Kurumlarda Kriptografik Anahtar Yapıları ve Kullanımları Üzerine Bir İnceleme

Mehmet Gülyurt[1], Ediz Şaykol[1]
[1] Beykent Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ayazağa, İstanbul

Özet: Günümüz bilgi teknolojileri dünyasında bilginin her geçen gün öneminin ve yaygınlığının artması, bilgiye her noktada erişilebilme isteklerinin artışa geçmesi ile beraber bu hususlara izin verecek olan teknolojik gelişmeler hızla gelişmektedir. Eski çağlardan bu yana bilginin korunması beraberinde bir çok çözümü getirmiş, Kriptoloji ise günümüze kadar en efektif şekilde kabul görmüş çözüm yolu olarak kendini ispatlamayı başarabilmiştir. Kriptoloji, bilginin korunmasında doğal bir antikor görevi görmüş, bilginiz nerede olursa olsun kontrolünüz dışındaki kişilerce erişilebilmesini engellemeyi başarmıştır. Artan saldırılar karşısında bilgiye anlık koruma sağlayan çözümler yetersiz kalmış, özellikle büyük kurumların sahip olduğu verilerin korunması için bilgilerin şifrelenmesi vazgeçilmez bir çözüm olmuştur. Bilgilerin korunmasında kullanılan kriptoloji her ne kadar etkili bir çözüm olarak görünse de yönetimi ve uygulanmasında yapılacak hatalar bu etkili çözümü etkisiz hale getirebilmektedir. Bilgilerin şifrelenmesinde göz önünde bulundurulması gereken en önemli hususların başında şifreleme anahtarlarının güçlü ve güvenilir olması, şifrelenen bu anahtarların kontrol altında tutulması gelmektedir. Bu çalışma, şifreleme anahtarlarının kullanım alanlarına göre nasıl yönetilmesi gerektiğini örneklerle açıklamaktadır.

Anahtar Kelimeler: Şifreleme Anahtarları, Anahtar Yönetimi, Şifreleme Teknolojileri, Donanım Güvenlik Modülleri

A Survey On Enterprise Key Management Structures and Their Usage

Abstract: Today with the prevalence and accessibility of information and data has become more important than yesterday. Based on this to protect information becomes more difficult then yesterday. One of the most effective ways to protect the data is using cryptology. Cryptology is the most reliable way to protect data from past to present. However, this effective solution depends on some important points. Management of the encryption key one of the most important things about protecting data with encryption solutions. If a ten years old key is used to protect data, this does not mean that it is safe. First of all, using the most effective solution to protect data depends on the encryption policies. One should have enough capabilities to change the encryption key without difficulty and report that which application is using those keys on the enviroment. In this project we present expressions about how to manage the encryption key including enterprise levels along with sample usages, procedures and policies.

Key Words: Encryption Keys, Key Management, Encryption Technologies, Hardware Security Modules.

1. Giriş

Günümüz bilgi teknolojileri dünyasında bilginin her geçen gün öneminin ve yaygınlığının artması, bilgiye her noktada erişilebilme isteklerinin artışa geçmesi ile beraber bu hususlara izin verecek olan teknolojik imkânlar her geçen gün hızla gelişmektedir. Eski çağlardan bu yana bilginin korunması beraberinde birçok çözümü getirmiş, Kriptoloji ise bunlardan günümüze kadar en efektif olan ve kabul görmüş çözüm yolu olarak kendini ispatlamayı başarabilmiştir.

