İş Odaklı Bakış Açısıyla Açık Anahtar Altyapısı

Bu yazı, ticari bir uygulama ortamında Açık Anahtar Altyapısının (AAA) kullanımını incelemektedir. Bunun için kurumların güncel güvenlik kaygılarından başlayarak bilgi güvenliğinin konuyla ilgili bileşenleri gözden geçirilmektedir. Yazıda elektronik ortamdaki riskleri azaltmaya yarayan ana güvenlik hizmetleri de tanımlanmıştır. Böylece kurumların ihtiyacı olan bilgi güvenliğine AAA tarafından getirilen sistematik ve entegre çözümler açıklanmış olmaktadır.

İş Dünyasının Bugünü

Son yıllarda e-ticaret kavramı ve uygulamaları geliştikçe ortaya konan yeni iş modelleri bir çok değişikliğe sebep olmakta. Satıcılar, tedarikçiler, müşteriler ve çalışanlar arasındaki iletişim rekabet açısından geçmişe göre çok fazla önem kazandı. Fikri mülkiyet hakları çok değerlendi ve bu hakları korumak artık çok daha önemli hale geldi. Finans, sağlık ve eğitim sektörleri için çıkartılan birçok kanun bilginin gizliliğinin ve güvenliğinin sağlanmasını zorunlu hale getirdi.

Bu değişikliklerin yanı sıra e-ticaret ile ilgili riskler de gündeme gelmekte. E-ticaret sistemleri kurmak veya kullanmak isteyen firmaların da tüketicilerin de en önemli kaygısı, ticari işlemlerde veya firmaların bilgisayar sistemlerindeki güvenlik açıkları sebebiyle maddi kayıplara uğrama olasılığı. Bir güvenlik açığı sadece yapılan e-ticarete duyulan güveni azaltmaz aynı zamanda ilgili firmanın itibarını da erozyona uğratır. E-ticaretle ilgili riskler sabotaj, hırsızlık, sahtekarlık, veri gizliliği ve bütünlüğünün bozulması ve güvenlik açıkları olarak sıralanabilir.

Bir çok uygulamada bilginin gizliliği en önemli nokta olarak görülmektedir. Bir kurum, kişilerin (örneğin müşterilerinin) şahsi bilgilerini güvenli olarak koruma sorumluluğunu alınca hem çok dikkatli davranmanın getirdiği yükü kaldırmak, hem de bu işin beraberinde gelen riskleri kabullenmek zorunda kalır. Bu risklerin arasında yetkili tarafların istedikleri anda bilgiye ulaşmasını sağlamak detaylı ve iyi düşünülmüş bir planlama gerektirir. Geleneksel ticari uygulamalarda benzeri riskleri en aza indiren, kanuni, mali ve fiziksel koruma öğelerinden oluşan bir altyapı zaten mevcuttur ve bütün bileşenleri çok iyi tanımlanmış ve herkes tarafından anlaşılmıştır. Hassas ve önemli bilgilerin elektronik ortamdaki iş akışına dayanan e-ticaret modellerinde de aynı risk denetimini sağlayacak altyapı ve güven sağlama sistemlerinin kurulmasına ihtiyaç vardır.

Bilgi Güvenliği

Günümüzde çoğu elektronik haberleşme yöntemi özel olarak korunması istenmemişse gizli yada güvenli değildir. Elektronik ortamdaki bilgiler taklit edilmeye, değiştirilmeye ve kopyalanmaya çok kolaya maruz kalabilmektedir. Bir ağ ortamında depolanan veya bir kullanıcıdan diğerine giden bilgi yetkisiz erişime ve yanlış yönlendirmeye karşı korunmalıdır. Bu nedenle elektronik ortama geçme tercihini yapan her kurum için ağ güvenliği en önemli konudur. Bilgi güvenliği, elektronik ortamdaki riskleri makul düzeye çekmek için üç tane çok önemli yaklaşıma ihtiyaç duyar:

- Kullanılabilirliği sağlamak
- Saldırıların tespiti ve engellenmesi
- Ağlar için sınır koruması

