T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DOKTORA TEZİ

SERVİS SAĞLAYICI İLE SIM KART ARASINDA KİŞİSEL ANAHTAR OLUŞTURMA VE PAYLAŞMA PROTOKOLÜ

Kerem OK

Enformatik Anabilim Dalı

Enformatik Programı

Danışman

Prof. Dr. Sıddık Binboğa YARMAN

II. Danışman

Doç. Dr. Vedat COŞKUN

Haziran, 2015

İSTANBUL

Bu çalışma 22/06/2015 tarihinde aşağıdaki jüri tarafından Enformatik Anabilim Dalı Enformatik Doktora Programında Doktora Tezi olarak kabul edilmiştir.

Tez Jürisi:

Prof. Dr. Sıddık Binboğa YARMAN (Danışman)
İstanbul Üniversitesi
Mühendislik Fakültesi

Prof. Dr. Sevinç GÜLSEÇEN
İstanbul Üniversitesi
Enformatik Bölümü

Doç. Dr. Seyhun ALTUNBAY
Işık Üniversitesi
Mühendislik Fakültesi

Doç. Dr. M. Elif KARSLIGİL
Yıldız Teknik Üniversitesi
Mühendislik Fakültesi

Doç. Dr. Hacı Ali MANTAR
Gebze Teknik Üniversitesi
Mühendislik Fakültesi

ÖNSÖZ

Doktora eğitimimde danışmanlığımı üstlenen Prof. Dr. Sıddık YARMAN hocama bu tez çalışmasını gerçekleştirmem için verdiği destek ve her zaman sağladığı önemli katkılar için teşekkürlerimi sunarım.

Yüksek lisans ve doktora eğitimim boyunca ihtiyaç duyduğum her anda yanımda olan ve hiç bir sorumu cevapsız bırakmayan, çalışmalarıma her zaman çeşitli desteklerde bulunan, bu tez çalışmasının meydana gelmesinde önemli katkıları ve üzerimde büyük emeği olan Doç. Dr. Vedat COŞKUN hocama şükranlarımı sunarım.

Tez izleme komitesinde yer alan bölüm başkanımız Prof. Dr. Sevinç GÜLSEÇEN hocama doktoram boyunca sunduğu katkılar için ve tez izleme komitesinde yer alan Doç. Dr. Ümit GÜZ hocama desteklerinden dolayı teşekkür ederim.

Birlikte çalıştığım değerli Büşra ÖZDENİZCİ arkadaşıma çalışmalarımın her aşamasında verdiği destekler için teşekkürlerimi sunarım.

Sevgili eşim Tuğba OK'a, canım annem Tülay OK'a ve abim Hüseyin OK'a hiç bir zaman desteklerini esirgemedikleri için teşekkür ederim.

Bu çalışmayı 1505-5130053 proje numarası ile destekleyen Turkcell Teknoloji A.Ş. ile TÜBİTAK'a teşekkürlerimi sunarım.

Haziran, 2015 Kerem OK

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Kısaltmalar	Açıklama
APDU	**:** Uygulama Kuralları Veri Birimi (Application Protocol Data Unit)
ASCII	**:** Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi (American Standard Code for Information Interchange)
DF	**:** SIM Kart Özel Dosya (Dedicated File)
ECC	**:** Eliptik Eğri Şifrelemesi (Elliptic Curve Cryptography)
EEPROM	**:** Silinip Programlanabilir Salt Okunur Bellek (Electronically Erasable Programmable Read-Only Memory)
EF	**:** SIM Kart Temel Dosya (Elementary File)
GSM	**:** Mobil İletişim İçin Küresel Sistem (Global System for Mobile Communications)
ICCID	**:** Entegre Devre Kartı Kimliği (Integrated Circuit Card Identifier)
IETF	**:** The Internet Engineering Task Force
IMSI	**:** Uluslararası Mobil Abone Kimliği (International Mobile Subscriber Identity)
ISO	**:** Uluslararası Standartlık Örgütü (International Standardization Organization)
ITU	**:** International Telecommunication Union
K_i	**:** SIM Kart Kimlik Doğrulama Anahtarı (SIM Card Authentication Key)
K_r	**:** Gizli Anahtar
K_u	**:** Açık Anahtar
LSB	**:** En Önemsiz Bit (Least Significant Bit)
MCC	**:** Mobil Ülke Kodu (Mobile Country Code)
MF	**:** SIM Kart Ana Klasör (Master File)
ms	**:** mili saniye (millisecond)
MNC	**:** Mobil Ağ Kodu (Mobile Network Code)
MNO	**:** Mobil Ağ Operatörü (Mobile Network Operator)
MSB	**:** En Önemli Bit (Most Significant Bit)
MSIN	**:** Mobil Abone Kimlik Numarası (Mobile Subscriber Identification Number)
NIST	**:** National Institute of Standards and Technology
OTA	**:** Havadan (Over the Air)
RAM	**:** Rastgele Erişilebilir Bellek (Random Access Memory)
ROM	**:** Salt Okunur Bellek (Read Only Memory)
RSA	**:** Rivest-Shamir-Adleman
SIM	**:** Abone Kimlik Modülü (Subscriber Identity Module)
SMS	**:** Kısa Mesaj İletimi (Short Messaging Service)
SSL	**:** Güvenli Giriş Katmanı (Secure Sockets Layer)
STK	**:** SIM Uygulama Yazılımı (SIM Application ToolKit)
UML	**:** Birleşik Modelleme Dili (Unified Modeling Language)
USAT	**:** USIM Uygulama Yazılımı (Universal SIM Application Toolkit)

ÖZET

DOKTORA TEZİ

SERVİS SAĞLAYICI İLE SIM KART ARASINDA KİŞİSEL ANAHTAR OLUŞTURMA VE PAYLAŞMA PROTOKOLÜ

Kerem OK

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Enformatik Anabilim Dalı

Danışman : Prof. Dr. Sıddık Binboğa YARMAN

II. Danışman : Doç. Dr. Vedat COŞKUN

Mobil iletişim teknolojileri ve hücresel veri iletişimindeki gelişim sayesinde cep telefonları kullanılarak ilk olarak sesli telefon görüşmesi ve kısa mesaj servisleri kullanıcılara sunulmuştur. Mobil teknoloji konusundaki gelişimin devamı ile birlikte geliştirilen Akıllı Telefonlar üzerinden mobil bankacılık ve navigasyon gibi pek çok katma değerli servis kullanıcılara sunulmuştur. Eşzamanlı olarak gelişen Akıllı Kart teknolojisi sayesinde de SIM kartlar güvenli veri depolama kabiliyetinden dolayı mobil imza, mobil ödeme ve benzeri güvenli işlemlerinin sunulmasını mümkün hale getirmiştir.

Telefondan bağımsız olarak SIM kart üzerinden verilen servisler arasında kimlik doğrulama, mobil imza, banka ve kredi kartı ile ödeme, e-bilet ve benzeri işlemler önemli yer tutar. Bu tür servislerin güvenli bir şekilde sunulabilmesi için ise ilgili Servis Sağlayıcı ile SIM kart arasında güvenli veri iletişimine gerek duyulmaktadır. Bu ise ancak Servis Sağlayıcı ile SIM kart arasında, MNO da dâhil diğer herhangi bir üçüncü aktörün iletilen verinin içeriğini göremeyeceği ve değiştiremeyeceği güvenli bir iletişim protokolünün kullanılması sayesinde gerçekleştirilebilir.

