Muharrem BÜYÜKBAHÇECİ (TurSign Dijital Sertifika Hiz. A.Ş.)

4 DÜNYADA ELEKTRONİK İMZAYA İLİŞKİN KURUMSAL ALTYAPI VE UYGULAMALAR

4.1 Avrupa Birliği

4.1.1 Kamu sektöründe izlenen politikalar, kullanılan AAA modelleri ve uygulamalar

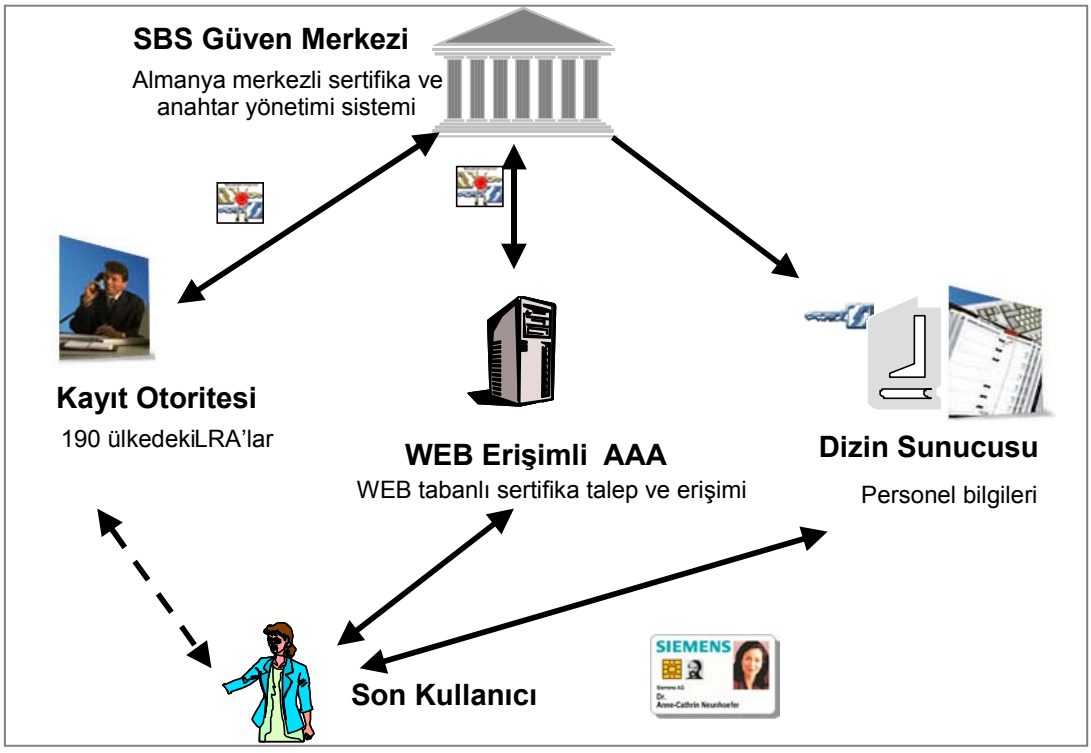
4.1.1.1 Örnek Uygulamalar

4.1.1.1.1 Siemens ve SBS Kurumsal PKI Projesi

Dünyanın en büyük kurulu sitelerinden birini kurmuş ve işletmektedir. Sertifika Otoritesi, tek merkezden tüm dünyadaki Siemens ve SBS çalışanlarına (2001'den itibaren 190 ülkede, 500 lokasyonda 484.000 kullanıcı) sayısal imzalar ve şifreleme yoluyla güvenlik çözümü sağlanmıştır.

İhtiyaçlar / Çözüm: E-posta, dosya ve veri şifreleme, logon, intranet ve ERP erişimi ve iş süreçleri yönetimi alanlarında güvenlik talep eden müşteriye sayısal imzalar, sayısal sertifikalar, sertifika yönetimi, son kullanıcı yazılımları sunulmuştur. Proje kapsamında Açık Anahtar Altyapısı hizmetleri Akıllı Kartlar ile bütünleşik halde sunulmuştur.

Faydaları: Kurum içi ve kurumlar arası güvenli iletişim, iyileştirilmiş ve otomasyonu sağlanmış iş süreçleri, zamandan tasarruf ve yönetilen Açık Anahtar Altyapısı sayesinde kolay uygulanabilen ve düşük maliyetli çözüm sağlanmıştır.

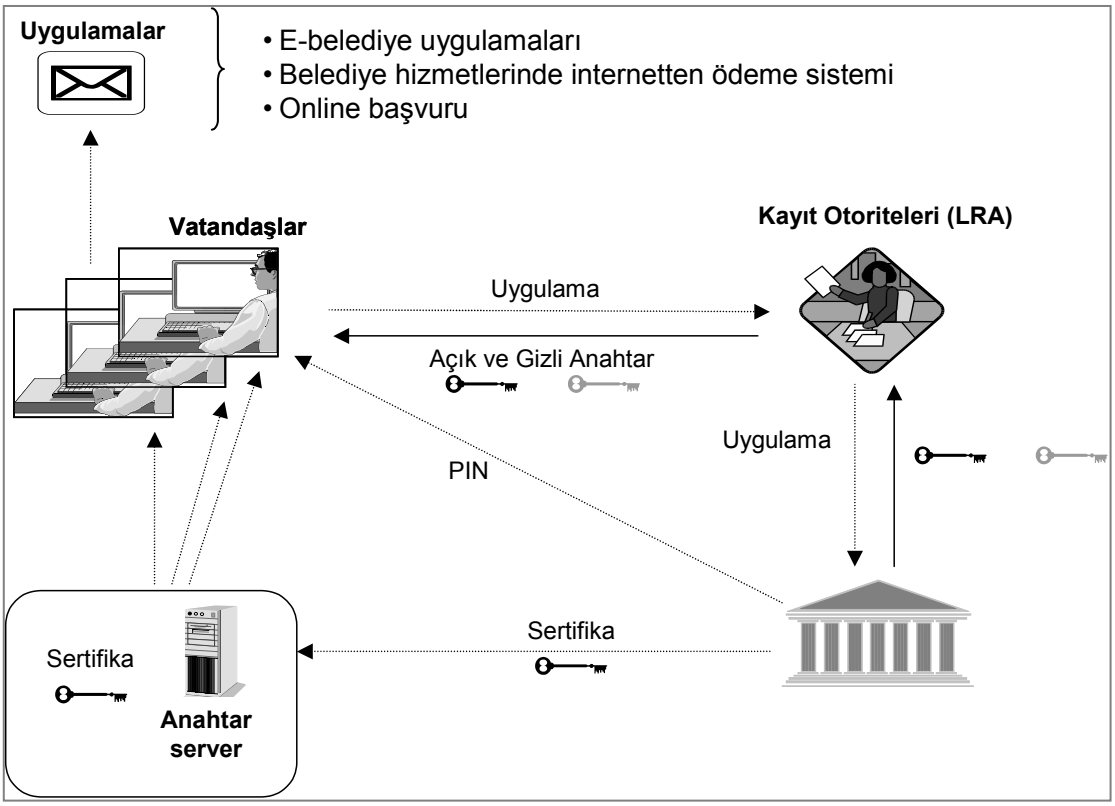


4.1.1.1.2 Sanal Şehir Hagen

Sanal Şehir Hagen projesi tüm kamu hizmetlerine sanal ortamda erişim sağlayarak "e-devlet" uygulamalarının temelini oluşturmuştur.

İhtiyaçlar / Çözüm: İhtiyaçları, erişimde gizlilik ve doğrulama, sayısal imzalar, açık, ileriye dönük ve standart bir çözüm, güvenli ödeme sistemleri, ve "e-devlet" ve "çevrim-içi yönetim"de yönetim süreçlerinin düzenlenmesi olan müşteriye yeni teknolojiye geçişte esnek bir yapı, gizliliğin, doğrulamanın şifreli veri transferi ve sayısal imzalarla sağlanması ve Açık Anahtar Altyapısı ile bütünleşik bir çözüm sunulmuştur.

Faydaları: Vatandaşın işini kolaylaştıran, "bilişim toplumu" için uygun olan bu çözümle yönetimsel süreçlerin düzenlenmesi ve hızlandırılması, vatandaşa ait bilgilerin gizliliğinin sağlanması, hizmetlere kolay erişim, sayısal imzaların kullanımıyla zaman kazanımı sağlanmıştır.



4.1.1.1.3 Fransa Maliye Bakanlığı

Fransa Maliye Bakanlığı, 1998 yılında kurumların internet üzerinden vergi beyanını mümkün kılmaya karar verdi. 15 milyon €'dan fazla geliri olan 20,000 firmanın vergi beyanlarını internet üzerinden gerçekleştirmesi zorunluluğu yasalarla getirildi.

Bakanlık, kendisi sertifika otoritesi olarak davranmak yerine bu kararını gerçekleştirmek üzere, sertifika dağıtımını yapmayı üçüncü partilere bırakmayı tercih etti.

İhtiyaçlar / Çözüm: Güvenlik alanında çözümler sunan Verisign'ın bölgedeki iş ortağı Certplus, belli başlı Fransız bankaları ile çalışarak kurumlara sayısal sertifikaların dağıtımı ve kurulumu için gerekli çalışmaları gerçekleştirmiştir. Certplus'ın ilk aşamada dağıttığı 25,000 sertifika aktif bir şekilde kullanılmaktadır. Bu sayı 80,000'lere ulaşmaktadır.

Sağlanan Faydalar: Sağlanan çözüm ile hem zaman, hem de maliyet ve insan kaynağından tasarruf sağlanmıştır.

4.1.1.1.4 Köln Şehri Kartı

Köln Şehir Kartı Projesi, belediye hizmetleri içerisinde bulunan iş süreçlerinin, çalışanlar ve vatandaşlar için güvenli elektronik bir ortama taşınması süreçlerini kapsamaktadır.

Ihtiyaçlar / Çözüm: Vatandaş ve belediye arasındaki elektronik iletişimin sağlanması, yasal olarak kullanılan sayısal imzalar için teknik altyapı ve açık, ileriye dönük ve standart bir çözüm gibi ihtiyaçlara yönelik olarak Açık Anahtar Altyapısı ile akıllı kartların bütünleştirildiği bir çözüm sunulmuştur. Buna bağlı olarak iş süreçleri sayısal imzalar yardımıyla iyileştirilmiş; çoklu uygulamalı kartlarla birlikte çözüm eğitim, kültür ve sağlık alanına da genişletilmiştir.

Sağlanan Faydalar: Proje "Bilişim toplumu"na geçişte önemli bir adım olarak görülmüştür. Yönetimsel süreçlerin düzenlenmesi ve hızlandırılması, bilgisayar ağları ve fiziksel erişimde aynı altyapının kullanılması, vatandaşa ait bilgilerin gizliliğinin sağlanması, hizmetlere kolay erişim ve sayısal imzaların kullanımıyla zaman kazanımının sağlanması sağlanan diğer önemli faydalar olarak sıralandırılabilir.

4.1.1.1.5 Italya İçişleri Bakanlığı Italyan Kimlik (ID) Kart Projesi

Italya Avrupa bölgesinde elektronik karta geçen ikinci ülkedir. Italyan İçişleri Bakanlığı'nın vatandaşlarının kimlik tanınmalarının geliştirilmesi ve vatandaş ile kamu otoriteleri arasındaki ilişkinin kamu kuruluş binalarının dışına taşınmasını sağlamak amacıyla oluşturduğu çözüm, akıllı kart teknolojisine dayalı yeni bir kimlik kartı üstüne kurulmuştur. Proje kapsamında merkezi PKI yönetimi ile güvenli, belediyelerde online elektronik kimlik kartı dağıtımı prosedürleri ve süreçleri gerçekleştirilmiştir. Proje pilot aşamasında Milano, Palma ve Roma'da bulunan 83 belediye ve 280,000 vatandaşı kapsamıştır. 5 yıl içerisinde İtalyan Hükümeti yaklaşık 40 milyon elektronik kimlik kartı oluşturacaktır.

4.1.1.2 Uygulamada karşılaşılan sorunlar ve sorunların çözümünde kullanılan yöntemler

4.1.1.3 Mevcut durumun değerlendirmesi

4.1.2 Özel sektörde izlenen politikalar, kullanılan AAA modelleri ve uygulamalar

4.1.2.1 Örnek Uygulamalar

4.1.2.1.1 Almanya DSV

DSV (Deutscher Sparkassen Verlag) Alman bankacılık sisteminin (Sparkassen Finanzgruppe) servis sağlayıcısıdır. Deutscher Sparkassen Verlag (DSV), sunduğu bankacılık alanına yönelik ürün ve hizmetleri ile yaklaşık 600 kuruluşu (tasarruf bankaları, kamu bankaları, kamu sigorta şirketleri, v.b.) ve 18,000 şubeyi içeren Sparkassen-Finanzgruppe (Almanya tasarruf bankaları kurumu) için ana tedarikçi konumundadır. DSV, Finans kuruluşlarına Pazarlama ve medya hizmetleri, debit ve kredi kartları basımı, elektronik ödeme sistemleri ve ATM'ler için terminaller de dahil olmak üzere fonksiyonel bazda ürün ve hizmet sunmaktadır.

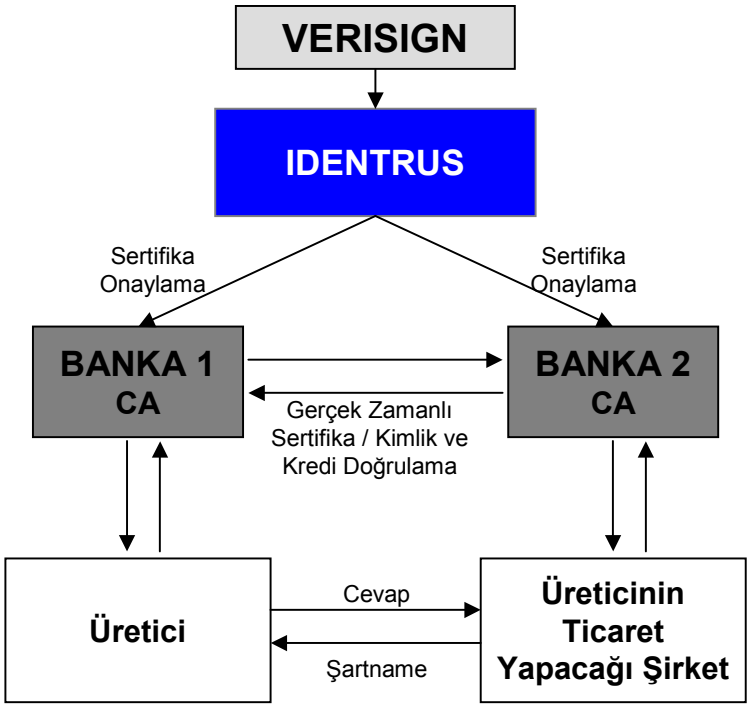
DSV, Mayıs 2001'de VeriSign ile yaptığı partnerlik anlaşmasıyla, sayısal sertifika kullanımına olanak sağlayan akıllı kartlar için Verisign'ın altyapısından faydalanmaya başlamıştır. Önümüzdeki yıllarda basılacak ***20 milyon akıllı kart***a, VeriSign'ın dijital sertifika hizmetlerini kullanarak sertifika eklemeyi ve 600 üye finans kuruluşunun ***e-mail doğrulama*** işlemleri için dijital sertifika altyapısı sunmayı planlamaktadır. Sayısal sertifikalı akıllı kartlar, kullanıcılarının doğrulanmasında ve kullanıcıların internet üzerinden daha güvenli işlem yapmalarına olanak sağlamaktadır.

Buna göre DSV, Verisign'ın yönetilen sayısal sertifika hizmetlerini genel bankacılık hizmetlerini daha güvenilir hale getirmek için kullanmaktadır.

4.1.2.1.2 Identrus

Nisan 1999'da 8 büyük banka (ABN AMRO Bank, Bank of America, Bankers Trust, Barclays Bank, Chase Manhattan, Citibank, Deutsche Bank ve Hypo Verinsbank) tarafından bir "güven şirketi" olarak kurulan Identrus, şu anda 60'ın üzerinde finansal kuruluşu bünyesine katmış durumdadır. Üye bankalardan ***10 tanesinin Türkiye***'de temsil edilmektedir. (ABN AMRO, BNP Paribas, Citigroup, Credit Lyonnais, Dresdner Bank, HSBC Group, ING Group, J.P.Morgan Chase & Co., Société Générale, West LB)

Identrus, Verisign'ın partnerliği ile, üye bankaların, müşterileri olan şirketlere dijital sertifika vermesini sağlayan sistem operatörlüğü görevini yürütmektedir



Identrus, bankalar, banka müşterilere ve devletler gibi pek çok partiye farklı açılardan avantajlar sunan bir sistemler bütünüdür. Identrus bankalara artan gelir, ilişki yaratma / yönetme daha etkin geleneksel hizmetler ve yeni hizmet sunma olanağı, marka yaratma ve risk yönetimi açılarından faydalar sağlamaktadır. Bu sistemle banka müşterilerine (şirketlere) ise daha düşük işlem maliyetleri, işlemlerin kaydının tutulması, gerçek zamanlı kimlik doğrulama, global pazara erişim şansı, kuralların tüm partilere tutarlı şekilde uygulanması, artan ciro, yeni pazarlar ve daha yüksek müşteri değeri gibi faydalar yaratılmıştır. Devlet açısından ise yeni diplomatik kanalların oluşumu, denetleme gücünün artması gibi pozitif etkileri vardır. ihaleye katılan firmanın kendisinin tanınmaması durumunda bile Identrus tarafından sertifikalanmış bir firmanın kredilitesinin yüksek kabul edilebilir olması, ihalelerde şirket tanınmalarında kolaylık sağlamaktadır.