Kriptoloji bilginin korunmasında doğal bir antikor görevi görmüş, bilginiz nerede olursa olsun bunun kontrolünüz dışındaki kişiler tarafından erişilebilmesini engellemeyi başarmıştır. Bilgiye artan saldırılar karşısında anlık koruma sağlayan çözümler yetersiz kalmış, özellikle büyük kurumların sahip olduğu verilerin korunması için bilgilerin şifrelenmesi vazgeçilmez bir çözüm olmuştur. Bilgilerin korunmasında kullanılan kriptoloji her ne kadar etkili bir çözüm olarak görünse de yönetimi ve uygulanmasında yapılacak hatalar bu etkili çözümü etkisiz hale getirebilmektedir. Bilgilerin şifrelenmesinde göz önünde bulundurulması gereken en önemli hususların başında şifreleme anahtarlarının güçlü ve güvenilir olması, şifrelenen bu anahtarların kontrol altında tutulması gelmektedir. [2] Örneğin bundan 10 sene önce kabul görmüş olan bir şifreleme algoritmasının günümüzde geçerliliği kalmamış, bu algoritma ile şifrelenen bilgiler rahatlıkla deşifre edilebilir duruma gelmiştir. Diğer bir husus olan anahtarların yanlış şekilde saklanması, anahtarların kontrolünüz dışına çıkması manasına gelir. Anahtarların başka kişilerce erişilebilir olması bilgilerinize zararlı kişilerin erişim riskini arttıracaktır.

Bütün bu hususlar doğrultusunda şifrelenen bilgilerin güvenliğini sağlamak her zaman yönetilebilir kılmak için bazı yöntem ve standartlara ihtiyaç duyulmuştur. Bu standartlar temel olarak bilgileri şifrelemek için kullanmış olduğunuz anahtarların nasıl oluşturulacağı, hangi kişilerin bu anahtarlara erişim yetkilerinin olması gerektiği, anahtarların gerektiğinde hızlı bir şekilde değiştirilmesinin planlarını ve bu anahtarlar ile şifrelenmiş verilere ilerleyen zamanlarda nasıl erişileceği gibi politikaları içermektedir.

Fakat ne yazık ki bugün şirketlerin en büyük problemi arasında kurumlarında kullanmış oldukları şifreleme anahtarlarının ve kullanım yetkilerinin kimlere ait olduğunu bilmemeleri ya da denetim altında tutmamaları gelmektedir. Özellikle binlerce şifreleme anahtarlarının bulunduğu kurumlar, anahtar yönetiminin yanlış yapılması sonucu oluşacak riskleri göze alamadıkları için bilinen birçok sorunu göz ardı etmektedir.

Şifreleme politikaları bilgilerin şifrelenmeye başlamadan önce belirlenmesi gereken en önemli hususlarından biridir. Anahtarlar ne kadar süre geçerli olacak, ne kadar sürede bir yenilenecek ya da kimin yönetiminde hangi amaç ile kullanılacak gibi bilgiler önemlidir. Bu duruma örnek olarak bilgi güvenliğini ve anahtar yönetimini belirli güvenlik standartları çerçevesinde (bkz. PCI DSS 2.0 Requirements 3 ve 4) yapan firmalar verilebilir. Bu firmalar bilgi güvenliğini sağlayan anahtarları önerilen prosedürler

eşliğinde belirli sürelerde değiştirmeleri gerekmektedir. [2] [3]

2. Temel Bilgiler

Şifreleme operasyonlarında kullanılan anahtarların yönetimi kullanıcıların ihtiyaçları ya da iş gereksinimleri doğrultusunda farklı kullanım alanlarını kapsayan bir kavramdır. Hangi tipte anahtar kullanımına ihtiyacınız olursa olsun, şifreleme nesnelerinin yönetimini belirlenmiş güvenlik politikaları dâhilinde yapılması gerekmektedir. Kripto anahtar yönetimi güvenlik politikalarınızın bir parçası olan kripto servislerinin kullanıma uyarlanması ile geliştirilmiş politikalar bütünüdür. En yaygın hali ile kripto anahtarlarının yönetimi aşağıdaki şekilde sınıflandırılabilir;

2.1. Güvenli Anahtar Yaşam Döngüsü

Bu alanda anahtarlara tüm yaşam döngüsü boyunca yapılacak olan operasyonların tanımları yer almaktadır. Bunlar;