Günümüzdeki en gelişmiş kartlar olan 512K ve 256K SIM kartlara kart üreticisi tarafından fabrika üretimi esnasında gizli anahtarlar yüklenmektedir. Kullanıcılara güvenli servis vermek isteyen bir Servis Sağlayıcı, SIM kartın kendisine tahsis edilen bir güvenli alanın anahtarını MNO'nun bilgisi dahilinde kart üreticisinden temin ederek

SIM kart ile güvenli bir şekilde iletişim gerçekleştirebilir. Ancak günümüzde en yaygın olarak kullanılan 64K SIM kartlar, MNO ile SIM arasında telefon görüşmesi ve SMS iletişimini mümkün kılacak kadar güvenli iletişimi sağlayacak şekilde tasarlanmış, fakat üçüncü bir aktörle daha güvenli erişim sağlamak ve yüksek güvenlik gereksinimleri olan servisler için yeterli altyapıya sahip değildir. Bu nedenden dolayı, Servis Sağlayıcılar bu kartlara sahip olan kullanıcılara servis sunamamaktadırlar.

Bu eksikliği gidermek üzere, tez çalışmasının amacı fabrika üretimi esnasında anahtarlar yüklenmemiş olan SIM kartlar ile Servis Sağlayıcı arasında güvenli iletişimi mümkün kılacak altyapıyı oluşturmaktır. Bu doğrultuda tez çalışması Servis Sağlayıcı ile SIM kart arasında uçtan uca güvenli iletişimi mümkün kılmak için ihtiyaç duyulan güvenlik anahtarının, SIM kart ve Servis Sağlayıcı arasında etkileşimli olarak üretilmesi için gerekli olan anahtar değişim protokolünün tasarımı, protokole ait prototip SIM kart yazılımının geliştirilmesi ve protokolün güvenlik testlerinin yapılma süreçlerini içermektedir.

Haziran 2015, 88 sayfa.

Anahtar kelimeler: SIM Kart, Akıllı Kart, Servis Sağlayıcı, Uçtan Uca Güvenli Şifreleme, Anahtar Değişim Protokolü

SUMMARY

DOCTORATE THESIS

A SECURE KEY AGREEMENT PROTOCOL BETWEEN SERVICE PROVIDER AND SIM CARD

Kerem OK

İstanbul University

Institute of Graduate Studies in Science and Engineering

Department of Informatics

Supervisor : Prof. Dr. Sıddık Binboğa YARMAN

Co-Supervisor : Assoc. Prof. Vedat COŞKUN

Through the advancements in mobile communication technologies and cellular data communication, mobile phones enabled voice communication at first and then short messaging services. The continuing evolution of the mobile technologies helped Smartphones to be developed and value added services such as mobile financial services and navigation to be provided to the users. At the same time, together with the enhancement of smart card technology, SIM cards are used for mobile signatures, mobile payments etc. due to the capability of secure data storage.

SIM card services are provided independently from the Smartphone; and most important such services include identification, mobile signatures, mobile payment with credit and debit cards, mobile ticketing and so on. In order to securely provide such services, the corresponding Service Provider and SIM card need to set up a secure communication. This can only be enabled with a secure communication protocol in which no party other than SIM card and Service Provider including MNO can reveal or modify the communication.

The most advanced SIM cards are 512K and 256K versions; and the required security keys are already installed onto the cards during manufacturing phase. A Service Provider who wishes to provide secure service to SIM cards needs to get the required keys from the SIM card issuer with the consent of MNO; and service provider can communicate with the SIM card securely afterwards. However, most widely used SIM

cards, including 64K SIM cards, do not have the required infrastructure to securely communicate with a Service Provider. Therefore, Service Providers cannot provide secure services to the owners of such SIM cards with their current capabilities.

Accordingly, the aim of the thesis is to provide the required infrastructure that enables end-to-end encryption between Service Provider and SIM cards, which do not have the required security keys previously. In this scope, this thesis includes the design of the key exchange protocol that creates the required symmetric keys by the collaborative effort of SIM card and Service Provider to enable end-to-end encryption between SIM card and Service Provider; the prototype implementation of the protocol for the SIM cards; and the security analysis of the protocol.

June 2015, 88 pages.

Keywords: SIM Card, Smart Card, Service Provider, End-to-End Encryption, Key Exchange Protocol

1. GİRİŞ

1.1. TEZ KONUSU VE ÖNEMİ

Özellikle son yılların lokomotif teknolojisi olarak Mobil İletişim, yer bağımsız olarak iletişim kurmak olarak tanımlanabilir; pratik anlamda ise iletişimin kablo kullanılmadan (kablosuz, wireless) yapılmasını da içerir. Hücresel Veri İletişimi (Cellular Data Communication) teknolojisi sayesinde cep telefonları kullanılarak ilk olarak sesli telefon görüşmesi, kısa zaman sonra da kısa mesaj hizmeti (SMS: Short Messaging Service) kullanıcılara sunulmuştur. Mobil konuşma ve mesajlaşma sisteminde Mobil Ağ Operatörü (MNO: Mobile Network Operator) ile Cep Telefonu Kullanıcısı birer aktör olarak yer almakta ve tüm ekosistem bu aktörlerin katılımı ile gerçekleşebilmektedir. Mobil konuşma ve mesajlaşma yapılabilmesi için bir MNO'dan kişiye özel telefon numarası ile eşleştirilmiş şekilde Abone Kimlik Modülü (SIM: Subscriber Identity Module) kartı temin edilerek, kullanılacak olan cep telefonuna takılması gerekmektedir. SIM kart, temel olarak Akıllı Kart olarak adlandırılan ve kimlik doğrulama, veri depolama ya da uygulama yükleme ve çalıştırma amaçlı olarak kullanılabilen kartların cep telefonları üzerinde kullanılmak üzere özelleştirilen bir çeşidi olarak tanımlanabilir.

Cep telefonları ilerleyen yıllardaki teknoloji ve ekosistemdeki hızlı değişime paralel olarak konuşma ve mesajlaşma yanında pek çok yeni işlevi de gerçekleştirebilecek şekilde evrim geçirerek Akıllı Telefon adını almıştır. Akıllı telefonlar mobil ticaret, mobil bankacılık ve navigasyon gibi pek çok katma değerli servisi kullanıcılara sunarken, gelişen akıllı kart teknolojileri sayesinde SIM kartlar da güvenli veri depolama kabiliyetinden dolayı kimlik doğrulama, mobil imza, banka ve kredi kartı ile ödeme ve benzeri güvenli işlemlerin sunulmasını mümkün hale getirmiştir. Bu doğrultuda Akıllı Telefon üzerinden kullanıcılara herhangi bir katma değerli servis sunan aktörlere ise Servis Sağlayıcı denilmektedir.

Verilen servisler, gereksinimlere bağlı olarak sadece akıllı telefonunun kaynaklarını kullanabilirken, akıllı kart kaynaklarını kullanan servisler de olabilmektedir. Sadece telefon kaynakları kullanılarak verilecek servisler için genel olarak SIM kartın bağlı