4.1.2.1.3 Kanada CIBC (Canadian Imperial Bank of Commerce)

CIBC, 9 milyondan fazla bireysel ve kurumsal müşterisi bulunan, Kuzey Amerika'nın lider finansal kuruluşlarından biridir. CIBC, kapsamlı elektronik bankacılık ağı boyunca müşterilerine bankacılık alanında uçtan uca ürün ve hizmetler sunmaktadır ve aynı zamanda Verisign'ın Kanada'daki iş ortağı, işleme merkezi (processing center) olarak da faaliyet göstermektedir. CIBC işleme merkezi, Verisign'ın PKI platformu, güven hizmetleri altyapısını ve işletme hizmetlerini içine almaktadır. CIBC temelde *web sunucu* ve *işletme sertifika* hizmetlerini sunmaktadır. CIBC,

Kanada çapında sertifika otorizasyon hizmetlerini sağlamakta ve sertifika işlemlerinin yanısıra pazarlama, satış, güvenlik, müşteri destek ve operasyon yönetimi gibi hizmetleri de sunmaktadır.

İhtiyaçlar / Çözüm: CIBC, imza gerektiren uygulama ve hizmetlerine online olarak ulaşma ve kullanma olanağını müşterilerine sunmayı ve böylelikle de müşteri rahatlığı ve memnuniyetini artırırken uygulama süreç maliyetlerini azaltmayı hedeflemiştir. Normalde bütün CIBC müşterileri VISA kartı, banka hesabı açtırma gibi işlemler için şubeleri ziyaret ederek, yada posta yoluyla başvuru talebini yaparak süreci başlatabiliyorlardı. Bütün başvuruların müşteri tarafından imzalanmış olması gerektiğinde müşterilerin fornu ya direk şubeden almaları yada posta yoluyla alıp imzalayıp tekrar geri göndermeleri gerekiyordu. CIBC bu süreci hızlandırmak ve kolaylaştırmak istedi. 2001'in Şubat ayında CIBC bireysel banka müşterilerine sayısal imza kullanarak uygulamaları imzalama ve bütün bankacılık hizmetlerini online olarak alabilme olanağını tanıyan Kanada'daki ilk banka olmuştur.

Sağlanan Faydalar: Daha fazla Kanadalı firmanın ve bireyin elektronik ticaret işlemlerini güvenli bir şekilde gerçekleştirmeleri sağlanmış, banka müşterilerinin memnuniyeti artarken, CIBC de maliyetlerden ve işlemler için harcanan zamandan tasarruf sağlamıştır.

4.1.2.1.4 İngiltere - Barclays

Barclays, temelde bireysel bankacılık, yatırım bankacılığı ve yatırım yönetimi konularında faaliyet gösteren, İngiltere'deki finansal hizmet sunan en büyük gruplardan biridir. Barclays'in 2003 sonu itibariyle 700,000'in üzerinde kurumsal müşterisi ve internet bankacılığını kullanan 4,5 (285,000'i kurumsal) milyon müşterisi bulunmaktadır.

İhtiyaçlar / Çözüm: Barclays, PKI altyapısını kurması ve işletmesi için BT Ignite ile çalışmaya karar vermiş, güvenlik çözümleri sağlayan bu kurum, elektronik ticaretin kullanımı sırasında hem Barclays grubu şirketlerini, hem de müşterilerini korumak üzere güvenli teknoloji çözümlerini (PKI) sağlamıştır. Bu hizmet ile Barclays, müşterileri ile arasında ve aynı zamanda kurum içerisinde, elektronik ortamdaki bilgi alışverişini güvenli hale getirmiştir. Ayrıca kurumsal müşterilerine kendi müşteri ve tedarikçileriyle internet ortamında daha güvenli işlemler gerçekleştirmelerini sağlayacak hizmetler geliştirme fırsatına sahip olmuştur.

4.1.2.1.5 Danimarka – KPMG

Dünya çapında 100,000'den fazla çalışanıyla, KPMG 152 ülkedeki şirketlere sigorta, vergi ve hukuk, finansal danışmanlık hizmetleri sunmaktadır. KPMG'nin, Danimarka'da ülke çapında 19 ofisinde yaklaşık 1400 çalışanı bulunmaktadır.

İhtiyaçlar / Çözüm: KPMG son zamanlarda müşteri tarafından gelen internet üzerinden güvenli iletişim talepleriyle karşı karşıya kalmaktaydı. Bu zamana kadar çok önemli belgelerin müşteri ile iletişimi normal posta ile gerçekleştirilmekteydi. PKI çözümünü kurarak, KPMG müşterileri ile arasında güvenli bilgi alışverişini gerçekleştirerek, müşteri arasındaki güven öğesini pekiştirirken müşteri memnuniyetini de artırmıştır. Çözüm kapsamında KPMG müşterilerine sertifika dağıtım ve onaylama işlemlerini gerçekleştirmiş ve yeni müşterilerin kolaylıkla eklenmesini sağlayan esnek ve varolan IT altyapısı ile tamamiyle bütünleşik bir sistem kurmuştur. Dünyaca tanınan Verisign sertifikaların kullanılmasıyla, KPMG ve müşterileri aynı zamanda güvenlik çözümleri açısından sadece ülke sınırları içerisinde geçerli bir sistem kullanmamış oldu.

4.1.2.2 Uygulamada karşılaşılan sorunlar ve sorunların çözümünde kullanılan yöntemler

4.1.2.3 Mevcut durumun değerlendirmesi

4.2 Asya Ülkeleri

4.2.1 Kamu sektöründe izlenen politikalar, kullanılan AAA modelleri ve uygulamalar

4.2.1.1 Örnek Uygulamalar

4.2.1.1.1 Japonya - Suzuken Firması

Suzuken, merkezi Nagoya'da yer alan ve ülke çapında 110.000 eczane ve ilaç kuruluşuna ilaç ve tanı medikal ekipmanı sağlayan bir ilaç toptancısıdır. Suzuken Grubu, Sanwa Kagaku Kenkyusho Co., Ltd. (ilaç şirketi), Nihon Seiyaku Kogyo Co., Ltd. (ilaç üreticisi), Kenzmedico Co.,Ltd. (ekipman üreticisi) ve Lifemedico Co., Ltd. (sağlık alanda faaliyet gösteren reklam şirketi) şirketlerinden oluşmakta olup sağlık hizmetleri alanında toplu bir güce sahiptir.

İhtiyaçlar / Çözüm: Suzuken, 2001 yılında ilaç şirketleri yani müşterileri ile olan bilgi alışverişi ve online ürün talepleri için web tabanlı bir satış destek sistemini hizmete sokmuştur. Bu

sistemdeki e-posta,ürün talep bilgileri ve diğer değerli bilgilerin güvenli için PKI teknolojisi kurulmuştur. Buna göre bir sertifika otoritesi her kurumdaki her bir satış temsilcisi için sertifika dağıtımını gerçekleştirmiş ve bu sertifikalar sayesinde kimlik doğrulama ve onay işlemleri gerçekleştirilmeye başlanmıştır. Müşterilerin ilk giriş sayfasında kimlikleri onaylandıktan sonra diğer sayfalarda tekrardan güvenlik için bilgi sormaya gereklilik ortadan kalkmış ve böylelikle de sistemin kullanıcılar tarafından kullanımı kolaylaşmıştır.

4.2.1.1.2 Hong Kong – Hong Kong Post

Hong Kong sertifika otoritesi 2000 yılından itibaren sadece 110,000 e-Cert (sayısal sertifika) satabilmiştir. Kurum sertifika kullanımını artırmak için, akıllı kimlik kart sahiplerine sertifikaları kartlarına yerleştirme olanağını bir yıl için hiç bir ücret almadan gerçekleştirme önerisiyle gitmiştir. Temmuz 2003'ten itibaren Hong Kong kimlik kartı sahipleri, varolan kimlik kartlarını akıllı kimlik kartları ile değiştireceklerdir. Bu süreç dört yıl sürecektir.

4.2.1.1.3 Yeni Zelanda Hükümetinde Kullanılan PKI Uygulamaları

Yeni Zelanda Hükümeti sayısal sertifikaları daha çok güçlü bütünlük, koruma ve güvenlik gerektiren uygulamalar için kullanmaktadır. Bu uygulamalara birkaç örnek vermek gerekirse:

•**SEEMail (Secure Electronic Environment):** Sayısal sertifikalar, internet üzerinden güvenli bilgi alışverişini sağlamak için kullanılmaktadır. Bu sistemi kullanan ve sayılarının artması beklenen 30'un üzerinde devlet dairesi bulunmaktadır.

• **Hazine:** Hazine Finansal Bilgi Sistemi (CFISnet) kullanıcılarının tarayıcı doğrulanması işlemi için sayısal sertifikalar kullanılmaktadır. Sistemin yaklaşık 290 kullanıcısının %25'i Hazine'den, %50'si diğer hükümet dairelerindendir. Hazine sayısal sertifikaları aynı zamanda kullanıcıların kurum dışı çalışma alanına girişleri, laptopları şifrelemek ve uzaktan giriş izinleri için de kullanmaktadır.

• **LINZ:** Kurum, Landonline sistemi kullanıcılarının kimliklerinin doğrulanması için sayısal sertifika kullanmaktadır. Sistemin şu anda 4000 kullanıcı bulunmaktadır.

•**Sağlık Sektörü:** Sağlık hizmeti sağlayıcılarının sağlık ile ilgili sistemlere girişleri için bu teknoloji kullanılmaktadır. Yaklaşık kullanıcı sayısı 10,000 kadardır.

• **Toplumsal Gelişim Bakanlığı** (The Ministry of Social Development): 1999 yılından beri PKI öğeleri, giriş işlemlerini şifreleme, kullanıcılara uygulamalara giriş izni verme gibi işlerde kullanmaktadır. Bakanlığın aynı zamanda kendi sertifika otoritesi olması, kritik birçok altyapı bileşeninde, otomasyona geçmiş kullanıcı yönetimi için maliyetten tasarruf ettiren bir yöntem

olduğunu kanıtlamıştır. Bu sayede bakanlık, yaklaşık 9000 kullanıcıyı yaklaşık kullanıcı başına 12NZ$'lık bir marjinal maliyetle yönetebilmektedir.

4.2.1.2 Uygulamada karşılaşılan sorunlar ve sorunların çözümünde kullanılan yöntemler

4.2.1.3 Mevcut durumun değerlendirmesi

4.2.2 Özel sektörde izlenen politikalar, kullanılan AAA modelleri ve uygulamalar

4.2.2.1 Uygulamada karşılaşılan sorunlar ve sorunların çözümünde kullanılan yöntemler

4.2.2.2 Mevcut durumun değerlendirmesi

4.3 Amerika

4.3.1 Kamu sektöründe izlenen politikalar, kullanılan AAA modelleri ve uygulamalar

4.3.1.1 Örnek Uygulamalar

4.3.1.1.1 ABD Savunma Bakanlığı Dışsal Sertifika Otoritesi Programı

ABD Savunma Bakanlığı, Bakanlık ile tedarikçiler arasındaki online işlemleri daha güvenli hale getirmek üzere bir sistem kullanmaya karar vermiş ve buna bağlı olarak da Verisign'ı gerekli olan sayısal sertifikaların sağlayıcısı olarak tercih etmiştir.

ECA programı (Dışsal Sertifika Otoritesi), ***Savunma Seyahat Sistemi, Elektronik Doküman Girişi ve Geniş Alan İş Akışı*** olmak üzere üç programı kapsamaktadır. İleriki dönemlerde program, bakanlığın 350.000'den fazla iş ortağını da kapsayan, daha geniş uygulamalar ile daha gelişmiş bir ECA programı haline gelecektir.

4.3.1.2 Uygulamada karşılaşılan sorunlar ve sorunların çözümünde kullanılan yöntemler

4.3.1.3 Mevcut durumun değerlendirmesi

4.3.2 Özel sektörde izlenen politikalar, kullanılan AAA modelleri ve uygulamalar

4.3.2.1 Uygulamada karşılaşılan sorunlar ve sorunların çözümünde kullanılan yöntemler

4.3.2.2 Özel sektör kuruluşlarında e-imza uygulamalarının incelenmesi;

4.3.2.3 Mevcut durumun değerlendirmesi

5 ÜLKEMİZDEKİ MEVCUT DURUM VE SORUNLAR

5.1 Kamu ve özel sektör kuruluşlarında elektronik imza uygulamaları ve mevcut oluşumlar,

5.1.1 Özel Sektör Kuruluşlarında Elektronik İmza Kullanımı

Özel sektör kuruluşlarından Turkcell ve Denizbank'ta gerçekleştirilmiş olan akıllı kart tabanlı PKI projelerinin kuruluş içindeki uygulama alanları ve proje detayları aşagıda sunulmuştur.

Turkcell

Turkcell'de pilot çalışması devam etmekte olan PKI projesinde akıllı kartlarla aşagıdaki uygulamalar saglanmaktadır;

- Turkcell Domain e login olma,
- Ras a baglanma,
- Wireless e baglanma,
- Vpn üzerinden Turkcell e baglanma,
- Outlook uygulamasından Encrypt Message gönderme.

Ileride kapı giriş/çıkış kontrol ile Workflow, Hr uygulamaları gibi Intranet'de çalışan web uygulamalarının da sisteme dahil edilmesi planlanmaktadır.

Schlumberger' in akıllı kartlarının kullanıldıgı bu sistemde, istemci tarafında WinXP işletim sistemi üzerinde Internet Explorer 6.0 kullanılmaktadır. Sistem ayrıca MS Office 2003 ile entegre çalışmaktadır.

Sistemde kullanıcılar kendilerine verilen akıllı karti web tabanlı bir uygulama ile özelleştirip, bir PIN belirleyerek kullanıma hazır hale getirirler. Şifre degiştirmek veya 3 kez yanlış şifre girilerek bloke edilmiş kartı aktive etmek web tabanlı uygulama ile kullanıcı tarafından gerçekleştirilir.

Denizbank

Kurumsal müşterilere Internet Bankacılıgı hizmetini daha güvenli sunmak amacıyla Denizbank bünyesinde bir PKI sistemi tasarlanıp, geliştirilmiştir. Web üzerinden kimlik dogrulama işleminin akıllı kartlarla yapıldıgı bu sistemde Gemplus' ın GemSafe 8K kartları ile Todos akıllı kart okuyucuları kullanılmıştır. Microsoft Sertifika Otoritesi yazılımı kurum içerisindeki sertifikaların yaratılması, dagıtımı ve iptal edilmesi işlemlerini gerçekleştirmektedir.

SBS Türkiye

Son 4 senedir şirket çalışanlarına güvenli haberleşme ve bazı uygulamalarda intranet erişim için sertifikalar sağlanmaktadır.

5.1.2 Kamu Kurumlarında Elektronik İmza Kullanımı

Bu çalışmada; Elektronik İmza Ulusal Koordinasyon Kurulu Altyapı Çalışma Grubuna ülkemizdeki kamu kurumlarında e-imza kullanımı konusunda bilgi sağlamak amaçlanmıştır. Bu kapsamda; kamu kurumlarında halihazırda kullanılan veya kullanılması planlanan e-imza altyapılarının kapasitelerinin, kullanım amaçlarının ve kullandıkları uygulamaların belirlenmesine yönelik bir anket hazırlanmış, ilgili kuruluşların yetkililerine gönderilerek cevaplamaları talep edilmiş ve bu kuruluşların 18 tanesinden cevap alınmıştır. Kuruluşların ankete verdikleri cevaplar sıkıştırılmış formatta ek olarak iletilmiştir.

Yapılan çalışmada ortaya çıkan en belirgin sonuç; henüz kamu kurumlarımızda e-imza kullanımı çok yaygınlaşmamış olsa da, tüm kuruluşların önümüzdeki dönemde e-imza kullanımını iş süreçlerine dahil etmeye istekli olduklarıdır. Anketlere alınan cevaplar değerlendirildiğinde kuruluşların çoğunun 1-2 yıl içerisinde e-imza kullanmayı planladıkları görülmektedir. Bazı kuruluşlar (DTM, TSE, NVİ, TİKA, TCDD) ise 6-12 ay gibi daha da kısa bir sürede e-imza uygulamalarını kullanıma almayı planladıklarını belirtmişlerdir.

Her ne kadar e-imza kullanımı kamuda fazla yaygınlaşmamış olsa da Adalet Bakanlığı, T.C. Merkez Bankası (TCMB), Sermaye Piyasası Kurulu (SPK), Türkiye Noterler Birliği (TNB) gibi kurumların iş süreçlerine e-imzayı dahil ettikleri gözlenmiştir. Bu kurumların e-imzayı özellikle

kurum içi ve diğer kurumlarla olan işlemlerinde kullandıkları göze çarpmaktadır. Vatandaş ile doğrudan ilişkisi olan ve e-imza kullanmayı planlayan bir çok kuruluş da vatandaş ile olan işlemlerinde e-imza altyapısından faydalanacağını belirtmiştir.

Sertifika yönetim platformu olarak Adalet Bakanlığı ve TCMB Globalsign ve Microsoft CA'i, SPK ise TÜBİTAK-BİLTEN'in ürünü olan ZEUGMA'yı tercih etmiştir. Önümüzdeki dönemde e-imzayı kullanmayı planlayan kurumların önemli bir kısmının yerli sertifika yönetimi ürünlerini de tercih ettikleri, bu konuda DTM'nin ZEUGMA, cevap veren diğer kuruluşların ise TUBİTAK-UEKAE ürünü olan ASYA yazılımlarını kullanmayı planladıkları dikkat çekmektedir. Geliştirilecek olan/geliştirilen uygulamalarda ekseriyetle yerli çözüm sağlayıcı firmalarla çalışılması tercih edilmektedir Her kurum altyapısının kapasitesini kurum içi ve birlikte çalıştığı kişilerle/kurumlarla ilişkilerindeki ihtiyaçlara göre kurmuştur/kurmayı planlamaktadır.

Halihazırda e-imza kullanmayan fakat kullanmayı planlayan kurumların hemen hepsi amaç olarak kurum içi ve kurumlar arası işlemlerin hızlandırılmasını ve elektronik ortamda yapılan işlemlere yasal geçerlilik ve güven unsuru kazandırılmasını göstermiştir. Bununla birlikte e-imza'nın özellikle kamu kuruluşları arasındaki işlemlerde ve kurumların iş ilişkisi içinde bulundukları bankalar, finansal şirketler ve ithalat ihracat şirketleri, medya kuruluşları gibi özel kurumlar ile yapılan elektronik ortamdaki belge ve veri alışverişi için kullanılmasının planlandığı göze çarpmaktadır. Vatandaşa sunulacak hizmetlere erişimin kolaylaştırılması kısıtlı oranda hedeflenmektedir. Bu alanlarda hemen hepsinde sistem erişimleri/loginleri'nin temel kullanım amacı olarak görüldüğü anlaşılmaktadır. Ayrıca kurum içinde elektronik belge/verilerin imzalanmasının ve kurumlar arasında bunların şifrelenmesine yönelik kullanımın amaçlandığı da göze çarpmaktadır. Vatandaşlara yönelik kullanımda çok yaygın olarak hedeflenen ise belge ve verilerin elektronik ortamda imzalı olarak iletilmesidir.