- Anahtar ve Anahtar Çifti Oluşturma
- Anahtar Taşıma ve Paylaşım
- Anahtar Yedekleme ve Onarım İşlemleri
- Anahtar ve Anahtar Çifti Kullanımını İzleme ve Kontrol Etme (Süre ya da kullanım adedi kısıtlamalı)
- Anahtar Rotasyonu, Yenileme
- Meta Data Yönetimi (Örneğin anahtar yetkisinin şifreleme/deşifreleme'den sadece deşifrelemeye ayarlanması)
- Anahtarın İmha edilmesi ya da güvenli bir şekilde saklanılması

2.2. Güvenli Anahtar Saklama

Anahtarlar kullanımda olduğu sürece güvenli bir şekilde saklanmalıdırlar. Anahtarların saklanacağı alan ve buna ait koruma gereksinimleri anahtarların kullanım alanına göre güvenlik politikalarında belirtilmelidir. Anahtarlar genellikle özel olarak tasarlanmış donanımlarda saklanmalıdır. Kimlik denetiminde kullanılan akıllı kart ve usb-tokenlar, donanım güvenlik modülleri bu cihazlara verilebilecek örneklerdendir. [1]

2.3. Anahtar Kullanım Yetkisi

Anahtar kullanımı yalnız ve yalnızca yetkisi tanımlanmış olan uygulamalar ve kişilere sağlanmalıdır. Anahtara erişim kontrolleri, kullanıcıların yetkilerinin denetlenmesi ve gizliliğin korunması bu hususta kritik konuların başında gelir.

2.3.1. Sorumluluk

Anahtar kullanımına yönelik tüm değişikler, erişim ve kullanım istekleri kayıt altında tutulmalıdır. Kayıtlar güvenlik standartları doğrultusunda değiştirilemeyecek şekilde saklanmalıdır.

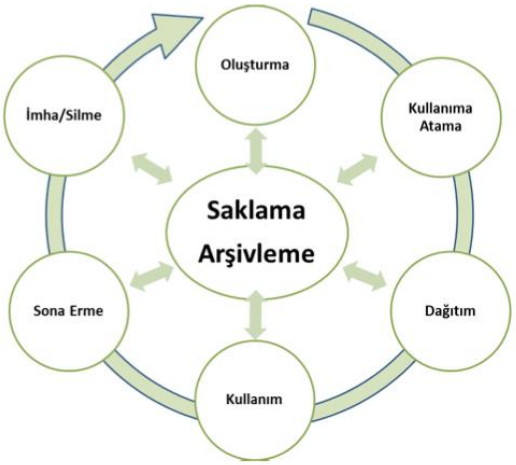
2.4. Anahtar Yönetimi ve Güvenlik Politikaları

Genellikle her bir kurum kendi özelliklerine yönelik güvenlik politikaları belirler. Fakat anahtar yönetimi gibi kritik bir hususta genel kabul görmüş standartların izlenmesi ve temel alınması politikalarınızın standardını yükseltecektir. Bazı standartlar kurumunuz için vazgeçilmez olması gerektiği gibi bir takım politikaların firmanız için değişikliğe

uğraması gerekebilir. Bu hususların derinlemesine tartışılıp standart dışı olan politikalarınızın yaratacağı olası risk ve etkiler değerlendirme altında tutulmalıdır.

2.5. Anahtar Yaşam Döngüsünde Dikkate Alınması Gereken Hususlar

Her bir şifreleme anahtarının, oluşturulmasından kullanım dışı kalmaları ve imha edilmelerine kadar belirli bir sırada yaşam döngüsü bulunur. Bu yaşam döngüsü Şekil 1'de verilmiştir. Bu adımları anlamak anahtar kullanımınızın planlanması açısından büyük önem taşımaktadır. Aşağıdaki önermeler NIST' in Anahtar Yönetimi Önerileri ve IEEE' nin Anahtar Yönetim Altyapısı standartları temel alınarak hazırlanmıştır. [1] [3]



Şekil-1. Şifreleme Anahtarlarının Yaşam Döngüsü

2.5.1. Anahtar Yaşam Döngüsünde Aktiviteler

Ön Operasyon: Ön aktivasyonun oluşması, doğrulama, tedarik etme ve yedekleme.
Operasyon: Aktif şifreleme, Deşifreleme, imzalama, doğrulama.
Kısıtlı Kullanım: Deşifreleme, doğrulama.
Operasyon Dışı: Kullanım dışı fakat kullanım için geri yüklenebilir.
Operasyon Sonrası: Güvenli bir şekilde imha edilir ve hiçbir şekilde geri dönüştürülemez.

