

1. NIST PKI Test Suite (PKITS)

http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pktesting.html

NIST (National Institute of Standards and Technology, ABD) Information Technology Laboratory tarafından yayınlanmış bir test suitidir.

a. Bu test suiti, X.509 Standardındaki sertifikaların doğrulanması işlemlerini belirleyen RFC (Request for Comments, IETF tarafından yayınlanır, 1969'dan beri İnternet teknolojilerini belirler) 3280'da belirtilen özelliklerin sağlanıp sağlanmadığını sınar.

b. X.509, elektronik sertifika veri formatıdır.

c. Açık Anahtar Altyapısında kullanıcının kendisine sakladığı özel anahtar (private key) ve tüm muhataplara dağıtılan genel anahtar (public key) vardır.

d. Açık anahtar altyapısı ile yapılan imzalamada, imzanın gerçekten söz konusu kişiye ait olup olmadığı, ilgili kişinin genel anahtarının, kontrolü yapacak tarafta doğru olarak bulunmasına bağlıdır.

e. Elektronik sertifikalar, genel anahtarın imzalı belgenin gönderildiği taraflarda garantili olarak elde edilebilmesini dağıtık ve güvenli bir mimari ile sağlar.

f. Elektronik sertifika formatı olan X.509'da şunlar gibi alanlar mevcuttur:

(1) Kişi tekil adı,

(2) Bu sertifikayı düzenleyen birimin tekil adı,

(3) Bu sertifikanın geçerlilik tarih aralığı,

(4) Kişinin genel anahtarı,

(5) Sertifika feshi için sorgulacak web servisi adresi,

(6) Tüm bu bilgilerin birleşiminden oluşturulan bir özet sayısal verisinin, sertifika düzenleyici tarafından imzalanması sonucu oluşan imza verisi.

g. Elektronik sertifikalar zincir yapısındadır.

h. Bu zincir yapısında en üstte Certification Authority vardır.

i. Zincir yapısında üstteki birim, bir alttaki birimin sertifikasını imzalayarak o sertifikanın içerdiği bilgilerin doğruluğunu onaylamış olur.

j. Zincir doğrulaması (Certification Path Validation) en alt daldan (kullanıcının sertifikası), onu doğrulamakta kullanılan tüm sertifikaların üzerinden geçilerek dijital olarak atılan imzanın geçerli ve doğru olduğunun test edilmesidir.

k. Bu özellik dijital imza kullanan tüm yapılarda çok önemlidir. İmza atılmış bir dökümanın kullanıcı tarafından güvenilir olup olmaması, uygulamanın bu zincir doğrulamasını uygun bir şekilde yapıp kullanıcıya sonucu doğru ve anlaşılır bir şekilde vermesine bağlıdır.

l. PKITS test suiti, geçerli imzaları kapsadığı gibi çeşitli negatif sonuç vermesi gereken testleri (yanlış veri içeren sertifikalar, süresi dolmuş sertifikalar gibi) de içerir.

m. Adobe Acrobat, bu test suitinde bulunan 250'den fazla testi başarıyla geçmiştir.

ADOBE ACROBAT GÜVENLİK SERTİFİKASYONLARI

2. SAFE Biopharma Association

<http://www.adobe.com/lifesciences/safe.html>

- a. SAFE - Signatures and Authentication for Everyone.
- b. İlaç endüstrisi içerisindeki ve endüstri-devlet kurumları (FDA – Federal Drug Agency ABD gibi) arasındaki süreçler için, dijital kimlik ve imzalama standardı oluşturarak kağıt tabanlı işlemleri hızlandırma amaçlı.
- c. Yeni bir ilacın piyasaya sürülmesi 10 ila 20 yıl arasında sürebiliyor. Phrma (Amerikan İlaç Araştırmacıları ve Üreticileri Birliği) tarafından yapılan araştırmaya göre arge çalışmaları maliyetlerinin %40'ını kağıt tabanlı süreçler oluşturmaktadır.
- d. SAFE, ilaç araştırma, geliştirme ve üretim aşamalarında kağıt temelli süreçlerin elektronik ortamda, daha hızlı, verimli ve bilgiye daha kolay erişilebilmesini sağlayacak bir "etkinleştirici" platformdur.
- e. Üyeleri tarafından yönetilen, kâr amacı gütmeyen bir organizasyon.
- f. SAFE kapsamında, kağıt formların dönüştürülmesi amacıyla PDF dosyaları kullanılmıştır. Bunun sebebi, PDF dosyalarının platform bağımsız olarak biçimlendirmeye en uygun, her ortamda aynı görüntüye sahip olmaları ve imza alanlarını formun içerisinde doğal bir şekilde barındırarak kullanıcılara kağıt üzerinde alıştıkları şeklin en yakınına sunmasından dolayıdır.
- g. Mevcut formların PDF'e dönüştürülerek, SAFE tarafından düzenlenen PKI altyapısı ile elektronik olarak imzalanarak, Adobe LiveCycle platformu ile yürütülen iş süreçlerine katılması şeklinde yapılan uygulama.
- h. PDF uygulaması hakkında bir sunum:
<http://www.safe-biopharma.org/images/stories/febupdates/SAFEDigitalSignaturesinPDF.pdf>
- i. SAFE kapsamında kullanılması için ürünlerin SAFE Teknik Spesifikasyonlarına uyması gereklidir.
- j. Bir ürünü sertifikalandırmak için SAFE Ürün Sertifikasyon Programı'nda yer alan testler belirlenmiştir.
- k. Bu testler sonucunda sertifika alan ürünler SAFE logo'sunu kullanma hakkı kazanır.
- l. Bu uygulamada kullanım için yapılan güvenlik testleri sonucunda Adobe Acrobat, Reader ve LifeCycle Document Security yazılımları SAFE uyumlu olarak sertifikalanmıştır.