Bu yazıda tartışılmakta olan sayısal imza ve Açık Anahtar Altyapısı (AAA) bu yaklaşımlardan birincisi tarafından ele alınmaktadır. Kullanılabilirliği sağlamak, sisteme entegre bir planın uygulamaya konmasını (güvenlik prensipleri) ve bu planın başarılı bir şekilde uygulanmasını destekleyecek altyapının geliştirilmesini beraberinde getirir. Bu güvenlik planı insanları, iş süreçlerini, kurumun teknolojisini ve yapısını göz önüne almalı ve bu parçaların güvenli e-ticaret için nasıl bir etkileşim içinde çalışacağını ortaya koymalıdır. Kurulan altyapı, veri gizliliği ve bütünlüğü, kimlik doğrulama, inkar edememezlik, bilginin erişilebilirliği gibi hizmetleri sağlamalıdır. Bu güvenlik hizmetleri elektronik ortamdaki risklerin azaltılmasını mümkün kılar. Kullanılabilirliği sağlamak ayrıca yeni iş fırsatlarının ortaya çıkarılabilmesini de sağlar. Böylece daha önceden çok riskli bulunan iş süreçleri de e-ticarete uygun hale getirilebilir.

Açık Anahtar kriptografisi kişiye özel bir bilginin herkese açık bir bilgiyle tamamlayıcı eş olarak kullanılmasını sağlar (özel-açık anahtar çifti). Böylece bilginin ortaya çıkma tehlikesi olmadan güvenli haberleşme yapılabilir. Haberleşmedeki taraflardan her biri kendi özel anahtarını (kişiye özel bilgi) korur ama açık anahtarını(herkese açık bilgi) kendisiyle haberleşmek/iş yapmak isteyen herkesin rahatça erişebileceği bir şekilde yayınlar.

Açık Anahtar Altyapısı

AAA kendisine özgü yapısıyla bilgi güvenliğine sistematik bir yaklaşımın gerekliliğini savunur. AAA güvenlik hizmetlerine duyulan ihtiyaçlara tek tek cevap vermek yerine bütün güvenlik hizmetlerini entegre bir şekilde sunmayı sağlayan bir altyapı oluşturur. Böyle bir sisteme yapılacak yatırımın uzun vadeli getirilerinden biri de gelecekte temel altyapıya hiçbir değişiklik yapmadan yeni uygulamaların sisteme eklenebilmesidir. Buna rağmen bir altyapının yapılan yatırımı karşılaması altyapıyı kullanan uygulamalara çok bağlıdır. AAA uygulamaları ile ilgili tablo bu alandaki muhtemel kazançların ne kadar büyük olabileceğini gözler önüne seriyor. Elektronik güvenlik altyapısının, tıpkı elektrik veya telefon şebekesi gibi, iş dünyasının hedeflerini (karı arttırmak, maliyetleri düşürmek, yönetmeliklere uyum sağlamak, riski azaltmak vb) gerçekleştirmek için çok gerekli hale geldiği görülmekte.

Benzersiz Teknoloji

Bu dokümanın asıl amacı AAA'nın e-ticaret iş modelleri açısından güvenlik konularını nasıl çözüme kavuşturduğunu açıklamaktır ama bunu yapabilmek için ilk önce kullanılan teknolojinin en önemli iki öğesinin kısaca açıklanmasında fayda var. AAA, güvenlikle ilgili ihtiyaçların tümüne çözüm sunan matematiksel yapılar üzerine inşa edilmiştir. Açık anahtar kriptografisi, rasgele üretilmiş olan ve birbirine benzemeyen sırların (sırların olmadığı yerde güvenlik olmaz!) sistemdeki her kişi ve varlığa (tüzel kişilik, bilgisayar vb) atanmasını mümkün kılar. Bu teknolojik gelişme ortaya çıkmadan önceki yıllarda güvenli haberleşme yapabilmek için sırrın bilgi değişimine katılan tüm taraflarca bilinmesi gerekliydi. Taraflar daima karşı tarafın sırrı korumak için ne kadar çaba harcadığından şüphe duyardı. Buna ek olarak, haberleşmek isteyen çok sayıdaki kişiye sırrın güvenli bir şekilde dağıtılması büyük gruplar için pratik olmayan bir hale geliyordu.