Anketlere alınan cevaplarda bir çok kurumun e-imza kullanımını planlamakta olduğu görülmekle birlikte teknik konularda bilgi eksikliği ve ülkemizde fazla da örneği olmadığından örnek alınabilecek uygulamaların azlığı nedenleri ile e-imza konusunda ilgili kuruluşların kamu kurumlarına yönelik bilgilendirme çalışmaları yapmalarının, kamu kurumlarının da ilgili personellerini bu konuda eğitmelerinin gerekliliği hususları vurgulanmıştır. Ayrıca e-imzayı aralarındaki ilişkilerde kullanacak kamu kurumları arasında koordinasyon ve bilgi bütünlüğü sağlanması gerekliliği hususu da ayrıca belirtilmiştir. Bu hususun, e-Dönüşüm Türkiye Projesi

Kısa Dönem Eylem Planı'nda yer alan "birlikte çalışabilirlik esaslarının belirlenmesi"ne yönelik eylem kapsamında dikkate alınması gereklidir.

Aşağıda anket sorularına tüm kurumlardan gelen cevaplar verilmiştir.

1 – Kurumunuzda Elektronik İmza kullanıyor musunuz? Cevabınız 'Hayır' ise; Ne zaman kullanmayı planlıyorsunuz?

Adalet Bakanlığı	Evet
Türkiye Noterler Birliği	Evet
Ankara Büyükşehir Belediyesi	Hayır. 12-24 ay içinde.
TÜBİTAK-BİLTEN	Hayır. 12-24 ay içinde
Denizcilik Müsteşarlığı	Hayır. 12-24 ay içinde
Devlet Meteoroloji İşleri GM	Hayır. 12-24 ay içinde
Devlet İstatistik Enstitüsü	Hayır. 12-24 ay içinde
Dış Ticaret Müsteşarlığı	Hayır. 0-6 ay içinde
Emekli Sandığı GM	Hayır. 12-24 ay içinde
Gümrük Müsteşarlığı	Hayır. 6-12 ay içinde
İstanbul Büyükşehir Belediyesi	Hayır. 12-24 ay içinde
Maliye Bakanlığı	Hayır. 12-24 ay içinde
T.C. Merkez Bankası	Evet
Nüfus ve Vatandaşlık İşleri GM	Hayır. 6-12 ay içinde
T.C. Devlet Demiryolları	Hayır. 12-24 ay içinde
TİKA	Hayır. 0-6 ay içinde
Türk Standartları Enstitüsü	Hayır. 6-12 ay içinde
Sermaye Piyasası Kurulu	Evet

2 - Elektronik İmza için kurduğunuz/planladığınız Açık Anahtar Altyapısı (Public Key Infrastructure - PKI) hangi teknoloji ile çalışıyor?

Adalet Bakanlığı	USB Token
Türkiye Noterler Birliği	USB Token
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	Soft sertifika, Akıllı Kartlar (Smartcard), USB Token

Devlet Meteoroloji İşleri GM	USB Token, Rasgele Şifre (One Time Password)Üreteçleri
Devlet İstatistik Enstitüsü	Akıllı Kartlar (Smartcard), USB Token
Dış Ticaret Müsteşarlığı	Akıllı Kartlar (Smartcard)
Emekli Sandığı GM	Soft sertifika, Akıllı Kartlar (Smartcard), USB Token
Gümrük Müsteşarlığı	Henüz karar verilmedi
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	Soft sertifika
T.C. Merkez Bankası	Soft sertifika
Nüfus ve Vatandaşlık İşleri GM	Henüz karar verilmedi
T.C. Devlet Demiryolları	USB Token
TİKA	Soft sertifika
Türk Standartları Enstitüsü	Soft sertifika
Sermaye Piyasası Kurulu	Akıllı Kartlar (Smartcard)

3 - Elektronik İmza için hangi Sertifika Otoritesi (Certificate Authority - CA) yazılımını kullanıyorsunuz/planlıyorsunuz?

Adalet Bakanlığı	Microsoft CA
Türkiye Noterler Birliği	Kendi uygulamaları ile 2001 Eylül'den bu yana pilot çalışma
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	TÜBİTAK BİLTEN – ZEUGMA
Denizcilik Müsteşarlığı	TÜBİTAK UEKAE-ASYA
Devlet Meteoroloji İşleri GM	TÜBİTAK UEKAE-ASYA
Devlet İstatistik Enstitüsü	TÜBİTAK UEKAE-ASYA, Verisign CA
Dış Ticaret Müsteşarlığı	TÜBİTAK BİLTEN – ZEUGMA
Emekli Sandığı GM	TÜBİTAK UEKAE-ASYA, GlobalSign CA
Gümrük Müsteşarlığı	TÜBİTAK UEKAE-ASYA
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	GlobalSign CA, Microsoft CA, GlobalSign firmasından temin edilen sınırlı sayıda kişisel sayısal sertifikalar kullanılmaktadır.
Nüfus ve Vatandaşlık İşleri GM	İhale sonucunda belirlenecek
T.C. Devlet Demiryolları	
TİKA	GlobalSign CA

Türk Standartları Enstitüsü	Henüz karar verilmedi
Sermaye Piyasası Kurulu	TÜBİTAK BİLTEN - ZEUGMA

4a. Mevcut hazır çözümlerin haricinde bu konuda ARGE çalışmaları yapıldı mı? Yapıldıysa: Hangi Kurum/Kuruluş ile işbirliği yapıldı?

Adalet Bakanlığı	Günlük uygulamalarda kullanmak üzere projelere entegre etmek amacıyla HAVELSAN A.Ş. ile 1 ay süreli çalışma yapıldı.
Türkiye Noterler Birliği	1 yıllık ARGE (2001) ve 3 yıllık üretim ve pilot çalışması mevcut
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	
Devlet Meteoroloji İşleri GM	
Devlet İstatistik Enstitüsü	
Dış Ticaret Müsteşarlığı	Özel bilişim sektörü firmaları, proje ile ilgisi olan diğer kurum ve kuruluşlar ile 8 ay süren ve etkin, verimli kullanımı ve diğer kurum/kuruluşlarla entegrasyonu sağlamak amacıyla bir çalışma yürütülmektedir.
Emekli Sandığı GM	
Gümrük Müsteşarlığı	
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	Kurum bünyesinde sistemi günlük uygulamalarda kullanmak üzere bir çalışma yürütülmektedir.
Nüfus ve Vatandaşlık İşleri GM	
T.C. Devlet Demiryolları	
TİKA	Dış İşleri Bakanlığı ile sistemi günlük uygulamalarda kullanmak amacıyla 3 aylık bir çalışma yürütülmüştür
Türk Standartları Enstitüsü	Bu konuda herhangi bir Arge çalışması yapılmadı. Ancak elektronik imzanın kullanım yeri olarak düşünülen doküman yönetimi ve elektronik iş akış programları ile ilgili görüşmeler yapılmaktadır.

Sermaye Piyasası Kurulu	TÜBİTAK BİLTEN'ın konuyla ilgili çalışmalarından faydalanılmıştır

4b. Bu konudaki sistemin çalıştırılması ve işletimi ile ilgili hangi yöntem tercih edilecektir ?

Adalet Bakanlığı	Tamamı kurum bünyesi ve imkanları ile yapılacaktır
Türkiye Noterler Birliği	Tamamı kurum bünyesinde, kendi ARGE çalışmaları ve imkanları ile
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	Tamamı kurum bünyesi ve imkanları ile yapılacaktır. İlgili firmalardan destek alınacaktır.
Devlet Meteoroloji İşleri GM	
Devlet İstatistik Enstitüsü	AB Projeleri kapsamında
Dış Ticaret Müsteşarlığı	Tamamı kurum bünyesi ve imkanları ile yapılacaktır
Emekli Sandığı GM	
Gümrük Müsteşarlığı	
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	Tamamı kurum bünyesi ve imkanları ile yapılacaktır
Nüfus ve Vatandaşlık İşleri GM	
T.C. Devlet Demiryolları	
TİKA	Tamamı kurum bünyesi ve imkanları ile yapılacaktır
Türk Standartları Enstitüsü	İlgili firmalardan talep edilecektir
Sermaye Piyasası Kurulu	Tamamı kurum bünyesi ve imkanları ile yapılacaktır (Sistemin işlediği yazılım ve donanım Kurum bünyesinde yönetilecektir). Sertifika Otoritesi olarak TÜBİTAK BİLTEN görev yapacaktır

Kullanılması planlanan yazılım ve donanımlarda teknolojilerin ve standartların değişmesi durumunda sürekliliğin korunabilmesi için ne gibi tedbirler düşünüldü ?

Adalet Bakanlığı	
Türkiye Noterler Birliği	SDK boyutunda entegrasyon mevcut ve tek bir DLL ile tüm uygulamaların güncellenmesi mümkün
Ankara Büyükşehir Belediyesi	

TÜBİTAK-BİLTEN	BİLTEN, TÜBİTAK'ın bir araştırma ve geliştirme enstitüsü olduğu için kendiliğinden sürekliliği sağlama becerisine sahiptir
Denizcilik Müsteşarlığı	
Devlet Meteoroloji İşleri GM	
Devlet İstatistik Enstitüsü	Yazılım ve donanımın teknolojilere ve standartlara uygun olarak alınması planlandı.
Dış Ticaret Müsteşarlığı	Mevcut yapıyı yazılım ve donanımlarda değişen teknolojilere ve standartlara adapte edeceğiz. Bu konuyla ilgilenecek eleman tayin ederek teknik bilgi becerisi kazandırmaya çalışacağız. Proje, uzun vadede ve daha geniş kapsamdaki olaylar düşünülerek planlandı. Olabilecek değişikliklerin entegrasyonunda aşırı bir zorluk çekilmesi beklenmemektedir.
Emekli Sandığı GM	
Gümrük Müsteşarlığı	
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	Farklı teknolojiler arasında transfere imkan veren kabul görmüş standartlar dikkate alınıyor.
Nüfus ve Vatandaşlık İşleri GM	
T.C. Devlet Demiryolları	Evrak otomasyonu şartnamesine bu konuda maddeler monte edilecek
TİKA	Veritabanı esnek bir yapıda kuruldu. Her ortamda çalışabilmesi için platformdan bağımsız olan java programlama dili ve Oracle Veritabanı yazılımı tercih edildi.
Türk Standartları Enstitüsü	
Sermaye Piyasası Kurulu	Konuya ilişkin Kurum personelinin gerekli eğitimleri alması ve güncel teknolojileri takip etmesi sağlanacaktır

6 – Kurumunuzda Elektronik İmza projesi nasıl hayata geçirildi/geçirilmesi planlanıyor?

Adalet Bakanlığı	
Türkiye Noterler Birliği	e-Yönetim Kurulu ve e-Vezne projeleri için kurum bünyesindeki ARGE çalışmaları ve bu konuda ürün geliştiren İSRAİL firmaları ile teknoloji ortaklığı ile

Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	Kurum bünyesi içindeki kaynaklarla
Denizcilik Müsteşarlığı	Bu konuda çalışan diğer kamu kurumlarının kaynakları ile ve yerli çözüm sağlayıcı firmalarla
Devlet Meteoroloji İşleri GM	Yerli çözüm sağlayıcı firmalarla
Devlet İstatistik Enstitüsü	Diğer
Dış Ticaret Müsteşarlığı	Kurum bünyesi içindeki kaynaklarla ve yerli çözüm sağlayıcı firmalarla
Emekli Sandığı GM	Yerli çözüm sağlayıcı firmalarla
Gümrük Müsteşarlığı	Kurum bünyesi içindeki kaynaklarla
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	Bu konuda çalışan diğer kamu kurumlarının kaynakları ile
T.C. Merkez Bankası	Kurum bünyesi içindeki kaynaklarla
Nüfus ve Vatandaşlık İşleri GM	Diğer
T.C. Devlet Demiryolları	Yerli çözüm sağlayıcı firmalarla
TİKA	Kurum bünyesi içindeki kaynaklarla
Türk Standartları Enstitüsü	Yerli çözüm sağlayıcı firmalarla
Sermaye Piyasası Kurulu	Yerli çözüm sağlayıcı firmalarla. (Yapılan proje İMKB ile birlikte ortak yürütülmekte olan bir projedir. Finansal kaynağı İMKB sağlamaktadır)

Hangi kurumlar ile hangi uygulamalar sebebi ile entegrasyon düşünüldü ?

Adalet Bakanlığı	Adalet Bakanlığı bünyesinde çalışmaları devam eden Ulusal Yargı Ağı Projesi(UYAP) kapsamında özellikle yargılama faaliyetleri kapsamında gerekli görülen Mernis, Takbis, Adli Sicil Kayıtları, Polnet, Say200i gibi projelerle entegrasyon öngörülmüştür. Bu antegrasyonlardan belgelerin elektronik ortamda elektronik imzalı bir şekilde alışveriş öngörülmektedir.
Türkiye Noterler Birliği	UYAP, MERNIS, TAKBİS, SSK, POLNET ile e-imzalı dijital bilgi akışına dayalı, XML tabanlı, verilerin Oracle ortamında muhafaza edildiği bir alışveriş düşünülmektedir.
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	

Denizcilik Müsteşarlığı	
Devlet Meteoroloji İşleri GM	e-devlet ve e-Türkiye eylem planları kapsamında; kurumumuz bünyesinde oluşturduğumuz elektronik evrak dolaşım sisteminin, bakanlığa bağlı diğer kurumlarda yaygınlaşması halinde, bilgi ve belge dolaşımı/paylaşımı için. DMİ-DSİ arasında mevcut olan uydu iletişiminde, meteorolojik data aktarımı için, Üniversitelerle yürütülen ortak projelerde veri paylaşımı için, Özellikle Abonemiz olan medya kuruluşları ile veri paylaşımında kullanılmak üzere entegrasyon planlanmaktadır.
Devlet İstatistik Enstitüsü	Başbakanlık, Devlet Planlama Teşkilatı, Bakanlıklar
Dış Ticaret Müsteşarlığı	İhracatçı Birlikleri Genel Sekreterlikleri (13 adet), Gümrük Müsteşarlığı, TOBB, Sanayi Bakanlığı, vb.
Emekli Sandığı GM	
Gümrük Müsteşarlığı	Gümrük Otomasyon projesi kapsamında yeralan EDI uygulamasında düşünüldü, entegrasyon ithalat,ihracat ve taşıma şirketleri ile olacak
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	Bankalar ve Saymanlıklar arasında veri alışverişi uygulamalarında entegrasyon düşünülmekte; henüz değerlendirme aşamasında
Nüfus ve Vatandaşlık İşleri GM	
T.C. Devlet Demiryolları	
TİKA	
Türk Standartları Enstitüsü	Enstitümüz ile iş ilişkisi bulunan kurumlar ile (Sanayi ve Ticaret Bakanlığı, TOBB, vb.) entegrasyon planlanmaktadır
Sermaye Piyasası Kurulu	Kurulan yapının ileride sermaye piyasası kurum ve kuruluşlarınca (İMKB Takas ve Saklama Bankası A.Ş.-TAKASBANK-, Merkezi kayıt Kuruluşu –MKK-, Türkiye Sermaye Piyasası Aracı Kuruluşlar Birliği –TSPAKB- ve diğer) kullanılması planlandığından ilgili kurum ve kuruluşlarla konuyla ilgili entegrasyon düşünülmektedir.

Diğer kurumlar ile entegrasyonda hangi yöntemler tercih edildi ?

Adalet Bakanlığı	
Türkiye Noterler Birliği	SDK, internet sayfası ve doğrudan XML ortamında yazılım erişimi ile veri akışı planlanmaktadır.
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	
Devlet Meteoroloji İşleri GM	Yazılım Geliştirme Araçları ile kurumun kendi yazılımlarına veri aktarım özelliğinin entegre edilmesi planlanmaktadır. Çevirimiçi web tabanlı sayfalar aracılığı ile veri aktarımı planlanmaktadır.
Devlet İstatistik Enstitüsü	Çevirimiçi web tabanlı sayfalar aracılığı ile veri aktarımı
Dış Ticaret Müsteşarlığı	Doğrudan Veri Aktarımı (sağlanan bir yazılım ile tercih edilen standartta hazırlanmış verinin gönderilmesi) Yazılım Geliştirme Araçları ile kurumun kendi yazılımlarına veri aktarım özelliğinin entegre edilmesi Çevirimiçi web tabanlı sayfalar aracılığı ile veri aktarımı
Emekli Sandığı GM	Doğrudan Veri Aktarımı (sağlanan bir yazılım ile tercih edilen standartta hazırlanmış verinin gönderilmesi) Yazılım Geliştirme Araçları ile kurumun kendi yazılımlarına veri aktarım özelliğinin entegre edilmesi
Gümrük Müsteşarlığı	Doğrudan Veri Aktarımı (sağlanan bir yazılım ile tercih edilen standartta hazırlanmış verinin gönderilmesi)
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	Değerlendirme aşamasında
Nüfus ve Vatandaşlık İşleri GM	Belirtilen yöntemlerin hepsinin kullanılması
T.C. Devlet Demiryolları	
TİKA	Entegrasyon yok
Türk Standartları Enstitüsü	Üç yöntem de planlarımız dahilinde düşünülmektedir
Sermaye Piyasası Kurulu	

Diğer kurumlar ile bilgi alışverişinde bilgi tekrarının önüne geçmek için ne tür tedbirler düşünüldü? Bilgi tekrarının gerekli olduğu düşünülmüş ise, bilgi güncelliği nasıl sağlandı ?