2.6. Kurumsal Anahtar Yönetimi Güvenlik Politikalarını Uygulamak

Aşağıdaki tanımlamalarda uygulamalar işlem ve mesajlaşma tabanlı olmak üzere dağıtık kullanımdaki veriler ve durağan veriler şeklinde kategorilere ayrılmıştır. Bu çeşitlendirmedeki amaç bilgileri saklandığı ya da taşındığı alanlara göre değil, kullanım alanlarına göre sınıflandırarak etkilerini daha iyi kavramaktır. İşlem tabanlı uygulamalar, bilginin gerçek zamanlı değişimi ve paylaşımı esasına göre hareket eder. Kısaca özetlersek "istek ve yanıt" esasına göre çalışır (Örneğin ATM cihazlarından para çekmek.) Bilgi genellikle küçük boyutlarda, transfer eden uygulama tarafından kontrol edilir ve korunur.

Mesajlaşma uygulamaları ise sakla ve yönlendir esasına göre çalışır. Genellikle tam zamanlı olmayan ve otomatik durum değişimi gibi sonuçlar üretmeyen bu tip verinin belirgin özelliklerinden birisi ise dosya boyutlarının işlem tabanlı uygulamaların aksine büyük ya da küçük herhangi bir boyutta olabilmesidir. Bu tip bilgiler genellikle bazı spesifik yetki seviyeleri ile korunurlar.

Durağan bilgiler için ise verinin bulunduğu ya da saklandığı ortamda korunması esastır. Örnek verirsek, geniş çapta bir veri depolama çözümü, Storage Area Networks, istemcilerin ya da sunucuların üzerinde yer alan disk ya da

dosyaların korunması bu alanda verilecek örneklerin başında gelir. Bilgiler herhangi bir boyutta olabilir ve korunması çok uzun süreler geçerli olabilir. Bilgiler uygulama ya da erişim kontrol tabanlı bir şekilde kontrole tabi tutulurlar.

2.6.1. Dinamik Bilgilerin Korunmasında Anahtar Yönetimi

Dinamik bilgilerin iki temel veri tipi olduğu belirtmiştik. Buna göre işlem ve mesajlaşma tabanlı uygulamalarda anahtar yönetimi aşağıda belirtildiği gibi özetlenebilir.

2.6.2. İşlem Tabanlı Uygulamalarda Anahtar Yönetimi

İşlem tabanlı uygulamaların iki önemli tipi ödeme sistemleri ve elektronik bilgi değişimi (EDI- Electronic Data Interchange) uygulamalarıdır. Genellikle işlem tabanlı uygulamalarda kullanılan anahtar tipi simetrik anahtar tiplerinden oluşmaktadır. [14] Simetrik anahtarlar, kurumlar tarafından iletişim hatları ya da çalışılan ortak kurumlar için ayrı ayrı yönetilir. Her bir bağlantı için en az iki simetrik anahtar gereklidir. Bir tanesi bilgilerin şifrelenmesi diğeri ise veri bütünlüğü ve doğrulama için (HMAC). Bazı durumlarda dört adet simetrik anahtar kullanımı mümkündür, bu durumlarda her bir bağlantı için birer anahtar kullanılmaktadır. Bağlantı sayısı arttıkça anahtar yönetimi inanılmaz bir şekilde zor hale gelmektedir.