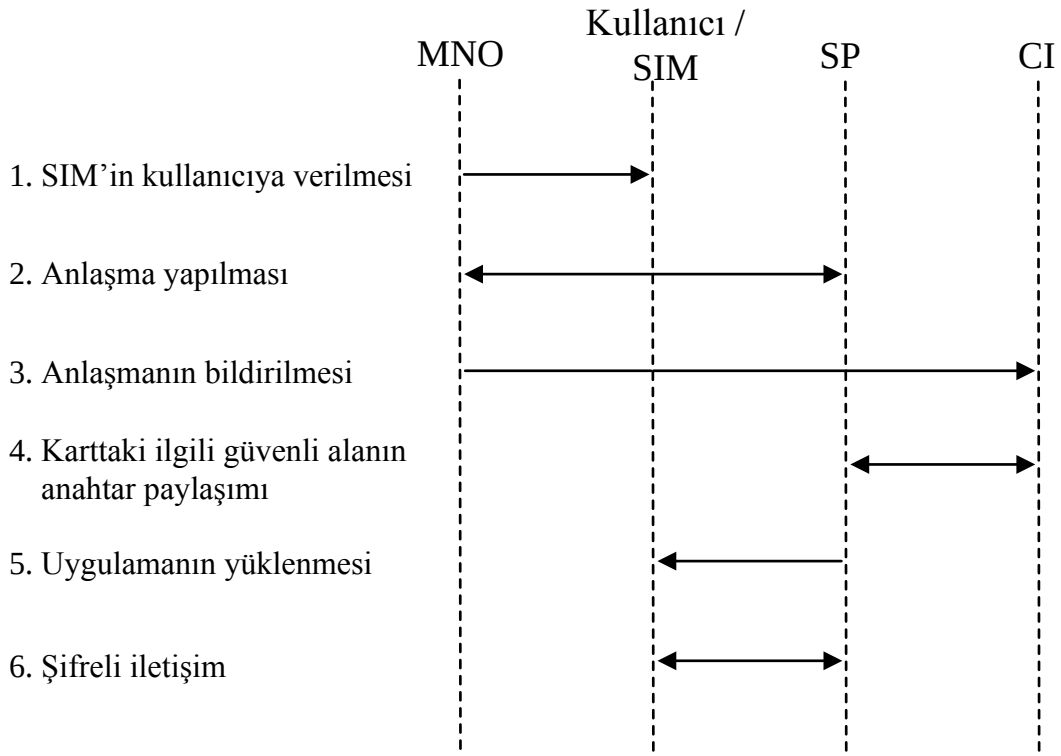
olduğu MNO'nun onayına ihtiyaç olmaz iken, bazı telefon markaları için telefon üretim firmasının iznine gerek duyulabilmektedir.

SIM kart üzerinden verilen servisler arasında kimlik doğrulama, mobil imza, banka kartı ya da kredi kartı ile ödeme ve benzeri işlemler önemli yer tutar. Bu tür servislerin güvenli bir şekilde sunulabilmesi için ise Servis Sağlayıcı tarafından SIM karta veriyi güvenli bir şekilde iletme ve bu veriyi SIM kart üzerinde güvenli şekilde depolama gereksinimleri vardır. Bu şekilde güvenli iletişim ise ancak Servis Sağlayıcı ile SIM kart arasında, MNO da dâhil diğer herhangi bir üçüncü aktörün hiçbir veriyi göremeyeceği ve değiştiremeyeceği güvenli bir iletişim protokolünün kullanılması sayesinde gerçekleşebilir.

MNO tarafından kullanıcıya teslim edilen SIM kartların yönetimi de yine MNO'larda olduğu için, kullanıcılara SIM kart altyapısını kullanacak şekilde servis vermek isteyecek olan bir Servis Sağlayıcı öncelikle ilgili MNO ile anlaşma yapmalı; sonrasında da Servis Sağlayıcı uygulaması SIM kart üzerine MNO tarafından izin verildiği şekilde yüklenmelidir. MNO ile yapılan anlaşma, SIM kart üzerindeki güvenli alanların bir tanesinin Servis Sağlayıcı uygulaması tarafından kullanılmasına izin verir, ve bu amaçla o alanın güvenlik şifresi de SIM kart üreticisi tarafından MNO'nun bilgisi dahilinde Servis Sağlayıcıya iletilir. Bu sayede, ilgili güvenlik şifresi kullanılarak Servis Sağlayıcı ile SIM kart arasında uçta uca şifreli iletişim mümkün hale gelir.

Bahse konu güvenli işlemlerin kolaylıkla gerçekleşebilmesi amacı ile, günümüzdeki en gelişmiş sürümler olan 512K ve 256K SIM kartlara kart üreticisi tarafından fabrikada üretim esnasında gizli anahtar yüklenmektedir. Bu SIM kartları edinen kullanıcılara yönelik ve uçtan uca güvenli iletişim gerektiren servis geliştirmiş olan bir Servis Sağlayıcı, bu servisi hizmete sokabilmek için ilgili karttaki güvenli alanın anahtarını MNO aracılığı ile SIM kartın üreticisinden talep eder. Üretici firma, Servis Sağlayıcıya ilgili alanın anahtarını Anahtar Değişim Töreni (key ceremony) ile verir. Bu sayede söz konusu alanın anahtarı yalnızca Servis Sağlayıcı ve SIM kart tarafından bilindiği için MNO dahil herhangi bir üçüncü aktör saklanılan verinin ve SIM kart ile Servis Sağlayıcı arasında gerçekleştirilen iletişimin içeriğine ulaşamaz. Bu kapsamda MNO, SIM kart, Servis Sağlayıcı ve Kart Üreticisi arasında gerçekleşen işlemler şu şekilde detaylandırılabilir (Şekil 1.1):

1. SIM kart MNO tarafından kullanıcıya verilir,
2. Servis Sağlayıcının SIM kartın ilgili güvenli alanı (Örnek: 1. alan) kullanması için Servis Sağlayıcı ile MNO arasında anlaşma yapılır,
3. Kart Üreticisi bu anlaşmadan haberdar edilir,
4. Karttaki ilgili güvenli alana (Örnek: 1. alan) ait şifreleme anahtarı (K_1), Anahtar Paylaşım Töreni ile Servis Sağlayıcıya iletilir,
5. SIM kart uygulaması, SIM karttaki ilgili güvenli alana (Örnek: 1. alan) MNO üzerinden yüklenir,
6. Servis Sağlayıcı ile SIM Kart arasında şifreli iletişim gerçekleşir.



Şekil 1.1: 256K ve 512K SIM kartlarda Servis Sağlayıcı ile SIM kart arasında güvenli iletişim.

Şekil 1.1'de anlatılan işlemler, SIM kart versiyonları arasında farklılık gösterebilmektedir. Günümüzde en yaygın olarak kullanılan SIM kartlar, 64K versiyonudur. Halen de MNO'lar yeni bir SIM kart talep eden kullanıcılara, özellikle güvenli bir servis talep etmemeleri durumunda düşük maliyeti olan 64K SIM kartları, güvenli servis talep eden kullanıcılara ise ancak ek bir ücret karşılığında 512K ya da 256K SIM kart vermektedir.

MNO ile SIM arasında telefon görüşmesi ve SMS iletişimini güvenli kılacak şekilde tasarlanan 64K SIM, daha yüksek güvenlik gereksinimleri olan mobil ödeme vb. servisler için yeterli altyapıya sahip değildir. Bu şekilde yüksek güvenlik gerektiren servisi talep eden bir kullanıcının, şu anki durumda 64K SIM kartını ek bir ücret karşılığında 512K ya da 256K SIM kart ile değiştirmesi gerekmektedir. İlk bakışta makul gibi görünen bu seçenek, aslında hem kullanıcılar hem de MNO açısından maliyetlidir. Kullanıcılar kart değiştirmek için ilgili servis noktalarına gitmek, MNO'lar da kart değişimi için servis vermek durumundadırlar. Her bir yeni kartın maliyetinin de kullanıcı ya da MNO tarafından üstlenilmesi de gerekmektedir. Ayrıca kullanıcıların sadece verilecek bir katma değerli servisten faydalanmak üzere kartlarını değiştirmek için bir çaba içine girmeleri için gerekli motivasyonu sağlamak da oldukça zordur. Bu olumsuzluklar, Servis Sağlayıcılar açısından yaşamsal önemi olan servislerin kullanıma sunulması ve yaygınlaşması önünde çok güçlü engeller olarak durmaktadırlar. MNO'lar da yeni servislerin kullanılması yolu ile oluşacak yüksek veri iletimi ve sonrasındaki katma değerden pay alma fırsatından mahrum kalmaktadırlar.

Netice olarak Servis Sağlayıcıların 64K SIM kartlar üzerinden de servis sunabileceği bir altyapının geliştirilmesi, hem potansiyel Servis Sağlayıcılar, hem de MNO'lar açısından hem de kullanıcılar açısından çok önemlidir.