Adalet Bakanlığı	UYAP'ın temel amaçlarından birisi belki de en önemlilerinden birisi, bilgi tekrarının önüne geçmektir. Bununla ilgili olarak Polnet ile C.Başsavcılıklarınca hazırlık soruşturmalarına ilişkin belgelerin (Fezleke) eletronik ortamdan gelmesi, buna ilişkin bilgilerin formatlı bir şekilde gönderilmesi düşünülmüştür. Bunun yanı sıra Polnet içerisinde bir alt sistem olan TAHDİT projesinde EGM ile mutabakata varılarak tahditin hakim tarafından doğrudan konulması benimsenmiş bu yönde çalışmalar yapılmıştır.
Türkiye Noterler Birliği	Uygun görülen kurumlar ile online veriambarı senkronizasyonu ile önlenmesi planlanmaktadır.
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	
Devlet Meteoroloji İşleri GM	
Devlet İstatistik Enstitüsü	Veriambarı mimarisinin kurulması ile kurum içerisindeki veriler tek bir havuzda toplanacağından bilgi tekrarı söz konusu olmayacaktır.
Dış Ticaret Müsteşarlığı	Bilgi tekrarının minimum seviyede olması arzu edilen bir durum. İhracatçı Birliklerin proje için sisteme doğrudan entegrasyonu sağlandığı için bilgi tekrarı çok minimum düzeyde olacaktır. Ancak diğer kurumlarla henüz bu entegrasyon sağlanmış değil.
Emekli Sandığı GM	
Gümrük Müsteşarlığı	
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	Kurum ve kuruluşlardan toplanan veriler işlenerek özet olarak ihtiyaç duyan kurumlara iletilmektedir. Diğer taraftan, aynı verileri toplayan kamu kurumlarına ait uygulamalar da bulunmaktadır.

Nüfus ve Vatandaşlık İşleri GM	
T.C. Devlet Demiryolları	
TİKA	Diğer kurumlarla şu anda bir entegrasyonumuz mevcut değil
Türk Standartları Enstitüsü	Bilgi tekrarının engellenmesi için web servisleri vb. Yöntemler ile bilgilerin tek kaynaktan kullanımı planlanmaktadır.
Sermaye Piyasası Kurulu	

10a – Kurumunuzdaki Elektronik İmza Açık Anahtar Altyapısı projesi kaç kullanıcı için tasarlanarak kuruldu/planlanıyor ?

Adalet Bakanlığı	10001 ve üzeri
Türkiye Noterler Birliği	5001- 10.000 kullanıcı
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	501 – 1000 kullanıcı
Denizcilik Müsteşarlığı	1001 – 5000 kullanıcı
Devlet Meteoroloji İşleri GM	501 – 1000 kullanıcı
Devlet İstatistik Enstitüsü	1001 – 5000 kullanıcı
Dış Ticaret Müsteşarlığı	5001 – 10000 kullanıcı
Emekli Sandığı GM	5001 – 10000 kullanıcı
Gümrük Müsteşarlığı	5001 – 10000 kullanıcı
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	1001 – 5000 kullanıcı
T.C. Merkez Bankası	
Nüfus ve Vatandaşlık İşleri GM	1001 – 5000 kullanıcı
T.C. Devlet Demiryolları	501 – 1000 kullanıcı
TİKA	10001 ve üzeri
Türk Standartları Enstitüsü	51 – 100 kullanıcı
Sermaye Piyasası Kurulu	1001 – 5000 kullanıcı

10b – Kurumunuzdaki Elektronik İmza Açık Anahtar Altyapısı projesi aktif olarak kaç kullanıcı tarafından kullanılmaktadır/ kullanılması planlanmaktadır?

Adalet Bakanlığı	10001 ve üzeri
Türkiye Noterler Birliği	Şu anda 1.000 kullanıcıya yazılım olarak eriştirilmiştir, 5.000 kullanıcı hedeflenmektedir.

Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	101 – 500 kullanıcı
Denizcilik Müsteşarlığı	501 – 1000 kullanıcı
Devlet Meteoroloji İşleri GM	501 – 1000 kullanıcı
Devlet İstatistik Enstitüsü	1001 – 5000 kullanıcı
Dış Ticaret Müsteşarlığı	5001 – 10000 kullanıcı
Emekli Sandığı GM	0 – 50 kullanıcı
Gümrük Müsteşarlığı	5001 – 10000 kullanıcı
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	1001 – 5000 kullanıcı
Nüfus ve Vatandaşlık İşleri GM	10001 ve üzeri
T.C. Devlet Demiryolları	
TİKA	10001 ve üzeri
Türk Standartları Enstitüsü	51 – 100 kullanıcı
Sermaye Piyasası Kurulu	1001 – 5000

11 - Elektronik İmzayı hangi tür iş süreçleri ve kaç için kullanıyorsunuz/kullanmayı planlıyorsunuz (birden fazla şık işaretleyebilirsiniz)?

Adalet Bakanlığı	Kurum içi kullanım Kamu kurumları arası kullanım Vatandaşlarla yapılan işlemler
Türkiye Noterler Birliği	Kurum içi (kurum / yönetim / bölgeler ve Noterler arası) kullanım Kurum iç kapasite: 150 kişi Noterler Arası kapasite: 5.000 kişi Kamu kurumları arası kullanım
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	Kurum içi kullanım Kamu kurumları arası kullanım Kamu – özel sektör arası kullanım Vatandaşlarla yapılan işlemler

Devlet Meteoroloji İşleri GM	Kurum içi kullanım : 500. kişi için Kamu kurumları arası kullanım : 50 kişi için Kamu – özel sektör arası kullanım : 100. kişi için Vatandaşlarla yapılan işlemler : 25 kişi için Üyesi olduğumuz uluslararası kululuşların (WMO, EUMETSAT, ECMWF, NATO v.b) toplantılarına katılan temsilcilerimizin ve buralarda geçici görevli personelimizin erişimleri için.
Devlet İstatistik Enstitüsü	Kurum içi kullanım : 2500 kişi için Kamu kurumları arası kullanım : 2500 kişi için Kamu – özel sektör arası kullanım
Dış Ticaret Müsteşarlığı	Kurum içi kullanım : 300-500 kişi için Kamu kurumları arası kullanım : 100 kişi için İhracatçı firmalar : 5000'den fazla kişi için
Emekli Sandığı GM	Kurum içi kullanım : 200 kişi için Kamu kurumları arası kullanım : 50. kişi için Kamu – özel sektör arası kullanım : 50. kişi için Vatandaşlarla yapılan işlemler : 5.000.000 kişi için
Gümrük Müsteşarlığı	
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	Kurum içi kullanım : 4500 kişi için Kamu kurumları arası kullanım : 300 kişi için Kamu – özel sektör arası kullanım : 1000 kişi için
Nüfus ve Vatandaşlık İşleri GM	Kurum içi kullanım : 5000 kişi için Kamu kurumları arası kullanım : 3000 kişi için Vatandaşlarla yapılan işlemler Yurtdışı kullanım
T.C. Devlet Demiryolları	Kurum içi kullanım : 1500 kişi için
TİKA	Kurum içi kullanım : Sınırsız kişi için Yurtdışı koordinatörlerimiz : Sınırsız kişi için
Türk Standartları Enstitüsü	Kurum içi kullanım Kamu kurumları arası kullanım

	Kamu – özel sektör arası kullanım için Vatandaşlarla yapılan işlemler
Sermaye Piyasası Kurulu	Kamu – özel sektör arası kullanım. SPK, İMKB, TAKASBANK, MKK, TSPAKB, İMKB'de işlem gören şirketler (299 Şirket), aracı kuruluşlar (117 Kuruluş) ve bağımsız denetim şirketleri (71 Şirket)

12a – Kurum içi kullanıyorsanız; hangi süreçlerde aktif kullanmayı planlıyorsunuz?

Adalet Bakanlığı	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Türkiye Noterler Birliği	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için Karar / destek süreçleri, yönetim ve idari süreçler Geliştirilen projelerin merkezden güvenlir olarak yönetilmesi ve denetlenmesi
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
Devlet Meteoroloji İşleri GM	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Devlet İstatistik Enstitüsü	Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için

	Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Dış Ticaret Müsteşarlığı	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Diğer: Geliştirilen projeye erişim ve bu proje çerçevesinde evrak akışının sağlanması (bir nevi elektronik olarak imzalanması).
Emekli Sandığı GM	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Gümrük Müsteşarlığı	Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
T.C. Merkez Bankası	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Nüfus ve Vatandaşlık İşleri GM	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
T.C. Devlet Demiryolları	Sistem girişleri (loginler) ve erişimler için Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
TİKA	Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için

Türk Standartları Enstitüsü	Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
Sermaye Piyasası Kurulu	Sistem girişleri (loginler) ve erişimler için (Planlanmaktadır) Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için (Planlanmaktadır) Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için (Planlanmaktadır)

12b – Kamu kurumları arasında kullanıyorsanız; hangi süreçlerde aktif kullanıyorsunuz/kullanmayı planlıyorsunuz?

Adalet Bakanlığı	Kurumlararası sistem girişleri (loginler) ve erişimler için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Türkiye Noterler Birliği	Kurumlararası sistem girişleri (loginler) ve erişimler için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	Kurumlararası sistem girişleri (loginler) ve erişimler için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
Devlet Meteoroloji İşleri GM	Kurumlararası sistem girişleri (loginler) ve erişimler için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Devlet İstatistik Enstitüsü	Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Kurumlararası bilgisayar ortamında belge ve verileri elektronik

	olarak şifrelemek için
Dış Ticaret Müsteşarlığı	Kurumlararası sistem girişleri (loginler) ve erişimler için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
Emekli Sandığı GM	Kurumlararası sistem girişleri (loginler) ve erişimler için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Gümrük Müsteşarlığı	
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
T.C. Merkez Bankası	Kurumlararası sistem girişleri (loginler) ve erişimler için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
Nüfus ve Vatandaşlık İşleri GM	Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için
T.C. Devlet Demiryolları	
TİKA	Kamu Kurumları arasında kullanmıyoruz
Türk Standartları Enstitüsü	Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için
Sermaye Piyasası Kurulu	Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak imzalamak için (Planlanmaktadır) Kurumlararası bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek için (Planlanmaktadır)

12c– Kamu ve özel sektör arasında kullanıyorsanız; hangi süreçlerde aktif kullanıyorsunuz/kullanmayı planlıyorsunuz?

Adalet Bakanlığı	
Türkiye Noterler Birliği	
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	Özel sektör çalışanlarının kurumunuz sistemlerine girişi için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için
Devlet Meteoroloji İşleri GM	Özel sektör çalışanlarının kurumunuz sistemlerine girişi için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için
Devlet İstatistik Enstitüsü	Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak şifrelemek için
Dış Ticaret Müsteşarlığı	Özel sektör çalışanlarının kurumunuz sistemlerine girişi için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için
Emekli Sandığı GM	Özel sektöre ait sistemlere giriş (loginler) ve erişimler için Özel sektör çalışanlarının kurumunuz sistemlerine girişi için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak şifrelemek için
Gümrük Müsteşarlığı	Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	Özel sektör çalışanlarının kurumunuz sistemlerine girişi için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için
T.C. Merkez Bankası	Özel sektör çalışanlarının kurumunuz sistemlerine girişi için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için Aranızda iletilen bilgisayar ortamındaki belge ve verileri

	elektronik olarak şifrelemek için
Nüfus ve Vatandaşlık İşleri GM	Özel sektöre ait sistemlere giriş (loginler) ve erişimler için Özel sektör çalışanlarının kurumunuz sistemlerine girişi için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak şifrelemek için
T.C. Devlet Demiryolları	
TİKA	
Türk Standartları Enstitüsü	Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için
Sermaye Piyasası Kurulu	Aranızda iletilen bilgisayar ortamındaki belge ve verileri elektronik olarak imzalamak için

12d – Vatandaşlar için kullanıyorsanız; hangi süreçlerde aktif kullanıyorsunuz/kullanmayı planlıyorsunuz?

Adalet Bakanlığı	Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak imzalamaları için
Türkiye Noterler Birliği	
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak imzalamaları için Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak şifrelemeleri için
Devlet Meteoroloji İşleri GM	Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak imzalamaları için
Devlet İstatistik Enstitüsü	
Dış Ticaret Müsteşarlığı	Vatandaşların kurumunuza ait sistemlere girişleri (loginler) ve erişimleri için Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak imzalamaları için
Emekli Sandığı GM	Vatandaşların kurumunuza ait sistemlere girişleri (loginler) ve

	erişimleri için Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak imzalamaları için Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak şifrelemeleri için
Gümrük Müsteşarlığı	
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	Vatandaşların kurumunuza ait sistemlere girişleri (loginler) ve erişimleri için Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak imzalamaları için
T.C. Merkez Bankası	
Nüfus ve Vatandaşlık İşleri GM	Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak imzalamaları için Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak şifrelemeleri için
T.C. Devlet Demiryolları	
TİKA	
Türk Standartları Enstitüsü	Vatandaşların bilgisayar ortamında kurumunuza yönelik belge ve verileri elektronik olarak imzalamaları için
Sermaye Piyasası Kurulu	

13 – Elektronik İmza uygulamalarını hangi amaçla kullanmaya başladınız/kullanmayı planlıyorsunuz?

Adalet Bakanlığı	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için
Türkiye Noterler Birliği	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Güvenli evrak akışını sağlamak için
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	Islak imzalı süreçleri ve kağıt stoklarını azaltmak için

Denizcilik Müsteşarlığı	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
Devlet Meteoroloji İşleri GM	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Daha geniş alanda vatandaşa ve kamu çalışanına ürün ve servislere erişim kolaylığı getirebilmek için Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
Devlet İstatistik Enstitüsü	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Gelişen ve değişen teknolojik standartlara uyma zorunluluğu için Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
Dış Ticaret Müsteşarlığı	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Daha geniş alanda vatandaşa ve kamu çalışanına ürün ve servislere erişim kolaylığı getirebilmek için
Emekli Sandığı GM	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Daha geniş alanda vatandaşa ve kamu çalışanına ürün ve servislere erişim kolaylığı getirebilmek için Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
Gümrük Müsteşarlığı	Islak imzalı süreçleri ve kağıt stoklarını azaltmak için

	Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
İstanbul Büyükşehir Belediyesi	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Daha geniş alanda vatandaşa ve kamu çalışanına ürün ve servislere erişim kolaylığı getirebilmek için Gelişen ve değişen teknolojik standartlara uyma zorunluluğu için Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
Maliye Bakanlığı	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için
T.C. Merkez Bankası	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Gelişen ve değişen teknolojik standartlara uyma zorunluluğu için Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
Nüfus ve Vatandaşlık İşleri GM	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Daha geniş alanda vatandaşa ve kamu çalışanına ürün ve servislere erişim kolaylığı getirebilmek için Gelişen ve değişen teknolojik standartlara uyma zorunluluğu için Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
T.C. Devlet Demiryolları	Islak imzalı süreçleri ve kağıt stoklarını azaltmak için
TİKA	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Gelişen ve değişen teknolojik standartlara uyma zorunluluğu için

Türk Standartları Enstitüsü	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Daha geniş alanda vatandaşa ve kamu çalışanına ürün ve servislere erişim kolaylığı getirebilmek için Gelişen ve değişen teknolojik standartlara uyma zorunluluğu için Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
Sermaye Piyasası Kurulu	İş süreçlerini daha hızlı ve güvenilir hale getirmek için Islak imzalı süreçleri ve kağıt stoklarını azaltmak için Elektronik ortamdaki iş akışlarını takip edilebilir ve kayıt edilebilir hale getirebilmek için Daha geniş alanda vatandaşa ve kamu çalışanına ürün ve servislere erişim kolaylığı getirebilmek için

14– Elektronik İmza uygulamalarını hayata geçirirken/planlarken ne tür temel sorunlarla karşılaştınız?

Adalet Bakanlığı	Islak imzanın kullanma mecburiyetinin yönetmelikler, kanunlar gereği devam etmesi Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde olmaması
Türkiye Noterler Birliği	
Ankara Büyükşehir Belediyesi	
TÜBİTAK-BİLTEN	
Denizcilik Müsteşarlığı	
Devlet Meteoroloji İşleri GM	Islak imzanın kullanma mecburiyetinin yönetmelikler, kanunlar gereği devam etmesi Türkiye'deki internet altyapısının yeterli derecede yaygın olmaması Kurum içinde elektronik imza altyapısına uygun olmayan istisnai süreçlerin bulunması Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde

	olmaması Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için Elektronik imza altyapısı konusunda yaşadığımız en ciddi sıkıntılardan bir tanesi; bütçe ve ödemelerle ilgili yazışmalarda ıslak imza mecburiyeti olması ve gelecekte bu sorunun nasıl çözüleceği konusu.
Devlet İstatistik Enstitüsü	
Dış Ticaret Müsteşarlığı	Öncelikle kurumda çalışanların elektronik imza uygulamaları konusunda yeterli teknik bilgi eksikliği olması nedeniyle çalışanların bu tür uygulamarı kabullenmesi ve inanması konusunda zorluk çekilmiştir. Ayrıca, elektronik imza kanunun projeye başlandıktan sonra çıktı. Bu kanun çıkıncaya kadar hukuksal anlamda bir boşluk olması nedeniyle projenin tam PKI yapısında başlanılamadı. Bunun yanında, PKI yapısına dayalı uygulamaların dünyada ve özellikle ülkemizde çok örnekleri olmaması ve bu konuda kamu/özel sektör uzmanlarının da yeterli teknik bilgiye sahip olmaması, hukuki ve teknik boşlukları doldurmaya çalışmamız projeyi hızlı bir şekilde devreye almamazı zorlaştırmıştır.
Emekli Sandığı GM	Islak imzanın kullanma mecburiyetinin yönetmelikler, kanunlar gereği devam etmesi Uygulamanın hayata geçirilmesinde kurum içi teknik yetkinliğin yeterli olmaması Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde olmaması
Gümrük Müsteşarlığı	
İstanbul Büyükşehir Belediyesi	
Maliye Bakanlığı	
T.C. Merkez Bankası	Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde olmaması
Nüfus ve Vatandaşlık İşleri GM	Islak imzanın kullanma mecburiyetinin yönetmelikler, kanunlar gereği devam etmesi

	Uygulamanın hayata geçirilmesinde kurum içi teknik yetkinliğin yeterli olmaması Elektronik ortama dayalı iş süreçlerine hukuksal dayanak oluşturmak için
T.C. Devlet Demiryolları	
TİKA	
Türk Standartları Enstitüsü	
Sermaye Piyasası Kurulu	Türkiye'deki internet altyapısının yeterli derecede yaygın olmaması Kullanıcıların bu uygulamalara adapte olacak bilgi seviyesinde olmaması

GÖRÜŞLER

Türkiye Noterler Birliği (TNB) : E-İmza adına kullanılmaya başlanan teknolojilere bağlı olarak hizmet verecek olan sertifika makamlarında hem teknik ve hukuki yeterliliğin, hem de güven unsurunun sağlanması hizmetin bütünlüğü açısından mühim bir nokta olarak göze çarpmaktadır. Bu kapsamda altyapı açısından TNB tarafından yapılmakta olan çalışmalar ve karşılaşılan sorunlar şu şekilde özetlenebilir.

