GÜVENİLİR BİLİŞİM İLE ELEKTRONİK OYLAMA

BAHADIR İSMAİL AYDIN

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AĞUSTOS 2009

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Mehmet Önder Efe

Müdür(Vekaleten)

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Doç. Dr. Erdoğan Doğdu

Anabilim Dalı Başkanı

Bahadır İsmail Aydın tarafından hazırlanan GÜVENİLİR BİLİŞİM İLE ELEKTRONİK OYLAMA adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

_____	_____
Yrd.Doç. Dr. Kemal Bıçakcı	Yrd.Doç.Dr.Bülent Tavlı
Tez Danışmanı	Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Doç. Dr. Kemal Bıçakcı _____

Üye : Yrd. Doç. Dr. M. Fatih Demirci _____

Üye : Yrd. Doç. Dr. Coşku Kasnakoğlu _____

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

.....

Bahadır İsmail Aydın

Üniversitesi : **TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü : **Fen Bilimleri**
Anabilim Dalı : **Bilgisayar Mühendisliği**
Tez Danışmanları : **Yrd.Doç.Dr. Bülent Tavlı, Yrd.Doç.Dr. Kemal Bıçakçı**
Tez Türü ve Tarihi : **Yüksek Lisans – Temmuz 2009**

Bahadır İsmail AYDIN

GÜVENİLİR BİLİŞİM İLE ELEKTRONİK OYLAMA

ÖZET

İletişim ve bilişim teknolojilerinin gelişmesiyle, insan hayatının pek çok alanı yeniden düzenlenmektedir. İnsanlar pek çok işini artık daha çabuk, kolay, ucuz ve etkileşimli olarak yapabilmektedir. Pek çok topluluğun demokrasiyle yönetildiği günümüzde hayatın pek çok yönü gelişmelere uygun şekilde yeniden tasarlanmışken, insanların kendilerini yöneten insanları seçmede de yeni teknolojileri kullanmaya başlamaları gerekmektedir. Fakat söz konusu olan seçimler olduğu için konunun sosyolojik yönü de göz önünde bulundurulmalı ve çok üst düzey teknolojiler yerine açık kodlu, anlaşılabilir ve güven veren bir sistem tasarlanmalıdır. Bu tez çalışmasında, hem yeterli güvenlik düzeyinde hem de güvenilir açıklık seviyesinde bir sistem önerilmiştir(Bölüm 4). Bu sistem bağımsız bir oylama makinesi içermekle beraber, sistemde sadece oylama makinesi değil tüm seçim süreci ele alınmıştır. Oylama makinelerinde güvenlik(security) ve güvenilirlik(trust) Güvenli Platform Modülü'ne(TPM) dayandırıldığı için Güvenilir Bilişim hakkında da detaylı bir inceleme sunulmuştur(Bölüm 2). Son olarak, Güvenli Platform Modülü kullanılarak geliştirilen bir demo uygulama ve TPM'nin pratikte nasıl kullanılacağı detaylı olarak anlatılmıştır(Bölüm 3).

Anahtar Kelimeler: Güvenilir Bilişim, Elektronik Oylama, Elektronik Seçim, Güvenli Platform Modülü

University : **TOBB Economics and Technology University**
Institute : **Institute of Natural and Applied Sciences**
Science Programme : **Computer Engineering**
Supervisors : **Asst.Prof.Dr. Bülent Tavlı, Asst.Prof.Dr. Kemal Bıçakçı**
Degree Awarded and Date : **M.Sc. – July 2009**

Bahadır İsmail AYDIN

ELECTRONIC VOTING WITH TRUSTED COMPUTING

ABSTRACT

With the development of communication and information technologies, many areas of human life is held again. People can accomplish many affairs quicker, faster, cheaper and more interactively. Today is convenient time for people to start using new technologies when choosing the people who to manage them, when many communities are governed by democracy and many aspects of life re-designed to fit the development. But when the elections are in question, the sociological aspect of the issue should be taken in consideration and an open-coded, comprehensible and trustworthy system should be designed rather than very high-level technologies. In this thesis a system, which is at a reliable clarity level as well as being secure enough, is suggested (Chapter 4). This system includes a standalone voting machine, but not just the voting machine entire election process is discussed. A detailed review about Trusted Computing is also presented as security and reliability of voting machines are based on Trusted Platform Module (TPM) (Chapter 2). Finally, a demo developed using the Trusted Platform Module and usage of TPM in practice are described in detail (Chapter 3).

Keywords: Trusted Computing, Electronic Voting, Electronic Election, Trusted Platform Module

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren çok değerli hocalarım Kemal Bıçakcı ve Bülent Tavlı'ya, akademik hayata adım atmamda büyük pay sahibi hocam Ali Aydın Selçuk'a, kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerine, her türlü bilgi paylaşımında bulunma imkanı sağlayan Yusuf Uzunay'a, çalışmalarım sırasında beni maddi açıdan destekleyen TÜBİTAK Bilim Adamı Yetiştirme Grubu'na, desteklerini esirgemeyen arkadaşlarıma ve bana verdikleri manevi destekten dolayı değerli aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Kısaltmalar	Açıklama
TPM	Güvenli Platform Modülü (Trusted Platform Module)
TC	Güvenilir Bilişim (Trused Computing)
TCB	Güvenilir Bilişim Temeli **(**Trusted Computing Base)
TXT	Güvenilir Yürütme Teknolojisi(Trusted Execution Technology)
AMD	Gelişmiş(Advanced Micro Devices)(Marka)
SVM	Güvenli Sanal Makine(Secure Virtual Machine)
HP	Hewlett-Packard(Marka-Özel İsim)
TCB	Güvenilir Bilişim Merkezi(Trusted Computing Base)
PCR	Platform Yapılandırma Belleği(Platform Configuration Register)
SRTM	Statik Güvenli Yönetim Zinciri(Static Root of Trust Management)
DRTM	Dinamik Güvenli Yönetim Zinciri(Dynamic Root of Trust Management)
RSA	Rivest-Shamir-Adelman (Marka-Özel İsim)
EK	Onay Anahtarı(Endorsement Key)
SRK	Depolama Kök Anahtarı(Storage Root Key)
AIK	Onaylama Kimlik Anahtarı(Attestation Identity Key)
API	Uygulama Programlama Arayüzü(Application Programming Interface)
TCG	Güvenilir Bilişim Gurubu(Trusted Computing Group)
TSS	Güvenilir Yazılım Kümesi(Trusted Software Stack)
BIOS	Temel Giriş / Çıkış Sistemi(Basic Input/Output System)
DES	Veri Şifreleme Standardı(Data Encryption Standard)
PDA	Kişisel Dijital Yardımcı(Personal Digital Assistant)
DMA	Dinamik Bellek Ayırma(Dynamic memory allocation)
YSK	Yüksek Seçim Kurulu

SEMBOL LİSTESİ

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
PCR[i]	i'ninci PCR bellek değeri
SHA1()	SHA1 özüt işlemi
SHA-1()	SHA1 özüt işlemi
SHA-256()	SHA256 özüt işlemi
||	Arka arkaya metin bağlama işlemi
yeniÖlçüm	PCR Extend işlemi sırasında kullanılan veri değeri
XOR	İkilik sistemdeki mantıksal ya da işlemi
I/O	Giriş/Çıkış
S_i	i'ninci seçmen için üretilen gizli doğrulama metni
S_{i1}	i'ninci seçmen için üretilen gizli doğrulama metninin seçmene sunulan parçası
S_{i2}	i'ninci seçmen için üretilen gizli doğrulama metninin kaydedilen parçası

1. GİRİŞ

Günümüzde pek çok ülke demokrasi ile yönetilmektedir. Demokrasi halkın yönetim yetkisini temsilciler aracılığıyla kendisinde bulundurması anlamını taşır. Bu temsilcilerin belirlenmesi de demokrasinin uygulanmasında büyük önem taşımaktadır. "Uygun temsilciler, tüm halk içinden nasıl belirlenmektedir?" sorusunun cevabı burada devreye girmektedir. Bu sorunun cevabı demokrasi yönetiminde seçimdir. Elbette, temsilcilerde liyakat vasfının aranması ya da temsilciliğe aday insanların belirlenmesi ve organizasyonu gibi konular beşeri bilimlerin ilgi alanına girmektedir. Etik olarak prensipler belirlenmesi bu çalışmanın kapsamı dışındadır ama bu prensiplerin etkili şekilde uygulanması yani organizasyon ve uygulama boyutunda milyarlarca insanı ilgilendirmesi hasebiyle günümüzde hayatı pek çok anlamda zenginleştiren ve kolaylaştıran teknolojinin getirilerinden yararlanmaması düşünülemez.

İnsanlar, bugün hayatın her evresinde akıllı makineleri kullanmaktadır. Fakat seçimler halen seneler öncesinin yöntemleriyle ve kağıt pusulalar aracılığıyla yapılmaktadır. Halbuki bilgisayar ya da teknoloji her alanda temelde aynı işin defalarca tekrarlandığı işleri otomatik şekilde halletmenin yollarını sunmaktadır. Milyonlarca hatta bazı ülkelerde milyarlarca insanın oy kullandığı seçimlerde de pek çok yönden avantajlar sağlayacak yeni teknolojik yöntemler kısa süre içinde tüm dünyada uygulanmaya başlayacaktır.

Bahsi geçen teknolojik seçim yöntemlerinin günümüze kadar uygulamalarının incelenmesi sonucu önündeki engeller tespit edilmiş ve günümüze kadar pek çok bilgisayar bilimcisi farklı yöntemler önermiştir. Bu çalışmada da biz yeni bir seçim sistemi önermekteyiz. Bizim önerimiz öncekilerden farklı olarak teorik değil pratik konulara ağırlık vermekte ve bugüne kadar denenen sistemlerin önündeki en büyük engellerden biri olarak görülen güven problemine odaklanmaktadır. Bu probleme çözüm getirmek için de güven problemini çözmek amaçlı tasarlanmış güvenilir bilişim donanım ve metotlarını seçim sistemine uyguladık. Sistemimiz günümüzde kullanılmakta olan kağıt pusulalarla birlikte kullanılabilecek şekilde tasarlandığı için teknolojik pek çok yeniliğin önünüzdeki en büyük engellerden biri olan geçiş ve adaptasyon sürecini kademeli bir şekilde ele almayı sağlayacaktır.

Bu tezde, önerdiğimiz sistemi detaylarıyla anlatmanın yanı sıra yararlandığımız yeni bir teknoloji olup ülkemizde üzerinde çok çalışılmamış olan güvenilir bilişimi, kullanımını ve getirilerini de kapsamlıca anlatmaya çalıştık. Geliştirdiğimiz örnek güvenilir bilişim uygulaması hakkındaki tecrübeler de bu tezde detaylarıyla anlatılmıştır. Bu tezde bu yönleriyle teorik yönünden çok sistem ve uygulama yönü ağırlıklı olan bir çalışmanın ürünü olduğu için sıkça grafiksel anlatım metotlarına ve ekran görüntülerine başvurulmuştur.

2. GÜVENLİ PLATFORM MODÜLÜ (TPM)

2.1 Güvenilir Bilişim

Mekân bağımlı sistemlerde en önemli problem, özel dizayn edilmiş yazılımların ve sistemlerin istenilen işlevlerin dışında farklı şekilde işlev görmesi ve sistemin güvenilirliğini zedelemesidir. Söz konusu farklı işlevler kasıtlı olarak programı yazanlar tarafından oluşturulabileceği gibi kodlama hataları olarak da oluşmuş olabilir. Bu tip hataların veya zararlı kodların fark edilmesi için en etkin çözüm kapalı kaynak koddan açık kaynak koda geçilmesi ve herkesin kodları incelemesine imkan sağlamaktır. Bu sayede kodların sağlıklı olduğu doğrulanabilir fakat bu sefer de karşımıza uygulamanın çalışması esnasında gerçekten doğrulanmış kodun çalışıp çalışmadığının tespit edilmesi problemi çıkmaktadır. Çünkü doğrulanmış kodun çalışmadan önce işletim sistemi üzerinde bulunan bir takım açıklardan veya kötü niyetli yazılımlardan kaynaklı değişikliğe uğraması söz konusudur. Bu problem literatürde güvenli platform problemi olarak da bilinmektedir. Güvenli platform problemi yıllarca üzerinde çalışılan çok önemli bir problemdir ve gerek sunucu sistemlerinde gerekse günlük kullandığımız masaüstü bilgisayarlarımızdaki birçok güvenlik probleminin de temelini teşkil etmektedir. Bugüne kadar sunulan birçok çözüm tamamen yazılım tabanlı ve çoğu zaman çok karmaşık sistemler içermektedir. Günümüzde güvenli platform problemine çözüm sağlayabilecek en önemli teknolojilerden birisi olarak "Güvenilir Bilişim"[1] çalışmaları gösterilmektedir. Güvenilir Bilişim çalışmaları büyük oranda TPM isimli bir yonga üzerine inşa edilmektedir. Güvenilir Bilişim yazılım bütünlük kontrolü, bilgisayarın güvenilir açılışı, erişim denetimi, aygıt doğrulama, kullanıcı doğrulama, güvenli e-posta, disk şifreleme, lisans hakları yönetimi gibi pek çok kritik konuda uygulama alanı sunmaktadır. Bu nedenle IBM, HP, Microsoft, Intel, AMD gibi çok önemli firmalar güvenilir bilişim çalışmalarına büyük destekler vermekte ve yeni çıkardıkları ürünlerini güvenilir bilişim teknolojisi destekli olarak piyasaya sürmektedirler (örneğin Intel'in TXT-Trusted Execution Technology [2], AMD'nin SVM-Secure Virtual Machine [3] teknolojileri, HP'nin "Embedded Security" teknolojisi [4], Microsoft'un Vista ile birlikte sunduğu TPM destekli Bitlocker aracı [5] v.b.). Güvenilir Bilişim üzerine akademik anlamda da özellikle son yıllarda önemli çalışmalar yapılmaktadır. Bu çalışmalardan bir kısmı bilgisayar üzerinde TPM destekli güvenli ve izole bir ortam oluşturma çalışmalarıdır [6][7][8]. Bu çalışmalardan bazıları işletim sisteminin açılışından itibaren bütün ara modüllerin güvenilirliğini test etmekte iken [6], diğer bazı çalışmalarda bilgisayarı tekrar başlatmadan güvensiz bir ortam üzerinden güvenli ve izole bir ortam oluşturulmaya çalışılmıştır [7]. Güvenilir Bilişim çalışmaları kapsamında oluşturulan güvenli platforma TCB (Trusted Computing Base) adı verilmektedir. TCB ne kadar küçük ise güvenlikle ilgili problemlerin daha da azalacağı kanaatiyle geçmişteki akademik çalışmaların bir kısmı TCB'nin boyut olarak küçültülmesi üzerine

odaklanmıştır [7][9][10]. TCB'nin küçültülmesi için önerilen önemli fikirlerden bir tanesi, mevcut işletim sistemi üzerinde güvenli bir şekilde özel ve minimal şekilde tasarlanmış sanal bir işletim sistemi çalıştırmaktır. Buna sanallaştırma (virtualization) denilmektedir [11][12][13][14][15]. Çalıştırılan sanal işletim sistemine literatürde Hipervizör (Hypervisor) de denmektedir. TCB'de hipervizör kullanımının amacı güvenli olarak çalıştırılmak istenilen yazılımın TPM destekli başlatılmış olan hipervizör (Örneğin: Xen, L4 v.b) üzerinde çalıştırılarak mümkün olduğu kadar daha alttaki işletim sisteminden etkilenmemesinin sağlanmasıdır.

Geçmiş çalışmalarda odaklanılan başka bir husus da bir yazılımın üçüncü bir parti tarafından nasıl sorgulanabileceğidir. Bu işleme kısaca kanıtlama (attestation) ismi verilmektedir. Güvenilir Bilişim kapsamında ismi daha çok uzaktan kanıtlama (remote attestation) olarak bilinen işlev, TPM tarafından güvenilirlik ölçümü yapılıp, TPM yongası üzerinde bulunan PCR ismindeki kaydedicilere kaydedilmiş olan değerlerin güvenli bir şekilde üçüncü bir parti tarafından sorgulanabilmesi anlamına gelmektedir. Son yıllarda uzaktan kanıtlama ile ilgili önemli çalışmaların yapılmış olması dikkati çekmektedir [16][17][18][19][20][21]. Bu çalışmaların büyük bir kısmında kanıtlama esnasında TPM tarafından üretilen kanıtlama anahtarlarının kullanılması için kanıtlama açık anahtarını sertifikalayacak bir sertifika otoritesine ihtiyaç duyulmaktaydı. Bu bağlamda "Doğrudan Anonim Kanıtlama" olgusu [22] kanıtlama işleminde sertifika otoritesine ihtiyacı ortadan kaldırarak güvenilir bilişim literatürüne çok önemli katkılar sağlamıştır.

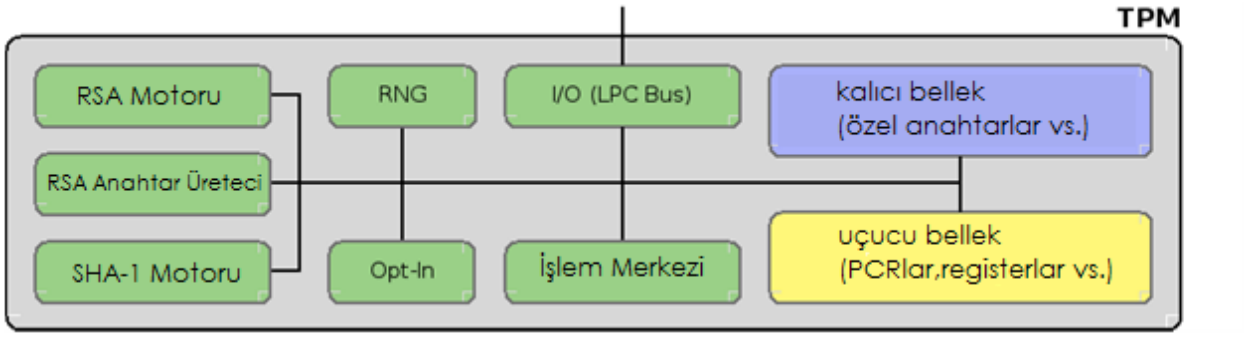
2.2 Güvenli Platform Modülü

TPM olarak bilinen Güvenilir Platform Modülü, günümüzde birçok bilgisayar üzerinde hazır gelen donanım tabanlı bir çeşit güvenlik ve kriptografi yongasıdır. Bu yonga içerisinde dijital sertifika, kriptografik anahtarlar, parolalar ve benzeri birçok bilgiyi barındırabilir. TPM aynı zamanda anahtar yönetimi, üzerinde çalıştığı PC'nin kimliğini doğrulama, elektronik belgeler ve e-postalar üzerinde güvenli elektronik imzalama, şifreleme, şifre çözme işlemlerini gerçekleştirme, tam-sürücü şifrelemeyi yönetme, çok yönlü doğrulamada ikinci faktör olarak görev yapma ve üzerinde bulunduğu bilgisayarın güvenliğini ve bütünlüğünü değerlendirmeye yardımcı olma gibi birçok alanda işlev görebilmektedir. TPM'nin katma değer sağladığı en önemli alanlardan birisi bir yazılımın değiştirilip değiştirilmediği doğrulamaya imkan sağlayacak donanım tabanlı doğrulama yapabilmesidir. TPM'nin güvenilir açılış özelliği sayesinde bilgisayarın açılışından itibaren kurulan bir güven zinciri ile çalışan bütün programların güvenilirliğinin tespiti mümkün hale gelmektedir. SRTM (static root of trust for measurement) olarak bilinen bu özellik bilgisayardaki bütün ara platformların güvenilir olmasını

öngörmektedir. TPM sürüm 1.2 ile birlikte DRTM (dynamic RTM) isminde yeni bir mekanizma geliştirilmiştir. Bu mekanizmanın kullanılması için INTEL ve AMD işlemcilerine yeni bir komut (senter ve skinit komutları) eklemişlerdir [2][3]. DRTM mekanizmasının en önemli özelliği çalışan işletim sisteminin güvenli olmasa dahi bir programı güvenli bir ortamda çalıştırabilecek izole bir ortam sunabiliyor olmasıdır. Bu izole ortamın oluşturulması esnasında bilgisayar üzerinde çalışan diğer yazılımların ortamı etkilememesi için bütün kesmeler etkisizleştirilir, DMA erişimi iptal edilir ve benzeri güvenlik önlemleri alınır. DRTM mekanizmasının geliştirilmesi yazılım güvenliği anlamında önemli avantajlar sağlamıştır.

2.2.1 TPM'nin donanımsal özellikleri

TPM genellikle ana kart üzerine takılı olarak bulunur. AMD 780v, Intel i7 yonga setli ana kartları TPM desteği sunmaktadır.



Şekil 2.2.1 TPM'nin iç yapısı

TPM çeşitli firmalar tarafından üretilmekte olup tüm modeller, spesifikasyonunda belirtilen özellikler bakımından aşağıda gösterilen şekildeki mecburi bölümleri içermektedir. TPM üreten firmalardan bazıları şunlardır:

- Infineon
- Intel
- Atmel
- ST Microelectronics
- Winbond
- Broadcom

- SinoSun

2.2.1.1 PCR

PCR ismi verilen kaydediciler, TPM ile yapılabilen pek çok işlemde kullanılabilen güvenli ortam kaydedicileridir. PCR 'ların en mühim özellikleri arasında şunlar gösterilebilir:

- Bütünlük kontrolü sağlar(160 bit)
- Korumalı
- Yazılamaz sadece Extend edilebilir.

$$\mathbf{PCR[i] = SHA1(PCR[i]||yeniÖlçüm)}$$

- Sınırsız ölçüm için kullanılabilir

TPM 1.1 spesifikasyonunda 16 adet olarak belirlenen PCR'ler, TPM 1.2 ile ilk 16'sı eski işlevleriyle son 8'i ise Dinamik Güven Kökü Ölçümleri(DRTM) için kullanılmak üzere 24 adet olarak belirlenmiştir.