2.6.3. Mesajlaşma Tabanlı Uygulamalarda Anahtar Yönetimi

Mesajlaşma konusu elektronik posta, doküman işleme, web tabanlı uygulamalar gibi geniş çapta bir kullanım alanına sahiptir. Mesajlaşmada güvenlik önlemleri uygulama seviyesinde uçtan uca uygulanmaktadır. Uçtan uca olan uygulamaların doğası gereği bilginin simetrik bir anahtar ile korunması, alıcı ve gönderici adedinin yoğun ve yüksek olmasından dolayı tercih edilmemektedir. Bunun için anahtar yönetimi daha kolay ve rahat olan asimetrik şifreleme algoritmaları kullanılmaktadır. Örneğin Diffie-Hellman ya da RSA tabanlı anahtar değişimi. [3]

2.6.4. Durağan Bilgilerin Korunmasında Anahtar Yönetimi

Durağan bilgilerin genellikle yer aldığı veri tabanları, büyük veri depolama sistemleri tahmin ettiğinizden daha da fazla veri boyutuna sahip olabilmektedir. Bu bağlamda bilgilerin korunmasında anahtar yönetiminin kesintisiz bir şekilde gerçekleşmesinin önemi çok büyüktür. Anahtarların yönetimi, rotasyonu, oluşturulması gibi konular için önemle ve büyük bir titizlikle çalışmak gerekir.

3. Ortak Anahtar Yönetim Teknikleri

3.1. Merkezi Üretim

Simetrik ya da Asimetrik anahtarların merkezi bir şekilde üretilmesinin kullanım amaçları genel olarak şöyle sıralanabilir; Simetrik ya da Asimetrik anahtarlar ile şifrelenen bilgilere daha sonra ulaşmada herhangi bir problem yaşamamak, hangi bilginin hangi anahtar ile deşifreleneceği bilgisini tek bir noktada tutmak önemlidir. Anahtarların merkezi bir şekilde üretilmesi onların arşivlenmesini kolaylaştırır ve tek bir noktadan kolay ve güvenli bir şekilde yönetilmesini sağlar. Ayrıca son kullanıcıların sahip olduğu donanımlar

üzerinde güvenli bir şekilde simetrik ya da asimetrik anahtarların üretilmesinin mümkün olmayacağından ve anahtar üretiminde en önemli hususlardan birisinin gerçek bir rastgele sayı üreteci kullanmak olduğundan anahtar üretiminin merkezi bir donanım üzerinden yapılması önemlidir. [4] [5]

3.2. Anahtar Taşınması

Sisteminizin tüm noktalarında anahtarların kullanımını sağlamanız için üretilen anahtarların güvenli bir şekilde kullanılacakları uç noktalara taşınması gerekir. Bu amaç için bazı yöntemler geliştirilmiştir, bunlardan bazıları hem simetrik hem asimetrik anahtarların taşınması için kullanılacağı gibi bazıları sadece simetrik anahtar taşınmasında kullanılır. Bu yöntem kısaca anahtarın parçalara ayırılıp her bir parçanın ayrı bir kişinin kontrolüne verilerek taşınması esasına dayanır. Bu teknik genellikle bir noktada kullanılacak olan ana şifreleme ya da taşıma anahtarını aşağıda belirtilen şekilde taşınmaya uygulanmasıdır.

3.2.1. Anahtar Sarmalı (Şifreleme)

Birçok noktada şifreleme için kullanılan anahtarlar belirli dönemlerde değiştirilmelidir ayrıca taşıması için her seferinde parçalara ayrılması gerekebilir. Bu noktalarda anahtarı (simetrik ya da asimetrik) başka bir anahtar ile şifrelemek mümkündür.

3.2.2. Anahtar Türetme

Simetrik anahtarların üretilmesinde kullanılabilecek bir diğer yöntem ise gerekli olduğunda daha önce belirlenmiş gizli anahtar ve anahtar oluşturmada kullanılabilecek özgün bir nesne ile (seri no, ip adresi vs.) birlikte yeniden anahtar oluşturulmasıdır. Birçok anahtar yönetim şemalarında ortak paylaşılan sır (shared secret) anahtar paylaşım oturumuna başlamada ilk adımı oluşturur. Bu sayede uç sistemler anahtar iletişimine geçerler.