TNB, dijital imza ile ilgili çalışmalarına 2001 yılı Ocak ayı itibarı ile başlamış olup, tüm çalışmaların kendi bünyesinde bir ARGE ekibince hazırlanmasına, teknolojilerin burada incelenmesi ve entegre edilmesine özen göstermiştir. Bu kapsamda 2001 yılı Ekim ayında, kullanmakta olduğu projelere dijital imzayı USB token'lar vasıtası ile SDK düzeyinde entegre etmiş, akabinde hem VPN altyapısını hem de internet sistemini dijital imza ile koruma altına almış, bu aşamalarda imza üretme, muhafaza etme, doğrulama, denetleme ve iptal etme işlemlerini gerçekleştiren tamamen pilot uygulama amaçlı bir yazılım geliştirmiştir.2003 yılında başlatılan bir proje ile Yönetim Kurulu'nun dijital imza güvenliği altında Yönetim Kurulu Toplantılarını intenet üzerinden de yapabilmesi sağlanmış, bu kapsamda evrak akışı ve karar süreçleri de dijital imza ile pilot bir uygulamaya başlamıştır.

Tüm bu çalışmalarda en çok karşılaşılan zorluklar, geçen süreçler içerisinde teknolojilerin değişmesi ve hazırlanan projelerin yeni teknolojilere uyumunun zorluğu, projenin bitiminden sonra kullanıcıların bilgilendirilmesi, proje boyunca gelişen süreçlere göre yöneticilerin konu ile ilgili

düzenli bilgilendirilmeleri, çalışmalar neticesinde diğer projeler ile veri entegrasyonunun zorluğu (bu kapsamda çok farklı standartlar ve uygulamalar ile karşılaşılması) şeklinde olmuştur.

Yapılan çalışmalarda, halen bir çok kurum ve kuruluş tarafından yeni bir kavram olarak gözlenen e-imza konusunda en can alıcı noktalardan biri olan bilgilendirme konusunun, ve akabinde yeni başlaması planlanan projeler için, kurumlar arası veri entegrasyonunun mevcut çalışmanın vazgeçilmez bir parçası olarak ele alınmasının, çalışmaların verimli ve ileriye yönelik olarak hazırlanmasında dikkate alınması gereken önemli hususlar olduğu düşünülmektedir.

TÜBİTAK-BİLTEN : TÜBİTAK BİLTEN tarafından geliştirilmiş *ZEUGMA Sertifika Hizmet Sağlayıcısı Yönetim Yazılımı* aşağıdaki projeler kapsamında ilgili kurumlarda kullanılmaktadır:

Sermaye Piyasası Kurulu (SPK) ve İstanbul Menkul Kıymetler Borsası (İMKB) Kamuyu Aydınlatma Projesi (KAP):
KAP, Türkiye'de elektronik imzanın kullanıldığı ilk resmi uygulamadır.
Projeyle, Sermaye Piyasası Kanunu ve ilgili mevzuat hükümlerinin temel dayanağı olan kamunun tam, doğru ve zamanında bilgilendirilmesi amaçlanmaktadır. Proje, Sermaye Piyasası Kurulu (SPK), İstanbul Menkul Kıymetler Borsası (İMKB) ve Türkiye Bilimsel ve Teknik Araştırma Kurumu Bilgi Teknolojileri ve Elektronik Araştırma Enstitüsü (TÜBİTAK BİLTEN) tarafından yürütülmektedir.
Borsada işlem gören şirketler ve aracı kurumlar, proje kapsamında özel olarak geliştirilen yazılım aracılığıyla, SPK'ya ve İMKB'ye göndermekle yükümlü oldukları bildirimleri internet üzerinden elektronik imzalı olarak sisteme gönderir. Bildirimler, şablon, elektronik imza ve bildirim zamanına ilişkin yapılan otomatik kontrollerin ardından sisteme kabul edilir ve bekletilmeksizin veri yayın kuruluşları ve SPK web sitesi aracılığıyla kamuya duyurulur.
Bildirimlerin şirket yetkililerince elektronik olarak imzalanması, akıllı kart üzerinde verilen elektronik sertifikalarla yapılır.

Sosyal Sigortalar Kurumu (SSK) Başkanlığı Sigorta İşleri Genel Müdürlüğü Merkez ve Taşra Teşkilatı Donanım Yaygınlaştırma ve Altyapı Projesi (e-sigorta, e-bildirge)
Proje kapsamında ZEUGMA Sertifika Hizmet Sağlayıcısı Yönetim Yazılımı kullanılmış, BİLTEN tarafından SSK'ya sertifika yönetim hizmetleri ile ilgili danışmanlık verilmiştir. Proje, elektronik imzanın yaygın kullanımını amaçlayan Türkiye'deki ilk uygulamadır.

Dış Ticaret Müsteşarlığı (DTM) Dahilde İşleme Rejiminin Elektronik Ortamda Gerçekleştirilmesi Projesi
Projede PKI yapısı, ZEUGMA Sertifika Hizmet Sağlayıcısı Yönetim Yazılımı kullanılarak sağlanmaktadır.

Merkezi Kayıt Kuruluşu (MKK) Bilgi Güvenliği ve Sertifika Hizmetleri Uygulama Projesi
Aracı kuruluşların yatırımcıların bilgisi dışında yatırımcı adına işlem yapmasını engellemek ve yatırımcıların sermaye piyasalarına olan güvenini arttırmak amacıyla, MKK kaydi işlemin gerçekleşmesi için aracı kurumdan işlem bilgisinin yanında, yatırımcı tarafından oluşturularak aracı kuruma bildirilmiş olan ve MKK tarafından doğrulanabilecek bir işlem referans numarası da isteyecektir. BİLTEN, referans numarasının yatırımcı tarafından üretilmesi ve MKK tarafından doğrulanması işlevini yerine getirecek güvenli bir yöntem geliştirecek ve bu yöntemin gerçekleştirimini yapacaktır.
MKK, internet üzerinden gerçekleştireceği başka bir uygulamada bilgi güvenliğinin elektronik sertifika ve elektronik imza teknolojileriyle sağlanmasını planlamıştır. Uygulama kapsamındaki kullanıcılara elektronik sertifika verilmesi ve ilgili hizmetlerin yürütülmesi işini 2 (iki) yıl süreyle BİLTEN gerçekleştirecektir.

Ayrıca, kamu web sitelerinin güvenliği açısından web sertifikalarına da ihtiyaç duyulmaktadır. Ankette yer almamış olmakla birlikte, bu ihtiyacın belirlenmesi de önemlidir.

TÜBİTAK BİLTEN, 2000 yılı başından bu yana açık tuttuğu “http://sertifika.bilten.metu.edu.tr” web sitesinde konu hakkında bilgi yayınlamanın yanı sıra, kamuoyunda teknoloji ve uygulamalar hakkında farkındalık yaratmak amacıyla, deneme amaçlı sertifika vermektedir. TÜBİTAK BİLTEN’in hedefleri arasında olmamakla birlikte, adı geçen web sitesini ziyaret eden bazı kuruluşların talebi üzerine aşağıdaki kurum ve kuruluşların web sunucularına TÜBİTAK BİLTEN tarafından sunucu sertifikaları verilmiştir ve bu sertifikalar halen kullanılmaktadır.

T.C. Başbakanlık – Milli İstihbarat Teşkilatı
TUSAŞ Havacılık ve Uzay Sanayi A.Ş. (TAI)
T.C. Çalışma ve Sosyal Güvenlik Bakanlığı Bağ-Kur Genel Müdürlüğü
UlakNet Ulusal Akademik Ağ
TÜBİTAK Bilim ve Teknik Dergisi

Denizcilik Müsteşarlığı : Böylesine önemli bir konuyu anket vasıtasıyla gündeme getirdiğiniz için teşekkür ederim. Ben Denizcilik Müsteşarlığı Bilgi İşlem merkezinde çalışmaktayım. Kurumumuz henüz elektronik imzaya geçmemekle birlikte en kötü ihtimalle önümüzdeki 1-2 yıl içinde bunu gerçekleştirmeyi düşünmekteyiz. Elektronik imzaya geçme konusunda diğer kurumlardan geride kalmak istememize rağmen bu konu teknik anlamda yeterince bir tanıtım ve yardım alamadık. Bence bu konudan diğer kurumlarda teknik anlamda yeterince bilgi sahibi değiller.

Şahsi kanaatim :
Kurumların e-imza konusunu sağlıklı bir şekilde yürütebilmesi için yeterli düzeyde tanıtım ve teknik toplantıların yapılması ve hatta bu konudan sorumlu Kuruluşun uzmanları diğer kurumlara bizzat giderek
bu konuyu genel ve teknik anlamda açıklığa kavuşturmalıdırlar. Aksi halde önemli aksaklıklar yaşanacaktır.

Dış Ticaret Müsteşarlığı : Elektronik imza uygulamalarını devreye alabilmek için, öncelikle kamu kuruluşlarında yöneticiler bazında bir bilgilendirmenin düzenli bir şekilde yapılması gerektiğini düşünüyorum. Örneğin bir Bilgilendirme Çalışma Grubu oluşturup düzenli bir şekilde birkaç kuruma (özellikle işlev ve görevleri nedeniyle birbirine yakın olan kurumları birleştirerek) giderek özellikle üst yöneticilerin de katılımı sağlanarak bilgilendirme yapmanın yararlı olacağı kanısındayım.

Kamu kurumları bütçe kaynağı sıkıntısı çekmektedir. PKI uygulamaları ise belli yatırımların yapılmasını gerektirmektedir. Bu nedenle kurumların talep ettikleri bütçeler çoğunlukla kesintiye uğramaktadır. TBMM ve Hükümet nezdinde bu konunun gündeme getirilmesi ve PKI uygulamaları için düşünülen bütçelerin kesintiye uğratılmaması sağlanması yönünde çalışmalar yapılmalıdır.

Kurumlar/Kuruluşlar arası PKI uygulamaları için kesin bir işbirliği ve entegrasyon yapılması için kurumlar üstü bir organ oluşturmak ve bu konuda çalışma yapması sağlanmalıdır. Çünkü her kurumun ayrı ayrı yapacağı PKI uygulamaları entegrasyon sağlanmadığı için sağlıksız ve verimsiz olacaktır.

Özel sektör, özellikle bilişim sektöründeki firmaların PKI uygulamaları ve bilgi güvenliği konularında daha etkin ve biraz da özverili olmaları gerekiyor.

Elektronik imza kanunundaki hukuksal ve özellikle sertifika hizmet sağlayıcıları konularındaki boşlukların bir an önce doldurulması gerekiyor. Kanuna göre kamu kurumları sertifika hizmet sağlayıcı olabilmektedir. Yapılacak düzenlemelerde bu durumun korunması gerektiği kanaatindeğim. Ancak, kamu kurumları için de bazı standartlar ve koşulların daha bağlayıcı olması gerektiğini düşünüyorum. Böylece bu koşulları yerine getiren belli sayıdaki kamu kurumu ile bu işleri organize ederek entegrasyon sağlanabilir ve e-devlet olma yolunda önemli bir adım atılmış olabilir. Yapılacak düzenlemelerle kamu kurumların sertifika hizmet sağlayıcı olması engellenirse, e-imza uygulamalarının ülkemizde kullanımının yaygınlaşması zorlaşır. Çünkü vatandaşın e-imza uygulamalarına entegrasyonu bence bankacılık ve kamu kurumları yoluyla olabilir.

Bilgi İşlem Merkezi olan her kamu/özel urum ve kuruluşların PKI uygulamaları, bilgi güvenliği konularında yeterli teknik eleman sağlamaları hatta bu elemanlara ek tazminat ya da başka türlü imkanlar sağlama yönünde mutlaka bir çalışma başlatılması gerekir. Çünkü en büyük sıkıntı PKI uygulamalarını yürütebilmek için önemli ölçüde teknik elemana ihtiyaç duyulmaktadır.

Son olarak, e-imza uygulamalarına artık yavaş yavaş geçilmesi gerektiğini düşünüyorum. Bazı uygulamalar yardımıyla e-imza kullanımındaki doğabilecek sorun ve aksaklıkları ülke olarak görmemiz ve bunlara çözüm aramamız gerekir. Yapılacak düzenlemelerin bir geçiş süresi için aşırı şekilde caydırıcı olmaması gerekir. Aksi takdirde başlatılmış/bitirilmiş ya da yakın bir tarihte başlatılacak/bitirilecek projelerin boşa gitmesi muhtemel olacaktır.

TİKA : Hayata geçirilmesini planladığımız E-DEVLET (E-TİKA KURUMSAL PORTAL VE OTOMASYON SİSTEMİ) projesini, son teknolojiye ve her türlü platforma uyumlu olacak şekilde tasarlanmaya çalışıldı. Bu sistemin hayata geçmesi durumunda Kurum için bir çok kolaylıklar ve tasaruf getireceği kanatindeyiz. Anket düzenlediğiniz için Kurum olarak sizlere teşekkür eder. İyi çalışmalar dileriz…

Türk Standartları Enstitüsü : Bu konuda özellikle kamu kuruluşları arasında koordinasyonun sağlanması ve ortak verilerin değerlendirilmesinin önemli olduğu düşünülmektedir.

Sermaye Piyasası Kurulu : Elektronik imza iş süreçlerinin hızlanması, verimlilik ve etkinlik konularında çok büyük avantajlar getirecektir. Bu bağlamda dijitalleşen süreçlerde mevzuat yönünden gerek duyulan düzenlemeler elektronik imza kanunu ile gerçekleştirilmiş bulunmaktadır.

Belirli konularda özellikle başlangıç aşamasında her alanda olduğu gibi bazı sıkıntıların yaşanabileceği muhakkaktır. Ancak bu husular yaşandıkça giderilerek beklenen kalite değerlerine ulaşılacaktır. Bu sebeple elektronik imza ve elektronik imza teknolojilerine dayalı uygulamara kurumları teşvik etmek gerekmektedir.

5.2 Türkiye'de elektronik sertifika hizmeti sunan ya da sunmayı planlayan (kendi içinde ya da diğer kişi/kuruluşlara) kurum ve kuruluşlar, söz konusu kurum ve kuruluşların sertifika hizmeti sunarken kullandıkları veya kullanmayı planladıkları ürünler, bu ürünlerin dayandıkları standartlar

5.3 Halihazırda elektronik imza uygulamalarında karşılaşılan sorunlar

5.4 Kamu ve özel sektördeki mevcut ihtiyaçlar ve elektronik imzanın uygulama alanı bulabileceği hizmetler (kurumsal işlemler ve vatandaşa dönük hizmetler)

5.5 Kamu ve özel sektörde AAA'larının birlikte çalışabilirliği için ortak ihtiyaçlar ve kaynaklar, ortak kullanımı/paylaşımı gerektiren durumlar

6 YAPILACAK DÜZENLEMELERDE ALTYAPIYA İLİŞKİN OLARAK DİKKATE ALINMASI GEREKEN HUSUSLAR

6.1 Elektronik İmza Kanunu'nun altyapıyla ilgili hükümlerinin değerlendirilmesi

6.2 Kurum tarafından yapılacak düzenlemelerde altyapıya ilişkin olarak yer almasında fayda görülen hususlar

Elektronik olarak imzalanan formlar, belgeler, kayıtlar dünyanın büyük bölümünde uzun süredir geçerli olmasının ardından artık ülkemizde de elle atılan ıslak imzalar ile eşdeğerde kabul edilecektir. Bu online süreçler maliyetleri azaltıp, iş süreçlerini hızlandırıp verimliliği yükseltirken güvenliği de ön plana çıkarmaktadır.

ATM'den kredi kartlarına kadar bir çok elektronik imza ve kayıt çözümlerinde dikkate alınması gereken belli noktalar bulunmaktadır:

- Teknoloji, gerekli teknik güvenlik ihtiyaçlarını karşılamalıdır (tanılama, veri bütünlüğü ve inkar edilememe)
- Gerekli ticari ve iş gereksinimlerini karşılamalıdır.
    - Yasa ve yönetmeliklere uygunluk
    - Kullanıcılar tarafından kabul görmeli (kullanım kolaylığı)
    - Kendini kanıtlamış olmalı (referanslar)
    - Standartlar bazlı olmalı
- Esneklik ve ölçeklik sunmalıdır.
- Halen kullanılan iş akış ve güvenlik çözümlerine entegre olmalıdır.

AB dahilinde üye ve aday ülkeler 1999/93/EC e-imza yönergesine uyumlu şekilde kendi düzenlemelerini yapmış yada yapmaktadırlar. Kullanılacak çözümler doğal olarak bu çerçeveye uygun olmalıdır. Ancak bunun yanında resmin tamamına da bakmakta yarar vardır.
Zira sadece yasal şartların yerine getirilmesinin yanında elektronik imza ve kayıtlar iş yapış şeklini tamamen değiştirecek yeni bir paradigma getirmektedirler. Son on yılda yurt içinde ve dışında bir çok kurum kendi içinde elektronik kayıtlar oluşturmakta ve bunları elektronik olarak imzalamaktadırlar. Çözümler sadece bir uygulama ve kurum bazlı olmamalı tedarik zinciri, sektör, resmi tüm uygulama ve alanları kapsayacak ve destekleyecek şekilde olmalıdır.

Yasal bağlayıcı elektronik işlemler hem özel hem de kamu kurumları için uzun dönemli ve önemli bir konudur. Birkaç istina dışında çoğu işler günümüzde kağıt ortamında gerçekleştirilmektedir. Kredi kartı endüstrisi son 25 senedir elektronik ağlar üzerinden yasal bağlayıcı elektronik işlemler gerçekleştirmektedir. EDI teknolojisi 70 ve 80'li yıllar boyunca özellikle bazı dikey sektörlerde yoğun olarak kullanılmaktadır.