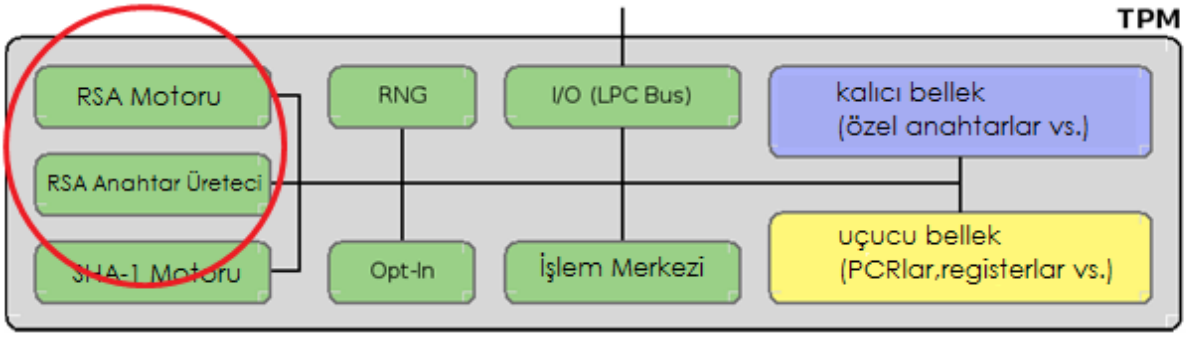
2.2.2 TPM'nin fonksiyonları

TPM'nin Güvenilir Bilişim işlemlerini yerine getirmesi için 4 temel fonksiyonu yapabilmesi gerekmektedir:

- Kriptografik fonksiyonlar: RSA, RNG, SHA-1, HMAC
- Güvenli depolama ve spesifik bir platform konfigürasyonunu belirten özet değerlerini barındırma
- Anahtar saklama ve veri damgalama
- Yönetim ve başlangıç fonksiyonları (opt-in)

Bunlardan bazılarının gerçekleştirilme detayları ve temel getirileri ise şu şekildedir:

2.2.2.1 RSA



Şekil 2.2.2 RSA ile ilgili kısımlar

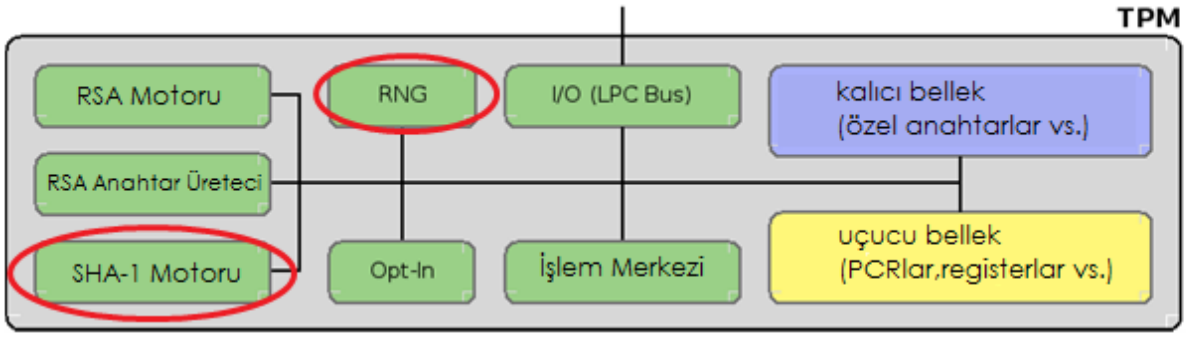
- Asimetrik anahtar üretme (512,1024,2048 anahtar uzunlukları)
- Asimetrik şifreleme ve şifreleme ve şifre çözme(RSA, DSA opsiyonel)
- Açık çarpan sabit: $2^{16}+1$
- TPM'e RSA işlemi yaptırmak için anahtar yüklenmeli

2.2.2.2 SHA-1

- Temel güvenilir özüt fonksiyonu
- Önyüklemede kullanılmak için çip dışından kullanıma açık
- Gelecekte başka özüt fonksiyonları

2.2.2.3 RNG

- TPM'deki rastlantısallığın kaynağı
- Güncel metin(Nonce), anahtar üretimi…



Şekil 2.2.3 Özüt ve Rastgele Sayı Üretim Merkezleri

2.2.2.4 Geçici ve Kalıcı depolama

- Anahtar slotları: Geçici ve dışarıdan
- Kalıcı depo
    - Özel anahtarlar(Onay Anahtarı (EK) ve Depolama Kök Anahtarı(SRK),…)
    - EK sertifikası

2.2.2.5 Opt-in

- TPM açık/kapalı
- Kullanıcı kararı

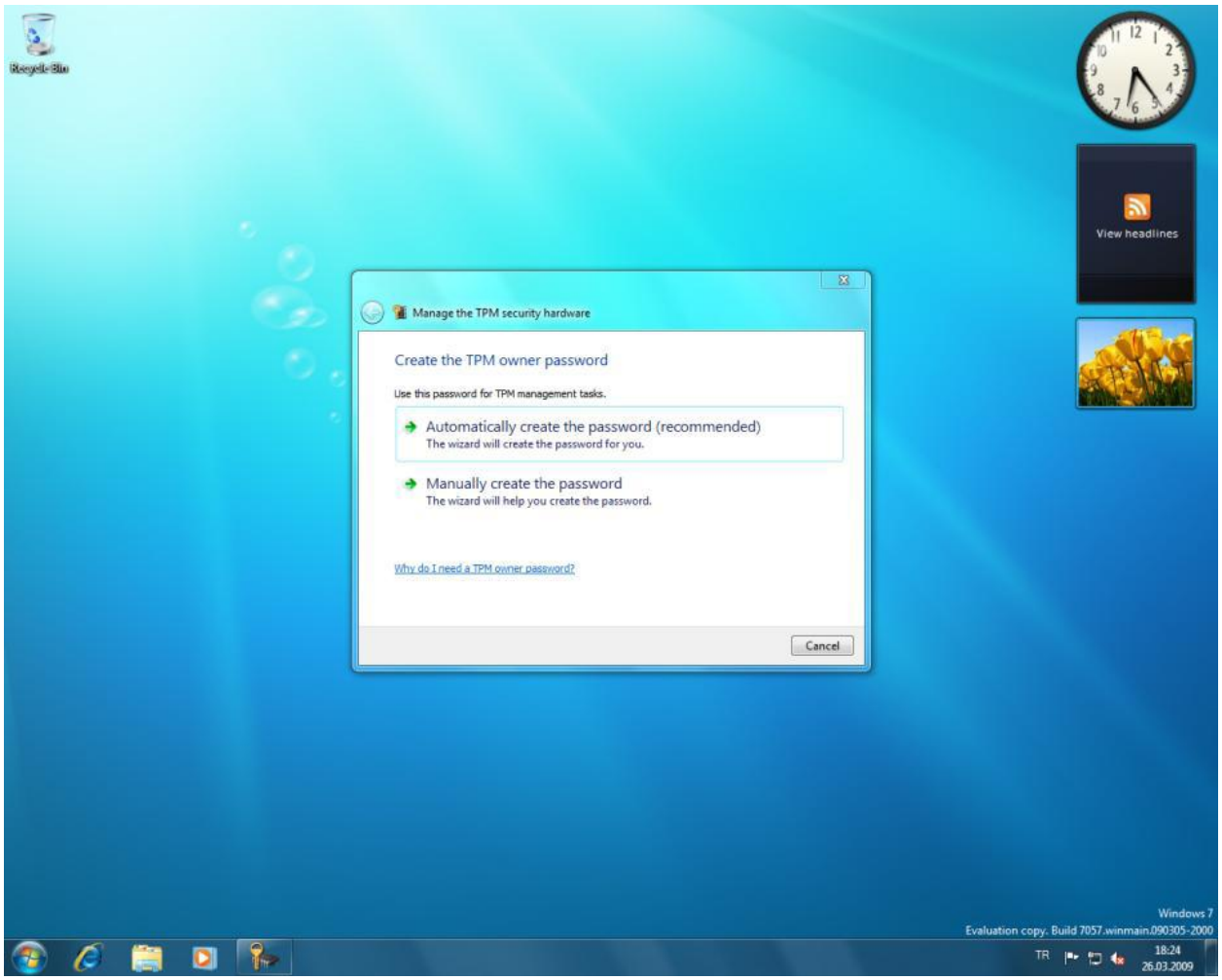
2.2.3 TPM'yi kullanmak

TPM'yi herhangi bir platformda kullanmak için geçilmesi gereken temel adımlar şunlardır:

- "TurnOn" ve "TakeOwnership"
- BIOS 'tan yönetim
- SRK üretimi (2048 RSA)
    - Dışarıdan erişilemez
    - Kaybolursa tekrar üretilemez

TPM istenirse fabrika ayarlarına döndürülebilir, o taktirde tüm kalıcı ve geçici depolar temizlenir. Bunun tek istisnası EK'dir. TPM temizlenirken dikkat edilmesi gereken mühim bir nokta şudur ki SRK da geri döndürülemeyecek şekilde temizlendiği için önceden TPM tarafından üretilip TPM'e bağlı anahtar yapısında saklanan anahtarlarla şifrelenmiş, damgalanmış veya imzalanmış belgeler tekrar geri döndürülemeyecekleri için bu işlemler iptal edilmelidir.

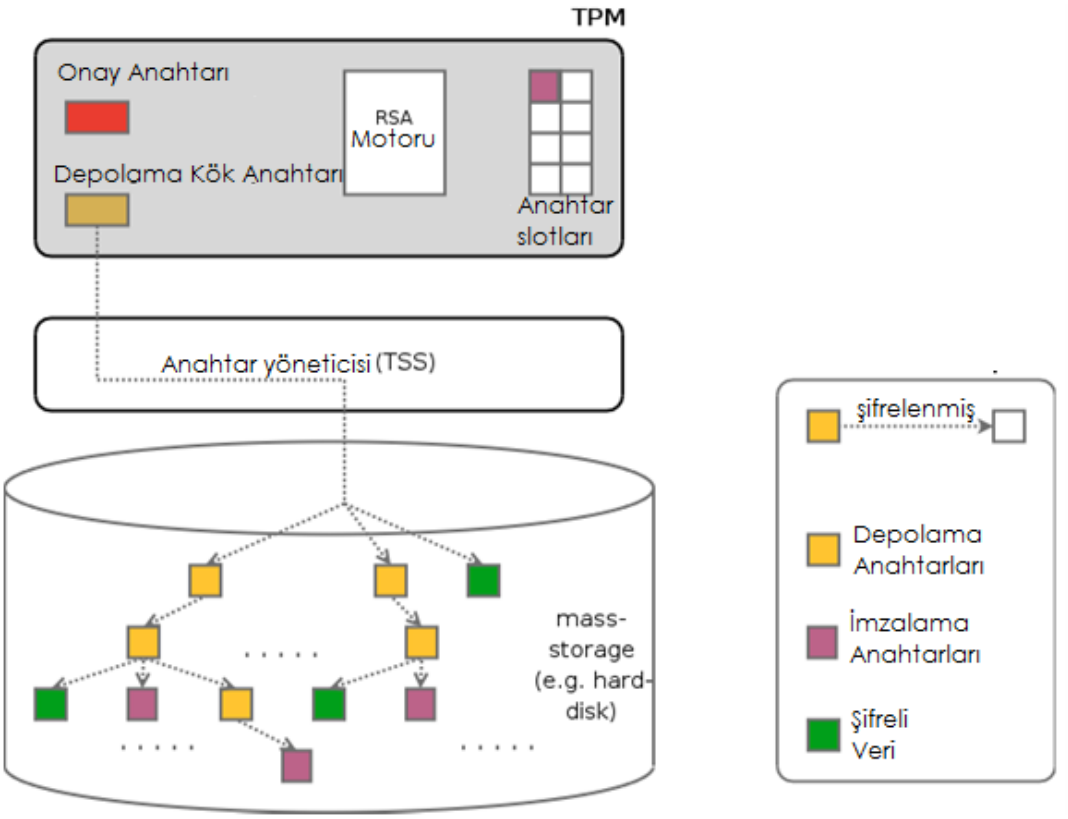
Vista ile TPM kullanmak için komut isteminden "tpm.msc" yazılarak TPM yönetimini kolaylaştıran Vista yönetim modülüne ulaşılabilir.



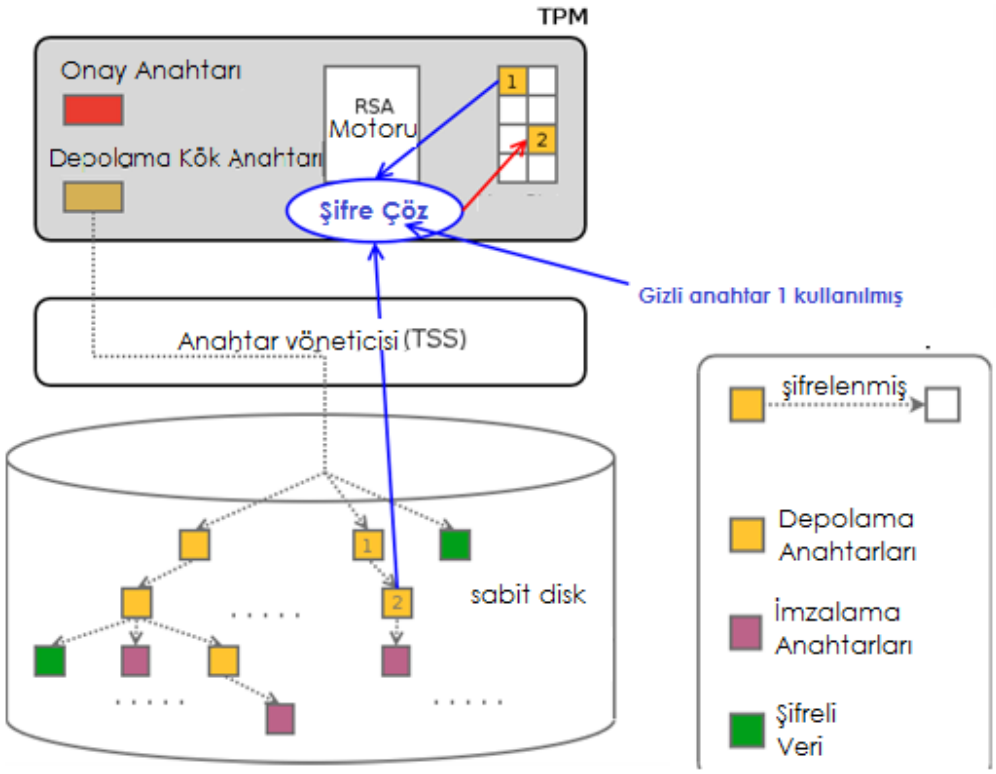
Şekil 2.2.4 TPM'yi Açma

2.2.3.1 SRK ve anahtar hiyerarşisi

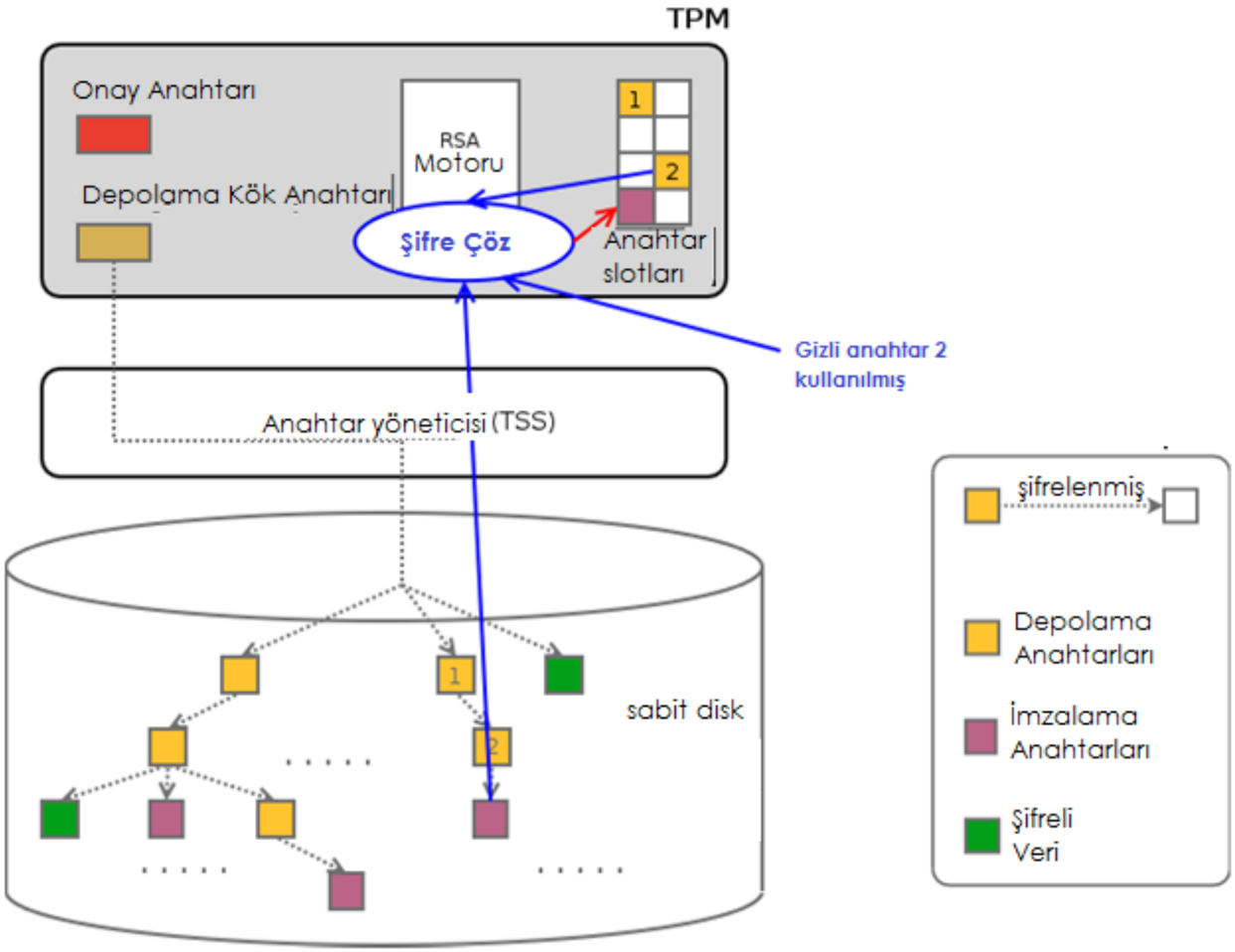
TPM'de kısıtlı anahtar kapasitesi olduğu halde aşağıdaki şekilde gösterilen bir anahtar hiyerarşisi ile çok sayıda anahtar TPM desteğiyle korunabilir.



Şekil 2.2.5 Sınırsız Anahtar Hiyerarşisi

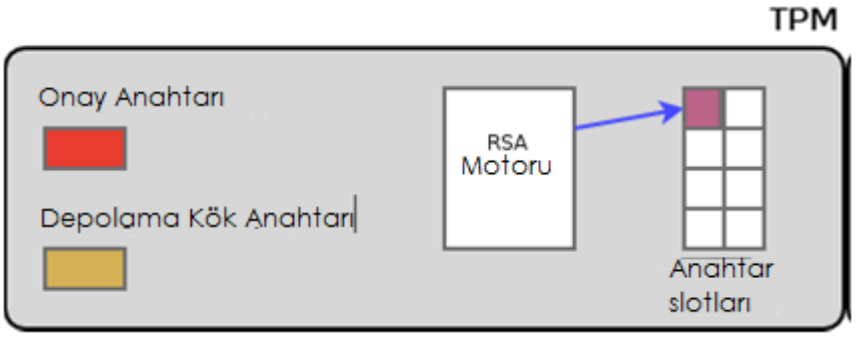


Şekil 2.2.6 Gizli Anahtar 2'nin Çözülmesi



Şekil 2.2.7 İmzalama Anahtarının Çözülmesi

TPM'de yeni bir anahtar üretildiğinde ise bu depolama yapısına dahil edilmesi aşağıdaki şekillerde gösterildiği şekilde gerçekleşmektedir.

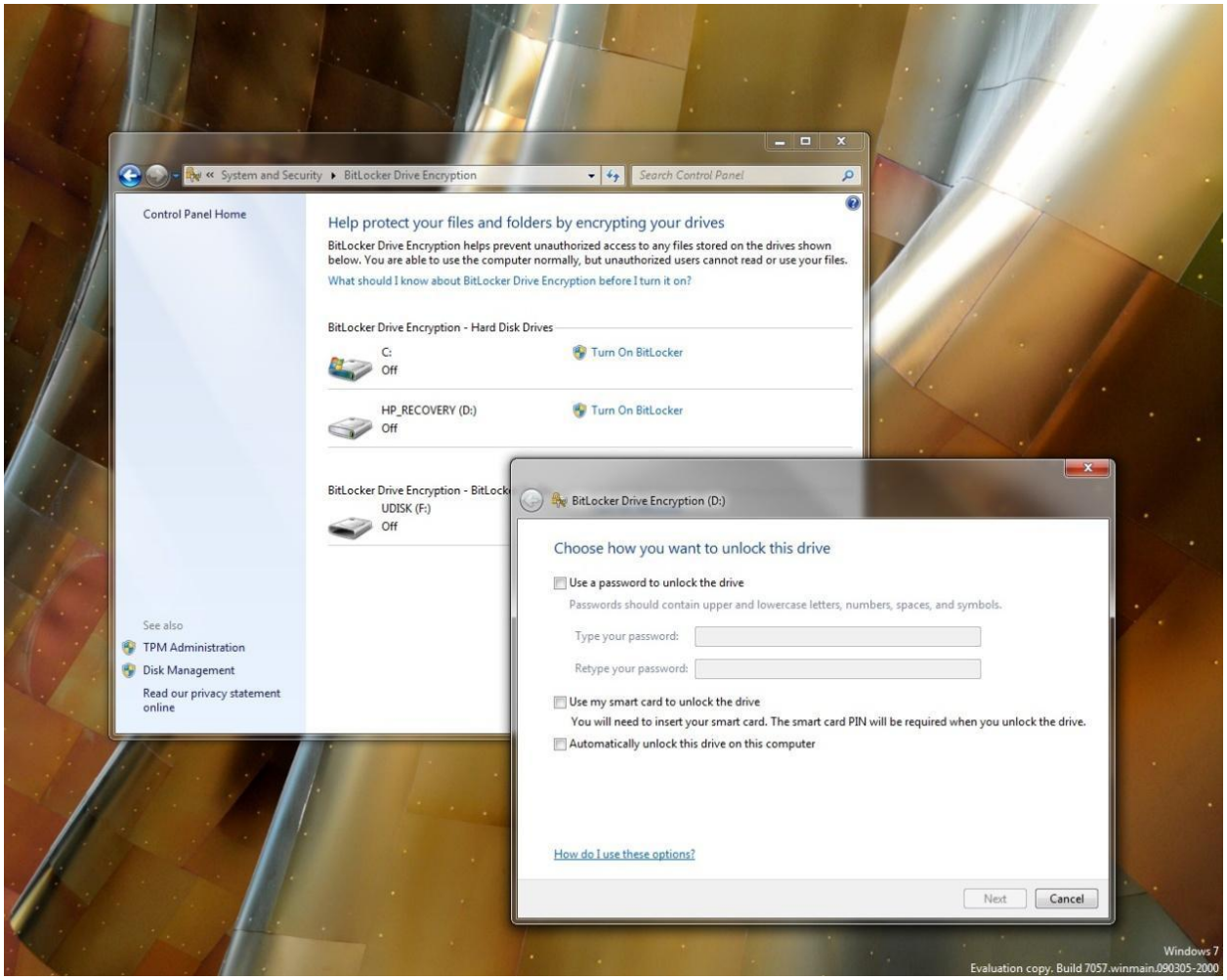


Şekil 2.2.8 Anahtar Üretimi

TPM ile yapılabileceklere bazı örnekler şunlardır:

2.2.3.2 Tüm disk şifreleme

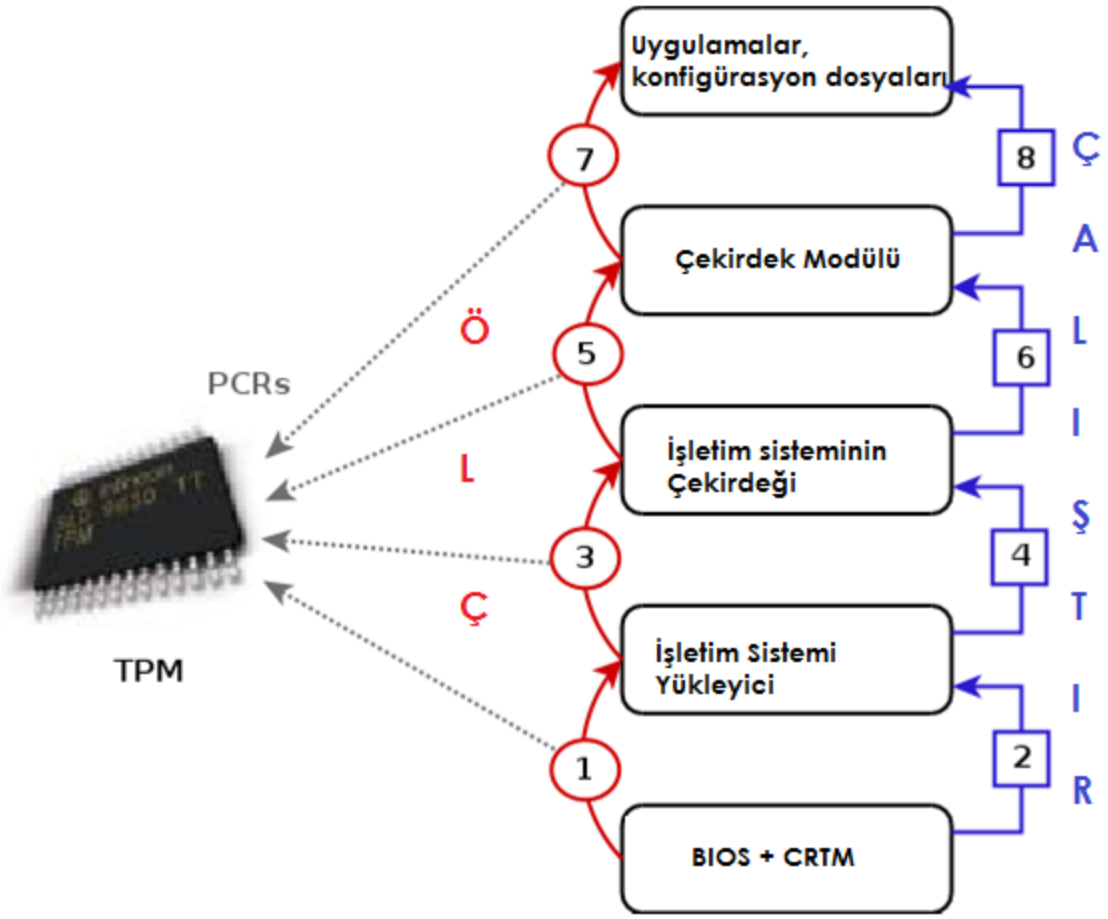
Bu yapıdaki bir anahtarı kullanmak gerektiğinde aşağıdaki şekillerde gösterildiği gibi onu şifreleyen depolama anahtarlarıyla açıp kullanılabilir. Bu depolama anahtarlarının yapısının kökünü oluşturan anahtara ise SRK yani Depolama Kök Anahtarı ismi verilir.