3.3. Anahtar Kullanımı Atanması

Bir çok kripto sistemi oluşturulan her anahtar için kullanım yetkisi tanımlayabilmektedir. Bu işlem ardından anahtarlar sistem yöneticisi ya da uygulamayı geliştiren kişinin kullanımına sunulur. Kullanıma sunulan bu anahtarların tutarlı bir şekilde ve tek bir amaç için kullanıldığından emin olunması gerekir. Aynı anahtar birden fazla sistem için kullanılamamalıdır. Anahtar yönetimini yapmış olduğumuz platform, anahtarın tek bir sistem için kullanıldığının emin olunması için gerekli politika ve izleme yöntemlerine sahip olmalıdır.

4. Önerilen Çözüm Yaklaşımı

4.1. Politika tanımlama

Anahtar yönetimi için politika tanımları yapmadan önce tanımlarda kullanılacak olan elementlerin kapsamını geniş ve açık bir şekilde tutmak gerekir.

4.2. Varlıkların Tanımı

Bu kategoride yapılacak olan tanımlar varlıkların detaylı bir şekilde açıklanmasını sağlayacak bilgilere sahip olmalıdır,
Bu tanımlarda yer alması gereken minimum bilgiler;
a) Anahtarlar
b) Depolanan Bilgiler - Yapısal (Örn: düzenli dosyalar, raporlar vs.)
c) Sertifikalar

d) Bağlantılar (Veri bağlantısı katmanı)
e) Belgeler ve işlemler
f) Bağlantılar (Ağ katmanı)
g) Depolanan Bilgiler - Yapısal Olmayan (Örn: düzensiz olan, rapor çekilmesi için
kullanılacak işlenmemiş bilgiler)
h) Bağlantılar (Oturum katmanı)
olarak belirlenebilir.

4.3. Kullanıcı Tanımı

Kullanıcı tanımı ister bir kişi, ister bir ürün olsun şifreleme altyapısını kullanacak olan kişi, ürünlerin belirlenmesi ve öz niteliklerinin ortaya konması yapılacak tanımlar açısından önemlidir. Kullanıcı kategorileri Kişi, Cihaz ve Ara Kullanıcı (Agent) olarak sınıflandırılabilir.

4.4. Erişim Yöntemi Tanımı

Her bir uygulama kendi tasarımı ve kullanım amacı gereği çeşitli erişim yöntemlerine sahiptir. Uygulamaların şifreleme servislerini kullanım ve erişim yöntemleri, geliştiriciler tarafından belirlenmiş olması gerekir. Uygulamalar tarafından şifreleme servislerine erişim denetlenmeli ve kontrol altına alınmalıdır. Bu tür yöntemler uygulama geliştiriciler tarafından geliştirme esnasında planlanarak tanımlanmalıdır.

5. Örnek Politika Uygulaması

Bu örnek uygulama finans kuruluşlarının özellikle takip ettiği PCI DSS Güvenlik Standartı temel alınarak hazırlanmıştır. Bu standartta yer alan üç ana gereksinim Kart Sahiplerine ait Bilgilerin Korunması ile ilgilidir. Bilgilerin korunması için şifreleme, kırpma, maskeleme ve karmaşık duruma getirme gibi yöntemler uygulanabilmektedir. Şifreleme sayesinde bilgiler kötü niyetli kişiler tarafından yapılan saldırılar sonucunda ele geçirilse bile saldırganın bu bilgileri okumasını ve kullanmasını mümkün olmayacaktır.

PCI DSS Güvenlik Standartları 3. gerekliliğine göre kart sahiplerine ait bilgilerin belirli standartlar çerçevesinde korunakli bir biçimde saklanmasını gerekmektedir. Buna göre kart sahiplerine ait bilgilerin saklanması beraberinde koruma gereksinimlerini getirir. Bu gereksinimlere göre bilgileri güvenli bir şekilde saklamanın yolu ise şifrelemektir.