1.2. TEZİN AMACI

Tez çalışmasının amacı fabrika üretimi esnasında şifreleme anahtarları yüklenmemiş olan 64K SIM kartlar ile Servis Sağlayıcı arasında güvenli iletişimi mümkün kılacak altyapıyı oluşturmaktır.

Bu amaç kapsamında gerçekleştirilen tez çalışması, Servis Sağlayıcı ile şifreleme anahtarları yüklenmemiş olan SIM kartlar arasında uçtan uca güvenli iletişimi mümkün kılmak için gerekli olan güvenlik anahtarının SIM kart ile Servis Sağlayıcının etkileşimli olarak üretmesi için gerekli olan protokolün tasarımı, protokole ait prototip SIM kart yazılımının geliştirilmesi ve protokolün güvenlik testlerinin yapılma süreçlerini içermektedir.

Bahse konu protokolü içeren SIM Kart yazılımı ilgili SIM karta yüklendikten sonra Servis Sağlayıcı ile SIM Kart güvenli bir şekilde tanımlanan protokol dahilinde simetrik

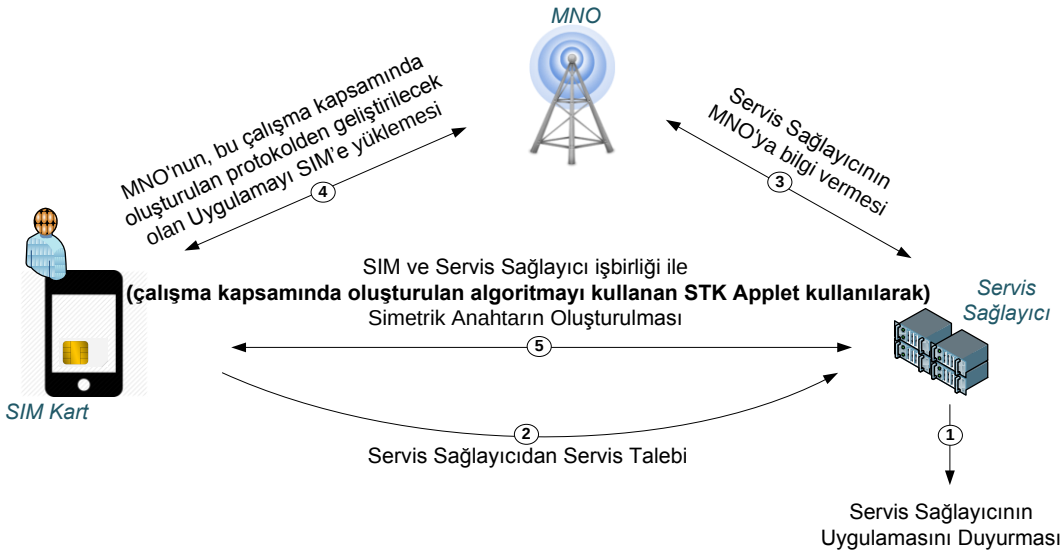
anahtar üretilebilecektir. Geliştireceğimiz protokolün hedefleri detaylı olarak aşağıda tanımlanmıştır:

1. SIM Kart ile Servis Sağlayıcı arasında güvenli iletişim için gerekli olan simetrik anahtarın oluşturulması,
2. Protokol tasarımı esnasında, detayları daha sonra verilecek olan güvenlik şartlarının sağlaması,
3. Protokolün düşük kapasiteli SIM kartların kısıtlarını dikkate alacak şekilde geliştirilmesi ve ilgili SIM kart yazılımının da bu doğrultuda üretilmesi.

Tasarlanacak olan anahtar oluşturma protokolüne ilişkin yazılımlar geliştirildikten sonra kullanımı ile ilgili kavramsal model Şekil 1.2'de verildiği üzere şu aşamalardan oluşmaktadır:

1. Servis Sağlayıcı, hizmetini kullanıcılara duyurur,
2. Hizmeti kullanmak isteyen kullanıcı, talebini Servis Sağlayıcıya iletir,
3. Servis Sağlayıcı Mobil Ağ Operatörü'ne ilgili kullanıcının kendisinden servis almak istediğini bildirir,
4. MNO, oluşturduğumuz protokolü kullanan uygulamayı kullanıcının SIM kartına Havadan (OTA: Over The Air) yükler.
5. SIM Kart ve Servis Sağlayıcı etkileşimli olarak bu çalışma kapsamında oluşturulan protokolü kullanan uygulamalar sayesinde simetrik anahtarı oluşturur.

Geliştirilen protokol, kavramsal modelin 5. aşaması olan simetrik anahtarların oluşturulması safhasında kullanılacak olup; bu aşamanın başarıyla tamamlanmasının ardından SIM Kart ile Servis Sağlayıcı, oluşturulan simetrik anahtarı kullanarak şifreli bir şekilde veri iletişimi sağlayacaklardır.



Şekil 1.2: 256K-512 K SIM kartlarda Servis Sağlayıcı ile SIM kart arasında güvenli iletişim.

Doktora tezi beş ayrı bölümden oluşmaktadır: birinci bölüm olan "Giriş" bölümünden sonra ikinci bölüm "Genel Kısımlar", üçüncü bölüm "Malzeme ve Yöntem", dördüncü bölüm "Bulgular" ve beşinci bölüm "Tartışma ve Sonuç" bölümleridir.

"Genel Kısımlar" bölümünde, konuyla ilgili yapılan çalışmalar ve literatür taraması, akıllı kartlarla ilgili bilgiler, SIM kart ile ilgili bilgiler ve standartlar, Java Card programlama dili ile ilgili bilgiler, konu ile ilgili olan güvenlik algoritmaları ve anahtar değişimi protokolleri verilmiştir.

"Malzeme ve Yöntem" bölümünde, tez çalışmasında uygulanan yöntem ve geliştirilen protokolde sağlanması gereken güvenlik şartları anlatılmıştır.

"Bulgular" bölümünde, Servis Sağlayıcı ile SIM Kart arasında anahtar üretim ve paylaşım protokolü detaylı olarak verilmiştir. Ayrıca protokolün güvenliği değerlendirilmiş ve SIM kart için geliştirilen akıllı kart uygulaması da verilmiştir. Protokolün güvenlik kriterlerine uygunluğu Casper/FDR güvenlik analiz aracı ile incelenmiş ve analiz sonuçları da aynı bölümde anlatılmıştır.

"Tartışma ve Sonuç" bölümünde, tezde yapılan çalışmalar özetlenmiş ve literatürde konu ile ilgili olan diğer çalışmalar ile karşılaştırılmıştır.

2. GENEL KISIMLAR

Bu bölümde tez konusu ile ilgili ön bilgiler ile, konu ile ilişkili olarak günümüze kadar yapılmış olan çalışmalar anlatılmaktadır. Bu doğrultuda, ilk olarak Akıllı kartlar ile ilgili genel bilgiler; daha sonra da SIM kartlar ile ilgili ve tez çalışması kapsamındaki önemli bilgiler; son olarak da Akıllı kartlarda yazılım geliştirmek için kullanılan Java Card programlama dili ile ön bilgiler verilerek konu ile ilgili teknik ön bilgiler anlatılmış olacaktır. Bir sonraki adım olarak da, tez çalışması kapsamında geliştirilecek olan anahtar paylaşım protokolünde kullanılacak olan güvenlik mekanizmalarına ilişkin bilgiler paylaşılmıştır. Günümüze kadar SIM kartlar üzerinde anahtar oluşturmaya yönelik yapılmış olan çalışmalara da yer verilerek bölüm sonlandırılmıştır.