Açık Anahtar kriptografisi kişiye özel bir bilginin herkese açık bir bilgiyle tamamlayıcı eş olarak kullanılmasını sağlar (özel-açık anahtar çifti). Böylece bilginin ortaya çıkma tehlikesi olmadan güvenli haberleşme yapılabilir. Haberleşmedeki taraflardan her biri kendi özel anahtarını (kişiye özel bilgi) korur ama açık anahtarını (herkese açık bilgi) kendisiyle haberleşmek/iş yapmak isteyen herkesin rahatça erişebileceği bir şekilde yayınlar. 1970'lerin ortalarından beri bilimsel dünyada bilinen ve çok dikkatlice incelenmiş olan bu yönteme Açık Anahtar Kriptografisi adı verilir.

AAA'nın sağladığı birçok güvenlik hizmetinin kalbinde "sayısal imza" kavramı yer alır. Geleneksel olarak kullandığımız "ıslak imza" adı da verilen, elle atılan imzalara eşdeğer olacak şekilde tasarlanan sayısal imza, yukarıda bahsedilen kişiye özel benzersiz özel anahtarın (sırrın) kullanımı esasına dayanır. Sayısal imzalama işleminde özel anahtar matematiksel bir formül içinde kullanılarak, özel anahtar ile imzalanan veri arasında bir bağlantı oluşturulur. Haberleşmek isteyen herkesin ulaşabileceği şekilde yayınlanan, özel anahtarın tamamlayıcı eşi olan açık anahtar sayısal bir sertifika şeklinde kullanılarak veriyi imzalayan kişinin kimliğini doğrulamak için kullanılabilir. Daha ileride bu yapının elektronik ortamda ticari ilişkiler kurmak ve yürütmek için ne kadar vazgeçilmez olabileceğini göreceğiz. Sayısal imzanın kullanımı birçok ülkede gerekli yasal düzenlemelerle desteklenmiştir. A.B.D'de 2000 yılında ve AB'de 2001 yılında kabul edilen sayısal imza kanunları bu eğilimin göstergeleridir.

Sayısal imzanın kullanımı birçok ülkede gerekli yasal düzenlemelerle desteklenmiştir. A.B.D'de 2000 yılında ve AB'de 2001 yılında kabul edilen sayısal imza kanunları bu eğilimin göstergeleridir.

Altyapının Önemi

Daha önce de bahsedildiği gibi bilgi güvenliği hizmetlerinin yerine getirilebilmesi için bir altyapıya gereksinim duyulur. Altyapı, güvenlikle ilgili parçaların birbiriyle uyum içinde çalışmasını garanti eden ve bu parçaları bir arada tutan büyük resmin çerçevesidir. Örneğin, bir ticari ilişkide bir kullanıcıyı ve onun özel anahtarını birbirine bağlayan güvenilir bir altyapı yoksa kullanıcının kimliğini ispat etmek için bu özel anahtarı kullanmasının pek bir değeri yoktur. Bu ilişkide kullanıcının kimliğini özel anahtarına bağlı olarak tespit etmek ancak altyapının verdiği garanti dahilinde sağduyulu bir davranış olarak kabul edilebilir. Altyapı bunun için gereken hizmetleri güvenilir bir şekilde sağlamalıdır. İyi inşa edilmiş bir altyapıdaki hizmetler kolay elde edilebilir, güvenilir ve şeffaf olmalıdır. Örneğin, elektrik şebekesinin sunduğu hizmette aboneler hizmetin nasıl sağlandığını bilmek zorunda değildirler ama hizmetin güvenilir olarak verildiğini ve elektrikli cihazlarda kolayca kullanılabileceğini bilirler.

AAA ismini Açık Anahtar Kriptografisinden almasına rağmen sağladığı bazı hizmetlerin kökleri teknik olarak kriptografinin bu dalının dışındaki dallardan gelir. AAA bu bilinen tekniklerin en iyilerini kapsar. AAA, sayısal imza ve anahtar yönetimi için kullanılan açık anahtar kriptografisinin ve şifreleme için kullanılan simetrik kriptografinin bir bütün olarak kullanılmasını sağlar.