Şifrelemede kullanılan anahtarlara erişim mümkün olduğunca az kişi tarafından yapılmalıdır ve bu erişimler denetlenmelidir. Anahtarlar mümkün olduğunca az yerde saklanmalı , sistem yapılandırmaları ve anahtarlar ayrı yerlerde saklanıldığından emin olunmalıdır.

PCI DSS 3.6 nolu gereksinimleri şifreleme için kullanılacak olan anahtarların yönetimi ile ilgili hususları içerir.

Bu hususlar şifrelenmiş olan kart sahibi bilgilerinde kullanılan anahtarlar için anahtar yönetim prosedürlerinin yazılmış olduğundan emin olunması, servis sağlayıcıların kredi kartı sahiplerini taşımada ya da saklamada kullandıkları anahtarlara ait prosedürlerin detaylı bir şekilde tanımlanmasını içerir. Politika ve prosedürler endüstri standartlarına göre belirlenmelidir. Bu standartlara örnek olarak çeşitli kaynaklara NIST üzerinden erişilebilir. (http://csrc.nist.gov)

Anahtar oluşturma, dağıtıma, saklama, anahtar değişimlerine ait politikalar,

kullanılan anahtar algoritmasına ya da anahtarın kendisine ait herhangi bir zafiyet veya şüpheli bir durum olması durumunda yapılacaklar, anahtarların kullanım süresi bitmesinde dikkat edilmesi gereken hususlar tanımlanmalıdır.

Ayrıca anahtarların şifresiz bir ortamda saklanmasında anahtarın tamamının tek bir kişi tarafından bilinmemesi, anahtarı birden fazla kişiye parçalanıp iletilmesi ve anahtarların kontrolünün birden fazla kişi tarafından gerçekleşebilmesi gerekir. Bütün bu işlemlerin ardından uygulanan politikaların anahtara erişimlerini ve dağıtımını yetkisiz kişilere karşı koruduğundan emin olunmalıdır.

Ayrıca tüm anahtar koruma işlemlerini gerçekleştirecek olan kişilerin sorumluluklarını anladıkları ve sorumluluklarını kabul ettiklerine dahil elektronik ortamda ya da kağıt üzerinde onay alınmalıdır.

6. Sonuç

Bilgilerin korunmasında kullanılan kriptoloji ve ilgili teknikler, her ne kadar etkili bir çözüm olarak görünse de yönetimi ve uygulanmasında yapılacak hatalar bu etkili çözümün etkisini azaltabilmekte hatta etkisiz hale getirebilmektedir. Bilgilerin şifreler ile korunmasında dikkat edilmesi gereken en önemli husus şifreleme anahtarlarının güçlü ve güvenilir olması, şifrelenen bu anahtarların kontrol altında tutulmasıdır. Bu çalışmada kurumsal ölçekte şifreleme anahtarlarının kullanım alanlarına göre nasıl yönetilmesi gerektiği örneklerle anlatılmıştır.

Kaynaklar

[1] IETF - Guidelines for Cryptographic Key Management, http://tools.ietf.org/html/rfc4107, Erişim tarihi Mart 2012.

[2] NIST - Recommendation for Key Management - Part 2, http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf, Erişim tarihi Mart 2012.

[3] PCI DSS Requirements and Security Assessment Procedures, v2.0 - p.32, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf, Erişim tarihi Şubat 2012.

[4] Alvand Solutions - Enterprise Key Management: A Strategic Approach, http://www.alvandsolutions.com/downloads/Enterprise_Key_Management_A_Strategic_Approach.pdf, Erişim tarihi Mayıs 2012.

[5] Insecure Mag – Issue 12 – Key Management For Enterprise Data Protection, p.59, http://www.net-security.org/dl/insecure/INSECURE-Mag-12.pdf, Erişim tarihi Haziran 2012.

[6] True Random Number vs Pseudo Random Number Generation, http://en.wikipedia.org/wiki/Random_number_generation#.22True.22_random_numbers_vs._pseudorandom_numbers, Erişim tarihi Temmuz 2012.