2.1. AKILLI KART

Akıllı kartlar, içlerinde veri saklayabilen ve işlem yapma yeteneğine sahip olan taşınabilir mikro bilgisayarlar olarak tanımlanabilir [1]. Akıllı kart konusunda 1968 yılında alınmış olan ilk patent sonrasında bu alanda günümüze kadar kaydedilen ilerleme neticesinde akıllı kartlar güvenlik dahil birçok alanda kapsamlı olarak kullanılabilir hale gelmiştir. İlk aşamada ön ödemeli telefon görüşmeleri için kullanılan Akıllı kartlar, günümüzde ise yaygın olarak banka ve kredi kartı olarak kullanılmaktadır. Cep telefonlarında kullanılan SIM kartlar da akıllı kartların yaygın bir örneğidir [2].

Akıllı kartların içerisinde kimlik doğrulama (authentication) amaçlı olarak kullanıcı verisini saklayan depolama birimi ile, hesaplama ve güvenlik işlemlerini gerçekleştirme yeteneğine sahip mikro işlemci bulunmaktadır.

Akıllı kartlar herhangi bir dahili güç kaynağı içermemekte; buna karşılık kullanım esnasında ihtiyaç duyulan güç kart okuyucusundan elde edilmektedir. Akıllı kartlar, kart okuyucu ile fiziksel etkileşim şekline göre *temaslı* ve *temassız* kartlar olarak sınıflandırılırlar. Temaslı kartlar, iletişim amacı ile kart okuyucunun özel tasarlanmış olan oyuğuna sokularak güç ve bilgi alışverişi kart ile okuyucunun devrelerinin fiziksel olarak temas etmesi yolu ile mümkün hale gelir. Temaslı kartlar ise kart okuyucuya

dokunma mesafesinde yaklaştırılır ve bu esnada kart okuyucusunun üretmiş olduğu elektromanyetik alandan güç alan Akıllı kart ile kart okuyucu temas etmeden iletişim kurarlar.

Akıllı kartlar ile ilgili standartların büyük çoğunluğu Uluslararası Standartlık Örgütü (ISO: International Standardization Organization) tarafından ISO/IEC 7816 standartlarında tanımlanmıştır [3]. Kartların fiziksel özellikleri, veri iletim protokolleri, komutlar, güvenlik mimarisi, kart yönetimi gibi konular bu standartlarda kapsamlı olarak tanımlanmıştır.

2.2. AKILLI KARTLARIN DEPOLAMA ÖZELLİĞİ

Akıllı kartlarda üç çeşit hafıza bulunmaktadır; Salt Okunur Bellek (ROM: Read Only Memory), Silinip Programlanabilir Salt Okunur Bellek (EEPROM: Electronically Erasable Programmable Read-Only Memory), ve Rastgele Erişilebilir Bellek (RAM: Random Access Memory) [4]. ROM, Akıllı kartın işletim sistemi ile, bazı sistem program ve verilerini barındırmaktadır; hafıza kartının gücü kesilse bile bilgileri saklamaya devam eder. EEPROM da ROM'un özel bir halidir ve üzerindeki bilgilerin belirli koşullarda değiştirilmesine izin verir; belirli koşullarda değiştirilmesine izin verilen PIN kodu ve şifreler bu bölümde tutulmaktadır. RAM ise geçici verileri tutan hafızadır ve akıllı kartın gücü kesildiğinde sakladığı verileri kaybeder.

Akıllı kartların program ve verileri saklamakta kullanılan bellek kapasitesi oldukça düşüktür. Kartların sahip oldukları belleğin bir kısmı kartın işletim sistem, ve diğer sistem programları tarafından kullanılır. Kart üzerinde çalışması hedeflenen programların da düşük bellek kapasitesini dikkate alarak geliştirilmesi gerekir; hem geliştirilecek programın uzunluğu, hem programın çalışırken RAM'de kullanacağı bellek, hem de sürekli olarak saklanmak üzere EEPROM'a kayıt edilecek bilgilerin uzunluklarında bu kısıt dikkate alınmak zorundadır. Aksi durumda programın kart yüklenmesi ya da yüklense de çalıştırılması teknik olarak mümkün olmayabilir ya da MNO bu programın karta yüklenmesine izin vermeyebilir.

2.3. AKILLI KARTLARIN İŞLEM YAPMA ÖZELLİĞİ

Akıllı kartların diğer özellikleri gibi işlem gücü de çok kısıtlıdır, bu nedenle uygulamalar da oldukça yavaş çalışmaktadır. Özellikle güvenlik ihtiyaçlarını karşılamak üzere kullanılan üst düzey akıllı kartlar, kripto işlemcisi adı verilen ve kripto işlemlerini

hızlı bir şekilde gerçekleştirebilen özel bir donanıma sahiptir. Kripto işlemciler yüksek hesaplama gücü gerektiren açık anahtar kriptografik algoritmalarındaki şifreleme ve veri çözme işlemlerini başarı ile gerçekleştirebilmektedir. [1].

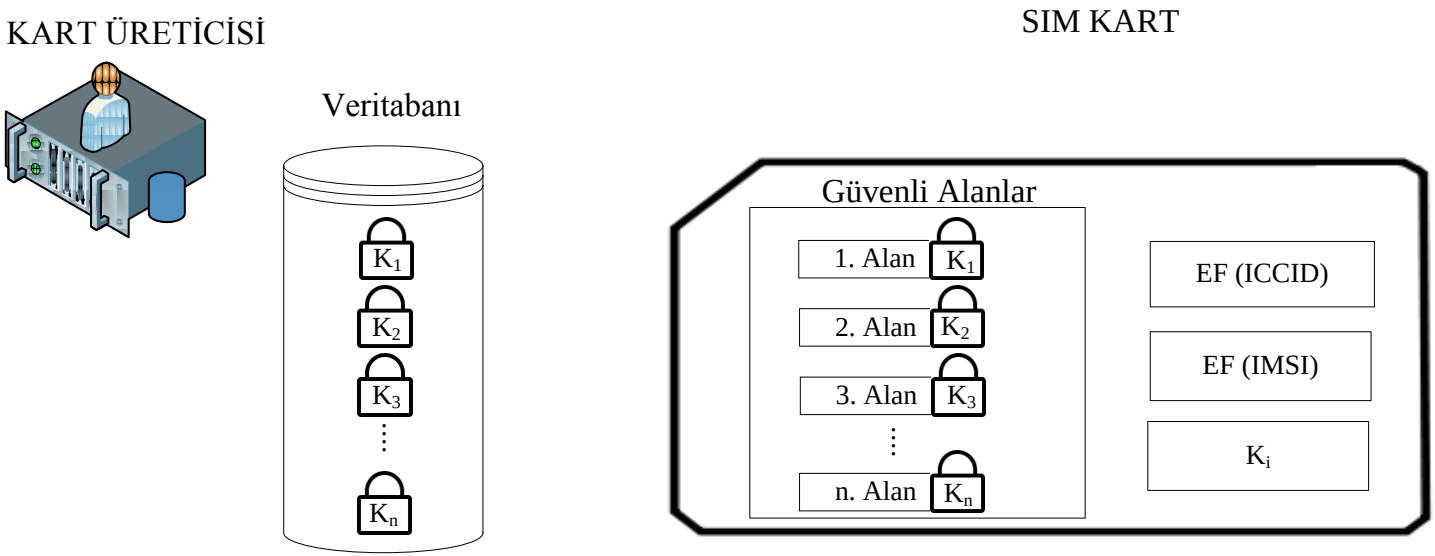
Akıllı kartların işlem yapma kapasitesi oldukça düşüktür. Kart üzerinde çalışması hedeflenen programların da düşük işlem yapma kapasitesini ve hedeflenen kartın özelliklerini dikkate alarak geliştirilmesi gerekir; aksi halde akıllı kartlar üzerinde çalıştırılamayabilir.