Son dönemlere kadar sadece ıslak imza ve kağıt yada hibrid(kağıt+e-imza) şekilde kullanılan belgeleri tamamen elektronik ve yasal bağlayıcı hale getiren yöntemler gelişmemişti. Veri bütünlüğü, tanılama, denetleme gibi zorunlukluların karşılanması ve yasal çerçevenin çizilmesiyle bu alanda gelişmeye başlamıştır.

Işlem kanıtı olan belgeler ve kayıtlar üç bölüme ayrılan yaşam döngüsüne sahiptir:
Bölüm 1: Yaratma, paylaşma ve inceleme: Işlem kaydını yaratma ve son şeklini verme.
Bölüm 2: Onaylama, bilgilendirme yada kabul: işlemin gerçekleştirildiğinin kanıtı (imzaların kullanılması ile).
Bölüm 3: Dağıtım, saklama ve yok etme: gönderme, dosyalama, arşivleme ve belge geri çağırma.

1.bölüm'deki işlemlerin hayat döngüsü'nün büyük bir kısmı masaüstü programlar, iş akışı programları, web bazlı formlar ve mainframe sistemler sayesinde otomasyona geçmiştir. Bu değişim kişi ve kurumlara büyük verimlilik artışı, zaman tasarrufu ve maliyet avantajı sağlamıştır.

2 ve 3. bölümler, diğer bir deyişle işlem gerçekleştirme böümüne ise elektronik belgelerin ve yasal bağlayıcı elektronik işlemleri destekleyecek hukuki altyapının düzenlenmesine kadar otomasyon uygulanamamıştır. Sadece özel, kapalı devre ilişkiler ile ara yollar bulunmuştur (kredi kartı yada EDI sistemleri gibi). Çoğu dünya devletlerinin olduğu gibi Türkiye'nin de elektronik imzanın kabul edildiğini düzenleyen yasayı çıkarmasının ardından 2 ve 3. bölümlerde de hızlı gelişmelerin olacağının beklenmesi gerekir.

Elektronik Belge Iş Akışı

Elektronik belgeler en genel şekli ile iki çeşide ayrılır:

Statik: Iş akışı statik belgeler (formlar yada uygulamalar, yeni hesap başvuruları, müşteri hizmetleri talepleri gibi) ile başlar. Buradaki veriler genellikle veritabanlarına yazılırken belgelerin kendileri dosyanın yada arşivin bir parçası olmaktadır.
Dinamik: Dinamik belgeler genellikle şablon olarak başlar ve her ihtiyaca göre özelleştirilir (örneğin anlaşmalar). Son haline gelip onaylanmasına kadar çok sayıda değişiklik ve şablon kullanılır.

Ilk jenerasyon elektronik imza çözümleri masaüstü uygulamalar olup çeşitli masaüstü dosyalarını (Microsoft Word, Excel, Adobe Acrobat, AutoCAD, text, v.b. gibi) yasal ve güvenlik şartlarını yerine getirerek imzalamakta, başkalarına e-mail olarak gönderilmesini sağlamaktadır.

Ancak artan ihtiyaçlar, yaşanan tecrübeler ve gelişen teknolojiler sunucu bazlı elektronik imza çözümlerinin gelişmesini ve diğerlerinin yerini almasını sağlamıştır. Böylece dinamik olarak web-bazlı belgeler yaratılabimekte, onaylama ve imzalama sağlanabilmektedir. Detaylı ve imzalı denetleme raporu, saklama sağlanırken dahili ve harici taraflar ile (iş akış programları, kredi kurumu, noterler, sertifika hizmet sağlayıcıları) entegrasyon da sağlanmaktadır.

Güvenli Imzalama ve Özel Anahtar

Türkiye Büyük Millet Meclisinde kabul edilen 5070 sayılı Elektronik Imza kanunu belli bir teknoloji seçilerek çıkarılmış olduğundan dijital imzalar hariç diğer elektronik imza yöntemlerini kabul etmemiştir. Bu bağlamda kişi ve kurumlar uygulamalarını PKI altyapısı altında çalışacak şekilde düzenleyeceklerinden imzayı atacak özel anahtarın güvenliği en önemli alan haline gelmektedir.

5070 sayılı Kanun'un 6. maddesinde güvenli elektronik imza oluşturma araçlarının özellikleri belirtilerek sağlaması gereken koşulların neler oldukları belirtilmiştir. Buna göre;

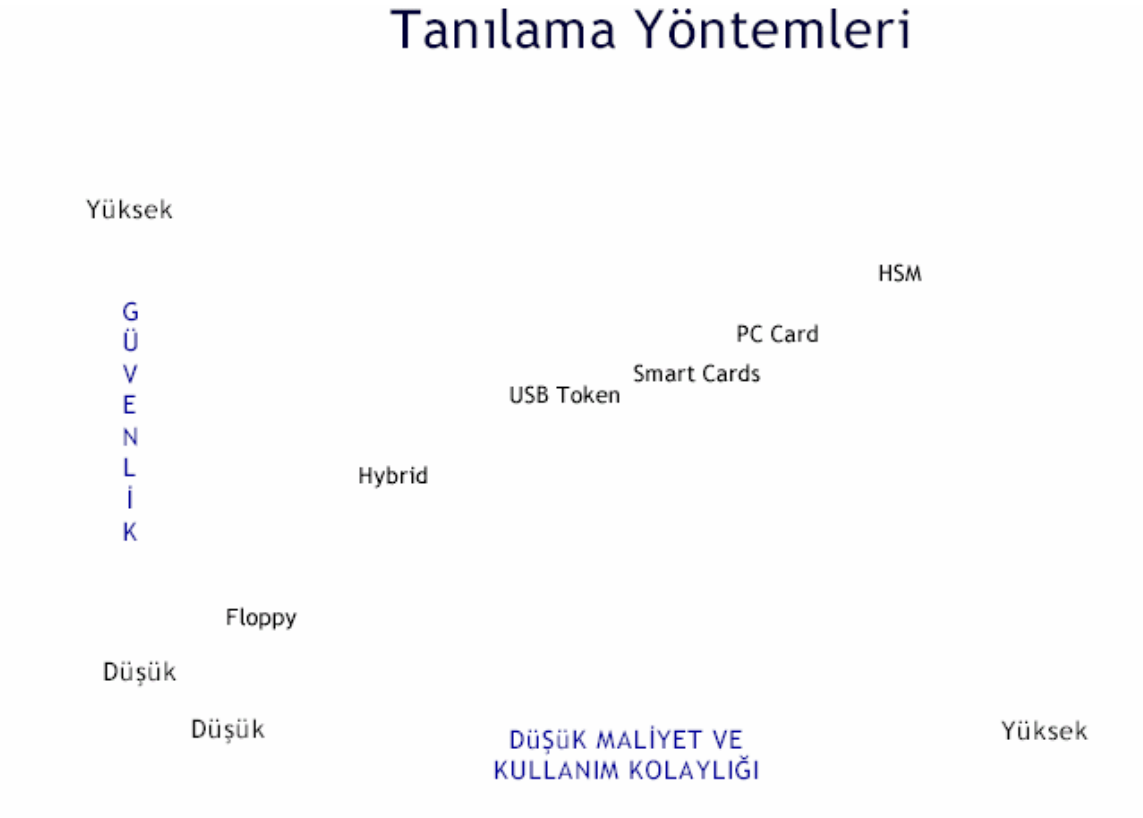
- . Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmaması,
- . Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiç bir biçimde çıkarılamamasını ve gizliliğini sağlaması,
- . Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesi, kullanılamaması ve elektronik imzanın sahteciliğe karşı koruması,
- . Imzalanacak verinin imza sahibi dışında değiştirilememesi ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesidir.

Her tür işlemler giderek daha fazla elektronik ortamda ve internet üzerinde -- -çalışanlar, müşteriler ve iş ortakları tarafından- gerçekleştirildikçe paylaşılan bu bilgilerin bütünlüğü ve güvenliğinin sağlanması zorunlu hale gelmiştir.

Bireyin iletişim yada işlem sırasında olduğunu iddia ettiği kimliğinin doğrulanması ve onaylanması işlemine tanılama denir. Bireyi tanılamada sadece üç farklı yöntem vardır: bilgi faktörü (kişinin bildiği birşey), sahiplik faktörü (kişinin sahip olduğu bir şey) ve biometrik faktör (kişinin bir

parçası). Bu seçenekler yüksek güvenlik ve “çok faktörlü tanılama” için istenilen kombinasyonda kullanılır.

Sahiplik faktörü bireyin sahip olduğu kapı anahtarı, yaka kartı yada kriptografik anahtar gibi herhangi bir simge olabilir. Genel olarak bunlara sahip olarak bireyler yetkili olduklarını garanti ederler. Bunu da sahip olunan simge tarafından yaratılan ve onaylanan bir veri ile kanıtlarlar. Eğer simge verisinin bütünlüğü ve tanılaması dijital imza gibi kriptografi kullanılarak yapılırsa onaylama süreci daha yüksek güvenlik seviyesi ile gerçekleşir.



Şekil 1: 1999 ABD Savunma Bakanlığı Tanılama Teknolojileri Çalışmasından

Elektronik ortamda tanılamanın nasıl yapılması gerektiği ile ilgili kararları alırken gerçek hayatta kullandığımız yöntemler ve kriterler büyük benzerlikler göstermektedir. Örnek olarak bir çok kişi servetlerini korumak için anahtarlı yada şifreli kilit kullanma arasında karar vermeye çalışmaktadır. Tanılama açısından şifreli kilitler bilgi faktörünü temsil ederken anahtarlı kilitler sahiplik faktörüdür. Benzerlikler bununla da sınırlı kalmamaktadır zira zorlukları da bunlara ekleyebiliriz: yedek plan (eğer anahtar kaybolur yada şifre unutulursa ne yapılacak), kolay kullanım (bir şeye sahip olmak mı yoksa hatırlamak mı daha kolay), mobilite, etkili güvenlik ve maliyet.

Kriterler

Güvenlik	Tanılama Seviyesi nedir?
Kabul Görme	Kullanıcılar bu yeni tanılama yöntemlerine ne kadar hızlı uyum gösterir?
Maliyet	Toplam kurulum ve kullanım maliyeti nedir? • Ürünün maliyeti • Bakım ve Destek (yaratma, kurulum, yenileme, çağrı merkezi desteği • Son kullanıcı kurulumu (manual, elektronik, uzaktan, yerel
Geleceğe Yatırım	Gelişen diğer iş ihtiyaçlarını karşılıyor mu? • Web-bazlı kurumsal uygulamalar ve extranetler • Cihaz bağımsız ve kablosuz/mobil istemciler (PDA, cep telefonları)
Ölçeklik	Ne kadar kolay ve optimum şekilde ölçekleme yapılabilir?

Tokenlar

Imzaların oluşturulma, saklanma ve kullanımına yönelik alternatiflerden biridir. USB tabanlı çalışan tokenlar sertifikalar için güvenli bir ortam yaratırlar ve içerisindeki bilgileri şifrelenmiş bir şekilde saklayabilirler. Sahip oldukları PIN/password ile kaybolması durumunda kullanılması koruma altına alınır.

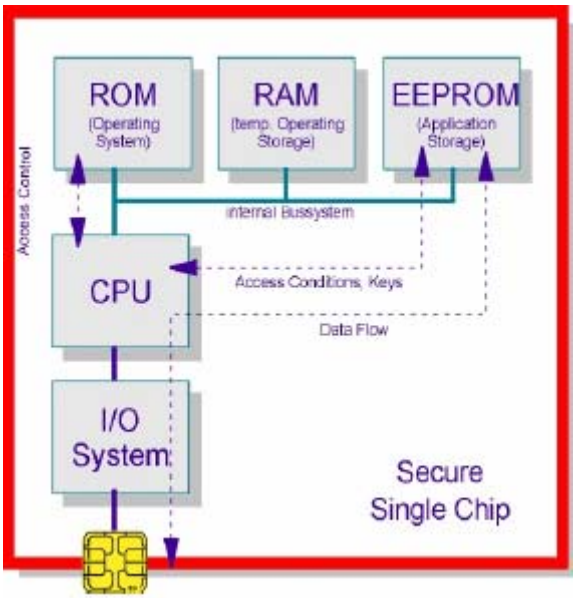
Akıllı Kartlar

Akıllı kartlar 80 ve 90'lı yıllar boyunca PKI'ın karşılaştığı zorlukların aynılarından -uyum, ölçeklik, yaygın kullanım, destek ve en önemlisi de gerçekçi bir iş modelinin olmamasından- aşırı derecede etkilenmiştir. Her biri için olumlu ve olumsuz argümanlar getirilebilir ancak PKI ortamlarında akıllı kart kullanımı diğer simge çeşitlerine göre giderek daha çok tercih edilen bir yöntem olarak kabul edilmektedir.

Kimlik yönetimi mimarisi olarak PKI uyumlu akıllı kartları kullanmanın bir çok faydası vardır. Güvenlik seviyeleri geçtiğimiz seneler boyunca giderek gelişen akıllı kartlar üçüncü taraflara inkar edilememe ki dijital imzalar ile sağlanır içerik bütünlüğü ve tanılama özelliklerinin sunulmasına izin verir. Dijital imzaların göreceli üstünlüğü özel anahtara erişim kontrollerinin oturtulmasına ve uygulanmasına bağlıdır.

- . Akıllı kartlar bireylerin özel anahtarlarını güvenli şekilde tutarlar.
- Dijital imzalar yaratırlar.
- . Akıllı kartlar entegre yongayı çalıştırmak için yerel tanılama (örneğin PIN, biometrik) sunarlar.
- . Çoklu uygulama özelliklerini desteklerler.

ISO 7816 ve diğer kurumlar tarafından standartları oluşturulan akıllı kartlar işlemci ve mikro bilgisayar içerir (RAM, ROM, EEPROM). Güç kaynağı bulunmadığından akıllı kart okuyucusuna ihtiyaç duyan donanım bazlı akıllı kartlar çok amaçlı uygulamaları (ödeme, tanılama, imzalama) desteklemektedir.



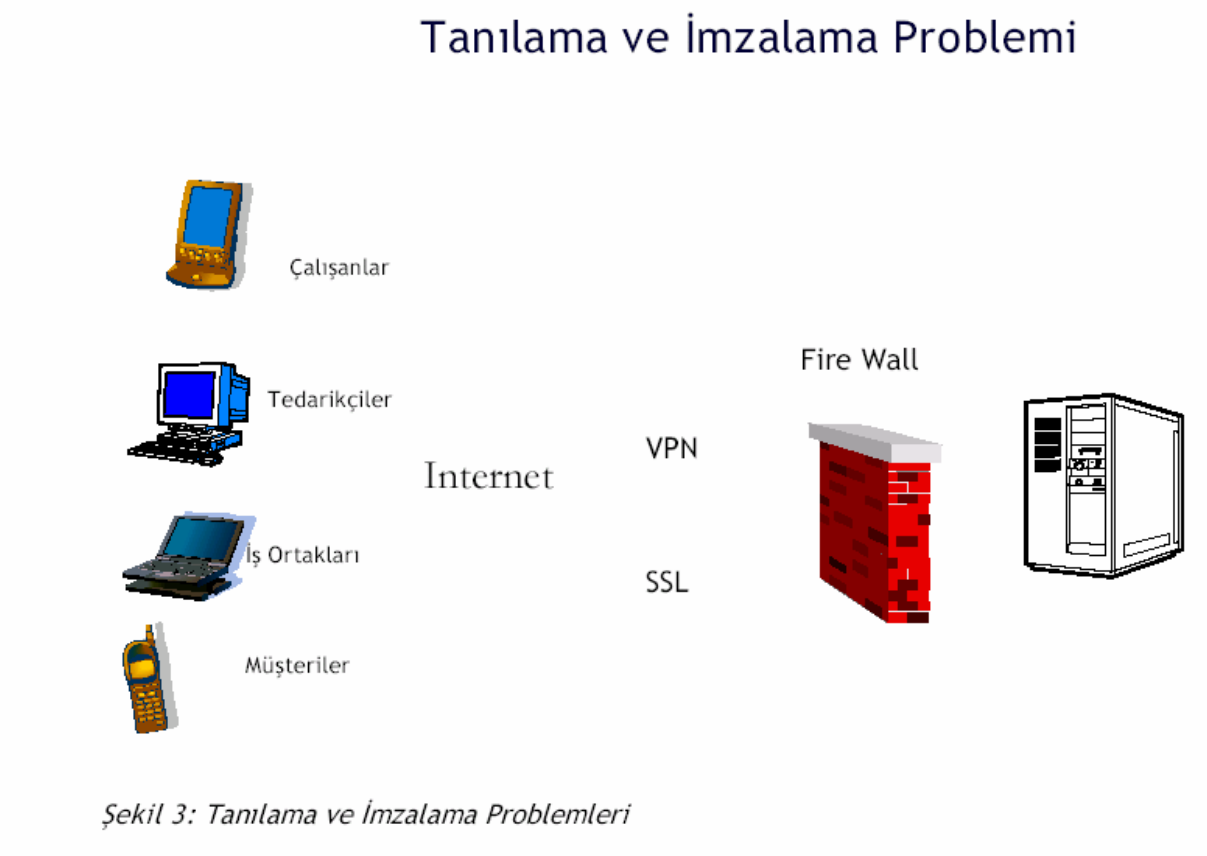
Şekil 2: Akıllı Kart bileşenleri

CEN ve ISO 7816 "Information Technology –Identification Cards –Integrated Circuit Cards with Contacts" akıllı kart spesifikasyonlarını tanımlayan çok taraflı uluslararası standartlardır. Bu standart elektrik ve fiziksel karakterisikler ile iletişim protokollerini açıklamaktadır. Bunlara ek olarak özellikle finansal uygulamalarda global liderlik gösteren Visa International, JCB, Identrus gibi kurumlar kendi standartlarını da geliştirmiş ve eklemişlerdir. Aşağıdaki tablo akıllı kartlar ile ilgili en çok kullanılan ve kabul edilen spesifikasyonları göstermektedir:

Standart/Spesifikasyon	Kurum
ISO 7810 ISO 7816	CEN/ISO
ISO 14443	ISO
PC/SC	Microsoft
OCF	Sun Microsystems
EMV	Europay/Mastercard/Visa
Java Card 2.1	Sun Microsystems
PKCS	RSA
Global Platform 3-D Secure	Visa
GSA Interoperability Spec.	General Services Administration
Identrus	Identrus Members

Yazılım Bazlı Akıllı Kartlar

Iletişim teknolojilerinin çok hızlı şekilde gelişerek hayatın tüm alanlarına girmesi ile elektronik iş uygulamaları büyük farklılıklar göstermeye başlamıştır. Zira sadece iş yapılan platformlar değil işleme katılan kullanıcıların rolleri, tanılama yöntemleri, imzalama yöntemleri aynı kalmamakta her yerden, her zaman ve her çeşit cihaz ile yüksek seviyeli
tanılama ve imzalama yapabilmek gerekmektedir. Donanım bazlı imzalama araçları tüm bunları sağlayamadığı için güvenli e-iş ve e-ticaret için yeni bir kategori olarak "yazılım bazlı akıllı kartlar" ortaya çıkmıştır. (Bakınız Şekil 3)
Özellikle internet ölçeğinde çok büyük sayılara ulaşan ve geleneksel olarak kullanıcı adı/şifre ve simge kullanılan uygulamalar (e-devlet, e-ticaret, finans, sağlık) için donanım bazlı akıllı kartların alternatifi ve/veya tamamlayıcısı olarak birlikte kullanılmaktadır.