Şekil 2.2.9 Tüm disk şifreleme

2.2.3.3 Güvenli Önyükleme

Güvenli ön yükleme TPM'nin sağladığı en temel özelliklerden biridir. Burada tüm sistem, açılışı sırasında TPM'den başlanarak bir güven zinciri ile ölçülerek herhangi bir değişikliğe uğrayıp uğramadığı kontrol edilebilir.



Şekil 2.2.10 TPM ile Güven Zinciri

Bu işlem için PCR'ler kullanılır. TPM 1.2'den itibaren bu özellik dinamik olarak da desteklenmektedir. Ölçüm zinciri yapısına bir örnek şu şekildedir:

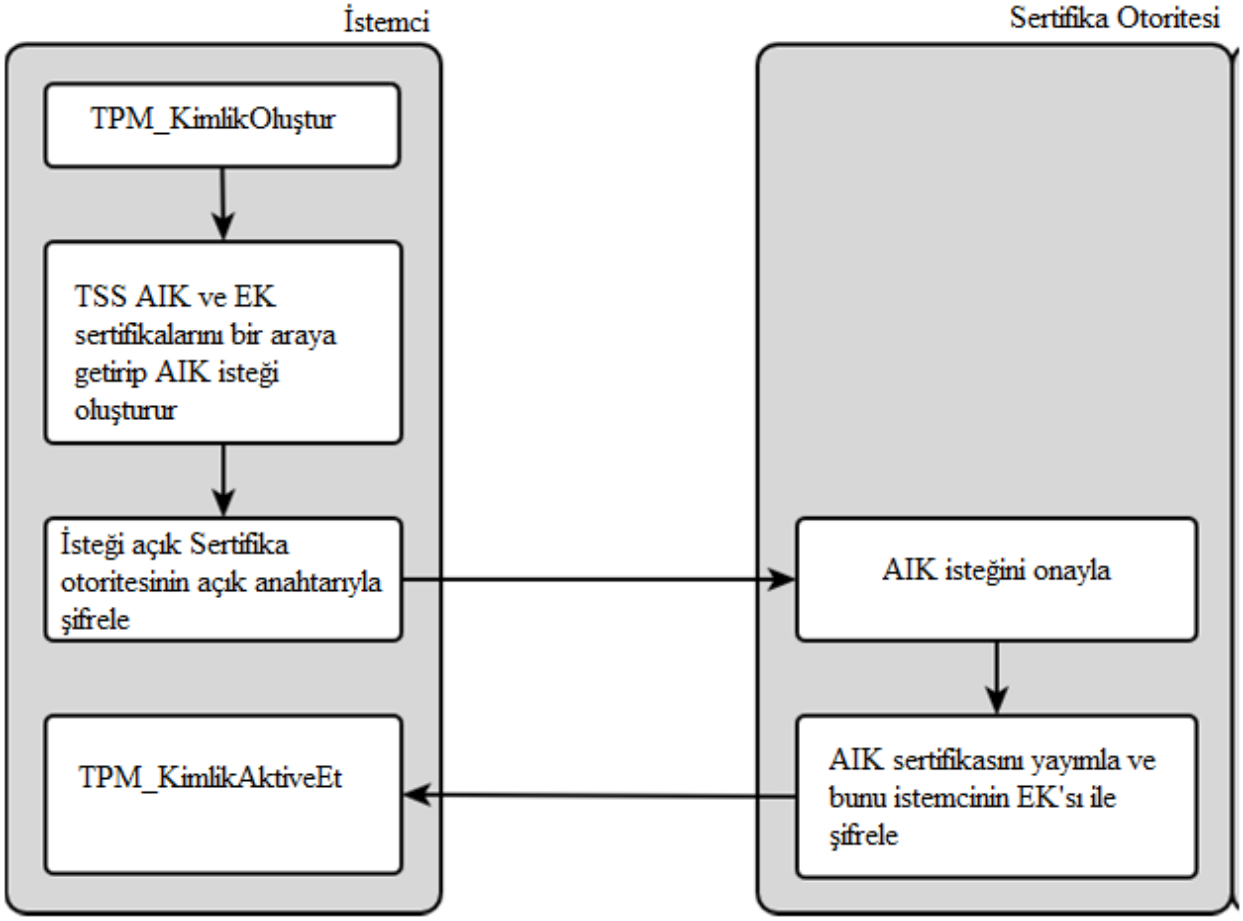
CRTM→BIOS→MBR→OS→Uygulama

2.2.3.4 Bellek Perdeleme

İşletim sistemlerinde kullanıcıların ya da programların kendilerinden başka kullanıcı ve programların bellek alanlarına erişmeleri istenmeyen bir durumdur çünkü kötü niyetli programlar başka programın verilerini bozabilir ya da çalabilir. TPM de bu amaçla kullanılabilir. Bellek perdeleme denilen sistemle donanım bazlı bir izolasyon sağlayabilir. Bu şekilde aynı zamanda kriptografik anahtarlar gibi özel verilerin de saklanabileceği korunmuş alanlar sağlanabilir. Hatta işletim sistemi bile bu alanlardaki veriyi okuyamaz[23]. İşletim sisteminin tam kontrolünü ele geçiren bir saldırgan dahi gizli verilere ulaşamamış olur.

2.2.3.5 Uzaktan Onaylama

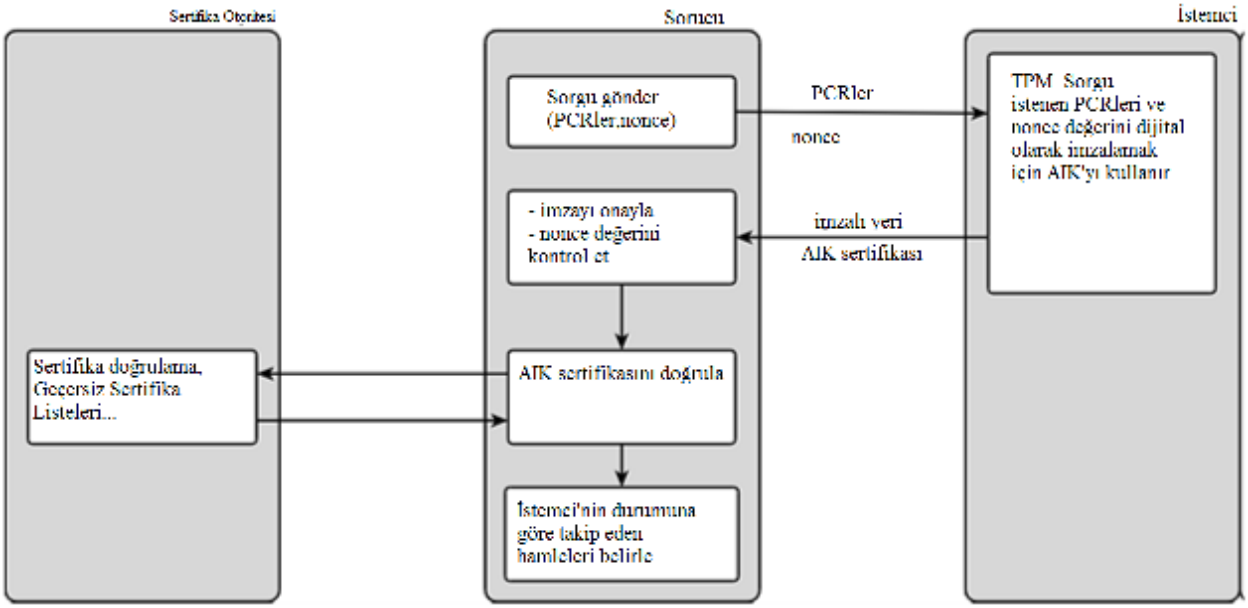
TPM tarafından üretilen ve yönetilen anahtar çeşitlerinden biri de AIK'lardır ve uzaktan onaylama için kullanılırlar. Burada bir PKI altyapısı ile üretilen anahtarların sertifikasyonu yapılabilir.



Şekil 2.2.11TPM ile uzaktan Onaylama: Sertifikasyon

Onaylama Kimlik Anahtarlarının(AIK) temel özellikleri şunlardır:

- 2048 bitlik RSA anahtarlardır
- Limitsiz sayıda üretilebilirler
- Belirsiz TPM onaylaması yapabilirler. Yani onaylayıcı imzaların bir TPM tarafından atıldığını bilebilirken hangi TPM tarafından atıldığını belirleyemez.



Şekil 2.2.12 TPM ile uzaktan Onaylama: Kanıtlama

2.2.4 TPM ile ilgili Projeler

Bugüne kadar ülkemizde, Avrupa'da ve dünyada TPM kullanılarak gerçekleştirilen ilgi çekici çalışmalardan bazıları şunlardır:

- vTPM
- OSLO
- TPM Emulator
- OPENTC
- TCG çalışma grupları
- Trusted GRUB
- TPM Uygulamaları

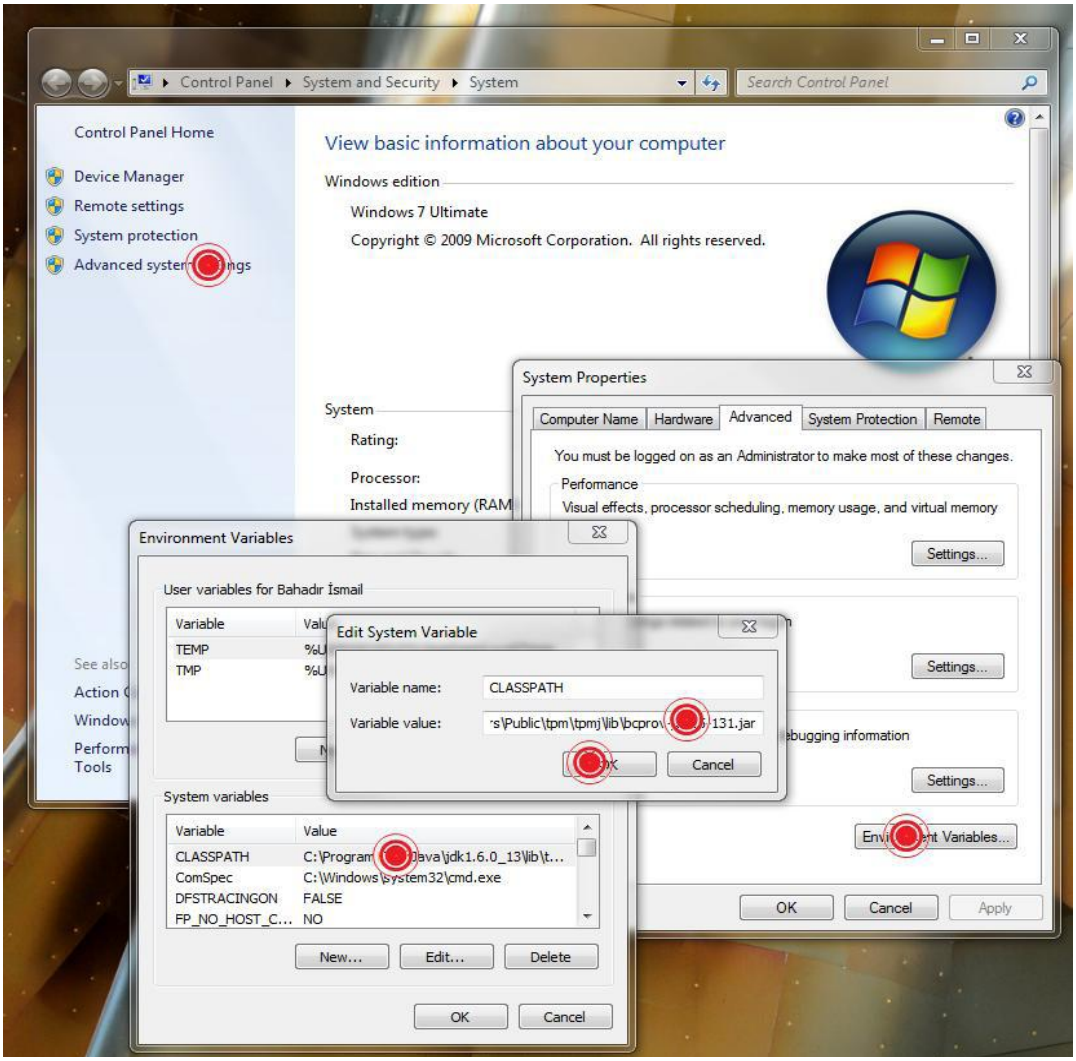
3. TPM/J ile DEMO

3.1 TPM/J

TPM/J TPM'e JAVA kullanarak alt düzey erişim sağlayan nesne-tabanlı erişim sağlayan bir API'dır. MIT' de Trusted Computing projesinin bir parçası olarak geliştirilmiştir[24]. TPM/J

TCG'nin TSS spesifikasyonlarına uygun olmaktan daha çok araştırmacı ve programcılara esnek nesnesel bir ara yüz sunmak için geliştirilmiştir. Vista'da TPM/J'yi kullanmak için uygulanması gereken adımlar şunlardır:

1. BIOS'taki güvenlik sekmesinden TPM'i açmak (Enable Embeded Device Security)
2. http://sourceforge.net/projects/tpmj/ adresinden TPM/J'yi edinmek
3. tpmj-alpha0.3.0 sıkıştırılmış klasörünü C:\Users\Public\tpm klasörüne yüklemek
4. ";C:\Users\Public\tpm\tpmj\lib\tpmj.jar;C:\Users\Public\tpm\tpmj\lib\bcprov-jdk15-131.jar" yollarını ortam değişkenlerine eklemek



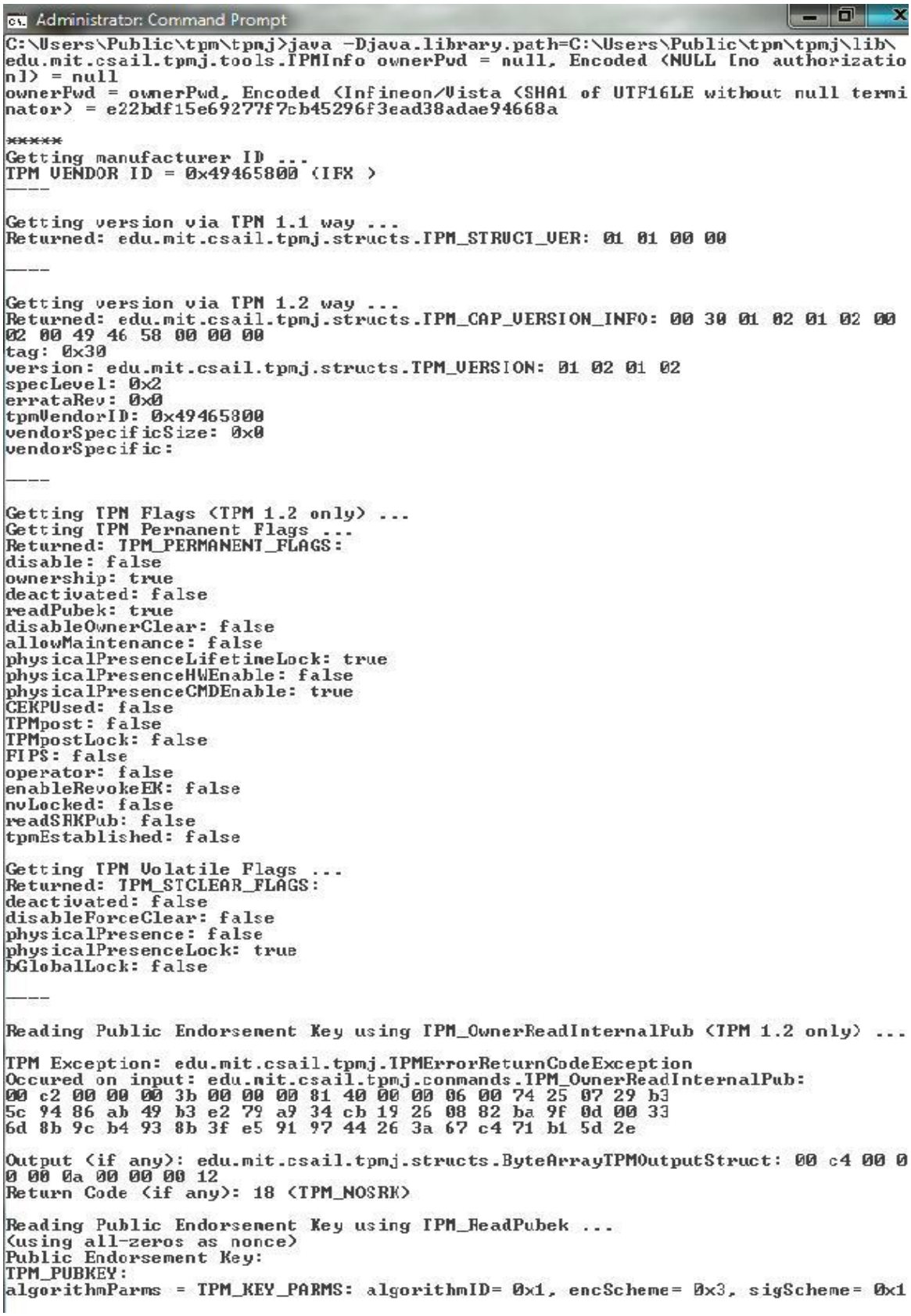
Şekil 3.1.1 Ortam Değişkenlerini Ekleme

5. Bu aşamaya gelene kadar bilgisayara TPM/J'yi yükledik ve artık bu kütüphaneyi kullanabilir durumdayız. Sıradaki işlem TPM/J'nin araçlarını kullanarak TPM'e erişebilmek için bir komut istemini Yönetici modunda çalıştırmak.

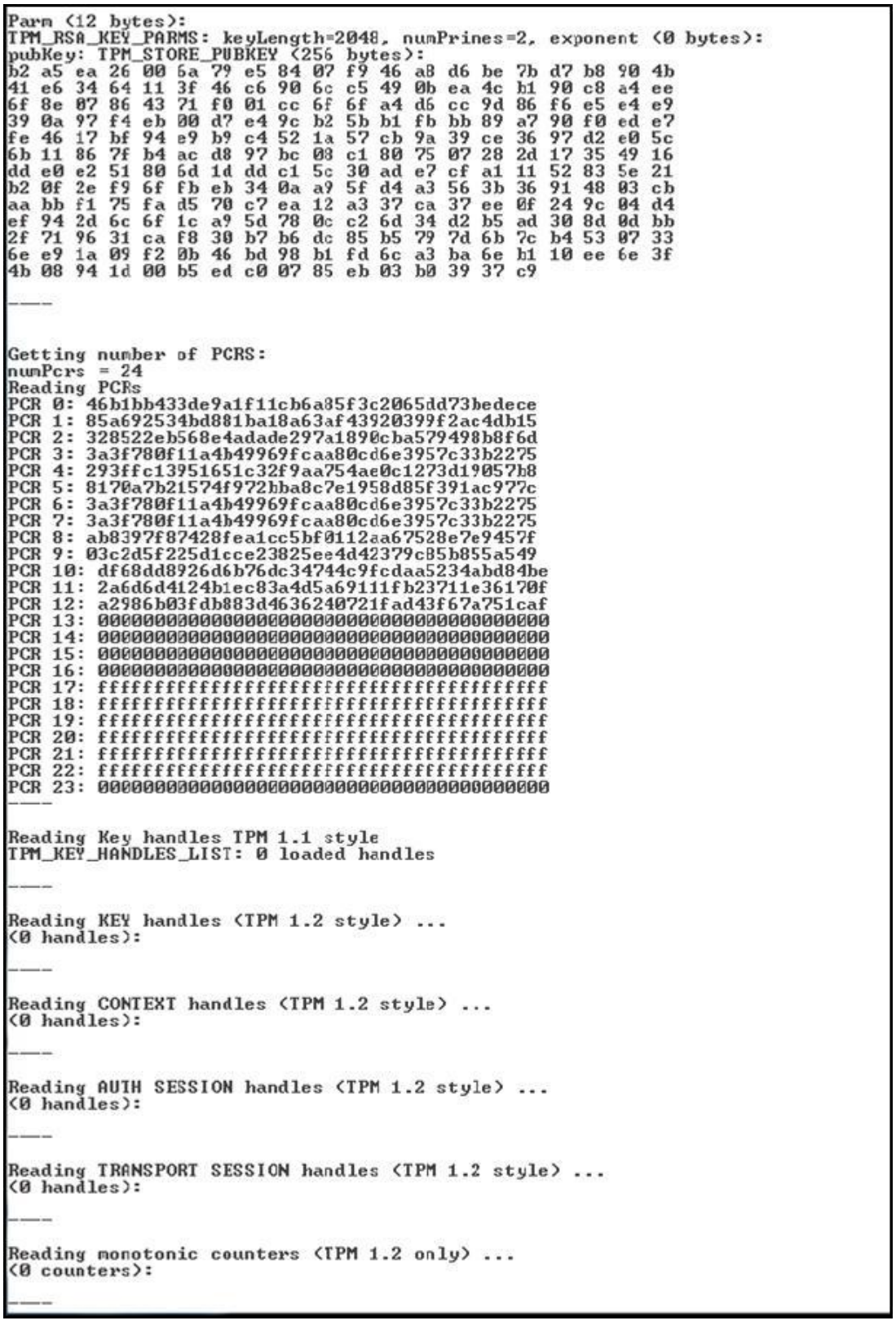
Şekil 3.1.2 TPM Yöneticisini Güvenli Çalıştırma

Şimdiki aşama TPM'nin şu anki durumunu TPM/J ile test etmek

>cd C:\Users\Public\tpm\tpmj >java -Djava.library.path=C:\Users\Public\tpm\tpmj\lib\ edu.mit.csail.tpmj.tools.TPMInfo ownerPwd = null, Encoded (NULL [no authorization]) = null