2.4. SIM KART

SIM kart (Şekil 2.1), cep telefonlarının MNO'nun verdiği servislerde kullanılması amacı ile özelleştirilmesini sağlayan bir Akıllı karttır.

Şekil 2.1: SIM Kart.

SIM kart, mobil ağ abonesinin hesap bilgilerini, Mobil İletişim İçin Küresel Sistem (GSM: Global System for Mobile Communications) sisteminde kimlik doğrulama ve diğer işlemler için gerekli olan verileri ve SIM uygulamalarını barındırır. SIM kart üzerinde ayrıca her biri değişik bir uygulama tarafından erişebilecek şekilde oluşturulmuş güvenli alanlar vardır. SIM karta yetkili erişim için kullanılacak olan anahtarlar ile, kart üzerindeki uygulamaların kullanacakları anahtarlar SIM kartlar üzerindeki bu alanlarda yer alır (Şekil 2.2).



Şekil 2.2: SIM Kart ve Güvenli Alan Anahtarları.

SIM kartlardaki verilerin tutulduğu dosyalar, standart bir yapıda oluşturulmuştur. En üstte Ana Klasör (MF: Master File). MF klasörünün altında ise DF-GSM, DF-Telecom ve DF-DCS1800 klasörleri ile EF-ICCID dosyası yer alır. MF ve DF (Dedicated File) klasörleri, EF (Elementary File) ise dosyaları ifade eder; DF aynı zamanda EF gibi veri de saklayabilir. MF, DF, ve EF içerisindeki başlık bölümlerinde ilgili klasör ya da dosyaya ilişkin kullanıcı haklarını belirten güvenlik bilgileri bulunmaktadır. SIM kartta yüklü olan her uygulama MF altındaki ilk seviyedeki klasörlerde gezebilir fakat sadece ilgili hakları olan uçlara ilerleyebilir [5].

SIM kartta tutulan dosyalardan en önemlileri Entegre Devre Kartı Kimliği (ICCID: Integrated Circuit Card Identifier), Uluslararası Mobil Abone Kimliği (IMSI: International Mobile Subscriber Identity), ve SIM Kart Kimlik Doğrulama Anahtarıdır (K_i: Authentication Key) [5].

2.4.1. ICCID

Standardı GSM 11.11 [5] ile belirlenen, en fazla 20 basamaktan oluşan evrensel olarak benzersiz bir sayısal tanımlayıcıdır ve şu parçaların birbirine eklenmesi ile oluşturulur:

- Endüstri Tanımlayıcı Öneki: Kartın kullanıldığı sektörü tanımlayan 2 basamaklı koddur.
- Ülke Kodu: Ülkeler için belirlenmiş 1-3 basamak arasında değişen ülke kodudur.
- Yayıncı Kimlik Numarası: Kart üreticisinin 1-4 basamak arasında değişen kodudur.
- Bireysel Hesap Kimlik Numarası: Abonelere ayrılmış değişken uzunlukta kimlik numarasıdır. Bir yayıncı altındaki bütün aboneler için kimlik numarası basamak sayısı ise birbirine eşittir.
- Kontrol Basamağı: Luhn algoritmasına göre hesaplanmış 1 basamaklı kontrol basamağıdır.

2.4.2. IMSI

Aboneye sağlanan evrensel olarak benzersiz 15 haneli bir sayısal karakterdir. ICCID verisine benzer bir yapıya sahip olup ve şu parçaların birbirine eklenmesi ile oluşturulur:

- Mobil Ülke Kodu (MCC: Mobile Country Code)**:** İlk üç basamak ülkeyi tanımlamaktadır.
- Mobil Ağ Kodu (MNC: Mobile Network Code)**:** Sonraki iki ya da üç basamaklı sayı (ABD ve Kanada için) operatörü tanımlamaktadır.
- Mobil Abone Kimlik Numarası (MSIN: Mobile Subscriber Identification Number)**:** Geri kalan basamaklar ise abonenin bilgisini tanımlamaktadır.

2.4.3. Kimlik Denetleme Anahtarı

SIM kartların kimliklerinin MNO tarafından denetlenmesi için kullanılmakta olup, 128 bit uzunluğundadır. Her SIM kart, evrensel olarak benzersiz bir K_i anahtarına sahiptir ve bu anahtar kartın kişiselleştirmesi aşamasında MNO tarafından karta yüklenmektedir. K_i'ye erişim hakkı sadece MNO'ya aittir [6].

2.5. JAVA CARD

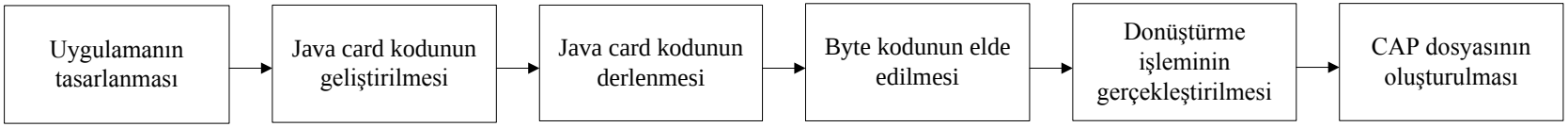
Java Card; Java teknolojisi temel alınarak geliştirilen ve Akıllı Kartlar üzerinde çalışacak uygulama yazımında kullanılan bir yazılım geliştirme ortamıdır. Firma bağımsız olarak standart bir uygulama geliştirme ve kullanım ortamı sağladığı için günümüzde akıllı kartların büyük çoğunluğu Java Card teknolojisi ile uyumlu olarak üretilmektedir ve akıllı kartların yaklaşık 90%'ı Java Card platformuna sahiptir [7, 8].

Bir Java Card uygulamasının geliştirme aşaması Şekil 2.3'de, uygulamanın SIM karta yüklenme aşaması ise Şekil 2.4'de gösterilmiştir.

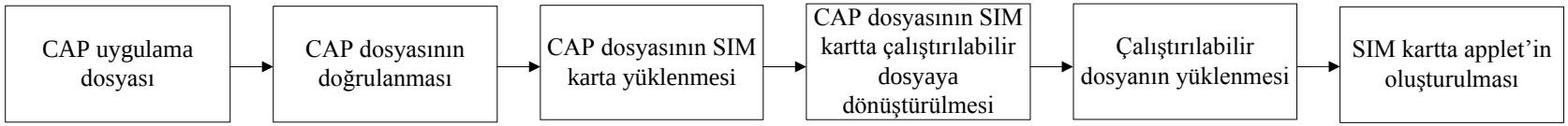
2.6. SIM UYGULAMA YAZILIMI

SIM Uygulama Yazılımı (STK: SIM Application ToolKit) SIM kart üzerinde çalıştırılmak üzere uygulama yazımında kullanılan bir yazılım geliştirme aracıdır. STK, SIM kartın kullanılan akıllı telefona bağımlı olmadan ve ihtiyaç duymadan dış dünya ile iletişim kurmasını sağlayan komutları içerir. Kullanıcıdan komut ya da veri alabilmek için telefon üzerinden veri girişi de STK uygulaması ile gerçekleştirilebilmektedir [9].

GSM 2G ağlarında STK, GSM 11.14 standardı tarafından tanımlanmıştır. Daha sonra bu standart 3G ağlarını için USIM Uygulama Yazılımı (USAT: Universal SIM Application Toolkit,) standartlarını da kapsayan 3GPP 31.111 ile güncellenmiştir.



Şekil 2.3: Java Card Yazılımını Geliştirme Süreci.



Şekil 2.4: Java Card Yazılımını SIM Karta Yükleme Süreci.

STK uygulaması geliştirebilmek için iki seçenek bulunmaktadır; birincisi kart üreticisi tarafından sağlanan platform ve programlama dili kullanılarak uygulamayı geliştirmek, diğeri ise daha da yaygın olan Java Card dili kullanılarak uygulamayı geliştirmektir.