Şekil 3: Tanılama ve İmzalama Problemleri

Yazılım Bazlı Akıllı Kartlar, kullanıcıların özel anahtarlarını donanım seviyesinde "Kriptografik Kamuflaj" teknolojisi ile darbelere dayanıklı bir bölümde güvenli şekilde korurlar. Sistemde HIÇBIR YERDE tutulmayan ve sadece kullanıcı tarafından bilinen PIN'ler ile aktive edilen softcard'lar ile kullanıcının özel anahtarı her türlü offline, brute force saldırılarına karşı korunur ve her tür PC yada internete bağlı cihazdan güvenli şekilde yüklenip kullanılabilir. Softcard'lar ile kullanıcılar her zaman ve her yerden akıllı kartlarını güvenli şekilde roam edebilir, herhangi bir okuyucuya gerek duymadan yüksek seviyede imzalayabilir ve güvenli şekilde tanılayabilirler.

Bu kategorinin sunduğu çok düşük maliyet (doğrudan yada destek maliyeti), donanım gerektirmemesi, kolay kullanım, taşınabilirlik, mobilite ve ölçeklenebilirlik gibi faydaların yanında ilk dönemlerde her yeni gelişen kategoride yaşanan kabullenme zorluklar ile de karşılaşılmaktadır. Ancak özellikle Visa, IEEE, Identrus, Amerikan Bankalar Birliği ve Irlanda, ABD gibi devletlerin standartlarını kabul ve teşvik edip uygulamalarında yoğun olarak kullanmaya başlamasıyla yaygınlığı daha da artmaktadır.

Yüksek seviyeli tanılama ve imzalama için 2 faktöre ihtiyaç vardır.

- . Bilmeniz gereken bir şey
- . Sahip olmanız gereken bir şey

Ister donanım ister yazılım bazlı akıllı kartlar olsun her iki faktörde sahip olmanız gereken şey karşılık gelen dijital sertifika ve bilmeniz gereken şey ise aynı ATM kartları gibi kartınızı aktive eden PIN'dir.

Şekil 3: Tanılama ve İmzalama Problemleri

Sonuç

Teknolojinin ve rekabetin gelişimi ile hedefler, karar alıcılar ve kriterler büyük değişime uğramış, iş yapış tarzlarında ve kararlarda büyük değişimler oluşmuştur.

	ESKİDEN Varlıkları Korumak	GÜNÜMÜZDE İşi Korumak
HEDEF	Varlık Odaklı: Kişileri dışarda tutarak kurum varlıklarını korumak	Müşteri Odaklı: İş süreçlerini kontrol ederek müşteri hizmetini yönetmek
KARAR ALICILAR	Güvenlik Uzmanı	Yöneticiler
KRİTER	Kullanılması önemli değil, kurşun geçirmez olsun	Esnek, ölçeklenebilir, kullanımı kolay, düşük maliyetli

Şekil 4: E-İş Uygulamaları İçin Yeni Düşünce Şekli

5070 sayılı kanununda Imza oluşturma aracı "Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını", Imza oluşturma verisi ise "Imza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler" şeklinde tanımlanmıştır.

Dijital sertifikalar yurt dışından farklı olmayarak ülkemizde de belli "trust domain"lerinin altında son kullanıcılara müşteri, iş ortağı yada eleman olarak kurumlar tarafından ulaştırılacaktır. Bu şartlara uyan ve zorunlulukları karşılayan ürünler ve teknolojiler piyasa koşullarında kurumlar tarafından seçilmektedir ve seçilecektir. Bilinmesi gereken hiçbir simgenin herkesin ihtiyaçlarını tam olarak karşılayamayacağıdır. Her zaman kullanım kolaylığı, birlikte işlerlik, maliyet ve güvenlik arasında seçimler yapılacaktır. AB komisyonunun WP8 D8.2 "PKI Challenge" çalışmasında belirtildiği gibi "birlikte
işlerlik, ancak bir PKI kullanıcısı olarak kurumunuz yurt içi ve dışında diğer PKI kullanıcısı kurumlar ile ilişki kurmayacaksa problem değildir."

Teknolojinin şirketlerin verimlilik ve rekabet güçlerini arttırmak için varolduğu göz önüne alındığında optimum çözümün şeçilmesi önemlidir.

6.3 Altyapıya ilişkin olarak uyulması gerekli standartlar ve kurallar

Bu çalışma Elektronik Imza Altyapı Çalışma Grubu'na katkı sağlaması için hazırlanmıştır.

6.4 Söz konusu standartlar ve kuralların Türkiye'ye uygulanması için yapılması gerekenler

6.5 Kullanıcıların altyapı kullanımı ile ilgili olarak dikkat etmesi gereken hususlar

Bu çalışmada, digital imzaların son kullanıcılar tarafından kullanılmasına yönelik bilgiler verilmektedir. Bu bilgiler, digital imzalar konusunda bilinen yanlışlar, çekinceler ve önlemler ile digital imza oluşturma araçlarının tanımı ve alternatifleri şeklinde özetlenebilir.

Digital imzadan amaç; hayatı, günün gerekleri dogrultusunda hızlandırmak, kolaylaştırmak ve bürokrasiyi azaltmaktır. Bunu yaparken, hayatın her alanında etkin olabilmesini sağlamak, teknik bütünleşme gereksinimlerine cevap sunabilecek esnekliğe sahip olmak, ilave bürokrasi yaratmamak, yönetimi ve sürdürülebilirliği (maintenance) kolaylaştırmak, yasal ve yönetsel sorun ve engeller çıkarmamak, genel-geçerli olmasını sağlamak, kisiye özgülüğü kaybetmemek, zaman aşımlarını hesaba katmak, güvenli kullanımı sağlamak gibi çok değişik parametrelerle sınırları çizilebilecek bir ortama uygun olarak kullanılabilirliğini sağlamak gerekecektir. Bu çok yönlü, neredeyse sonsuz kombinasyonları gereğince yönetebilecek ve düzenleyebilecek araçların seçilmesi ve bu seçimlerde de en ekonomik çözümlerin üzerinde durulması gerekiyor. Bunlar olmazsa, karmaşanın önüne geçilmesi ve yasal boslukların da bir şekilde suistimal edilmesi kaçınılmaz olacaktır. Bu açıdan bakıldığında, sayısal imza oluşturmak için kullanılacak araçların bu çerçeveye oturması gerekecektir.

Sürecin üç yönü ön plana çıkıyor. Bir, imzanın oluşturulması; iki, imzanin korunması ve üç, imzanın doğrulanması. Tümünün bir güvenlik yönü var ki, yukarıda sayılanların hepsi burada kilitleniyor. Günlük hayatta noterlerin, kriminolojinin, mahkemelerin bir kısmının, v.b. varlığı da bu noktada anlam kazanıyor. Yeni yasa, hangi şekilde çıkarsa çıksın, karşılaşılabilecek en önemli ve zarar verici sorun da burada, yani güvenlikte, düğümlenecektir. Amacın tanımı düzgün yapılmadığında, aslında bir teknik sorun olarak araç seçimi için doğru referans bulunması olanaksız olacaktır.

5070 sayılı Elektronik İmza Yasası, geleneksel imzanın hukuki, idari, ticari vb. ortamlarda kullanım amacını genişletip, elektronik ortamda da kullanılmasına olanak sağlamaktadır. Fakat konu hakkında bilinen yanlışların başında, kağıt ortamında kullanılan imzanın bir tarayıcı tarafından taranıp, elektronik ortamda saklanması ve kullanılması gibi algılanması gelmektedir. Hatta bu yanlış algılanma sonucunda üretilen ve kullanılan örneklerine de rastlanmaktadır. Yasa yürürlüğe girmeden önce kamuoyunun bu konuda aydınlatılması, gerekirse bu konuda bir kılavuz hazırlanması uygun olacaktır.

Elektronik imzanın, günlük hayatta kullanılan imzanın yerine geçmesi için belirli bir sertifikasyon makamı tarafından verilmesi ve kullanım anında onaylanması gerekmektedir. Bu alandaki uyulması gereken standartlarla ilgili çalışmalar çalışma grubu içerisinde yer alan diğer arkadaşlarca yapılmıştır. Kullanıcıları ilgilendirecek bölümü ise, bu imzaların hangi şekilde üretileceği, nereye müracaat edileceği, nasıl saklanacağı ve nasıl kullanılacağı ile ilgilidir.

Digital imza oluşturma araçları, sertifikasyon makamı tarafından verilen imzaların güvenli bir şekilde oluşturulmasını sağlayan yazılım, donanım veya ikisinin bir arada kullanılmasını sağlayan araçlardır. Bu tip donanım veya yazılımlarda, imzaların güvenli bir şekilde oluşturulması ve saklanabilmesi için PKCS#11, Capi, X.509 Sertifika depolanması, ISO 7816, FIPS 140-1, ITSEC LE4 smartcard security certification vb. uluslararası standartlar veya bu standartların TSE tarafından Turkiye şartlarına uyarlanmış benzeri standartları aranması uygun görülmektedir.

Yasa, digital imza oluşturma araçları tanımını yaparken sadece belirli tipte donanım (smartcard, token vs.) gibi kısıtlamalar getirmek yerine belirlenecek standartlar çerçevesinde çeşitli alternatiflerin kullanım imkanını getirebilir. Bu alternatiflerden birisi digital imzaların oluşturulması, saklanması ve kullanılmasını bir kurum kendi bünyesinde tutacağı özel bir sunucu veya donanım ile sağlayabilir. Burada dikkat edilmesi gereken, bu imzanın sadece o kurum bünyesinde tutulmasının getireceği zorluklar olmasıdır. Kurum, bu digital imzaların kullanılması esnasında digital imza sahiplerin imzalarını güvenli bir şekilde kullanılmasını sağlayacak altyapıyı oluşturmalıdır. Digital imzanın bireysel kullanımının yaygınlaşmasını kısıtlamakla birlikte, yurtdışında bu tip kullanımlara rastlanmaktadır.

Bir diğer alternatif, bu imzaların soft token olarak da adlandırılan, yazılım temelli olarak PC'ler üzerinde oluşturulması, saklanması ve kullanılmasıdır. Bu alternatifteki dezavantaj digital imzanın mobil olmamasıdır. İmza sadece o PC üzerindeyken kullanılabilir, mobil olarak taşınması ve PC

dışında kullanılması mümkün değildir. Güvenlik açısından riski ise, PC'nin başkaları tarafından kullanılması veya internete açık ortamlarda virüs vb. herhangi bir sebeple zarar görmesi, silinmesi, kopyalanması şeklinde karşımıza çıkmaktadır. Bu alternatiflerin tercih edilmesi durumunda söz konusu dezavantajlar ve risklerin kullanıcı tarafından bilinmesi gerekmektedir.

İmzaların oluşturulma, saklanma ve kullanımına yönelik en uygun alternatifler ise, mobil olması ve imzaların güvenli bir ortamda tutulması, kopyalanmasının mümkün olmaması gözönüne alındığında bu amaç için özel olarak üretilmiş olan, imzalar ve sertifikalar (Açık anahtar uygulamaları) için aranan standartları destekleyen smartcard'lar veya smartcard teknolojisini kullanan USB tabanlı tokenlardır. Bu alternatifler, sertifikalar için güvenli bir ortam yaratırlar ve içerisindeki bilgileri şifrelenmiş bir şekilde saklayabilirler. Sahip oldukları PIN/password ile kaybolması durumunda kullanılması koruma altına alınabilir. Yine kötü niyetli erişim için PIN/password'un kırılıp içindeki bilgilerin kullanılmasını önleyici mekanizmalara sahiptirler. Portatif ve mobil özelliği sayesinde imza sahibi imzasını sürekli yanında taşıyabilir ve ihtiyaç duyulabilen heryerde güvenli bir şekilde kullanabilir. Bu alternatiflerdeki dezavantajlar ise, kullanılacak donanımların smartcard reader gerektiriyor olması veya ilgili araçların kullanımı esnasında kullanılacak işletim sistemi vb. ortamlar için driver yüklenmesinin gerekebileceği şeklinde sıralanabilir.

Tüm bu açıklamalar dikkate alındığında, kamuoyunun digital imzalar konusunda bilgilendirilmesi, digital imza oluşturma araçları için standartların belirlenmesi gerekmektedir. Yine alternatifler sunulurken bu alternatiflerin avantaj/dezavantajlarının ve taşıdığı risklerin belirtilmesi ve geleneksel imzanın olduğu gibi digital imzanın da korunmasının önemi vurgulanmalıdır.

Son kullanıcıların Dijital Sertifika Alırken Dikkat Etmesi Gereken Temel Noktalar;

- Sertifikanızı "Tarafsız ve Güvenlir Üçüncü Parti Sertifika Otoritesi"nden aldığınızdan emin olun.
- Dijital sertifikanızın şifreleme standartı Dünya Standart'ı olan 128 bit'den aşağı olmamalı.
- Sertifikanızın geçerliliğini ilgili Sertifika Otoritesi'nin "Sertifika Iptal Liste (CRL)" lerinden gerçek zamanlı kontrol edilip edilmediğini öğrenin.
- Sertifikanızın "Sigorta Kapsam"ında olup olmadığını öğrenin.
- Dijital Sertifikalar sanal ortamdaki dijital kimliğiniz olduğu için kimlik doğrulama evraklarının sertifika otoritesi tarafından tam olarak istendiğinden emin olun.

- Sertifika Uygulama Prosedürlerini (Evrakların kontrolü, sertifikanın yayınlanması vs...) kaç gün içerisinde yerine getirdiklerini öğrenin.
- Sertifika Uygulama Prosedürlerinin Sertifika Dağıtan kurum tarafından nasıl bir süreç ile doğrulama işlemlerinin yapıldığını öğrenin. Bu işlemin takibinden ve gerçekçi olduğundan emin olun.
- Sertifika otoritesinin kök sertifikalarının IE ve Netscape gibi günümüzde kullanılan popüler browser'larda yüklü olup olmadığını kontrol edin.
- İleride karşılaşacağınız problemler karşısında teknik destek konusundan emin olun. (Anonim Anahtar Yaratma Süreci (CSR), Sertifikanın server'a kurulması, Sertifika yedeğini alınması, Sertifika yedeğinin kurulması vs...)

7 GENEL DEĞERLENDİRME, SONUÇ VE ÖNERİLER

Doküman genelinde yeralan bilgiler olarak yönetici özeti kısmında anlatılabilir.(Sertaç Bey)

7.1 Türkiye'nin hukuki, ekonomik ve teknolojik koşullarına uygun olabilecek AAA mimarilerinin karşılaştırmalı analizi,

7.2 Türkiye için vatandaşa hizmeti esas alan, ulusal güvenlik gereklerini dikkate alan, kamu ve özel sektörün farklı gereksinimlerini karşılayabilecek esnekliğe sahip, varolan hizmetlerin elektronik ortama taşınmasını teşvik ederek ülkemizde e-dönüşümün gerçekleştirilmesine destek olacak, yeni uygulamaların önünü açacak, yeni yatırımları ve ülkemize yabancı sermaye girişini özendirirken mükerrer yatırımlar sonucu kaynak israfını ve ülkemizin teknoloji çöplüğüne dönmesini engelleyecek model ve politikaların önerilmesi,

7.3 Altyapı konusunda özellikle kamu sektörüne yönelik öneriler ve bu hususta Kurumdan beklenenler

8 EKLER

EK-1) DÜNYADA ELEKTRONİK İMZAYA İLİŞKİN KURUMSAL ALTYAPI VE UYGULAMALAR YARARLANILABİLECEK KAYNAKLAR

EK-2) BAZI ÜLKELERDEKİ E-İMZA İLE İLGİLİ YASALAR

AB Üyesi Ülkeler:

1) Belçika: Sertifika Servisleri ve Elektronik İmzaların Hukuki Çerçevesinin Esasları Hk.Yasa, 14 Haziran, 2001 tarihinden itibaren geçerli olmuştur.

2) Danimarka: Elektronik İmzalar Hk.Yasa, 1 Ekim 2000 tarihinde geçerli olmuştur.

3) Fransa: 2 ayrı yasa bulunmaktadır. Mart 2000 tarihli, 2000-230 sayılı yasada, elektronik imza ve belgelere, ispat konusunda kağıda dayalı belgelere benzer esaslar getirmektedir. 2001 tarihli, 2001-272 sayılı yasa ile de AB Direktifinde yer alan hususların çoğu tanınmaktadır.

4) Almanya: AB Direktifinden önce, 1997 tarihinde hazırlanıp 1998 de yürürlüğe giren Alman Sayısal İmza Yasası anılan direktifle uyumsuz hükümler içerdiğinden, üç senelik tecrübe ve AB Direktifi ilkelerine göre hazırlanan yeni Alman Elektronik İmza Yasası, 22 Mayıs 2001'de yürürlüğe girdi.

5) İtalya: AB Direktifini yürürlüğe henüz koymadı, ancak Mart 1997 tarihli, 59 sayılı Yasa ve 1997 tarihli Kararname ile Açık Anahtar Altyapısı (PKI) esasına dayanan, sayısal imzalarla ilgili esasları tanımıştır.