Bir Açık Anahtar Altyapısı, açık-özel anahtar çiftlerini kullanarak sadece verdiği hizmetleri inşa etmez, aynı zamanda bu hizmetleri veren güvenilir altyapıyı da kurmuş olur. Kullanılan yöntemler ve metodoloji sisteme duyulan güveni arttırır. Bir açık anahtar altyapısı tasarım olarak güvenilir bir mimari üzerine inşa edilmiş, birbiriyle uyum içinde çalışan hizmetlerden oluşur. Uygulama programlarına sunulan hizmetlerin, iletişim yöntemlerinin ve protokollerin iyi anlaşılmış bileşimi bir Açık Anahtar Altyapısını oluşturur.

Güvenli E-Ticaret Hizmetleri

Daha önce tanımladığımız güvenlik hizmetleri özellikle ağ üzerinde ticaret yapmayla ilgili riskleri en aza indirmek için tasarlanmıştı. Dış dünya ile bağlantısı olmayan ağlar bile incelenmesi gereken riskler taşır. Günümüzde birçok kişiye göre kurum içinden kaynaklanan saldırılar şirketlerin kaynakları için en büyük tehdidi oluşturmaktadır. Her güvenlik hizmeti desteklemek üzere tasarlandığı ticari amaç kapsamında tarif edilebilir.

Kimlik doğrulamanın çok önemli olduğu çalışanların şirket ağına uzaktan erişimi, e-posta hizmeti, endüstriyel web portalleri üzerinden müşteri ve tedarikçilerin veritabanına erişimi gibi uygulamalarda sayısal imzanın kullanılması kaçınılmazdır.

Kimlik Doğrulama

Bir ticaret ortamında en önemli temel ihtiyaç, ticari işleme taraf olan kişinin, tüzel kişiliğin, uygulama sunucusunun, müşterinin veya tedarikçinin kimliğini kesin bir doğrulukla tespit etmektir. Elektronik ortamda bu güvenlik hizmetine kimlik doğrulama adı verilmektedir. Örneğin, bir alışveriş sırasında kredi kartı numarasını ağ üzerinden gönderen kullanıcı, kredi kartı numarasını kendi şahsi harcama zevkleri için çalmak isteyen bir sahtekar ile değil güvenilir bir tüccarla haberleşiyor olmak ister. Eğer kullanıcı bu tüccarın kimliğini doğrulayabilirse kredi kartıyla ilgili bilgilerini gönül rahatlığıyla gönderebilir. Günümüzde bir açık anahtar altyapısı bu hizmeti online perakende alışveriş ve online bankacılık için hemen hemen her yerde verebilir. SSL ve TLS gibi haberleşme protokollerinin kullanımı kullanıcılara perakende satış veya bankacılık hizmeti veren tarafın güvenilirliği ile ilgili daha fazla güvence verir. Bu protokoller her iki yönde de güvence vermek için kullanılabilir. Kimlik doğrulamanın çok önemli olduğu çalışanların şirket ağına uzaktan erişimi, e-posta hizmeti, endüstriyel web portalleri üzerinden müşteri ve tedarikçilerin veritabanına erişimi gibi uygulamalarda sayısal imzanın kullanılması kaçınılmazdır. AAA kimlik doğrulamayı sağlamak için erişim talebinde bulunan kişi ile sayısal imzanın bağlantısını güvence altına alır ve bu bağlantının doğrulanması için gereken yolu sağlar.

Simetrik kriptografi haberleşen tüm tarafların aynı gizli anahtarı bilmesini gerektirir. Açık anahtar kriptografisi bu gizli anahtarın hızlı ve verimli bir şekilde dağıtılmasını mümkün kılar. Gizli anahtarlı kriptografi (simetrik) büyük miktarda verinin şifrelenmesi için çok daha etkin bir tekniktir.

Gizlilik

Gizlilik ticari işlem yapılan her sistemde çok önemli bir rol üstlenir. İş planları, para hareketleri, fikri mülkiyet hakları, şahsi kayıtlar, çalışan kayıtları vb gibi hassas bilgiler meraklı gözlerden çok iyi bir şekilde korunmalıdır. Veri bir ağ üzerinde hareket ederken (örneğin bir iş ortağına, müşteriye e-posta olarak giderken) veya durağan haldeyken (örneğin uygulama sunucusu üzerindeki bir veritabanında kayıtlıyken) korunmalıdır.