3. CNIPA Onayı

- a. CNIPA - İtalya Kamu Yönetimi Ulusal Enformatik Merkezi.
- b. Başbakanlığa IT konusunda danışmanlık yapıyor.
- c. Bilişim hakkında çıkan yasaları inceleyerek öneride bulunuyor.
- d. CNIPA tarafından Adobe PDF, dijital imza için geçerli bir ortam olarak belgelendirilmiştir.
- e. İtalya Kamu Çalışanları Ulusal Emekli Sandığı Yönetimi (INPDAP) 1994'te kurulmuştur.
- f. Emekli maaşları, ikramiyeleri, krediler ve yaşam standardı çalışmaları yürütmektedir.
- g. INPDAP kağıt ağırlıklı süreçlerini hızlandırmak ve verimini artırmak için sayısallaşma yolunu seçmiştir.
- h. Elle veri girişini azaltmak, iletişimi hızlandırmak, arşivlemeyi kolaylaştırmak ve kurumsal bilgi deposunu gerçekleştirmek için INPDAP mevcut formlarını Adobe PDF haline dönüştürmüştür.

ADOBE ACROBAT GÜVENLİK SERTİFİKASYONLARI

i. Adobe PDF teknolojisinin CNIPA tarafından dijital imza onayı alması sayesinde imza gerektiren uygulamalarda da PDF formlarının kullanılması mümkün olmuştur.

4. Alman İmza Kanunu – Common Criteria

j. Common Criteria for Information Technology Security Evaluation – ISO / IEC 15408

k. Kanada, Fransa, Almanya, Hollanda, İngiltere ve ABD devletleri tarafından ortak bir şekilde geliştirilmiştir.

l. Common Criteria (CC), güvenlik kriterleri belirlemez.

m. Bunun yerine uygulamaların ihtiyaç duyduğu güvenlik özelliklerini standart bir şekilde tanımlayabilecekleri bir çerçeveye oluşturur.

n. Bu şekilde kullanıcılar ihtiyaç duyduğu güvenlik özelliklerini belirtebilir, üreticiler buna uygun sistemler geliştirebilir, güvenlik seviyeleri konusunda beyanda bulunabilir ve bağımsız denetçiler bu beyanları değerlendirebilir.

o. Direkt olarak Adobe ürünlerinin CC değerlendirmesi yapılmamış.

p. Alman Dijital İmza Yasası'na (SigG) uygun olarak üretilen OpenLimit SignCubes PDF ürünlerinin Common Criteria değerlendirilmesi yapılmış ve SigG'ye uygunluğu Alman Federal Bilgi Güvenliği Ofisi (BSI - <http://www.bsi.bund.de/>) tarafından onaylanmıştır (<http://www.commoncriteriaportal.org/public/files/epfiles/0299a.pdf>).

5. PriceWaterHouseCoopers – PDF için Alman Vergi Kanunu Uyumluluğu Onayı

a. Alman vergi yasası, vergi iadesi alabilmek için ibraz edilen faturaların elektronik ortamda sunulmasına izin veriyor.

b. Bunun için:

(1) Fatura düzenleyen tarafın kimliğinin doğrulanmasının ve

(2) Fatura içeriğinin bütünlüğünün garanti edilmesi şartı konuluyor.

c. Dökümanın içeriğinin bütünlüğünün ve imzalarının doğruluğunun en az 10 sene ulaşılabilir olması gerekmekte.

6. ABD Department of Defense Sertifikasyonu

http://jitc.fhu.disa.mil/pki/vendor/adobe_acrobat_7_0_pro.html

d. ABD Savunma Bakanlığı'ndaki çoğu program kimlik kontrolü, gizlilik, inkar edilememe ve erişim kontrolü gibi güvenlik servislerine ihtiyaç duyar.

e. Bu sertifika, açık anahtar altyapısı kullanan yazılımların ABD Savunma Bakanlığı uygulamalarında kullanılabilmesi için gerekli şartları sağlayıp sağlamadığını belgeler.

f. Adobe Acrobat Reader ve Professional 7.0 ve üst versiyonlarının, döküman imzalama ve şifreleme için ABD Savunma Bakanlığı nezdinde gerekli şartları sağladığı bu sertifika ile belgelenmiştir.