Şekil 3.1.3 TPM'ye ilk erişim

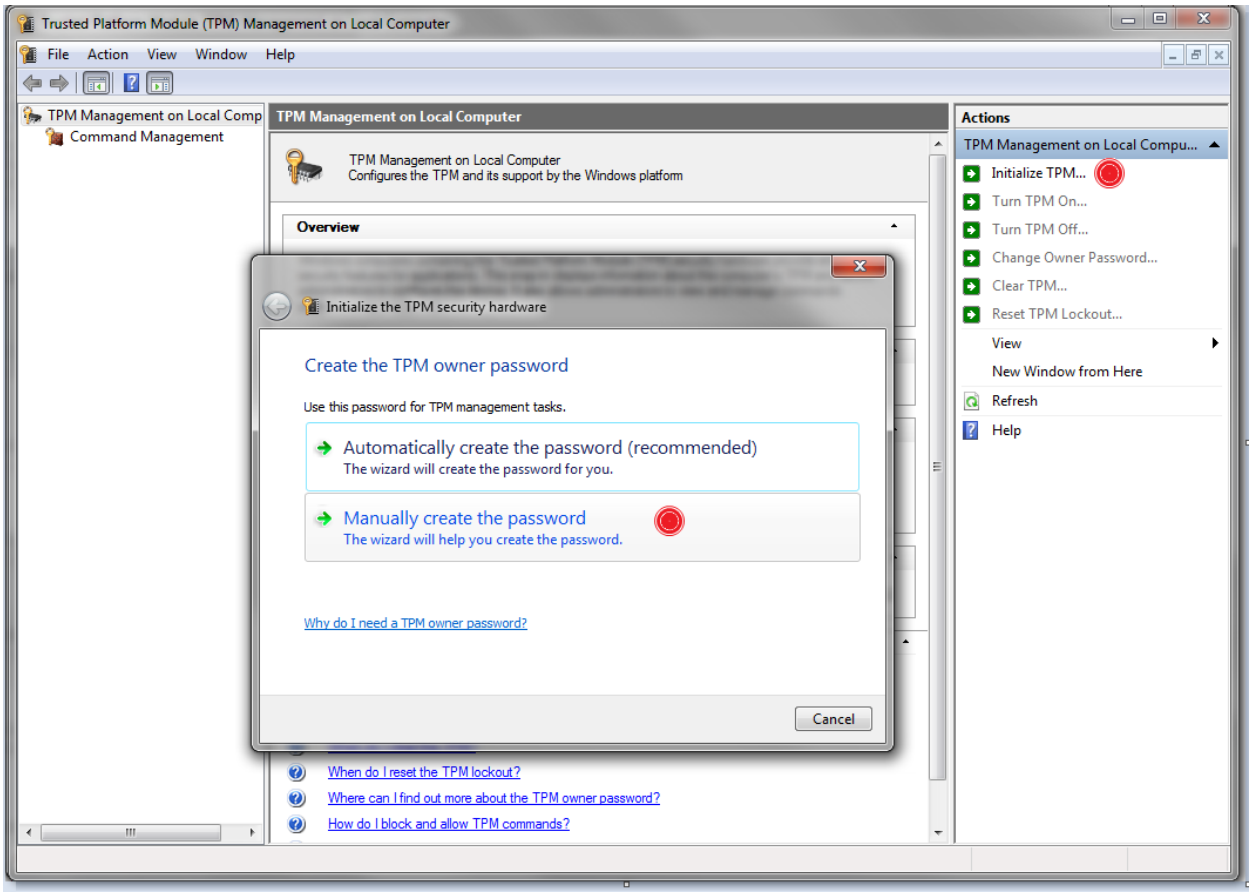


Şekil 3.1.4 TPM'ye ilk erişim

7. TPM'i sahiplenmek için Vista TPM Yönetici Programı'nı çalıştırmak

>tpm.msc

8. TPM'i başlatmak ve sahiplenmek



Şekil 3.1.5 TPM sahiplik şifresi belirleme

9. Sahiplendikten sonra TPM'nin durumunu TPM/J ile test etmek

>java-Djava.library.path=C:\Users\Public\tpm\tpmj\lib\ edu.mit.csail.tpmj.tools.TPMInfo ******* ownerPwd = *******, Encoded (Infineon/Vista (SHA1 of UTF16LE without null terminator) = e22bdf15e69277f7cb45296f3ead38adae94668a (Burada ******* kısmına TPM'nin yönetici parolası yazılmalıdır)

10. TPM/J'nin diğer bazı araçlarını kullanarak TPM'nin temel fonksiyonlarını test etmek
>cd C:\Users\Public\tpm\tpmj\tpmjdemo

a. AIK anahtarı ürettirmek için:

>java-Djava.library.path=C:\Users\Public\tpm\tpmj\lib\ edu.mit.csail.tpmj.tools.TPMCreateAIK aik.key test 0x1234567890123456789012345678901234567890 ******* (Burada ******* kısmına TPM'nin yönetici parolası yazılmalıdır)

b. Kalıt (legacy) anahtarı ürettirmek için:

>java-Djava.library.path=C:\Users\Public\tpm\tpmj\lib\edu.mit.csail.tpmj.tools.TPMCreateKey testkey.key l test SRK /m test

c. PCR değerlerini listelemek için:

>java-Djava.library.path=C:\Users\Public\tpm\tpmj\lib\ edu.mit.csail.tpmj.tools.TPMReadPCRs

d. Bir PCR'ı extend etmek için(Aşağıdaki örnekte 15.PCR):

>java-Djava.library.path=C:\Users\Public\tpm\tpmj\lib\ edu.mit.csail.tpmj.tools.TPMExtend 15 0x1234567890123456789012345678901234567890

Bu testte ilk değeri 0000000000000000000000000000000000000000 olan bir PCR'ı 1234567890123456789012345678901234567890 değeriyle extend edince sonuç d70c2b7c26f239e78542ad24bf4c3e64337a6bea olmalıdır.

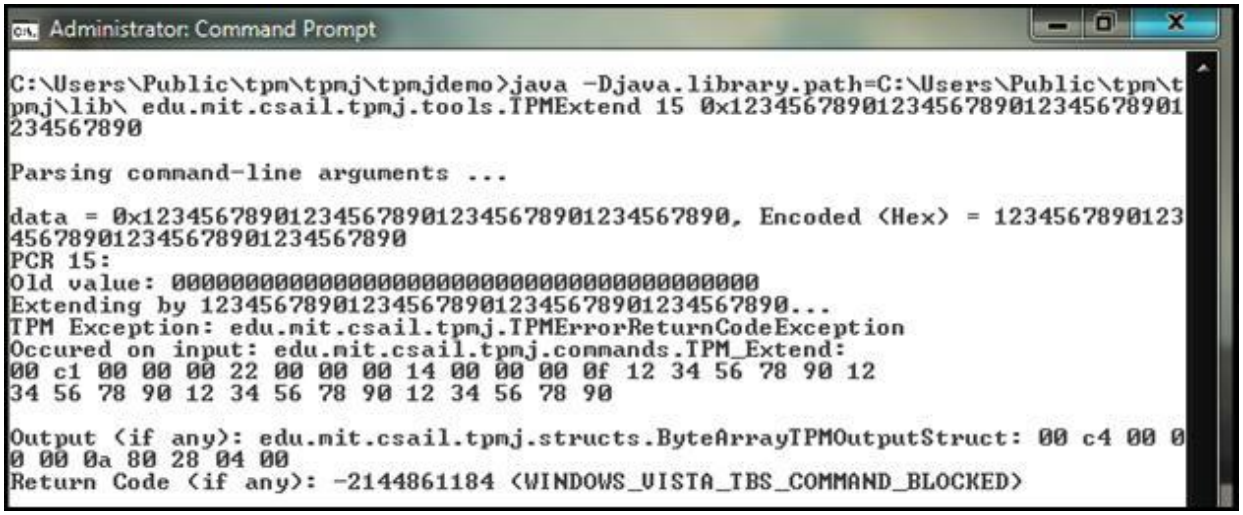
e. Bir dosyayı damgalamak için:

>java-Djava.library.path=C:\Users\Public\tpm\tpmj\lib\ edu.mit.csail.tpmj.tools.TPMSeal deneme.txt SRK "" foo

f. Bir dosyanın damgasını kaldırmak için:

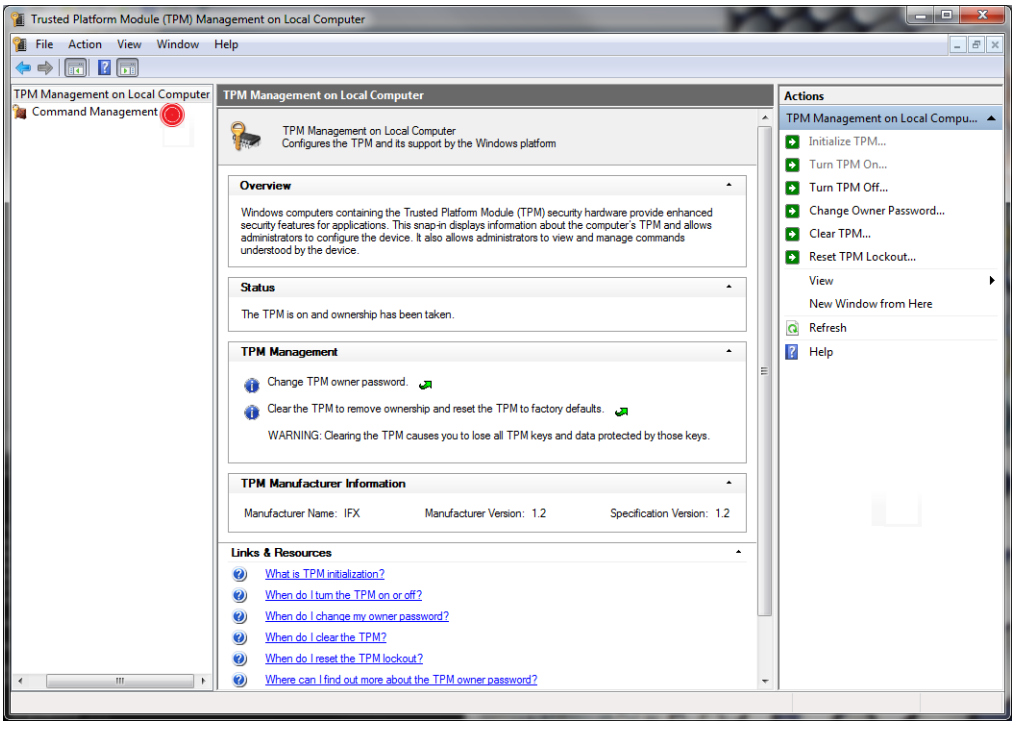
>java -Djava.library.path=C:\Users\Public\tpm\tpmj\lib\ edu.mit.csail.tpmj.tools.TPMUnseal deneme.txt.sealed SRK "" foo

11. Bir önceki adımdaki testlerden biri sırasında bir hata ile karşılaşılırsa bunun en muhtemel nedeni Vista'nın bazı TPM komutlarını kısıtlamış olmasıdır. Örneğin PCR Extend etme sırasında aşağıdaki şekildeki gibi bir TPMErrorReturnCodeException hatası alınabilir.



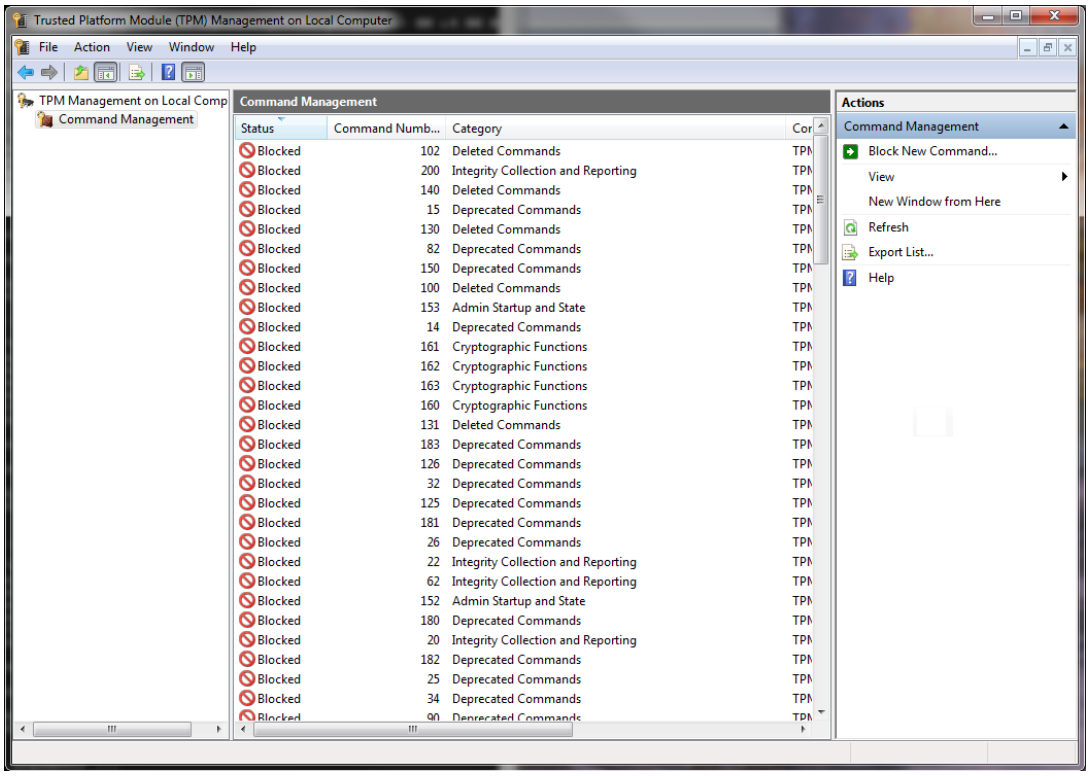
Şekil 3.1.6 TPM Extend işlemi

Bu durumda herhangi bir komutun Vista tarafından kısıtlanıp kısıtlanmadığını kontrol etmek için Vista TPM Yönetici Programı çalıştırılmalıdır >tpm.msc



Şekil 3.1.7 TPM Komut Yönetimi

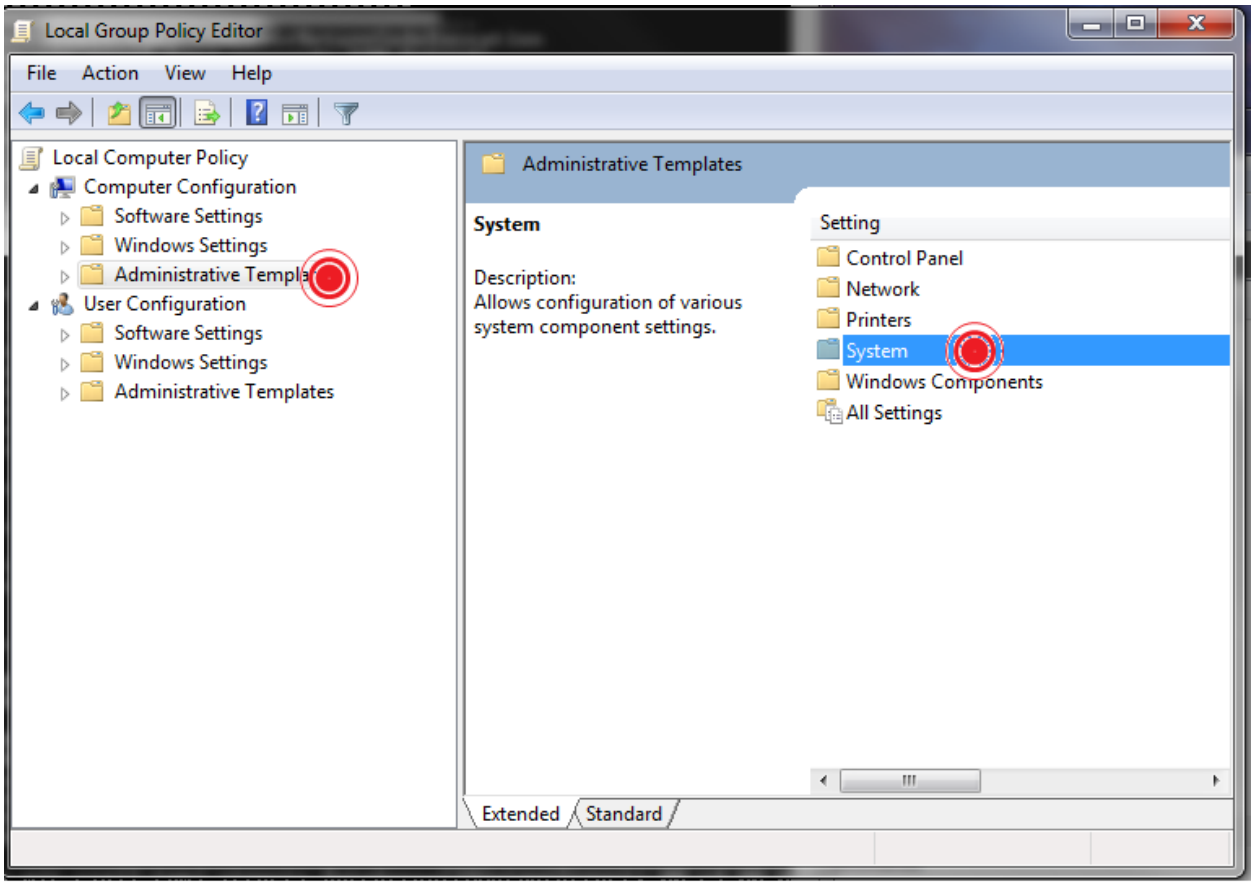
12. Burada Komut Yönetimi bölümünde hangi komutların aktif hangilerinin kısıtlandırılmış olduğu görülebilir.



Şekil 3.1.8 Kısıtlı ve Erişilebilir Komutlar

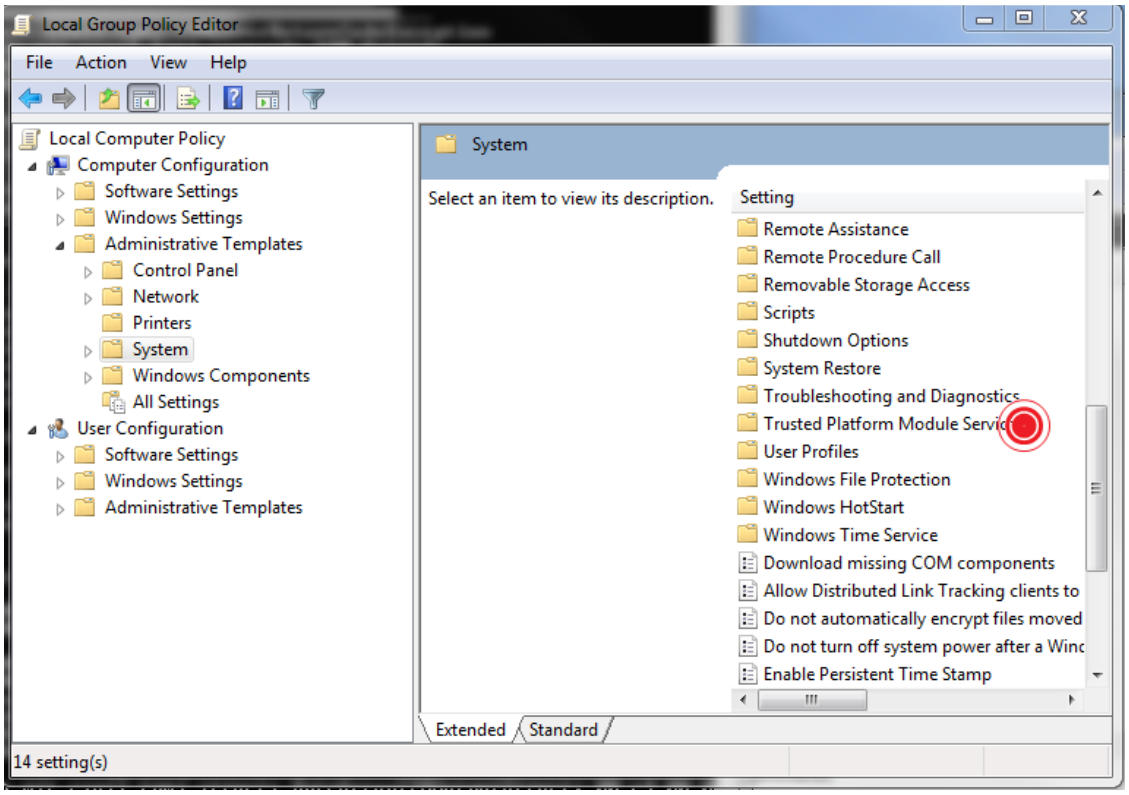
13. Kısıtlı bir komuta erişim izni vermek için Vista'nın Grup Politikalarını değiştirmek gerekmektedir.

>gpedit.msc



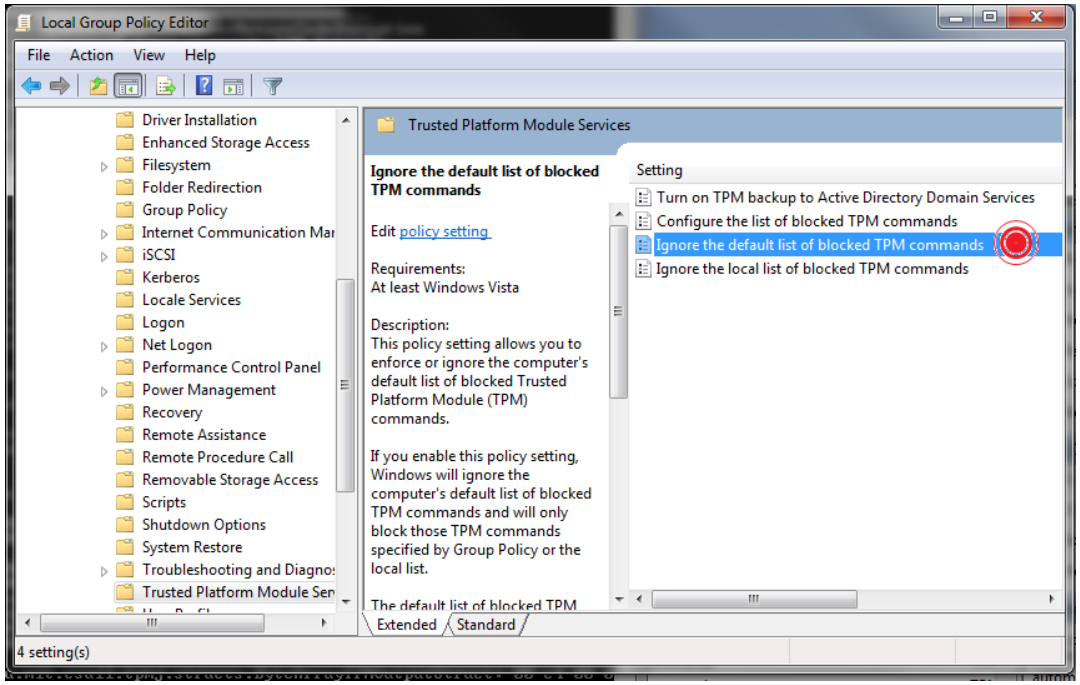
Şekil 3.1.9 Grup Politikaları

TPM ile ilgili Grup Politikaları'nı görüntülemek için Sistem kısmından TPM'le ilgili dosyaya ulaşılmalıdır.