Şifreleme, gizliliği sağlamak için kullanılan matematik temelli bir yöntemdir. Daha önceden de belirtildiği gibi bunu sağlamak için simetrik anahtarlı teknikler kullanılır çünkü bu teknikler asimetrik (açık anahtarlı) olanlara göre çok daha hızlı ve verimlidir. Şifrelemenin

yaygın olarak kullanımı için şifrelemeyi kullanacak sistemlerle uyumlu bir anahtar dağıtım sistemine sahip olmak gereklidir. Açık anahtar kriptografisi anahtarların güvenli dağıtımı için ölçeklenebilir tek seçenektir. Bir AAA sistemi gizliliği desteklemek için her iki tekniği de kullanır.

Gizlilik sadece verinin şifrelenmesinden daha geniş bir anlamda yorumlanabilir. Gizlilik bilgiye yetkisiz erişim yapılamamasını da içerir. Bu daha geniş bağlamda, veri gizliliği hizmetleri kimlik doğrulama hizmetleri ile beraber, bir kurumun kişilerin mahremiyeti ve şahsi bilgilerinin gizliliğinin korunması ile ilgili kanunlara ve yönetmeliklere uyumunu düzenleyen stratejik planının bir parçasını oluşturur. AAA bu gereksinimleri karşılamaya yardımcı olmak için çok uygundur.

Veri Bütünlüğü

Veri bütünlüğü depolanan veya iletilmekte olan bilginin yanlışlıkla veya bilerek değiştirilip değiştirilmediğini bulmaya yarayan bir hizmettir. Örneğin elektronik ortamdaki bir iş teklifini düşünün. Tanesi 50 USD olan bir maldan 50 adet alma teklifi iletişim sırasında değiştirilerek 50,000 adetlik bir teklife dönüşememelidir. AAA verinin, kimliği bilinen göndericiden çıktıktan sonra yolda değiştirilmediğini veriyi alan tarafa ispatlayabilmek için sayısal imzayı kullanır. Kötü niyetli saldırıların olmadığı bir durumda bile verinin doğruluğu hakkında kesin olarak bilgilendirilmek çok önemli bir ticari gereksinimdir ve açık anahtar teknolojisi için çok uygun bir kullanım alanıdır.

AAA tarafından verilen ve yönetilen bir sayısal sertifika bir varlığı/kişiyi bir grup yetkiyle ilişkilendirmek için kullanılabilir ve erişim yönetiminde çok değerli bir araç olabilir.

İnkar Edememe

Üçüncü bir şahısa ispat edilebilen veri bütünlüğü ve kimlik doğrulamaya inkar edememe hizmeti denir. Bu hizmet haberleşmede alıcı tarafa, gönderen tarafın onayladığı, imzaladığı yada oluşturduğu bir doküman veya işlemi inkar edemeyeceğinin garantisini verir. Bu özellikle parasal işlemlerde çok önemlidir. Örneğin kendisine gelen faturayı ilgili hizmeti isteyen taraf olmadığını söyleyerek ödemeyi reddeden bir kişiyi tespit etmek bu hizmet sayesinde mümkün olabilir. Hizmeti sağlayan taraf müşterinin gerçekten hizmeti istediğini ve kullandığını sağlam kanıtlarla ispat ederek faturanın geçerliliğini ortaya koyabilir. Açık anahtar kriptografisinin prensiplerini hatırlayacak olursak, özel anahtar (ve bu anahtarla atılan sayısal imza) sadece bir kişi tarafından bilinir. İnkar edememezlik, açık anahtar altyapısının bu özelliği uygun prensiplerle ve süreçlerle beraber kullanılarak sağlanabilir. Bu yüzden sayısal imza kullanarak bağlayıcı sözleşmeler imzalamak da mümkün olur.

Sayısal imzalar inkar edememezlik hizmetini vermez ama bu hizmetin kurulabilmesini sağlar. Teknoloji inkar edememezlik hizmetini sağlamak için gereken bileşenlerden sadece birisidir. İnkar edememezliği sağlamak için elle atılan imzalar da (ıslak imza) olduğu gibi uygun prensip ve süreçler kullanılmalıdır ve bazı durumlarda bunun için insanların işin içine girmesi gerekebilir.