STK'nın standartlaştırılması ve SIM kartın donanımsal özelliklerinin geliştirilmesi ile birlikte, SIM kart katma değerli ve güvenlik gerektiren servislerin verilebildiği bir platform haline gelmiştir. STK kullanılarak yazılan ve SIM karta yüklenen programın kartın içinde bulunduğu mobil cihaz ile iletişim kurmasının da sağlanması neticesinde, cihaz üzerinden SIM karttaki uygulamaya erişilebilmesi ve yönetilebilmesi de mümkün hale gelmiştir.

SIM kart ile mobil cihaz arasındaki iletişimin nasıl gerçekleştirilmesi gerektiği "ISO/IEC 7816-12 Cards with contacts - USB electrical interface and operating procedures" standardında verilmiştir [10]. Mobil cihaz ile SIM kart arasındaki iletişimde mesajlar, Uygulama Kuralları Veri Birimi (APDU: Application Protocol Data Unit) formatında iletişmektedir. İki çeşit APDU mesajı bulunmaktadır; akıllı karta komutlar göndermek için kullanılan *komut APDU* ve gönderilen komuta ait cevapları almak için kullanılan *yanıt APDU*.

Komut ve yanıt APDU mesajlarının içeriği "ISO/IEC 7816-4" standardı ile tanımlanmıştır [11].

Örnek bir komut APDU Tablo 2.1'de, yanıt APDU ise Tablo 2.2'de verilmiştir.

Tablo 2.1: Komut APDU formatı.

Alan adı	Uzunluğu (byte cinsinden)	Açıklama
CLA	1	Uygulamaya özel açıklama sınıfı
INS	1	Açıklama
P1	1	Komut için kişisel açıklama parametresi
P2	1	Komut için kişisel açıklama parametresi
L_c	0, 1 ya da 3	Komut verisinin byte cinsinden uzunluğu
Komut verisi	N	Komut verisi
L_e	0, 1, 2 ya da 3	Yanıt APDU için beklenen en yüksek byte uzunluğu (Opsiyonel)

Tablo 2.2: Yanıt APDU formatı.

Alan adı	Uzunluğu (byte cinsinden)	Açıklama
Yanıt verisi	en çok N_e kadar (L_e alanında belirtilen uzunluk)	Yanıt verisi
SW1-SW2	2	Komut durumu (Başarılı işlemler için “90 00” byte'ları döndürülür)

2.7. MOBİL AĞ OPERATÖRÜ VE SERVİS SAĞLAYICI

İçlerinde SIM kart barındıran Akıllı Telefonlar kullanılarak telefon görüşmesi, mesajlaşma ve Internet erişimi, Mobil Ağ Operatörlerinin sağladığı altyapı ve üzerinde verdiği hizmet sayesinde mümkün olabilmektedir. Bu servislerden faydalanmak isteyen kullanıcıların, seçtikleri bir MNO’dan SIM kart alarak, telefonlarını aktif hale getirmeleri gerekmektedir. Şu anda telefon görüşmesi ve ilgili hizmetleri verme konusunda MNO’lar tekel durumundadırlar. Yüksek veri iletişim kapasitesi ve hızının da mümkün olması ile birlikte, Akıllı Telefon ve SIM kart üzerine yüklenecek uygulamalar aracılığı ile finansal, sosyal, ticari vb. katma değerli servislerin de

verilmesi mümkün ve pratik hale gelmiştir. Akıllı telefon kullanıcılarına herhangi bir şekilde servis veren firmalara Servis Sağlayıcı denilmektedir. Verilecek olan servisin özelliğine göre, gerekli uygulama Akıllı Telefonlara serbestçe yüklenebileceği gibi, belirli markalar için telefon üreticisinden izin almak dahi gerekebilmektedir. Bazı durumlarda ise servisin verilebilmesi için SIM kartın veri depolama bölümlerinin kullanılması, hatta uygulamanın SIM karta yüklenmesi gerekebilir. Bu gibi durumlarda, ilgili servis sağlayıcının kartın yöneticisi durumundaki MNO'dan izin alması gerekecektir.

2.8. GÜVENLİK

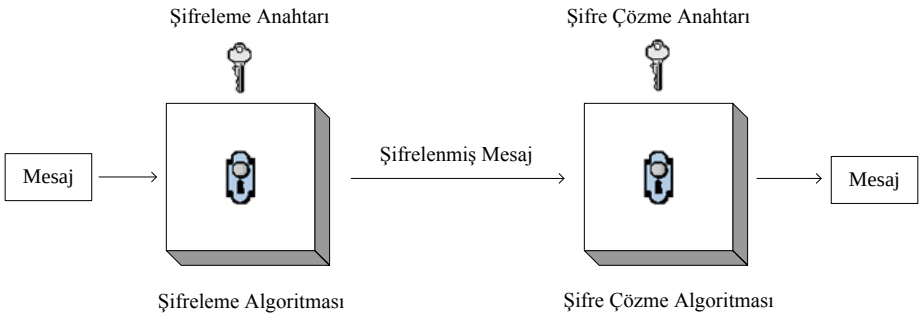
Tez kapsamında geliştirilen protokolün en önemli parçalarından biri de güvenliktir. Tez çalışmamıza temel teşkil eden altyapı ve güvenlik algoritmaları konuları bu bölümde incelenmiştir. İki aktör arasında sayısal veri iletişimi için herhangi bir güvenlik gerektiğinde, bu verinin şifreleme yolu ile gönderici tarafından şifrelenmesi, alıcı tarafından da şifreli metnin şifresinin çözülmesi gereklidir. Şifreleme ve şifre çözme algoritmaları bilinen yöntemleri içerirken, gönderici ve alıcının bu işlemlerde kullanacakları ve anahtar adı verilen bilgilerin gizli kalması, talep edilen güvenlik hedeflerine ulaşmayı mümkün kılar. Bu algoritmalar, gönderici ve alıcının kullandıkları anahtarların sayısı ve özelliğine bağlı olarak sınıflandırılırlar.

2.8.1. Gizli Anahtarlı (Simetrik) Şifreleme

Şifreleme ve şifre çözme işlemleri için aynı anahtarın (ya da birbirinden kolaylıkla elde edilebilecek iki anahtarın) kullanıldığı sistemlerdir (Şekil 2.5). Özellikleri:

- Hem şifrelemede, hem de şifre çözmede kullanılan ortak anahtarın sadece gönderici ve alıcı tarafından bilinmesi nedeni ile taraflar arasında iletilen şifrelenmiş bilgiler, bu iki kullanıcı dışındaki kişilerden gizlenmiş olur. (Gizlilik sağlanır)
- Göndericiden alıcıya gönderilmiş olan bilgi üçüncü bir kişi tarafından değiştirildiği taktirde, değiştirilmiş olan bu bilgi alıcı tarafından açılmaya çalışıldığında bozulmuş bir netice ortaya çıkacağı için, dokümanın yetkisiz bir kişi tarafından değiştirilmiş olduğu anlaşılmış olur ve dolayısı ile Bütünlük sağlanır.

- Göndericiden alıcıya gönderilmiş olan bilgi, alıcı tarafından anahtar kullanılarak açıldığında alıcı, bilgiyi göndericinin göndermiş olduğundan emin olur ve dolayısı ile Kimlik Doğrulama sağlanır.
- Hem gönderici hem de alıcı aynı anahtarı bildiği için, şifrelenmiş olan bir bilgiyi göndericinin mi alıcının mı şifrelediği, üçüncü bir kişiye karşı ispat edilemez ve dolayısı ile İnkar Edememe sağlanamaz.