6) Lüksemburg: 14 Ağustos 2000 tarihli E-Ticaret Yasası, AB Direktifi ile uyumlu.

7) İsveç: 1 Ocak 2001'de yürürlüğe giren Nitelikli Elektronik İmza Yasası, AB Direktifi ile uyumlu.

8) Portekiz: Ağustos 1999 tarihli, 290-D/99 sayılı yasa elektronik imza ve elektronik belgelerin geçerliliği hususunda esasları belirlemektedir. AB Direktifine uyum sağlamadı henüz.

9) İspanya: 17 Eylül 1999 tarihli Elektronik İmza Yasası ile AB Direktifini yürürlüğe koydu.

10) İngiltere: AB Direktifini yürürlüğe koyacak herhangi bir düzenleme yapılmadı, ancak, 2000 Elektronik Komünikasyon Yasası bir ölçüye kadar elektronik imzaların kullanımı ve hukuki geçerliliği ile ilişkili.

11) İrlanda: 10 Temmuz 2000 tarihli Elektronik Ticaret Kanunu, elektronik imzayı ve kayıtları düzenliyor.

11) Avusturya: Federal Elektronik İmza Kanunu, 1 Ocak 2000'de yürürlüğe girdi.

12) Finlandiya: AB Direktifi ile uyumlu bir yasayı görüşüyor, yasada ABD yasasından alınmış bazı esaslar da bulunuyor.

13) Çek Cumhuriyeti: Elektronik İmza Yasası 1 Ekim 2000'de yürürlüğe girdi. AB Elektronik İmza Direktifi ile uyumlu.

14) Macaristan: Elektronik İmza Yasası 1 Eylül 2001'de yürürlüğe girdi. AB Direktifi ile uyumlu.

15) Polonya: Elektronik İmza Yasası Temmuz 2002' de yürürlüğe girecek.

16) Bulgaristan: Elektronik Belgeler ve Elektronik İmzaya ilişkin bir taslak Meclise sunuldu.

17) Estonya: 15 Aralık 2000'de yürürlüğe giren Sayısal imza Yasası.

18) Malta: Mayıs 2000'de yayımlanan bir raporda, Elektronik Ticaret, Veri Korunması ve Bilgisayarların kötüye kullanılmasına ilişkin üç yasa hazırlanması öngörülüyor.

19) Slovak Cumhuriyeti: Elektronik İmza Yasasının hazırlanmasına yönelik bir çalışma grubu teşkil edildi, çalışmalar devam ediyor.

20) Slovenya: 22 Ağustos 2000'de Elektronik Ticaret ve Elektronik İmza Yasası yürürlüğe girdi.

II) Diğer Avrupa Üyeleri:

21) İzlanda: Nisan 2001 tarihli Elektronik İmza Yasası kabul edildi

22) Norveç: Elektronik İmzaların Kullanımı ve Tanınması Hk.Yasa Temmuz 2001'de yürürlüğe girdi. AB Direktifi ile uyumlu

23) Ukrayna: Elektronik belgelere ilişkin yasasını çıkardı, UNCITRAL Model Yasası esas alınmış.

III) Amerika:

24) ABD: Yukarıda belirtildiği gibi, halen ABD'de elektronik ticaretle ilgili olarak eyaletlere ilişkin yasalar ve Federal yasalar olmak üzere uygulamalar devam etmektedir.

25) Kanada: 10 Nisan 2001'de yürürlüğe giren Elektronik İşlemler Yasası, tüm elektronik işlemlerle ilgili.

26) Arjantin: 15 Ağustos 2001 tarihli Sayısal İmza Kanunu.

27) Bermuda: 1999 tarihli Elektronik İşlemler Yasası, elektronik imza ve kayıtları kapsıyor.

28) Brezilya: 1999 tarihli bir taslak yasa var, sayısal imzalarla ilgili.

29) Kolombiya: 21 Ağustos, 1999 tarihli, 527 sayılı Elektronik Ticaret Yasası var. 1996 tarihli UNCITRAL Model Elektronik Ticaret Yasası örnek alınmış.

30) Ekvator: Elektronik ticaret, elektronik imza ve veri mesajlarını kapsayan bir taslak hazırlandı.

31) Meksika: Ticaret Kanununda elektronik imzaları kapsayacak bir değişiklik yapılamak isteniyor.

IV) Asya:

32) Japonya: 24 Mayıs 2000'de kabul edilip, 1 Nisan 2001'de yürürlüğe giren Elektronik İmzalar ve Sertifika Hizmetleri Hk.Yasa.

33) Singapur: 29 Haziran 1998 tarihli Elektronik İşlemler Yasası.

34) Hindistan: 1998 tarihli Elektronik Yasası ve 2000 tarihli Bilgi Teknolojisi Yasası.

35) Hong Kong: 7 Nisan 2000'de yürürlüğe giren Elektronik İşlemler Yönetmeliği.

36) Çin Cumhuriyeti: İnternet bankacılığına ilişkin yasal düzenlemeler var.

37) Rusya: Rusya Federasyonu Bilişim Yasası, Ocak 1995 tarihli, elektronik imzalara ilişkin.

38) Malezya: 1 Ekim 1998'de yürürlüğe giren Sayısal İmza Yasası

39) Güney Kore: Elektronik Ticaret Temel Kanunu ile Elektronik İmza Kanunu hazırlanıyor.

40) Tayvan: Elektronik İmza Yasası yasalaşma süreci içine girdi.

41) Tayland: Elektronik İşlemlerle ve Elektronik İmzalarla ilgili iki yasa taslağı birleştirildi ve taslak Kabine tarafından onaylandı.

V) Diğerleri:

42) İsrail: 5760 sayılı, 2000 tarihinde çıkarılan Elektronik İmza Yasası.

43) Avustralya: Çeşitli bölgelerin 2000 tarihli Elektronik İşlemler Yasaları bulunmaktadır.

44) Yeni Zelanda: Ticaret Yasasında düzeltmeler ve elektronik ticaretle ilgili yasal düzenlemeler taslak halinde.

45) Gibralta: Elektronik Ticaret Yönetmeliği, çeşitli e-ticaret konularına ilişkin.

EK-3) KAMU KURUMLARI'NDA ELEKTRONİK İMZA ALYAPISI UYGULAMALARI ANKETİ

EK-4) YAPILACAK DÜZENLEMELERDE DİKKATE ALINMASI GEREKEN HUSUSLAR / CA KRİTELERİ

6Ek. WebTrust CA Criteria.doc

EK-5) YARARLANILABİLECEK BİLGİLER

EK-6) YARARLANILABİLECEK KAYNAKLAR

PKI APPLICATIONS AND VERTICAL MARKETS

Financial Sector

Brokering Trust In Financial Services (Presentation)

ISO Presentation On PKI For Financial Services (pdf)

Orbian

Universal Value eXchange (FSTC-UVX)

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

NACHA -The Electronic Payment Association

The World Bank

Federal Reserve Bank (US)

Wachovia Corporation Certification Authority Certificate Policy (49 pp - pdf)

eLynx, Ltd. electronic data and document delivery mortgage banking industry

Real Estate Finance Security Management Organization

Government

A M E R I C A S

FirstGov.gov (US Gov Portal)

Access Certificates for Electronic Service (ACES)

Canadian Government Communications Security Establishment

Cryptography's Role in Securing the Information Society (National Research Council)

CyberCemetery (Web sites and publications of defunct U.S. government agencies and commissions)

DISA DoD PKI Homepage

DOC Export Administration Commercial Encryption Export Controls

Federal Computer Incident Response Capability (FEDCIRC)

Federal Directory Forum Discussion Site

Federal Public Key Infrastructure

FedWorld Information Network

FORTEZZA Support

Government of Canada Treasury Board PKI Documents Site(use search)

US Gov Printing Office

National Academy of Sciences Computer Science

United States Federal Judiciary

US Government White Pages Directory

US GSA Access Certificates for Electronic Services (ACES)

Argentine Federal Digital Signature Infrastructure (PKI FERMA)

Federal PKI Working Group (US)

US Patent Application Information Retrieval (PAIR)

Common Criteria (NIST)

US Partnership for Critical Infrastructure Security (PCIS)

NASA Public Key Infrastructure

Chief Information Officers (CIO) Council (US)

Information Assurance Support Environment DoD (US)

Information Analysis Infrastructure Protection - Homeland Security Dept (US)

Federal Information Processing Standards (US)

Government of Canada Public Key Infrastructure

Electronic Crimes Task Force (US)

US State Governments

State Of Alabama

State Of Alaska

State Of Arizona

State Of Arkansas

State of California

State Of Colorado

State Of Connecticut

State Of Delaware

State Of Florida

State Of Georgia

State Of Hawaii

State Of Idaho

State Of Indiana

State Of Illinois

State Of Iowa

State Of Kansas

State Of Kentucky

State Of Louisiana

State Of Maine

State Of Maryland

State Of Massachusetts

State Of Michigan

State Of Minnesota

State Of Mississippi

State Of Missouri

State Of Montana

State of Nebraska

State Of Nevada

State Of New Hampshire

State Of New Jersey

State Of New Mexico

State Of New York

State Of North Carolina

State Of North Dakota

State Of Ohio

State Of Oklahoma

State Of Oregon

State Of Pennsylvania

State Of Rhode Island

State Of South Carolina

State Of South Dakota

State Of Tennesee

State Of Texas

State Of Utah

State Of Vermont

State Of Virginia

State Of Washington

State Of West Virginia

State Of Wisconsin

State Of Wyoming

District Of Columbia

Information Security in State Government Information Technology (NASCIO)

Survey of State Electronic & Digital Signature Legislative (ILPF)

EUROPE AND THE MIDDLE EAST

Act on Electronic Service in the Administration (Finnish Ministry of Justice)

UK Government Communications-Electronics Security Group

eEurope

Ireland Irish Post

Belgium Ministry of Finance

ASIA/PACIFIC

New Zealand S.E.E. PKI

Africa

REPUBLIC OF SOUTH AFRICA ELECTRONIC COMMUNICATIONS\AND TRANSACTIONS BILL

Healthcare

ITSG Trust Center (in German)

MEDePass

Healthcare PKI (Tunitas Group)

HealthKey

HIC (Australia)

Regional Secure Healthcare Networks RESHEN (Europe)

Health Insurance Portability and Accountability Act (HIPAA) US Department of Health and Human Services

Harmonisation for the secuRity of web technologies and aPplications (HARP)

UK Dept of Health - NHS LifeHouse Project

Health Informatics/Security ISO/TC 215/WG 4 Documents

American Health Information Management Association (AHIMA)

Medical Information System Development Center (Japan)

FDA 21 CFR Part 11 Electronic Records; Electronic Signatures (US)

Workgroup for Electronic Data Interchange(electronic connectivity in the healthcare industry)

Insurance

Safety Insurance

STANDARDS AND PROTOCOLS

IPSec

HSC IPSec Links

MIME Security

S/MIME FAQ (RSA)

S/MIME Working Group (IETF-IMC)

RSA's S/MIME Interoperability Center

S/MIME and OpenPGP

S/MIME Freeware Library

S/MIME Mail Security (IETF)

S/MIME Utility (+ SMIMEUtil:: perl module)

PKIX

IETF PKIX-WG

Time-stamping, DCS, etc.

Secure Socket Layer (SSL) & Transport Layer Security (TLS)

BSAFE patches for SSLeay

Enabling Network Security with SSLeay

Introduction to SSL(Netscape)

OpenSSL PKCS#12 Program FAQ (Stephen Henson)

OpenSSL web site

OpenSSL: The Open Source toolkit for SSL/TLS

pilotSSLeay: port of SSLeay-0.8.1 to the Pilot

PureTLS(ver 0.9b4)

SSL 3.0 SPECIFICATION (Draft)

SSLeay Documentation

SSLeay and SSLapps FAQ

SSL Encryption Check

The TLS Protocol Version 1.0 (RFC 2246)

Secure Electronic Transactions (SET)

SET Secure Electronic Transaction LLC

Security Standards Documents: Formal, De Facto, Proposed etc.

ANSI Home Page

CEN/ISSS Electronic Signatures (E-SIGN) Workshop

Certificate Authority Interoperability Pilot (Internet Council)

Certified Electronic Mail (CEM)

Digital Signatures: The Law and High-fidelity IP Pipes (David G. Masse)

Draft Internet PKIX Standards

Economic modelling and risk management in Public Key Infrastructures (David G. Masse)

ESCA: Electronic Signatures and Certification Authorities (ITU)

ETSI Electronic Signatures and Infrastructures

European Certification Authority Forum (ECAF)

IEEE Standards Home Page

IEEE P1363 standard for RSA, Diffie Hellman and Related Public-Key Cryptography (Elliptic Curves)

Internet Engineering Task Force (IETF)

SPKI WG XML Key Management Specification (XKMS)

PKIX WG

IPSEC WG

S/MIME WG

SPKI: Simple Public Key Infrastructure (Carl Ellison)

TLS WG

Joint Working Group of the IETF and W3C XML Signature

ISO/IEC JTC1/SC27

IMC Pointers to Email Related Standards

Internet RFCs

ISETO: The International Secure Electronic Transactions Organisation

ITU Recommendations

PKI-related activities at NIST

DISA PKI Interoperability Master Test Plan

Secure Internet Programming - Princeton University

Simple PKI Draft

Security and Encryption Links (Peter Gutmann)

Sirene Publications

X.509 Style Guide (Peter Gutmann)

X.509, 1997 version, prepublication draft

X.500 Directory Related standards

X9 Home Page

W3C: Electronic Payment Schemes (Phillip Hallam-Baker)

Open Source Implementation of a PKI (IDX-PKI)

Free ICP Project

World Wide Web Consortium (W3C)

XML Key Management Specification (XKMS)

XML Advanced Electronic Signatures (XAdES)

RFCs and internet drafts:

The IETF Security Area and related IETF working groups

PKIX: Public Key Infrastructure (X.509)

RFC 2459: "Certificate and CRL Profile"

RFC 2510: "Certificate Management Protocols"

RFC 2511: "Certificate Request Message Format"

RFC 2527: "Certificate Policy and Certification Practices Framework"

RFC 2528: "Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates"

RFC 2559: "Operational Protocols - LDAPv2"

RFC 2560: "Online Certificate Status Protocol - OCSP"

RFC 2585: "Operational Protocols - FTP and HTTP"

RFC 2587: "LDAPv2 Schema"

RFC 2797: "Certificate Management Messages over CMS"

RFC 2875: "Diffie-Hellman Proof-of-Possession Algorithms"

RFC 3029: "Data Validation and Certification Server Protocols"

RFC 3039: "Qualified Certificates Profile"

RFC 3161: "Time-Stamp Protocol (TSP)"

RFC 3279: "Algorithms and Identifiers for the PKIX Certificate and Certificate Revocation List (CRL) Profile"

RFC 3280: "Certificate and CRL Profile"

RFC 3281: "An Internet Attribute Certificate Profile for Authorization"

RFC 3379: "Delegated Path Validation and Delegated Path Discovery Protocol Requirements"

S/MIME: S/MIME Mail Security

RFC 2311: "S/MIME Version 2 Message Specification"

RFC 2312: "S/MIME Version 2 Certificate Handling"

RFC 2630: "Cryptographic Message Syntax"

RFC 2631: "Diffie-Hellman Key Agreement Method"

RFC 2632: "S/MIME Version 3 Certificate Handling"

RFC 2633: "S/MIME Version 3 Message Specification"

RFC 2634: "Enhanced Security Services for S/MIME"

RFC 2785: "Methods for Avoiding the 'Small-Subgroup' Attacks on the Diffie-Hellman Key Agreement Method for S/MIME"

RFC 2876: "Use of the KEA and SKIPJACK Algorithms in CMS"

RFC 2984: "Use of the CAST-128 Encryption Algorithm in CMS"

RFC 3058: "Use of the IDEA Encryption Algorithm in CMS"

RFC 3125: "Electronic Signature Policies"

RFC 3126: "Electronic Signature Formats for long term electronic signatures"

RFC 3183: "Domain Security Services using S/MIME"

RFC 3185: "Reuse of CMS Content Encryption Keys"

RFC 3211: "Password-based Encryption for CMS"

RFC 3217: "Triple-DES and RC2 Key Wrapping "

RFC 3218: "Preventing the Million Message Attack on Cryptographic Message Syntax"

RFC 3274: "Compressed Data Content Type for CMS"

RFC 3278: "Use of Elliptic Curve Cryptography (ECC) Algorithms in CMS"

RFC 3369: "Cryptographic Message (CMS)Syntax"

RFC 3370: "Cryptographic Message Syntax (CMS) Algorithms"

RFC 3394: "Advanced Encryption Standard (AES) Key Wrap Algorithm"

RFC 3537: "Wrapping a Hashed Message Authentication Code (HMAC) key ..."

RFC 3560: "Use of the RSAES-OAEP Key Transport Algorithm in CMS"

RFC 3565: "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in CMS"

TLS: Transport Layer Security

RFC 2246: "The TLS Protocol Version 1.0"

RFC 2712: "Addition of Kerberos Cipher Suites to TLS"

RFC 2817: "Upgrading to TLS Within HTTP/1.1"

RFC 2818: "HTTP Over TLS"

RFC 2830: "LDAP v3: Extension for Transport Layer Security"

SPKI: Simple Public Key Infrastructure (*Note: WG has concluded*)

OpenPGP: An Open Specification for Pretty Good Privacy

XML-DSig: XML Digital Signatures (see also: IETF/W3C XML Signature WG

IPSEC: IP Security Protocol

IPSRA: IP Security Remote Access

The PEM specification:

RFC 1421 --- ASCII --- PostScript (195 KB)

RFC 1422 --- ASCII --- PostScript (156 KB)

RFC 1423 --- ASCII --- PostScript (76 KB)

RFC 1424 --- ASCII --- PostScript (46 KB)

RFC 1847: "Security Multiparts for MIME"

RFC 1848: "MIME Object Security Services (MOSS)"

RFC 2015: "MIME Security with Pretty Good Privacy (PGP)"

RFC 2480: "Gateways and MIME Security Multiparts"

RFC 3156: "MIME Security with OpenPGP"

RFC 3174: "US Secure Hash Algorithm 1 (SHA1)"