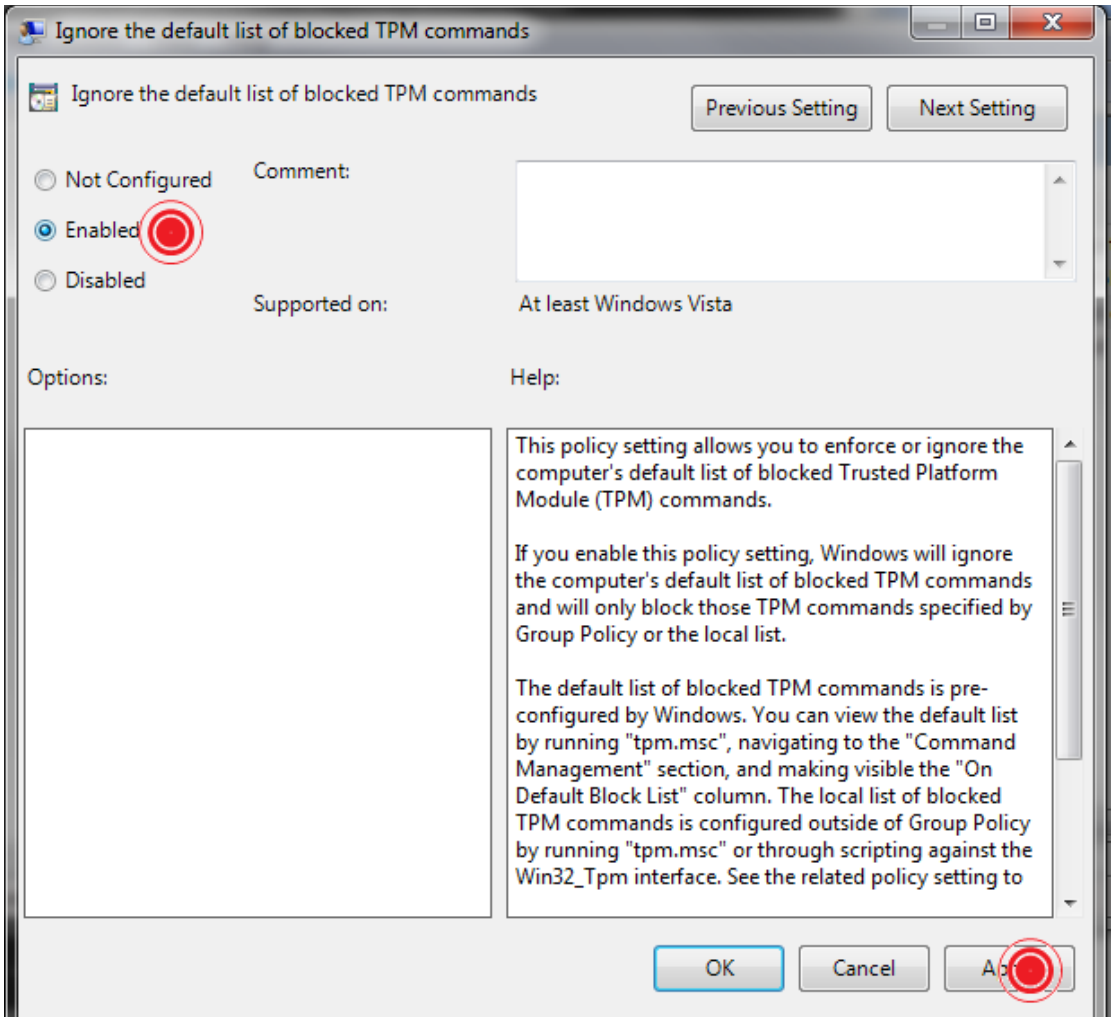


Şekil 3.1.10 Komut Kısıtlandırmalarını Kaldırma

Bu kısımda engelli tüm komutlara izin vermek için "Varsayılan kısıtlanmış TPM komutları listesini yok say" özelliği aktive edilmelidir.

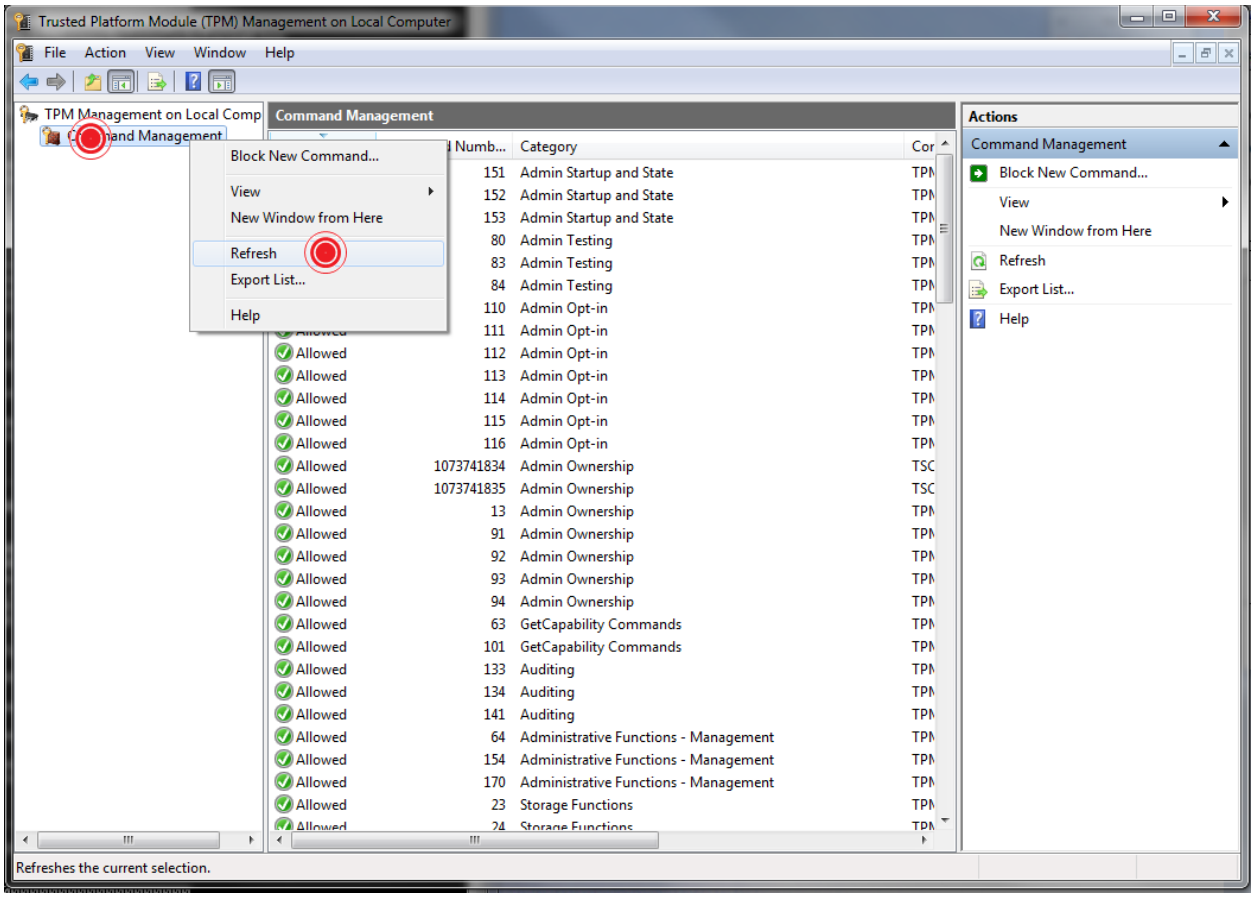


Şekil 3.1.11 Komut Kısıtlandırmalarını Kaldırma



Şekil 3.1.12 Komut Kısıtlandırmalarını Kaldırma

Bu işlemi yaptıktan sonra tüm işlemlere erişim sağlanabilir.



Şekil 3.1.13 Tüm komutlar izinli

Eğer kullanıcı kendi istediği bazı komutları engellemek isterse yine bunu da Grup Politikaları ile yapabilir.

3.1.1 Damgalama Uygulaması

Proje kapsamında bir örnek program TPM/J'nin damgalama fonksiyonları kullanılarak TPM SRK'sı ile damgalanıp kullanılacağında tekrar açılmaktadır. Burada tüm programı damgalayıp açmak zaman olarak çok verimsiz olacağı için program içinde bir DES key üretilmekte program bu anahtarla şifrelendikten sonra bu anahtar TPM tarafından damgalanmaktadır.

3.1.2 Temel Program

TPM ile damgalanan program basit bir e-Oylama uygulamasıdır.

Şekil 3.1.14 Demo program: Giriş Ekranı

Burada kayıtlı kullanıcılar önce kimliklerini belirterek sisteme giriş yapmaktadırlar.

Şekil 3.1.15 Demo program: Parti Seçimi

Daha sonra seçmenler, biri bağımsız olmak üzere 2009 Türkiye Yerel Seçimleri'ne katılan 20 parti arasından bir tercihte bulunmaktadırlar.

Şekil 3.1.16 Demo program: Seçim Onay

Seçmenlerin, tercihlerini onaylamak için en alttaki onay düğmesine basmaları gerekmektedir.

Şekil 3.1.17 Demo program: Seçmen Oturum Sonlandırma

Onaylama düğmesine basılmasıyla beraber başarılı bir oy kullanma işlemi tamamlanmış olur. Kullanıcıya oyunun istediği partiye sayıldığına dair cümle gösterilerek kullanıcının oturumu otomatik olarak sonlandırılır.

Şekil 3.1.18 Demo program: Geçersiz seçmen girişi

Eğer ismi kullanıcı listesinde olmayan yahut listedekiler arasından oyunu halihazırda kullanmış bulunan bir kullanıcı sisteme giriş yapmak isterse buna izin verilmemektedir.

Şekil 3.1.19 Demo program: Geçersiz Seçmen girişi engellendi

Kullanıcıya uyarı mesajı gösterilerek otomatik olarak tekrar sisteme giriş ekranına dönülür.

Şekil 3.1.20 Demo program: Seçim Görevlisi Sonlandırma Ekranı

Tüm kayıtlı seçmenler oy kullandıktan sonra yahut program kapatılmaya çalışılırsa yönetici parolası istenmektedir.

Şekil 3.1.21 Seçim Sonuçları

Geçerli yönetici parolası girildikten sonra seçim sonuçları görüntülenir. Tekrar kapatma istemi yapılmasıyla program sonlandırılır.

3.1.3 Damgalama Paketleri

Yukarıda anlatılan program TPM/J kütüphanesine eklediğim tr.edu.etu.biaydin paketi kullanılarak damgalanmakta ve damgası açılmaktadır. Bu paketteki kaynak kodlar ekler bölümünde verilmiştir. Bu kaynak kodlar TPM/J'nin TPMSeal ve TPMUnseal araçları baz alınarak üretilmiş ve şifreleme işlemleri için de DES algoritması CBC ve PKCS5 ekleme yöntemiyle kullanılmıştır. Ekteki kodlar incelendiğinde görülecektir ki, TPM SRK'si ile şifrelenen program değil DES anahtarıdır. Bu ekstra bir güvenlik açığı getirmemektedir çünkü yukarıda bahsi geçtiği üzere SRK hiyerarşisi içerisindeki her anahtar SRK kadar güvenli kabul edilebilir. DES'in ele geçirilip programın başka bir bilgisayarda şifresinin kırılması ihtimali bir güvenlik eksiği değildir çünkü böyle bir durumda veri SRK ile direk şifrelense o da DES anahtarı gibi ele geçirilebilecek demektir. Yani DES anahtarı bu senaryoda paketlenen verinin bir parçasıdır ve açık şekilde ancak programla beraber bulunabilir. Bu damgalama işlemi tam bir güvenlik değil sadece uygulamanın değiştirilmeden ve platforma bağlı olarak çalıştırılmasını sağlamaktadır.

3.1.4 Şifreleme ve Damgalama İşlemleri

Damgalama paketleri kullanılarak damgalama yapmak için Yönetici modunda çalıştırılmış bir komut istemi ekranından damgalanacak paketin bulunduğu klasörde şu komutu çalıştırmak gerekmektedir: >java tr.edu.etu.biaydin.SealExec Damgayı açmak için de damgalanmış paketin bulunduğu klasörde >java tr.edu.etu.biaydin.UnsealExec komutu çalıştırılmalıdır.

3.1.5 Tasarım Süreci

Burada anlatılmış olan program sadece TPM'nin kullanılmasında pratikte karşılaşılacak sorunları da tanımlayıp dökümante etmek için yazılmış olup, aşağıda anlatılacak olan güvenli e-seçim uygulaması adına bir başlangıçtan öte bir bilgi birikimi sağlamaktadır. Buna rağmen geliştirilen demo programı önerilen sistemdeki oturum yönetimi, seçim görevlisi tarafından seçimin sonlandırılması gibi özellikleri içerdiği için bu program oylama programı olarak da kullanılabilir. Bunun için programın seçmen listesini bir dosyadan okuyup oyları da aynı şekilde dosyaya yazması gerekmektedir. Fakat önerilen sistemin uygulamaya konulması için geliştirilmesi gereken oylama programı değil öncesinde bilgisayarın hazırlanması ve bu aşamada TPM'nin kullanılmasıdır. Bu nedenle bu programı geliştirme aşamasına gelene kadar edinilen tecrübeler ve bu deneyim kullanılarak önerilen sistemi geliştirmeye dair önerileri sunmakta fayda var.

TPM'i pratikte kullanabilmek için öncelikle konseptleri anlamak ve alanı tanımak gerekti. Bu aslında en uzun süreçti denebilir çünkü yeni sayılabilecek bir alan olduğu için bilgi sahibi çok fazla insanla karşılaşamadık. Yurtdışından bazı bağlantılarımızı kullanmanın dışında yaptığımız kaynak taraması sırasında alana dair pek çok makaleyi tarama fırsatı bulduk. Bu kaynaklar arasında hem e-Oylama konusu hem de Güvenilir Bilişim'le ilgili çalışmalar mevcuttu. Bunu da bir takım çalışması olarak haftalık bir okuma grubu ile yaptık. Bunun dışında konu ile ilgili düzenlenen bir kısım konferansları da takip etmeye çalıştık. Okuduğumuz ve özetlediğimiz bir kısım makaleleri hazırladığımız blog'ta sunduk.[25][26]. Bu alan tanıma çalışması, sadece teorik bir araştırmadan ibaret olmayıp TPM'i Java ile nasıl kullanabileceğimizi de içermekteydi.

Yeterli bilgi düzeyine gelip uygulama geliştirmeye karar verdiğimizde TPM'i edinmek de vakit alıcı bir aktivite olarak karşımıza çıktı. Günümüzde üretilen pek çok ana kart TPM için bir yonga yeri içermekte olmakla beraber genelde bu ana kartlar üzerinde çip bulunmamaktaydı. AMD işlemcilere uyumlu ana kartlar için bu sorun daha geçerli durumdaydı. TPM'i kendi başına edinip monte etmek de çok mümkün olmadığı için TPM'li hazır bir AMD makine aradık. HP dc5850 modeli iş amaçlı geliştirilmiş olduğu için güvenlik adına TPM çipini bulundurmaktaydı. Bundan haberdar olduktan sonra uzun süren bir ihale süreciyle bu makineyi edindik.

TPM'li makinemizi edindikten sonrasında TPM'i kullanabilmek adına açma, sahiplenme ve tanıma süreci başladı. Bu hususlarda karşımıza çıkan sorunların çözümleri detaylı şekilde bu bölümde anlatılmıştır. Güvenilir, açık kodlu ve olabildiğince küçük koda sahip bir işletim sistemi seçimi de güven problemine karşı önemli bir adımdır. Bu sebeple denememizi kapalı kaynak kodlu Vista'da geliştirmemize rağmen demo programını platform-bağımsız Java diliyle yazdık. İşletim sistemi olarak seçilecek bir açık kaynak kodlu sistemde de bu program çalıştırılabilecektir.

3.1.6 Gelecek Çalışmalar

Yukarıda analatılan tasarım sürecinde ve demo uygulamayı geliştirirken edinilen deneyimler sonucu aşağıda anlatılan seçim sisteminin geliştirilmesine dair bazı fikirler edindik. İlk önce, açık kaynak kodlu işletim sistemi olarak seçilecek bir Linux sistemine Trusted Grub işletim sistemi yükleyicisiyle güvenli bir şekilde ulaşılabilir. Söylemek gerekir ki sadece demo olarak geliştirildiği halde, bunun üzerinde çalıştırıldığında bu demo programı da güvenli bir şekilde işlev görecek ve yeni seçim sistemi içinde kullanılabilecektir.

Sonrasında yapılacak gelişmeler için önerilerimiz şu şekildedir:

- Sistemde kullanılacak makine HP dc5850 modeli olarak seçilmiş kabul edilebilir. Bunun üzerinde uygulama geliştirildiktin sonra, şu şekilde modifikasyonlar yapılabilir:
    - Önerdiğimiz sistemde sabit disk kullanılmamaktadır. İşletim sistemi ve geliştirilen oylama programı bir harici bellekten yüklenip çalışacak şekilde ayarlandığı takdirde sabit diske ihtiyaç kalmayacak ayrıca veriler sabit diskte saklanmadığı için depolanmış verilere yapılabilecek ataklardan kaçınılmış olacaktır. Bunun için bahsi geçen modeldeki sabit disk çıkarılabilir.
    - Sistemde kullanılacak makine mekan bağımlı ve ağ bağlantısız şekilde önerilmiştir. Bu da internet üzerinden doğabilecek pek çok atağı engellemektedir. İnternete bağlantı için kullanılan ethernet kartı sistemden çıkarılabilir.
    - Bilgisayara akıllı kart okuyucu/yazıcı arabilimler entegre edilip güvenilir sürücüler yüklenmelidir.
    - Sistemde gereken çıktılar için bir yazıcı eklenmelidir.
- Anahtar üretim ve paylaşımı için güvenilir bir program geliştirilmeli veya halihazırda bu fonksiyona sahip bir uygulama incelenip sisteme entegre edilmelidir.
- Sistemle iletişim için wireless ya da bluetooth gibi kablosuz protokoller bazı açıklar doğurabileceği için seri bağlantı protu ya da USB üzerinden haberleşme kullanılacaktır. Geliştirilen uygulama, bilgisayarda çalışan yazılımın denetlenmesi için kullanılacak bu arabirimler üzerinden veri giriş/çıkışı yapabilmelidir.
- Program geliştirildikten sonra işletim sistemiyle birlikte CD veya DVD'den çalıştırılabilecek şekilde önyükleme komut dosyaları hazırlanmalı ve bu şekilde işletim sistemi, program ve seçmen listeleri paketlenip harici bir diske yüklenmelidir.
- Oyunu kullanan seçmene oy pusulası ve seçim sonrası oy sonuçlarının çıktısını verebilecek şekilde baskı fonksiyonu uygulamaya eklenmelidir.

4. GÜVENİLİR SEÇİM SİSTEMİ

İçinde bulunduğumuz zaman dilimi pek çok yeni teknolojinin yardımıyla iletişimin önceki zamanlara göre çok daha hızlı, kolay ve ucuz şekilde gerçekleştirilebildiği, bu sebeple de "İletişim Çağı" olarak isimlendirilmiş bir haberleşme dönemidir. Bu da pek çok iş modelinin

yeniden yapılandırılıp çok daha etkileşimli şekilde ele alınabilmesini sağlayacak şekilde evirilmesine neden olmuştur. Elbette, bireyin devletle olan ilişkilerini gerçekleştirdiği alanlar da bu değişim ve gelişimden payını almış ve alacaktır. Özellikle son çeyrek asırda internetin hızla gelişmesi ve hayatın içinde kabul görmesiyle pek çok devlet işi de bu mecradan yürütülebilecek şekilde düzenlenmiştir. Bu gelişim sadece devletin işlerini daha hızlı ve kolay yapılabilir kılmamış aynı zamanda fonksiyonel değişiklikler de getirmiştir. Yani, daha yeni iletişim teknolojileri devletçe sadece kullanılmamış devletin yapısını da etkilemiştir. Burada en bariz örnek olarak bilgiye erişimin kolaylaşmasıyla insanların pek çok farklı fikre ve bakışa kolayca ulaşıp politik olaylara daha objektif yaklaşma imkanını bulmalarını gösterebiliriz. İşte bu gelişmeler, katılımcı ve etkin demokrasiye yeni imkanlar sunacak bir modelin ortaya çıkmasına yol açmıştır. Bu modelin adı ***"e-devlet"***tir[27].

Günümüzde insanların büyük bölümü, halkın temsilciler kanalıyla kendisi tarafından yönetildiği demokratik sistemlerde yaşamaktadırlar. E-devletin en önemli özelliklerinden biri bu yönetim biçiminin olabildiğince etkileşimli ve katılımlı olmasını sağlamaktır. Bu özelliğin sağlanmasında iletişim teknolojilerinin kullanılmasıyla "e-demokrasi" kavramı doğmaktadır. E-demokrasi kavramı "elektronik" ve "demokrasi" kelimelerinin bir araya getirilmesiyle oluşmuştur ve yukarıda geçtiği üzere elektronik haberleşme teknolojilerinin sağladığı olanaklardan faydalanarak daha katılımlı bir demokratik yönetim süreci oluşturmayı ifade etmektedir.

E-seçim ise e-demokrasinin en can alıcı noktalarından biridir. E-seçim kavramı tüm seçim sürecindeki aktiviteleri kapsamakla beraber, bu süreçte teknolojinin getirilerinden en çok faydalanılabilecek temel aktivite de e-oylamadır. E-oylamanın sunduğu fırsatlar arasında oy sayım işleminin kısaltılması, kullanılan her oyun sayıldığına ve fazladan oy eklenmediğine dair kanıtlar sunulması, oy sahtekarlığı veya oy kullanımı sırasında oluşabilecek hataların yok derecesine kadar azaltılmasını sağlama ve özel ihtiyaçları olan bireyler için sistem kullanımının kolaylaştırılması dolayısıyla da onların da yönetime katılımının ciddi düzeyde artırılması sayılabilir[28],[29].

Bugüne kadar akademik alanda pek çok elektronik oylama sistemi önerilmiş, bunlardan bir kısmı da pratikte kullanılmıştır. Bu sistemlerde genellikle yoğun olarak kriptografik algoritmalardan yararlanılmış ve sistemin fonksiyonel özelliklerinden çok teorik kriptografik algoritmalar üzerinde çalışılmıştır.

Önerilen elektronik oylama sistemlerini de işlevsel olarak temelde iki farklı şekilde ele almak mümkündür. Bunlardan birincisi oylama aşamasını da herkesin kendi bilgisayarı başından ve ağ üzerinden gerçekleştirebileceği uzaktan oylama sistemleridir. Bizim çalışmamızda üzerinde duracağımız model oylamanın belirli bir gün ve mekânda gerçekleştirildiği fakat kâğıt oy

pusulaları yerine güvenilir ve fonksiyonel oylama makinelerinin kullanıldığı şekildedir. Çünkü bu çalışmada amacımız teori ağırlıklı bir çalışma yapmaktansa hayata geçirilebilecek bir sistem önerebilmektir. Bu sistemde ise en temel nokta olan güven problemini TPM'nin sağladığı olanaklardan faydalanarak çözmeye çalışacağız. Günümüzde pek çok ülkede elektronik oylama makineleri(temel olarak dokunmatik ekranlı PC'ler) deneme aşamasında yahut hâlihazırda kullanımdadır. Geçtiğimiz dönemlerde de pek çok seçimde elektronik oy makineleri denenmiş fakat birçok sistem çaresizce kâğıt oy pusulalarına geri dönmüştür. Çünkü bu adım yağmurdan kaçarken doluya kapılmak gibiydi, bu makineler klasik oylama sistemleri kadar problemli olmasının yanı sıra bir de yeniden sayımları imkânsız hale getirmektedir. Bu yeni problem ve 2000 Florida Başkanlık seçimlerindeki oylama fiyaskosu gibi büyük bir hata insanların bu sistemler hakkında şüphe duymasına sebep olmuştur. Biz elektronik oylama makinelerinin kâğıt oy pusulalarına nazaran gerçek avantajları olduğuna inanıyoruz fakat burada oylama sadece bir parçası olacak şekilde tüm seçim sürecini ele almak gerekmektedir. Çok karmaşık bir sistem insanların şüphelerini artıracağından dolayı biz yeterli güvenliğe sahip olmanın yanı sıra pratik bir oylama sisteminin tüm bileşenlerini tanımlamaya çalıştık.Daha önceki çalışmaların tersine, gelişmiş bir kriptografi yerine ağırlıklı olarak sistem özellikleri üzerinde derinlemesine durduk. Sistemin detaylarından önce son olarak şunu belirtmeliyiz ki; önerdiğimiz sistem eski sistemle beraber hibrit bir şekilde de uygulanabilir. Detaylar kısmında yeri geldikçe bahsedeceğimiz üzere yeni sisteme uyum sağlayamayanlar ya da makineler aracılığıyla oy kullanamayanlar şu anda kullanılmakta olan kâğıt oy pusulaları vasıtasıyla oylarını kullanabileceklerdir. Bu sebeple seçim sisteminin değişimi sırasında kademeli bir sistem uygulanıp önerdiğimiz oylama makineleri ilk planda opsiyonel olarak seçmenlerin kullanımına sunulabilir.