Hizmet sağlayıcı inkar edememezlik hizmeti sağlayan bir sistem kullanarak bir hizmet talebinin gerçekten yapıldığını aksi iddia edilemez bir şekilde ispat eder ve bu hizmet için kestiği faturanın meşruluğunu ortaya koyar.

Yetki Yönetimi

Yetki yönetimi bir ağ üzerinde saklanan hassas veriye erişimi düzenleyen prensiplerin güvenli bir şekilde yönetilmesi hizmetidir. Bu kişisel sağlık veya finans bilgisinin gizliliğini veya fikri mülkiyetleri ve rekabetçi ticari planları korumayı güvence altına almak için önemli olabilir. AAA tarafından verilen ve yönetilen bir sayısal sertifika bir varlığı/kişiyi bir grup yetkiyle ilişkilendirmek için kullanılabilir ve erişim yönetiminde çok değerli bir araç olabilir. Böylece bir yönetici bir varlığın/kişinin erişim yetkilerini ona erişim izni vermeden önce tespit edebilir.

Altyapının Omurgası

Altyapının sorumluluğunun hizmetleri güvenilir bir şekilde sunmak olduğunu hatırlarsak aklımıza bir çok soru gelecektir. Bir şahısla anahtarının bağlantısını kim kurar? Bir varlığın/kişinin kimliği nasıl doğrulanır? Bir kişinin/varlığın özel anahtarının açığa çıktığı nasıl anlaşılır? Bu soruların birçoğunun cevabı temel bir ticari ihtiyaç olan güvendir. Açık anahtar altyapısı güven ortamını oluşturmak için temel olarak Sertifikasyon Makamına, Kayıt Makamına ve prensiplere dayanır.

Açık anahtar altyapısı güven ortamını oluşturmak için temel olarak Sertifikasyon Makamına, Kayıt Makamına ve prensiplere dayanır.

Sertifikasyon Makamı (SM)

Sertifika Makamı AAA'nın kalbidir ve sertifika sahiplerinin kimliğini açık anahtarı ile ilişkilendirme işinden sorumludur. Bu ilişkinin doğruluğunu ispat etmeye yarayan kanıtlar uygulanan güvenlik prensipleri ile belirlenir. Bu prensipler bir kurumun işlerini yürüttüğü ortamla ilgili olarak yaptığı risk ölçümlemesini temel alır. Son kullanıcı kayıtları için yüz yüze görüşme yöntemine ihtiyaç duyulabileceği gibi sadece e-posta adresi gibi herkesin açıkça erişebileceği bir bilgi de bu kayıt için yeterli bulunabilir. Açık anahtar ile kullanıcı arasında kurulan bağın değeri bu kayıt süreci tarafından belirlenir. AAA'nın kuvvetli yönlerinden birisi de en kısıtlayıcı gereksinimler de dahil olmak üzere çoklu kayıt modellerini desteklemesidir.

SM ayrıca sertifikaların iptal edilmesi sorumluluğunu da taşır. Çoğu sertifika yayınlanır ve sertifika ömrü boyunca geçerli kalır ama bazı durumlarda sertifikayla ilişkili yetkilendirmeler geçersiz hale gelebilir. Bu bir banka hesabının kapatılması veya iş değiştirme gibi normal faaliyetler sonucunda olabilir veya özel anahtarın ele geçirilmesi ihtimali gibi durumlar iptali gerektirebilir. İptal işlemlerinin nasıl yürütülebileceğini gösteren çeşitli modeller vardır ama bunlar bu dokümanın kapsamı dışında kaldığı için ele alınmamıştır.

Kayıt Makamı (KM)

Bir Kayıt Makamı kullanılarak aralarında son kullanıcı kayıtları da bulunan yönetimle ilgili iş yükleri Sertifika Makamından alınabilir. Bu özellikle kullanıcı kaydı için yüz yüze görüşme şartı koşan, büyük ve coğrafi olarak dağınık bölümleri olan kurumlar için kullanışlıdır. Bütün kullanıcıları şirket merkezinde bulunan kayıt merkezine gitmeye zorlamak yerine kayıt makamları kurumun bölge ofislerine kurularak kayıt işlemi kolaylaştırılabilir.