Bizim burada temel olarak aldığımız sistem Tanenbaum ve ekibi tarafından önerilmiş çalışmadır[30]. Bizim önerdiğimiz sistem bu çalışmadaki sistemin ülkemize uyarlanmış halidir. Bu uyarlama esnasında ülkemiz verilerini temel almanın yanı sıra bizim seçim sistemimize daha uygun olacak şekilde küçük modifikasyonlara gidilmiştir. Mesela bahsi geçen çalışmada oylar insanların daha sonra internet üzerinden kendi tercihlerini görebilecekleri şekilde kaydedilmekte iken bizim çalışmamızda bu şekilde olmamaktadır. Çünkü bu özellik insanların oylama sonuçlarından şüphe duymamasına yardımcı olurken bir yandan da oy satımını mümkün kılmaktadır. Bizim ülkemizde oy satımını engellemek, aşağıda bahsedilecek güvenilirlik önlemlerine ekstra bir tane daha eklemekten daha önemli olabilmektedir. Bunun gibi küçük değişiklikler dışında bu çalışmada bahsi geçen sistem temel şablon olarak alınmış ve anlatılmıştır.

4.1 Sistemin Aşamaları

Önerdiğimiz sistem 9 adımdan oluşmaktadır ve süreç oylama işleminden yaklaşık bir yıl önce başlamaktadır. Bu adımlar:

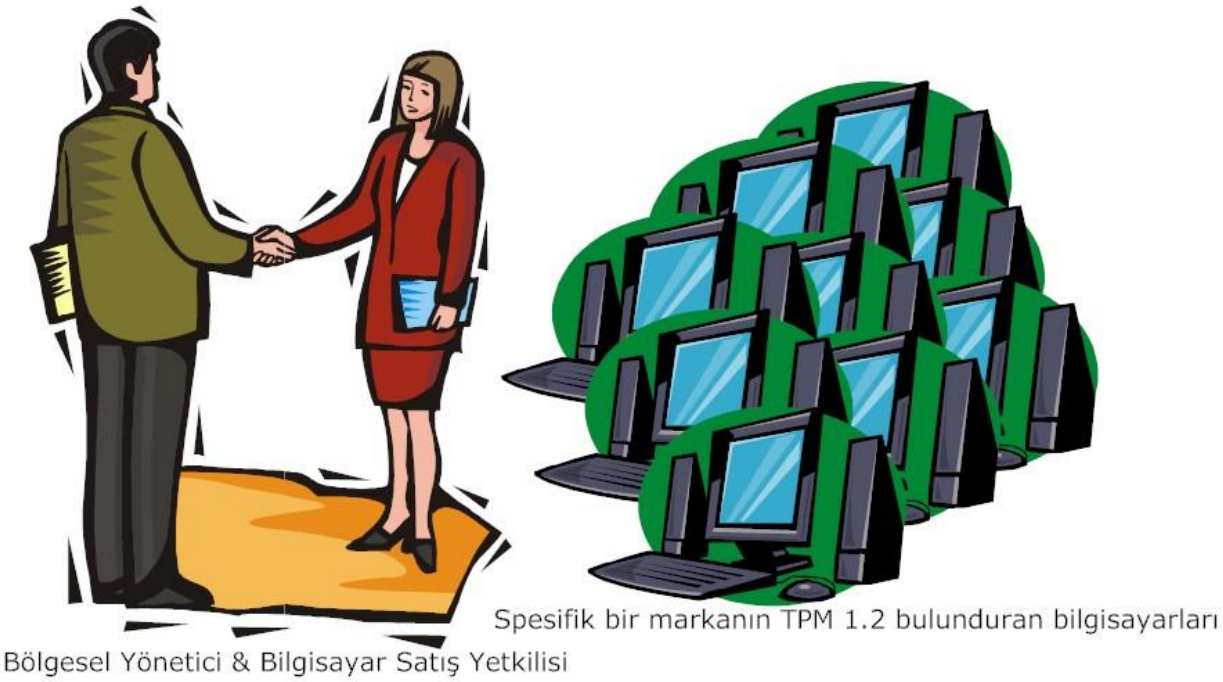
1. Ana anahtar üretimi ve dağıtımı
2. Seçmen kaydı
3. Seçmenlere seçim kartlarının postalanması
4. Oylama makineleri hazırlanması
5. Her seçim bölgesinde anahtar birleştirilmesi
6. Seçmenlerin gelmesi ve giriş yapması
7. Oy Kullanımı
8. Oylamanın sonlandırılması
9. Sonuçların yayınlaması

Bu adımlara daha detaylı olarak bakalım:

4.1.1 Ana anahtar üretimi ve dağıtımı

Biz de sistemimizde güvenlik amaçlı kriptografik algoritmalar kullandık. Bu sistemdeki kriptografik algoritmalar yeni önerilmiş ve teorik işlemler değil pratikte de kullanılan algoritmalardır. Örneğin hesaplama zamanı bir sorun olmadığı için (oylama makinelerinde ortalama birkaç dakikada sadece bir oy kullanılacaktır) RSA gibi güvenilen açık anahtarlı sistemler tercih edilebilecektir. Tüm seçim bölgeleri için birer açık-gizli anahtar çifti oluşturulacaktır. Seçim bölgesiyle seçimlerde oy kullandırılan binaları (genelde okullar) kastediyoruz.

Her bölgede donanım ve yazılımsal olarak birbirinin aynı olan onlarca makine bulunabilir. Bu sayede seçmenlerin şu anda olduğu gibi belirli bir sandıkta oy kullanma zorunluluğu olmaması bina içindeki herhangi bir makinede oylarını kullanabilmeleri sağlanacak ve seçmenler oylarını daha çabuk kullanabileceklerdir. Mesela 29 Mart 2009 Mahalli İdareler seçimlerinde Ankara'nın Çankaya ilçesinde 602.249 seçmen 116 seçim bölgesinde(mahalle) toplam 1964 sandıkta oy kullanmıştır[31]. Bizim senaryomuzda böyle bir seçimde bu ilçe için 1964 makine için toplam 116 anahtar çifti üretilecek ve ortalama her 17 makine de birbiriyle aynı olacaktır. Bir seçim bölgesinde oy kullanan ortalama 5192 seçmenden her biri de bu 17 makineden istediği birinde oyunu kullanabilecektir.



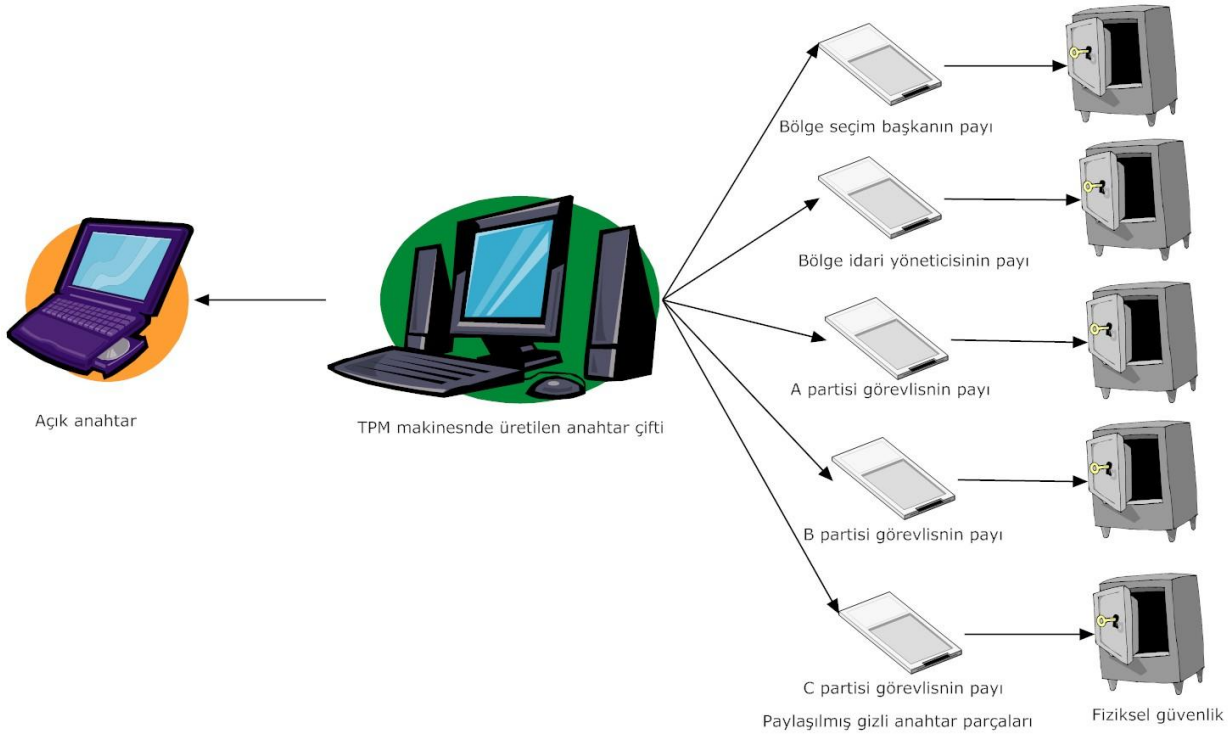
Şekil 4.1.1 Bilgisayar alımı

Seçim süreci Yüksek Seçim Kurulu tarafından TPM 1.2 destekli belirli bir marka bilgisayarın seçilip ihale yoluyla sandık sayısınca bu bilgisayardan alınmasıyla başlar. Alım yapılmasına karar verilen bilgisayarlar belirlendikten sonra bütün medya ve siyasi parti yetkililerinin hazır bulunduğu bir ortamda anahtar üretilmesi gerçekleştirilir. Teknik görevliler makinenin TPM yongasındaki EK'lerin uygun olup olmadığını inceleyebilir. Ayrıca gerekirse TPM'in de standartlara uygunluğu incelenebilir veya bağımsız bir teftiş kurulu ya da şirketi tarafından incelenmesi talep edilebilir. İnceleme aşamasının bu şekilde halka açık yapılması ve parti yetkililerinin inceleme şansı bulması sistemin güvenilirliğini artıracak ve de ileri de çıkarılması (özellikle de seçimi kaybedenler tarafından) muhtemel spekülasyonların önünü kesecektir. O bakımdan bu adım mühimdir çünkü bir seçim sistemi objektifliğiyle özellikle kaybedeni ikna edebilmelidir.

Şekil 4.1.2 Teknik İnceleme

İncelemeler tamamlanıp onay verildikten sonra anahtar üretilmesine geçilebilir. Her bir bölge için birer anahtar çifti bu aşamada üretilecektir. Bu üretim aşaması TPM'nin dışında yapılabilir. Üretilen açık anahtarlar imzalı bir şekilde bir dizüstü bilgisayarda kaydedilir. Üretim işleminden önce bilgisayarların güvenilirliği kontrol edildiği için üretilen anahtarlar güvenilirdir. Dilenirse kaydedildikleri dizüstü bilgisayarda açık anahtarlara farklı güvenilirlik testleri de uygulanabilir.

Gizli anahtar çiftleri ise farklı bir işleme tabi tutulmalıdır. Bu anahtarlar iki veya daha çok parçaya bölünmelidir. Bu bölme işlemi basit bir şekilde XOR bit işlemi sonucu anahtarı verecek parçaların üretilmesi şeklinde olabileceği gibi farklı bilgi paylaşım metotları da kullanılabilir. Bu metotlar parça sahiplerinden bazılarının sahtekârlık yapması durumunda anahtarın geri kalan parçalardan tekrar üretilmesine imkân verecek şekilde de seçilebilir[32][33][34]. Üretilen anahtar parçaları yine güvenilir ve çok karmaşık olmayan kayıt cihazlarına yüklenebilir. Mesela basit bir I/O sürücüsüne sahip olan akıllı kartlar kullanılabilir.



Şekil 4.1.3 Anahtar üretimi ve Gizli anahtarın paylaştırılması

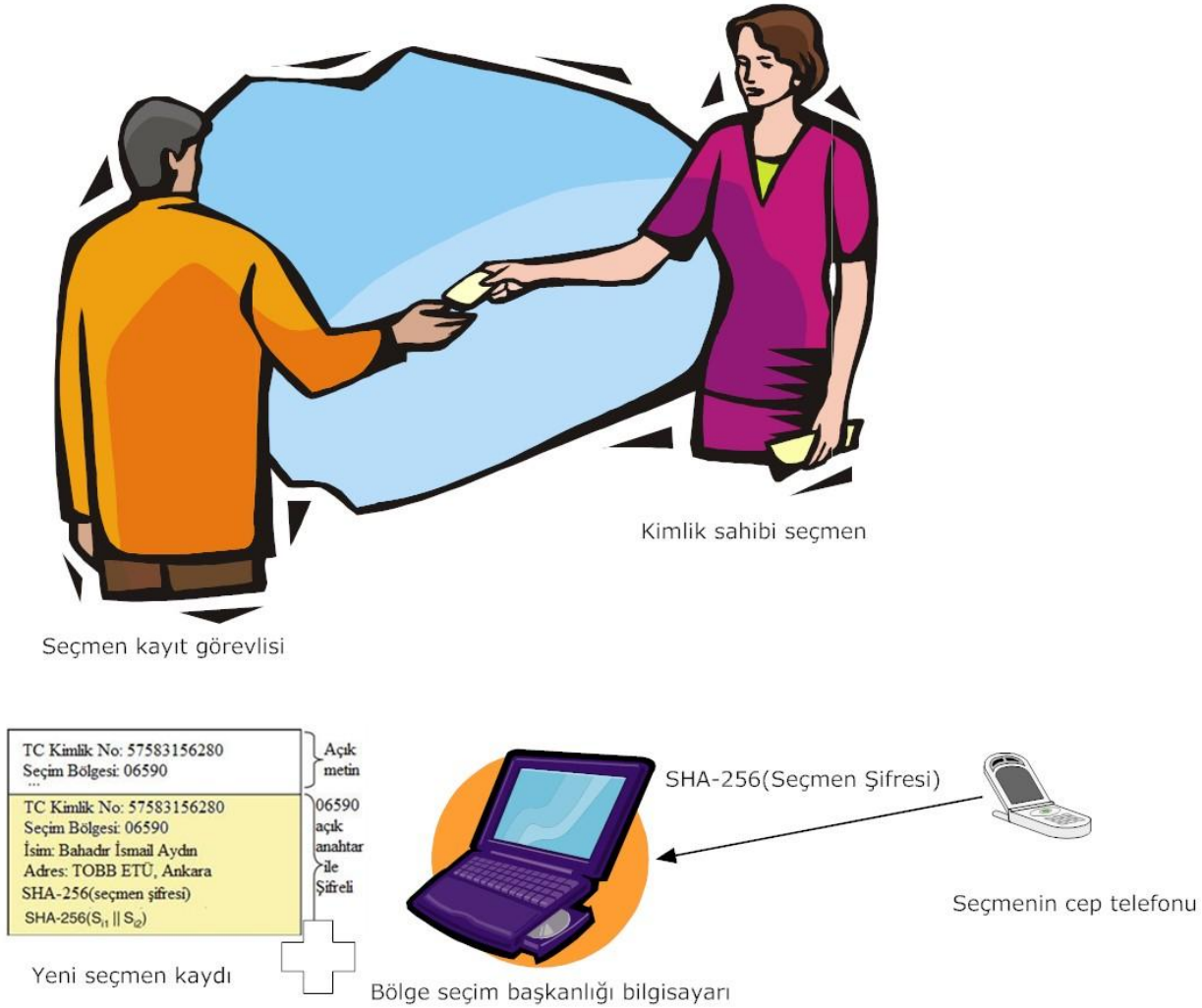
Bütün anahtar parçaları aynı gün içinde üretilip kartlara yüklendikten sonra bu parçalar güvenli bir şekilde paylaşanlara dağıtılabilir. Paylaşanların kimler olacağı siyasi yetkililer tarafından karar verilebilir. Mesela bir parça bir evrak çantasına konulup kilitlenerek ilgili seçim bölgesinin baş görevlisine teslim edilebilir. Bir diğer parça da aynı şekilde bir başka kilitli çanta içinde seçim bölgesinin idari yetkilisine (örneğin mahalle için muhtar) teslim edilebilir. Dilenirse parti yetkililerine veya en büyük bir kaç parti görevlisine de parçalar verilerek anahtar üretimi ve dağıtımı sağlanmış olur.

Seçimden uzunca bir süre önce tüm oylama makinelerindeki TPM'lere ait EK sertifikaları ve seçim bölgelerinin açık anahtarları Yüksek Seçim Kurulu'nun internet sayfasında yayınlanmalıdır.

4.1.2 Seçmen kaydı

Anahtar üretimi ve paylaşımı tamamlandıktan sonra seçim görevlileri seçmenlere duyuru yapıp seçmen kayıtlarını başlatabilirler. Kayıt olabilmek için şu anda olduğu gibi bizim sistemimizde de fotoğraflı bir nüfus cüzdanı gereklidir. Eğer o anda seçim kanununda başka belgeler de isteniyor yahut nüfus cüzdanı yerine geçerli sayılıyorsa bunlar bizim sistemimiz için de direkt olarak geçerli kılınabilir.

Seçmenlerin kayıt bilgileri sadece yazılabilen bir dosya yapısında saklanır. Bu kayıt bilgileri içerisinde klasik nüfus veya ulaşım bilgileri dışında da seçmenin seçim sırasında oy kullanabilmesi için gerekecek bir de şifre bulunur. Bu şifre sözlük ataklarına karşı kuvvetli olacak düzeyde uzun fakat seçmenin hatırlayabileceği kolaylıkta seçilmelidir. Seçmenler bu şekilde birer şifre seçmeleri hususunda teşvik edilebilirler. Yahut şifreleri bilgisayar tarafından üretilip seçmenlere verilebilir. Bu takdirde grafiksel şifreler de akıllıca bir tercih olabilir[35]. İlk planda bu konuya dair bazı kafa karışıklıkları olabileceği düşünülebilir fakat insanlar bu sisteme kolaylıkla uyum sağlayabileceklerdir. Günümüzde insanlar e-posta şifrelerini veya bilgisayar giriş şifrelerini kolaylıkla hatırlayabilmektedirler.



Şekil 4.1.4 Seçmen kaydı

Seçmenler şifrelerinin seçim görevlilerince öğrenilmesinden çekiniyorlarsa ya da dilerlerse şifrelerini seçim kurulunun internet sayfasında yayımlanacak yardımcı açık program vasıtasıyla evlerinde üretip bu şifrenin SHA-256 özüt değerini cep telefonlarında, cep veya dizüstü

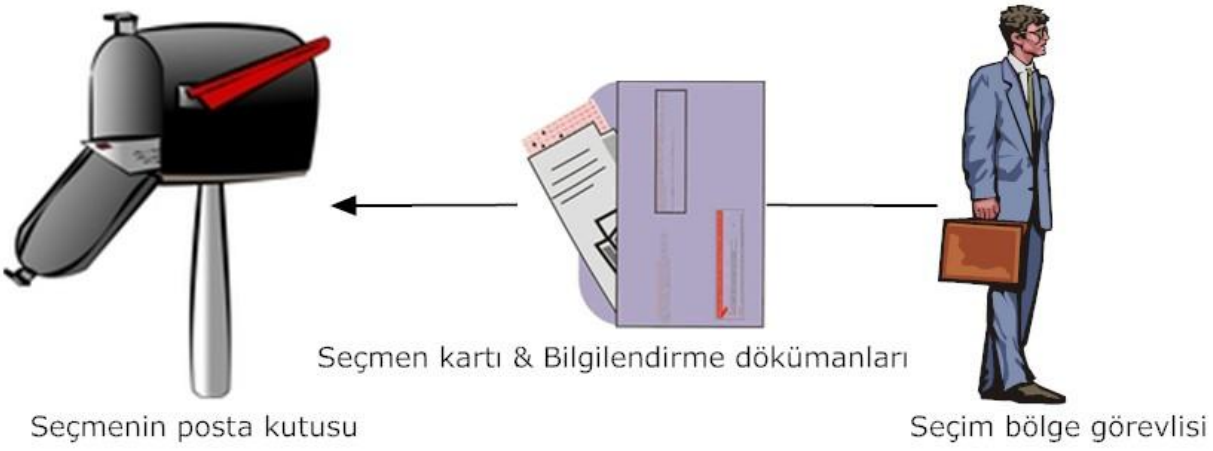
bilgisayarlarında belirlenmiş bir formatta saklayarak bu değeri güvenli bir veri yoluyla bölgesel seçim yetkilisinin bilgisayarına yükleyebilirler.

Dilenirse kayıt sırasında sınav kayıtlarındaki gibi seçmenlerin fotoğrafı çekilebilir. Bu fotoğraflar ileride basılacak seçmen kartlarında kullanılıp seçim günü seçmen girişi için bir güvenlik önlemi olarak kullanılabilir.

Bu şifreye ek olarak bölgesel görevlinin bilgisayarında *i*'ninci seçmen için rastgele bir güvenlik kelimesi S_i üretilir ve bu kelime $S_i = S_{i1} \,||\, S_{i2}$ (|| is arka arkaya ekleme ya da XOR işlemi olabilir) olacak şekil iki parçaya bölünür. Seçmen kaydında bu güvenlik kelimesinin özüt bilgisi SHA-256($S_{i1} \,||\, S_{i2}$) yani değeri de saklanır.

Bir kayıt oluşturulduktan hemen sonra seçim bölgesine ait açık anahtarla şifrelenir ve sadece yazılabilir dosyaya eklenir. Şifreli bu kayıtların başına açık bir şekilde kısa birer başlık eklenmelidir ki hangi kaydın hangi seçmene ait olduğuna ileride ulaşılabilsin. Bu başlık seçmenin TC Kimlik numarası ve oy kullanacağı seçim bölgesinin numarasını içermelidir. Böylelikle seçimlere kadar seçmen kayıtlarına erişilmesi ya da kayıtların değiştirilmesi engellenmiş olacaktır.

4.1.3 Seçmenlere seçim kartlarının postalanması



Şekil 4.1.5 Seçmen kartı ve bilgilendirme belgelerinin postalanması

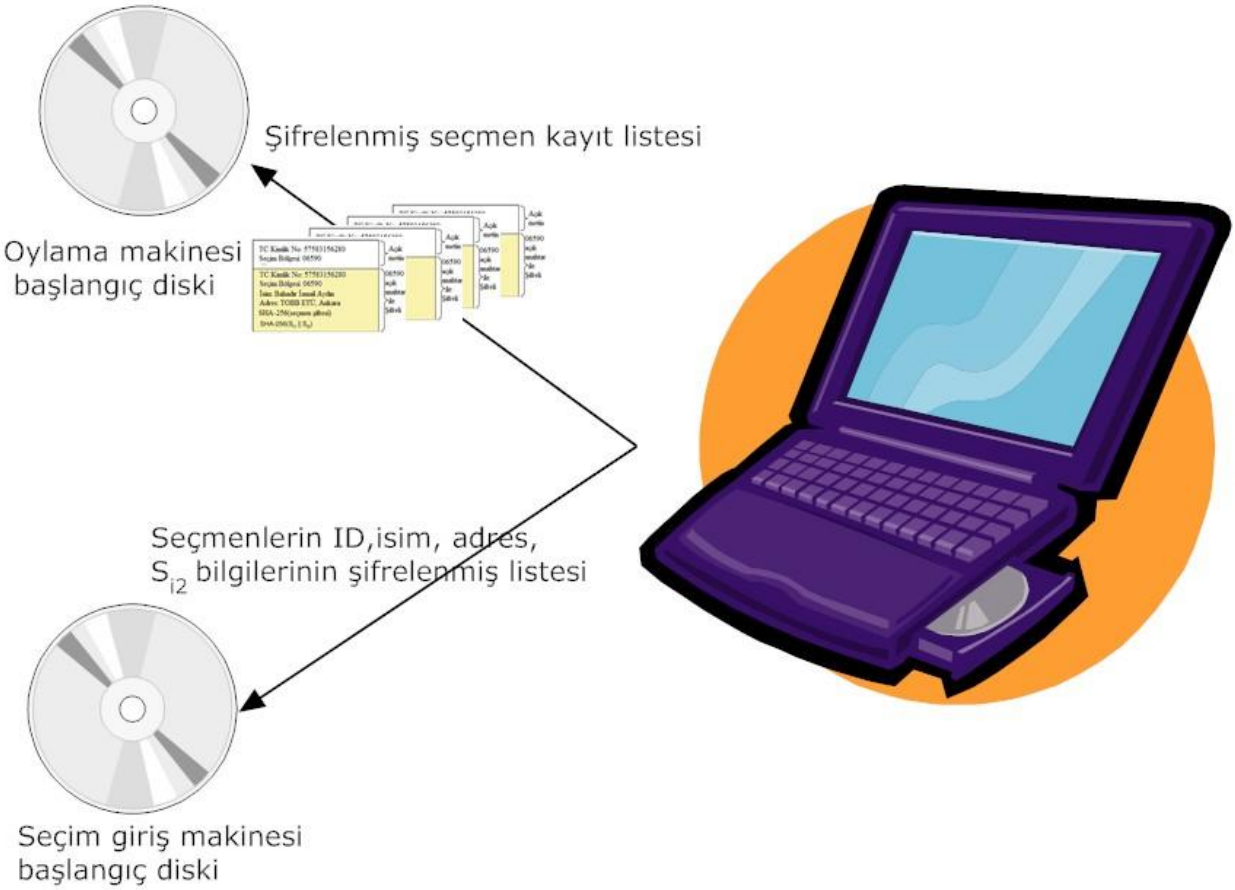
Seçimden bir ay kadar önce seçim müdürlüklerince seçmenlere bir posta yollanır. Yollanan zarfın içinde seçimde nasıl oy kullanılacağına dair bilgilendirme dokümanları ile seçmen kartı bulunacaktır. Seçmen kartı kolay kullanılabilen güvenli ve ucuz bir kart (örneğin üzerinde çip bulunan otobüs biletleri için kullanılan kartlar) olup hem seçmenin seçim günü kullanacağı nüfus kartı yerine geçer hem de kayıt

yaptırdığının göstergesidir. Bu kart aynı zamanda kayıt sırasında oluşturulan S_{i1} bilgisini de içermelidir. Bu bilgi ister kart üzerine açıktan yazılabilir, istenilirse de karta kaydedilebilir. Seçmen kartları yukarıda bahsedildiği gibi fotoğraflı da olabilir. Bu kart aynı zamanda seçmenin oy kullanacağı binanın adres bilgilerini, oy kullanma tarih ve saatlerini içermekte ve şifresini hatırlaması ya da bir cihaza yüklemişse yanında getirmesini hatırlatan bir uyarı yazısı bulundurmaktadır.

4.1.4 Oylama makineleri hazırlanması

Daha önce bahsettiğimiz TPM 1,2 çip bulunduran makinelerin hazırlanması işlemi oylama gününden önce yapılmalıdır.

Bir seçim bölgesindeki har makine için o bölgede oy kullanacak tüm seçmenlerin listesini içeren bir dosya hazırlanır. Bu liste ilgili tüm seçmen kayıtlarını şifreli bir şekilde bulundurmaktadır. Seçim bölgesindeki tüm makinelerde aynı listenin (o bölgedeki tüm seçmenlerin listesi) bulunması sayesinde bir seçmen kendi bölgesindeki istediği makinede oyunu kullanabilecektir. Bu da daha önce de bahsettiğimiz üzere daha adil bir dağılım sayesinde seçmenlerin oylarını daha çabuk kullanmasını sağlayacaktır. Bir seçmen yanlış bir seçim bölgesine gitmişse oyunu geçerli sistemdekine benzer oy pusulaları vasıtasıyla kullanabilir çünkü kayıtlı olmadığı bir bölgede oy kullanması mümkün olmayacaktır. Aynı şekilde günümüzde olduğu gibi havaalanı gibi bazı istisnai mekânlarda oy kullanmak durumunda kalmışsa oyunu kağıt oy pusulaları vasıtasıyla kullanabilir.



Şekil 4.1.6 Bilgisayar Başlangıç Disklerinin Hazırlanması

Liste hazırlandıktan sonra tüm liste de kayıtlar gibi seçim bölgesine ait açık anahtarla şifrelenir ve sadece okunabilir bir cihaza kaydedilir (örneğin CD). Bu cihaz oylama makinelerini başlatmak için kullanılacaktır. Listenin şifrelenmesinin nedeni listeye ekleme çıkarma yapılmasını engellemektir. İkinci bir başlangıç diski ise seçim giriş bilgisayarı için hazırlanır. Bu disk o bölgede oy kullanacak seçmenlerin TC kimlik numaraları, isim, adres ve S_{i2} değerlerini içeren bir liste bulundurmaktadır. Bu dosya da aynı amaçla seçim bölgesinin açık anahtarıyla şifrelenir.

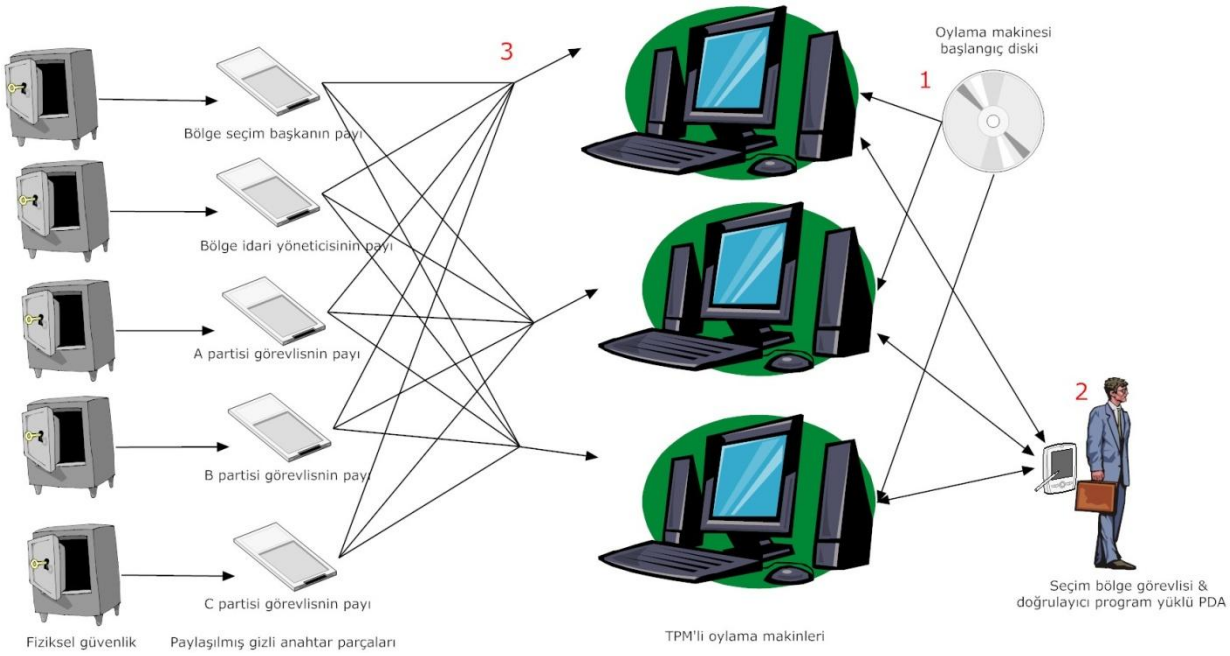
Oylama ve giriş makineleri yukarıda bahsedilen başlangıç disklerinden başlatılacağı için birer sabit diskleri olması gerekmemektedir.

4.1.5 Her seçim bölgesinde anahtar birleştirilmesi

Seçim günü seçim saatinden bir süre önce seçim bölgesi görevlileri seçim bölgesine gelmelidir. Bu uygulama zaten hâlihazırdaki sistem için de geçerlidir. Mesela seçimler sabah saat 08:00'de

başlıyorsa saat 07:00'de seçim bölgesine ait gizli anahtar parçalarına sahip bulunan görevli ve temsilciler seçim bölgesinde buluşurlar. Her biri evrak çantalarının kilidini açar ve akıllı kartlarını seçim bölgesi baş görevlisine teslim ederler. Bu hususta kanuni yaptırımlar sayesinde seçimi engellemek isteyebilecek girişimler engellenmelidir. Her halükarda yine de anahtarın yeniden oluşturulmasını sağlayacak şekilde anahtar paylaşımı yapılabileceğine 4.1.1'de değinmiştik. Oylama makineleri, hazırlanan başlangıç diskleri kullanılarak başlatılmadan önce geçen süreçte herhangi bir sahtekârlığa uğramadıklarından emin olmak için son bir incelemeden geçirilebilir. Sonra makineler 4.1.4'te hazırlanan disklerle başlatılır.

Böylelikle burada bir TPM zinciri oluşmuştur. Yani TPM ilk önce güvenli şekilde önceden incelenmiş BIOS'u ve önyükleyiciyi kontrol eder. Sonrasında CD'den başlatılan işletim sisteminin de önceden kontrol edildiği şekilde olup olmadığı ölçülür. Son olarak da oylama programı kontrol edilir. Böylelikle zincir tamamlanmış olur.



Şekil 4.1.7 Oylama Makinelerinin Başlatılması

İşletim sistemi ve oylama programı yüklendikten sonra seçim görevlileri PDA'lar kullanarak yazılımı kontrol ederler. Kullanılan yazılım kesintileri (interrupts) ve DMA'yı engellediği için bu aşamadan sonra yetkisiz hiç bir yazılım programı engelleyemeyecektir. TPM'nin yukarıda bahsedilen güvenlik özellikleri işte bu güvenlik ve kontrol aşamasında devreye girmektedir.

Herhangi bir ağ mevzu bahis olmadığı için de pek çok tehdit bizim sistemimiz için söz konusu değildir.

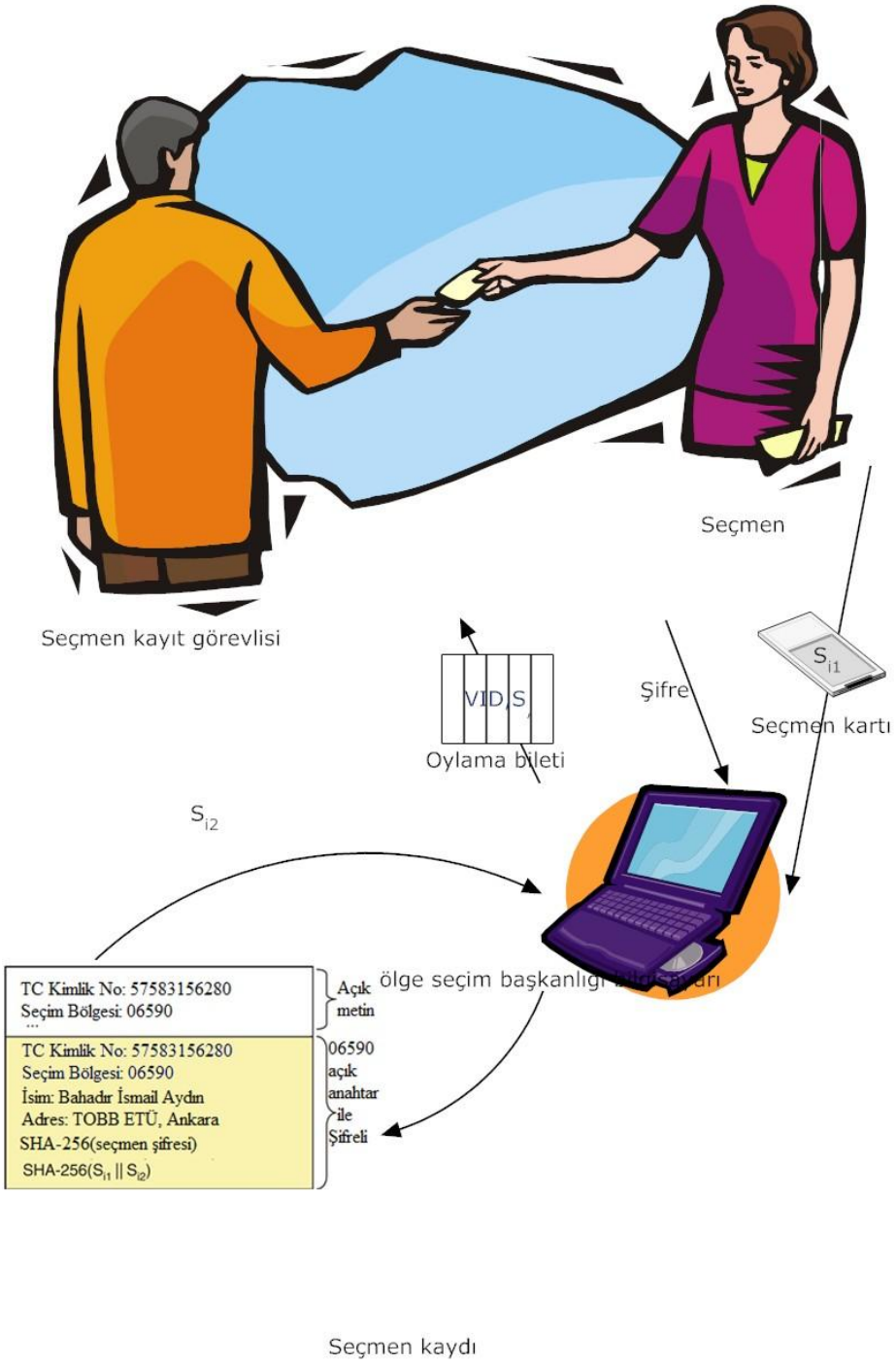
Yazılım da test edilip onaylandıktan sonra seçim baş görevlisi topladığı akıllı kartlara kendininkini ekler ve gizli anahtarı oluşturup CD'lerde gelen listelerin ve bu listelerdeki kayıtların şifresini çözer. Bu anahtar oluşturulması TPM'nin dışında gerçekleştirilebilir çünkü tüm yazılım güvenli bir şekilde çalışmaktadır.

Bu adımdaki işlemler seçim giriş makineleri için de aynı sırayla gerçekleştirildiğinde artık her şey seçimin başlatılması için hazır olacaktır.

4.1.6 Seçmenlerin gelmesi ve giriş yapması

Kapılar açıldığında seçmenler sırayla seçim giriş bilgisayarına gider ve kendisine postalanan seçmen kartlarını teslim ederler. Seçmen kartını getirmemiş olanlar geçerli bir kimlik bulundurdukları takdirde kâğıt oy pusulası ile oy kullanabilirler. Seçim giriş görevlisi seçmenin TC kimlik numarasını seçim giriş bilgisayarına girer ve ilgili kaydı görür. Görevli kayıttaki ve karttaki isim ve adres bilgilerinin eşleşip eşleşmediğini kontrol eder. Eğer seçim kartları fotoğraflıysa görevli kartı veren seçmenin fotoğraftaki kişiyle aynı olup olmadığını kontrol eder. Bu ekstra bir güvenlik sağlayacaktır. Daha sonra görevli seçmene şifresini hatırlayıp hatırlamadığını sorar. Burada seçmen görevliye şifresini değil sadece şifresini hatırlayıp hatırlayamadığını söyleyecektir. Hatırlayamadığı takdirde görevli klasik kâğıt oy pusulası verir ve seçmen hâlihazırdaki sisteme benzer şekilde oy kullanır.

Seçim görevlisi seçmen kartı olarak kullanılan akıllı kartın çeşidine göre bir barkot ya da kart okuyucu vasıtasıyla kartta yüklü olan S_{i1}'i seçim giriş makinesine yükler. Daha sonra S_{i1} değeri kayıtlı olan S_{i2} değeri ile birleştirilip $S_i = S_{i1} \,||\, S_{i2}$ tekrar elde edilir. Daha sonra bir oylama bileti oluşturulur. Bu da yine bir akıllı karttır ve üzerinde *TC Kimlik No* ve S_i değerleri yüklüdür. Seçmen oylama biletini alır ve kaydı giriş yaptığı belirtilerek tekrar şifrelenir. Bundan sonra seçmen seçim bölgesindeki (bulunduğu bina) istediği seçim makinesinde oyunu kullanabilir.



Şekil 4.1.8 Seçmen Girişi

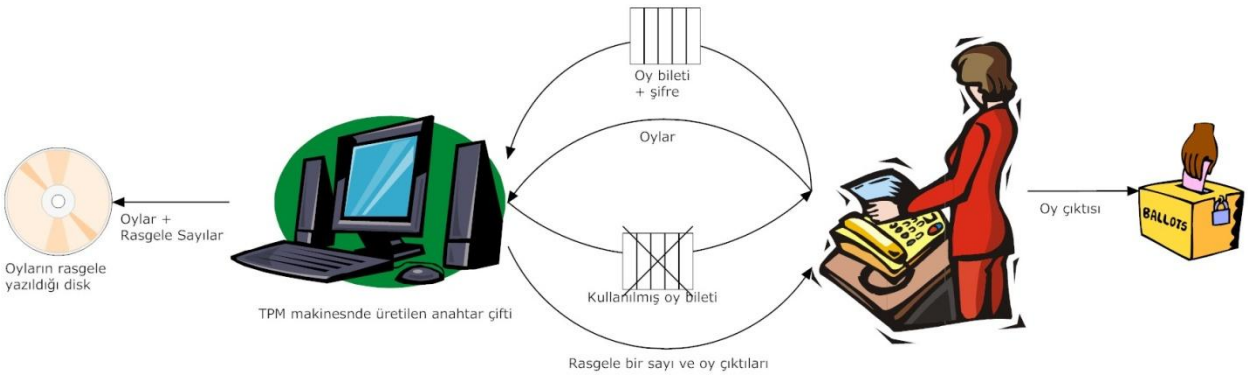
4.1.7 Oy Kullanımı

Oylama sürecine kadar donanım ve yazılım birden çok test ve incelemelere tabi tutulmuş olmasına rağmen, dilerse bir seçmen oylama esnasında YSK'nın sitesinde yayınlanan açık kaynak kodlu programın çalışıp çalışmadığını test edebilir. Bu durumda seçmenin yapacağı şey

seçim görevlisinin yaptığı yazılım testinden farklı değildir. Yani bir taşınabilir cihaz (cep telefonu,PDA…vs) vasıtasıyla oylama makinesine bir rastgele metin(challenge) gönderip, cevap olarak dönülen metnin yolladığı metnin ve çalışan yazılımın doğru şekilde imzalanmış bir özeti olup olmadığını kontrol edecektir. Bu imza TPM içinde üretilecektir çünkü TPM'nin gizli anahtarı dışarı çıkarılamamakta olduğu için işletim sistemi tarafından bilinemez. TPM'nin uzaktan doğrulama özelliğinden faydalanarak tasarladığımız seçmen tarafından kontrol edilebilme yeteneğinin elektronik seçim sistemlerine geçişin önündeki en büyük sosyolojik engel olarak gözüken güven problemine karşı çözüm sunduğuna inanıyoruz.

Oy kullanmayı anlatmadan önce belirtmek gerekir ki elektronik oylamanın avantajlarının en belirgin şekilde ortaya çıktığı aşamalardan bir tanesi budur. Oy vermenin interaktif, doğrulanabilir, ses veya değişik mültimedya özellikleri kullanılarak engelli bireylerin işini kolaylaştıran fonksiyonların sağlanması, farklı dil seçeneklerinin sunulması gibi özelliler kazanması bu aşamada elektronik oylamayı tercih sebebi yapmaktadır.

Sistemimizde, bir seçmen oylama makinesinin başına geldiğinde, ekranda kendisinden oylama biletini sokmasını isteyen talimatı görecektir. Oylama biletinden seçmenin TC kimlik numarası okunup, SHA-1($S_{i1}||S_{i2}$) özüt değeri hesaplanacak ve bu değer, kaydedilmiş olan değerle kıyaslanacaktır. Bu değerlerin eşlenmesi sonucunda, seçmenin postalanan kartı aldığı(S_{i1} değerini bulundurduğu için) ve seçim giriş makinesi aracılığıyla kimliğini doğrulatarak giriş yaptığı (S_{i2}'yi bulundurduğu için)anlaşılmış olduğu için oy kullanmasına onay verilecek ve şifresinin sorulduğu ekran belirecektir. Şifresinin özütü alınıp kayıtlardan kontrol edilip oy kullanması istenecektir. Burada şifresini girerken hata yapmış olma ihtimaline karşın çok fazla olmayan bir k sayısına kadar deneme hakkı tanınabilir. Bu şifre çalıntı seçmen kartları ya da sahtekâr seçim görevlilerine karşı güvenlik sağlamaktadır.