AAA Prensipleri

Bir AAA'yı etkin olarak gerçeklemek için AAA'yı yönetmek için ortaya konmuş bir takım prensiplerin ortaya konması gereklidir. Bu prensipler Sertifika Uygulama Kuralları (SUK) ve Sertifikasyon Prensipleri (SP) gibi dokümanlarda dile getirilir. Bir SUK, sertifika verme ve yönetme işlerindeki uygulamaları tanımlar ve AAA yönetimini idare eder. Bu doküman hizmet önerilerini, sertifika yaşam çevriminin yönetimini, işlemlerle ilgili bilgileri vb içerebilir. Bunlardan başka SUK, Sertifika Makamının yükümlülüklerini ve sorumluluklarını

tarif eden yasal bir çerçeve sunar.

Bir SP dokümanı ise bir sertifikanın ortak güvenlik ihtiyaçları olan belirli bir grup kullanıcıya veya uygulamaya uygulanabilirliğini belirten kuralları içerir. SP genelde üst seviyedeki prensip ihtiyaçlarını ortaya koyarken SUK, altyapının işleyişini detaylı ve kapsamlı olarak ortaya koyar ve teknikleri ve süreçleri anlatır.

Sonuç

Günümüzde iş modelleri güvenlik modellerini kullanmakta. Bütün kurumlar gelirleri arttırma, giderleri azaltma, yasal ve endüstriyel düzenlemelere uyma ve riski azaltma konusunda baskıya maruz kalmakta. Bu konular ticareti elektronik ortamda yürütme isteğiyle birleşmekte. Kimlik doğrulama, gizlilik, veri bütünlüğü ve inkar edememezlik gibi güvenlik hizmetleri bu hedeflere ulaşmak için kurulduktan sonra dikkatin, ticaret süreçlerinin başarısını destekleyebilecek bir uygulama planına çevrilmesi gerekir. AAA, ticari uygulamaların ihtiyaç duydukları güvenle yürütülebilecekleri dış sistemlerle entegre bir çerçeve sunmaktadır. AAA elde edilebilen en iyi kriptografik teknikler üzerine kurulmuştur ve günümüzün iş dünyasındaki ihtiyaçlara kapsamlı bir yaklaşım sunar.

AAA Uygulamaları Listesi

Pazar	Uygulama Sınıfı	Örnek Uygulama
Finans Hizmetleri	Ödemede kimlik doğrulama	Hisse senedi alımları Öğrenci bursunun havalesi
	Erişim kontrolü	Internet bankacılığı
	Güvenli mesajlaşma	E-posta
	Güvenli doküman saklama / erişim	Elektronik tapu/ ipotek
	Elektronik noter	Vekaletnameler, Sözleşmeler
	Teminat Mektubu	İşlemlerin güvenli yapılması
Sigorta	Sayısal imza	Online • Fiyat teklifi • Başvuru • Onay
	Ödemede kimlik doğrulama	Online ödemeler • İkramiyeler • Geri ödemeler
	Doküman yönetimi	Erişim denetimi, sürüm yönetimi
	Erişim denetimi	Müşteri kayıtlarına yetkili erişim
Sağlık	Ödemede kimlik doğrulama	Masraf ödemeleri
	Güvenli mesajlaşma	Kayıtların e-postayla gönderilmesi
	Güvenli doküman saklama / erişim	Hasta kayıtlarına erişim, işleme ve aktarma
	Doktor kimlik kartı	Sadece doktorların kullanabileceği programlara erişim
Devlet	Nüfus Cüzdanı	Pasaport, ehliyet
	Erişim denetimi	Bina giriş denetimi
	Ödemede kimlik doğrulama	Emekli maaşı ödemeleri
	İhale yönetimi	Fiyat tekliflerinin alınması
	Ulaşım	Temassız kartlarla ödeme
	Yönetim	Güvenli e-posta ile vatandaşa bilgi verme
B2B	Güvenli doküman saklama / erişim Erişim denetimi Satın alma Sayısal İmza	Online kataloglar Online sözleşme imzalama Güvenli para transferi

*Bu makale **WWW.PKIFORUM.ORG** tarafından Nisan 2002'de yayınlanan "PKI Basics - A Business Perspective" adlı whitepaper'dan tercüme edilmiştir.*