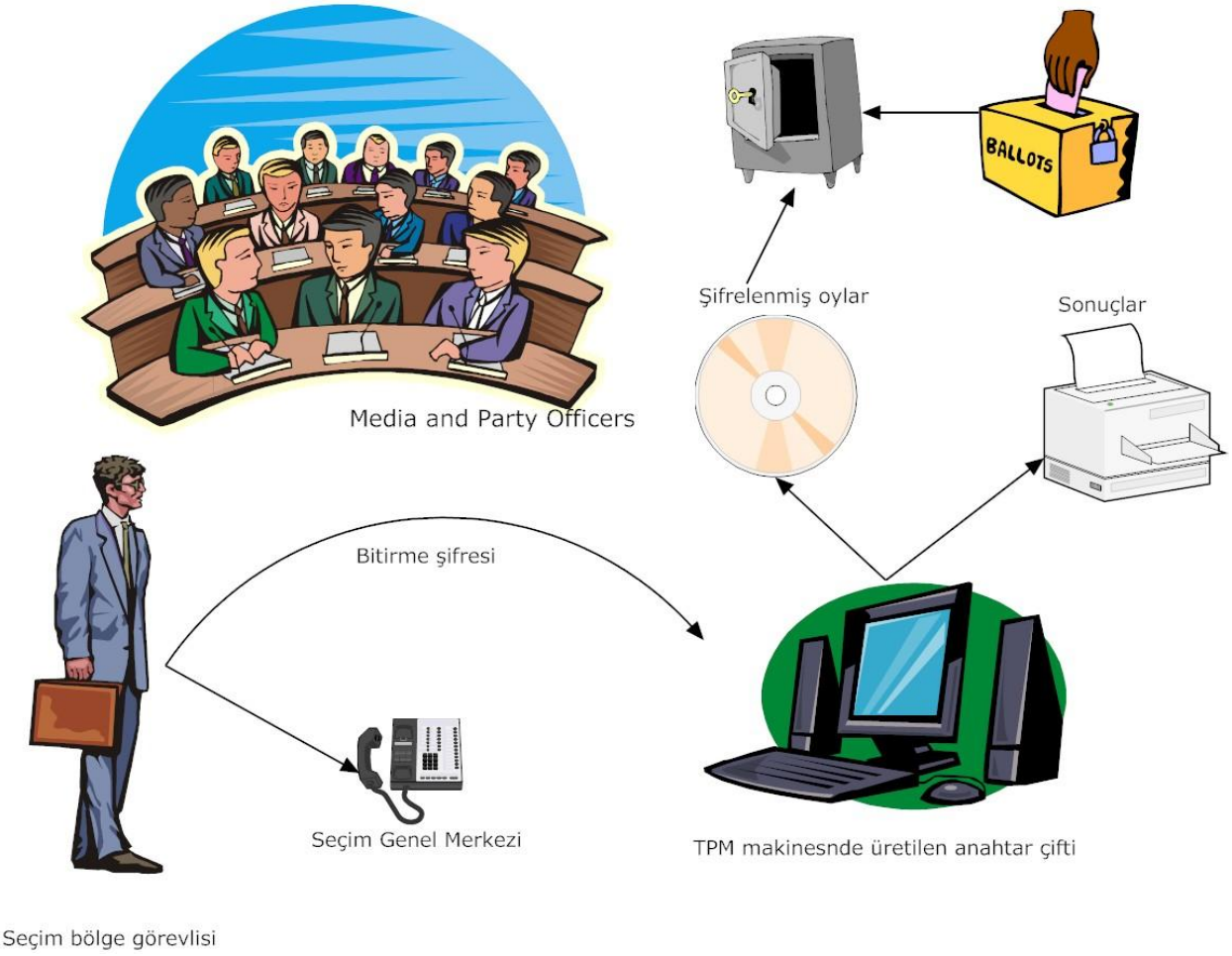


Şekil 4.1.9 Oylama

Doğru şifreyi giren seçmen artık oyunu ya da oylarını girebilir. Oylamayı tamamladıktan sonra da seçmeme tercihlerini bulunduran, istediği seçimleri yapmadığını kontrol ettiği bir onay ekranı gösterilir. Seçmen dilerse oylarını değiştirebilir. Seçmen oylarını onayladıktan sonra bu oylar harici bir bellek ünitesine (CD veya flash bellek)kaydedilir ve oylama bileti de yeniden kullanılamayacak şekilde yeniden yazılır(rastgele sayılarla doldurulabilir). Yalnız burada dikkat edilmesi gereken bir husus oyların kullanıcıların oy kullanmasıyla paralel değil karışık şekilde kaydedilmesi gerektiğidir. Bu şekilde seçim görevlilerinin kimin hangi oyları kullandığının tespit edebilmesinin önüne geçilmiş olacaktır. Son olarak makine seçmene oylarının basılı olduğu bir oy pusulasının çıktısını verecek ve seçmen oylarının istediği şekilde işlendiğini görüp bu basılı pusulayı şu anki sistemde olduğu üzere kapalı şekilde seçim görevlilerinin nezaretinde oy sandığına atacaktır. Sistemin hibrit özelliğine katkıda bulunan bu metot, üzerinde derinlemesine durduğumuz güvenirlik adına da çok mühim bir getiri sağlamaktadır. Seçim sonuçlarına dair bir şaibe olduğunda ya da adayların aldıkları oylar arasında belirsizlik doğuracak kadar az fark oluştuğunda bu kâğıt oy pusulalarının tekrar sayımına başvurulabilecektir. Sonuçta her halükarda, resmi kesin sonuçlar bu basılı oy pusulalarının oluşturduğu toplamlar olacaktır.

4.1.8 Oylamanın sonlandırılması

Seçim saati dolunca seçim bölgesinin girişler kapatılır ve seçim bölgesinin baş görevlisi bölgedeki her oylama makinesine gizli kodu girerek seçimi sonlandırır. Tüm oylar şifrelenir ve elektronik oyların sonuçları parti yetkililerinin gözetimi altında çıktı olarak basılır. Tüm oy makinelerinde oturum kapatılıp sonuçlar basılınca oyların kaydedildiği bellek ünitesi ve oy sonuçlarının çıktıları bir evrak çantasına konulup kilitlenir. Oy sandığıyla beraber bu evrak çantası seçim genel müdürlüğüne teslim edilebilir. Elektronik (ön)sonuçlar ise ağ aracılığıyla otomatik olarak değil baş seçim görevlisi tarafından telefonla merkeze bildirilir çünkü makineler ağa bağlı değildir ve çok da zor bir iş olmayan bu bildirimi otomatik olarak sağlamak için makineleri ağa başlamak pek çok yeni saldırıyı mümkün kılabilir.



Şekil 4.1.10 Oylamanın Sonlandırılması

4.1.9 Sonuçların yayınlaması

Oyların bulunduğu diskler seçim merkezlerinde bulunan ve gerekli güvenlik testlerinden geçirilmiş makinelerde okunarak (dilenirse birkaç defa ya da birkaç farklı makinede) kesin elektronik sonuçlar hesaplanır ve sonuçlar gerekli mercilere ve siyasi partilere bildirilir. Sonuçlar son olarak YSK'nın internet sayfası aracılığıyla tüm kamuoyuna ilan edilir.

5. SONUÇLAR

Günümüzde insanlar eskiden beri yapageldikleri pek çok işi yeni yöntem ve teknolojilerle yapmaktadırlar. Hayata dair pek çok alanda teknolojilerin getirilerinden özellikle de akıllı sistemlerden yararlanılmaktadır. Dünya üzerindeki hemen tüm insanları ilgilendiren ve kısıtlı bir zaman aralığında milyonlarca insanı birden işleme tabi tutmayı gerektiren seçim işlemlerinde

hala günümüz teknolojisinden yararlanamıyor olmamız çok büyük bir eksikliktir ve artık bu alanda da yeni bir sisteme geçmek gereklidir.

Hayatı kolaylaştıran yenilik insanlar tarafından kolaylıkla kabul edilemeyebiliyor. Yiyeceklerini pişirmek için tandırları kullanan insanların daha pratik de olsa fırını hemen kabul etmeleri beklenmemelidir. Ama hayatın gelişiminde bu geçiş yapılmalıdır. İlk planda mühim olan çok kapasiteli fırınlar kullanmak değil bu geçişi sağlamaktır. Bunu takiben fırını kullanmaya alışan insan daha akıllı ve daha özellikli fırınlara kolayca alışabilmiştir. Aynı şekilde seçim sistemi de pek çok avantaj kazanılacak olmasına rağmen alışma zorluklarından ötürü kolaylıkla değiştirilemeyebilir. Bunun yanı sıra seçim gibi insanların yönetilmesinde ehemmiyet taşıyan bir konuda diğer durumlara nazaran ekstra zorluklar söz konusu olmuştur. Bundan ötürü pek çok deneme yarım kalmış, akademik olarak çok gelişmiş pek çok teknik sunulmuş olmasına rağmen hayata geçme imkanı bulamamıştır.

Artık seçim sisteminde yeni metotların kullanılmasının zamanı geldiğine inanıyoruz. Bu sebeple sistemin genelini ele alıp teknolojik imkanlardan yararlanılan yeni yöntemler önerdik. Bugün bu alanda teknolojiden mahrum kalmanın nedeni önerilen sistemlerin karmaşıklığı ve zaten insanların küçük bir ihtimalden bile şaibe doğurmaya hazır olduğu bir alanda bu karmaşıklıktan kaynaklanan şüpheyse yapılması gerekenin yeni ve var olanlardan çok daha gelişmiş yöntemler geliştirmek değil olabildiğince basit ve bu basitlikten dolayı insanların güvenebileceği bir sistem önermektir. Biz de öyle yaptık. Önerdiğimiz sistemde hep önceliğimiz insanların güvenini kazanmak oldu. Kağıt pusulalardan oylama makinelerine geçişi sağladıktan sonra en önemli değişikliğin sağlanmış olacağı ve daha sonra daha gelişmiş sistemlerin kullanılabileceği aşikardır. Zaten ilk planda yeterli güvenlik düzeyi sağladıktan ekstra güvenlik önlemleri almak trafiğe tankla çıkmaya benzer ki bu bir yandan ilk planda aciliyeti olmayan fonksiyonlar için güvenden feragat etmeyi gerektirmektedir. Bugüne kadar önerilen pek çok sistemin uygulanamamasının nedenlerinin başında bu durum gelmektedir.

Yukarıda detaylarıyla anlattığımız sistem, seçimlerde yeni teknolojilerin kullanılmasını sağlayacak geçişe yol açacaktır çünkü öncelikle insanların güvenini kazanabilecek basitlikte ve açıklıktadır. Bunun yanı sıra uyum sorununu aşmak adına kademeli bir geçişi sağlayacak hibrit bir yapı önerdik yani kağıt pusulalar da yeni sistemle beraber kullanılmaya devam edebilecektir. Bir gün muhakkak gerçekleşeceğine inandığımız bu geçişin ekonomik boyutu da önemlidir. 29 Mart 2009 mahalli seçimlerinde 22677450 seçmen 74975 sandıkta oy kullanmıştır[36]. On binlerce sandığın yerini alması gerekecek on binlerce oylama makinesi değişimi engelleyen ciddi bir ekonomik sorundur. Bizim önerdiğimiz sistemde bu makineler basit birer kişisel bilgisayardan ibarettir ve sabit diskleri bile mevcut olmak durumunda değildir. Kolaylık açısından dokunmatik ekranlar pek çok önerilecek sistemdeki gibi bizim sistemimiz için de daha

uygun olsa da zorunlu değildir. Kullandığımız özel donanım olan TPM ise maliyeti $1 gibi uygun fiyatlarla temin edilebilecek bir çiptir. Bu durum, yeni teknolojilere uyum sağlama yolunda ekonomik olarak en uygun tercihin önerdiğimiz sistem olacağını göstermektedir.

Bugüne kadar yapılan denemelerden yola çıkarak en uygun sistem olarak önerdiğimiz bu çalışma, deneme imkanı bulunursa daha da geliştirilebilecektir. Geçişi sağlamak için ilk ve en önemli adım atıldıktan sonra önerilmiş olan gelişmiş algoritmalar da bu sistem sayesinde pratikte uygulanma imkanı bulabilir. Hem güvenlik hem de güven göz önünde bulundurularak tasarlanmış bu sistem sayesinde artık seçimlerimizi çağın şartlarına uygun yapabilmek mümkün olacaktır.

KAYNAKLAR

[1] Trusted Computing Group Web Sitesi, Erişim adresi: https://www.trustedcomputinggroup.org, Erişim tarihi: 27.07.2009.

[2] "Intel Trusted Execution Technology Overview" Erişim Adresi: http://www.intel.com/technology/security/downloads/TrustedExec_Overview.pdf , Erişim tarihi: 09.04.2009.

[3] "AMD Secure Virtual Machine Reference Manual" Erişim adresi,: http://www.mimuw.edu.pl/~vincent/lecture6/sources/amd-pacifica-specification.pdf, Erişim tarihi: 09.04.2009.

[4] "HP ProtectTools Embedded Security technical whitepaper", Erişim Adresi: ftp://ftp.compaq.com/pub/products/security/embedded_security_-_implementation.pdf, Erişim tarihi: 09.04.2009.

[5] "Windows Bitlocker Drive Encryption", Erişim adresi: http://www.microsoft.com/windows/windows-vista/features/bitlocker.aspx, Erişim tarihi: 09.04.2009.

[6] Kauer , B., OSLO: Improving the security of trusted computing, 16th USENIX Security Sempozyumu, Boston, MA, USA, 6-10 Ağustos, 2007.

[7] McCune, J.M., Parno, B., Perrig, A., Reiter, M.K., Isozaki, H., Flicker: An execution infrastructure for TCB minimization, ACM European Conference in Computer Systems, EuroSys 2008, 2008.

[8] Pfitzmann, B., Riordan, J., Struble, C., Waidner, M., Weber, A., The PERSEUS system architecture. In Dirk Fox, Marit K¨ohntopp, and Andreas Pfitzmann, editors, VIS 2001, Sicherheit komplexen IT-Infrastrukturen, 1–18. Vieweg Verlag, 2001.

[9] McCune, J.M., Parno , B., Perrig, A., Reiter, M.K., Seshadri, A., "How Low Can You Go Recommendations for Hardware-Supported Minimal TCB Code Execution". Architectural Support for Programming Languages and Operating Systems (ASPLOS), Mart 2008.

[10] Seshadri, A., Luk, M., Qu, N., Perrig, A., "SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes". ACM Symposium on Operating Systems Principles (SOSP), ACM, Ekim, 2007.

[11] Rosenblum, M., Garfinkel. T., Virtual Machine Monitors: Current Technology and Future Trends. IEEE Computer, 12/5, Mayıs 2005.

[12] King, S., Dunlap, G., Chen, P., Operating System Support for Virtual Machines, Usenix 2003.

[13] Whitaker, A., Shaw M., Gribble, S., Scale and Performance in the Denali Isolation Kernel. OSDI, 2002.

[14] Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., Warfield. A., Xen and the Art of Virtualization. SOSP 2003.

[15] Chandra, R., Zeldovich, N., Sapuntzakis, C., Lam, M. S., The Collective: A Cache-Based System Management Architecture NSDI, 2005.

[16] Seshadri, A., Luk, M., Perrig, A., van Doorn, L., Khosla, P.K., Externally verifiable code execution, Communications of the ACM 49 (9) (2006) 45-49.

[17] Seshadri, A., Luk, M., Shi, E., Perrig, A., van Doorn, L., Khosla, P.K., Pioneer: Verifying code integrity and enforcing untampered code execution on legacy systems,: A. Herbert, K.P. Birman (Eds.), 20th ACM Symposium on Operating Systems Principles 2005, SOSP 2005, Brighton, UK, 23-26 Ekim, 2005, ACM, 2005.

[18] Seshadri, A., Perrig, A., van Doorn, L., Khosla, P.K., SWATT: SoftWare-based ATTestation for embedded devices, in: 2004 IEEE Symposium on Security and Privacy, S&P 2004, 9-12 Mayıs 2004, Berkeley, CA, USA, IEEE Computer Society, 2004.

[19] Shi, E., Perrig, A., van Doorn, L., BIND: A fine-grained attestation service for secure distributed systems, in: 2005 IEEE Symposium on Security and Privacy, S&P 2005, 8-11 Mayıs 2005, Oakland, CA, USA, IEEE Computer Society, 2005.

[20] Schellekens, D., Wyseur, B., Preneel, B. 2008. Remote attestation on legacy operating systems with trusted platform modules. Science of Compuer Programming. Vol 74, 1-2, pp:13-22 (Aralık 2008).

[21] Sailer, R., Zhang, X., Jaeger, T., van Doorn, L., Design and implementation of a TCG-based integrity measurement architecture, in: 13th USENIX Security Symposium, 9-13 Ağustos, 2004, San Diego, CA, USA, USENIX, 2004.

[22] Brickell, E., Camenisch, J., Chen, L., Direct anonymous attestation. CCS '04: Proceedings of the 11th ACM conference on Computer and communications security, 16–145, New York, NY, USA, 2004.

[23] "Trusted Computing: Promise and Risk," Electronic Frontier Foundation, Erişim adresi: http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.pdf, Erişim tarihi: 3 Ağustos 2009.

[24] Uçkan, Ö., "E-Devlet, E-Demokrasi ve E-Yönetisim Modeli: Bir Ilkesel Öncelik Olarak Bilgiye Erisim Özgürlügü", Erişim adresi: www.inet-tr.org.tr/inetconf8/program/166.html, Erişim tarihi: 07.11.2003.

[25] Santin, A.O. Costa, R.G. Maziero, C.A. , A Three-Ballot-Based Secure Electronic Voting System, IEEE Security & Privacy, Volume 6 Issue 3, pp 14-21, Haziran 2008.

[26] http://www.secim.info., Erisim Tarihi: 30.05.2009.

[27] http://esecim.wordpress.com., Erisim Tarihi: 30.05.2009.

[28] Byrne, M., Greene, K., Everett, S., "Usability of Voting Systems: Baseline Data for Paper, Punch Cards and Lever Machines", CHI 1997 Proc. Politics & Activism, ACM Press, vol.1,1997, pp.171-180.

[29] http://www.ysk.gov.tr/ysk/docs/2009MahalliIdareler/SecmenSayilari/Ilce.htm., Erisim Tarihi: 27.07.2009.

[30] Paul, N. Tanenbaum, A.S., Trustworthy Voting: From Machine to System, IEEE Computer, Volume 42 Issue 5, pp 23-29, Mayıs 2009.

[31] Blakley, G.R., 1979. Safeguarding cryptography keys. In: Proc. of the AFIPS 1979 National Computer Conference, vol. 48, 313–317.

[32] Karnin, E.D., Greene J.W., Hellman, M.E., On secret sharing systems, IEEE Trans. Inf. Theory **29** (1983), 35–41.

[33] Shamir, A., How to share a secret?, *Comm. ACM* **22** (1979) (11), 612–613.

[34] Bicakci, K., "Optimal Discretization for High-Entropy Graphical Passwords", 23. International Symposium on Computer and Information Sciences, IEEE ISCIS 2008, , İstanbul, Türkiye, 27-29, Ekim 2008.

[35] http://www.ysk.gov.tr/ysk/docs/2009MahalliIdareler/ResmiGazete/Buyuksehir.pdf, Erişim tarihi: 27.07.2009.

EKLER

Ek. A Geliştirilen Kod - DesEncrypter.java

```
package tr.edu.etu.biaydin;
import java.io.*;
import java.security.spec.*;
import javax.crypto.*;
import javax.crypto.spec.*;
public class DesEncrypter {
   Cipher ecipher;
   Cipher dcipher;
   DesEncrypter(SecretKey key) {
      // Create an 8-byte initialization vector
      byte[] iv = new byte[]{
         (byte)0x8E, 0x12, 0x39, (byte)0x9C,
         0x07, 0x72, 0x6F, 0x5A
      };
      AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
      try {
         ecipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
         dcipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
         // CBC requires an initialization vector
         ecipher.init(Cipher.ENCRYPT_MODE, key, paramSpec);
         dcipher.init(Cipher.DECRYPT_MODE, key, paramSpec);
      } catch (java.security.InvalidAlgorithmParameterException e) {
      } catch (javax.crypto.NoSuchPaddingException e) {
      } catch (java.security.NoSuchAlgorithmException e) {
      } catch (java.security.InvalidKeyException e) {
```

```
        System.out.println("Invalid key");
    }
}
// Buffer used to transport the bytes from one stream to another
byte[] buf = new byte[1024];
public void encrypt(InputStream in, OutputStream out) {
    try {
        // Bytes written to out will be encrypted
        out = new CipherOutputStream(out, ecipher);

        // Read in the cleartext bytes and write to out to encrypt
        int numRead = 0;
        while ((numRead = in.read(buf)) >= 0) {
            out.write(buf, 0, numRead);
        }
        out.close();
    } catch (java.io.IOException e) {
    }
}

public void decrypt(InputStream in, OutputStream out) {
    try {
        // Bytes read from in will be decrypted
        in = new CipherInputStream(in, dcipher);

        // Read in the decrypted bytes and write the cleartext to out
        int numRead = 0;
```

```
            while ((numRead = in.read(buf)) >= 0) {
                out.write(buf, 0, numRead);
            }
            out.close();
        } catch (java.io.IOException e) {
        }
    }
}
```

Ek. B Geliştirilen Kod - SealExec.java

```
package tr.edu.etu.biaydin;
import edu.mit.csail.tpmj.tools.TPMSeal;
import edu.mit.csail.tpmj.util.FileUtil;
import java.io.*;
import javax.crypto.*;
public class SealExec
{
    public static void writeByteArray( String fileName, byte[] buf )
        throws IOException
    {
        File f = new File( fileName );
        FileOutputStream fos = new FileOutputStream( f );
        fos.write( buf );
        fos.flush();
        fos.close();
    }
    public static void main( String[] args )
    {
```

```
String keyFile = "des.key";
String keyHandle = "SRK";
String keyPwd = "";
String dataPwd = "sifre";
try {
   SecretKey key = KeyGenerator.getInstance("DES").generateKey();
   writeByteArray( keyFile, key.getEncoded() );
   String[] strArray = new String[] {keyFile, keyHandle, keyPwd, dataPwd };
   TPMSeal.main( strArray );

   // Create encrypter/decrypter class
   DesEncrypter encrypter = new DesEncrypter(key);

   // Encrypt
   encrypter.encrypt(new FileInputStream("e-Voting.jar"),
      new FileOutputStream("e-Voting.crypt"));
   new File("e-Voting.jar").delete();
   encrypter.encrypt(new FileInputStream("gifs/who.jpg"),
      new FileOutputStream("gifs/who.crypt"));
   new File("gifs/who.jpg").delete();
   for(int i=0;i<20;i++)
   {
      encrypter.encrypt(new FileInputStream("gifs/"+i+".gif"),
         new FileOutputStream("gifs/"+i+".crypt"));
      new File("gifs/"+i+".gif").delete();
   }
   new File(keyFile).delete();
```

```
        } catch (Exception e) {
        }
    }
}
```

Ek. C Geliştirilen Kod - UnsealExec.java

```
package tr.edu.etu.biaydin;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import javax.crypto.spec.SecretKeySpec;
import edu.mit.csail.tpmj.tools.TPMUnseal;
import edu.mit.csail.tpmj.util.FileUtil;
import javax.crypto.*;

public class UnsealExec
{
    public static void main( String[] args )
    {
        String keyFile = "des.key";
        String keyHandle = "SRK";
        String keyPwd = "";
        String dataPwd = "sifre";
        String[] strArray = new String[] {keyFile, keyHandle, keyPwd, dataPwd };
        TPMUnseal.main( strArray );
```

```
        try
        {
            new File(keyFile.concat( ".sealed" )).delete();
            new File(keyFile.concat( ".unsealed" )).renameTo( new File(keyFile) );
            SecretKey key = new SecretKeySpec(FileUtil.readIntoByteArray( keyFile ), "DES");
            DesEncrypter encrypter = new DesEncrypter(key);
            encrypter.decrypt(new FileInputStream("e-Voting.crypt"),
                new FileOutputStream("e-Voting.jar"));
            encrypter.decrypt(new FileInputStream("gifs/who.crypt"),
                    new FileOutputStream("gifs/who.jpg"));
            for(int i=0;i<20;i++)
            {
                encrypter.decrypt(new FileInputStream("gifs/"+i+".crypt"),
                        new FileOutputStream("gifs/"+i+".gif"));
            }
            Runtime.getRuntime().exec("java -jar e-Voting.jar");
        }
        catch ( Exception e ){
        }
    }

}
```

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : AYDIN, Bahadır İsmail

Uyruğu : T.C.

Doğum tarihi ve yeri : 30.01.1984 Ankara

Medeni hali : Bekar

Telefon : 0 (312) 319 75 18

Faks : 0 (312) 292 41 80

e-mail : biaydin@etu.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Bilkent Üniversitesi/Bilgisayar Mühendisliği	2008

İş Deneyimi

Yıl	**Yer**	**Görev**
2007-2008	E-İmza Bilişim	Yazılım Uzmanı
2008-2008	Institut Eurecom	Stajer Araştırmacı
2008-2009	TOBB Ekonomi ve Teknoloji Üniversitesi	Araştırma Görevlisi

Yabancı Dil

İngilizce

Fransızca

Yayınlar

-