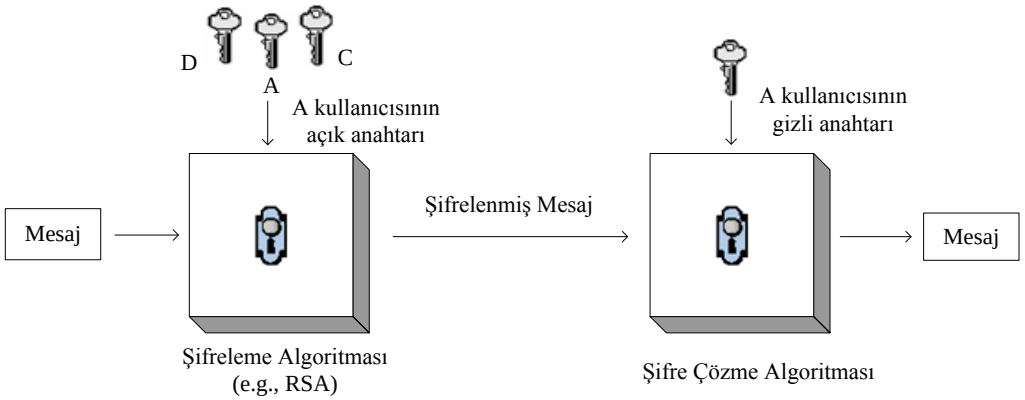


Şekil 2.5: Gizli Anahtarlı Şifreleme.

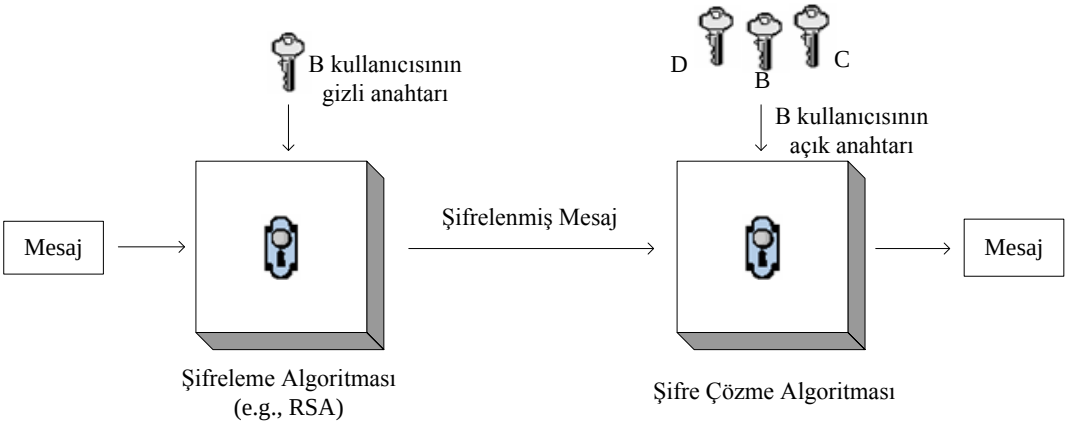
2.8.2. Açık Anahtarlı (Asimetrik) Şifreleme

Şifreleme ve şifre çözme işlemleri için iki farklı anahtarın kullanıldığı kripto sistemlerdir. Bu anahtarların birisini elde eden kişi, diğerini üretemez. Özellikleri:

- Açık anahtar kullanılarak herhangi bir kişi tarafından şifreleme yapılıp şifre çözme anahtarına sahip olan tek kişi tarafından şifre çözme seçeneğinde (Şekil 2.6) Gizlilik sağlanır.
- Gizli anahtara sahip olan tek kişi tarafından şifreleme yapılıp herhangi bir kişi tarafından açık anahtar ile şifre çözme seçeneğinde (Şekil 2.7) Kimlik Doğrulama ve İnkar Edememe sağlanır.
- Gizli ya da açık herhangi bir anahtar kullanılarak şifreleme yapıldığında, veri yetkisiz bir kişi tarafından bozulduğu taktirde diğer anahtar ile şifre çözme yapılamayacağı için Gizlilik sağlanır.



Şekil 2.6: Açık Anahtarla Şifreleme Yöntemi.



Şekil 2.7: Asimetrik Şifreleme - Gizli Anahtarla Şifreleme Yöntemi.

2.8.3. Hash Alma

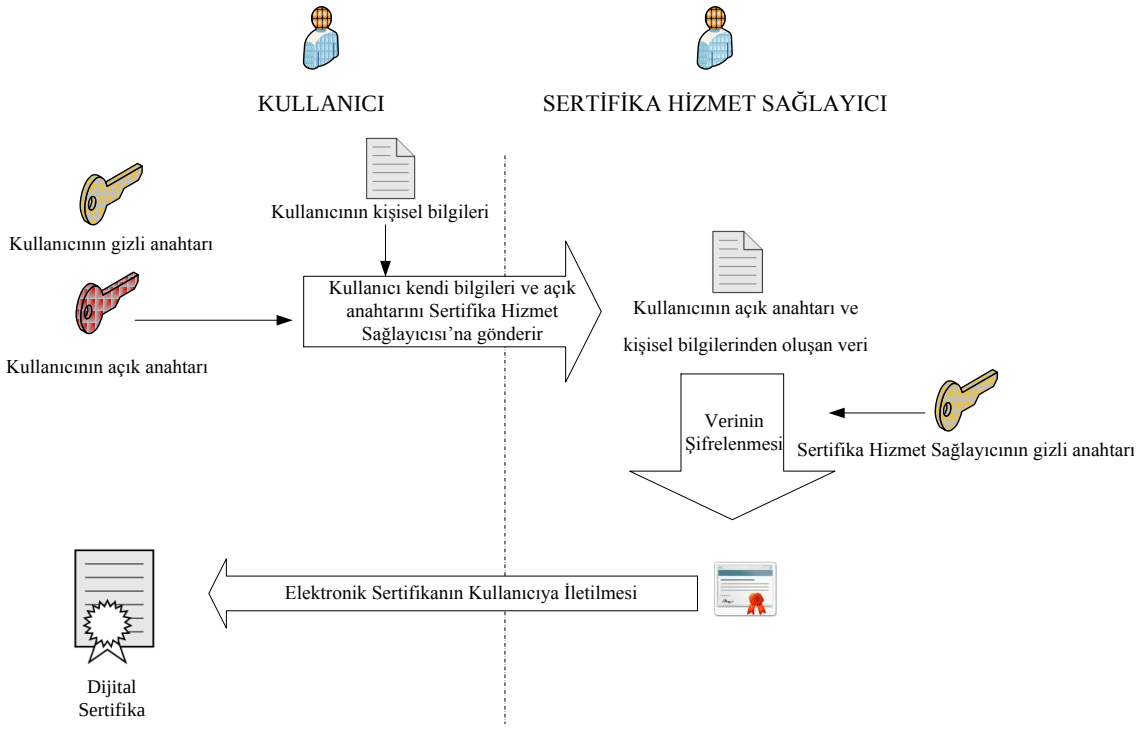
Hash alma, uzun bir bilgiyi daha kısa bir içeriğe dönüştürmek üzere matematiksel tek yönlü (geri çevrilemeyen) işlem kullanılarak bir hash değeri üretilmesidir. Orijinal ve değiştirilmiş iki ayrı bilginin hash değerlerinin karşılaştırılması neticesinde fark olması durumunda dosyanın değiştirilmiş olduğunun (veri bütünlüğünün bozulduğunun) anlaşılacağı temeline dayanır. Hash alma işlemi *gizlilik* gerekmeyen, fakat *bütünlük* gereken durumlarda kullanılır; şifreleme yöntemlerine nispeten daha kolay ve daha hızlı çalışır ve daha az depolama yerine ihtiyaç duyar.

2.8.4. Elektronik Sertifika

Elektronik sertifika bir kişinin, bilgisayarın ya da organizasyonun kimliğinin inkar edilemez şekilde doğrulanması için kullanılan ve elektronik imza sahibinin imza doğrulama verisi ile kimlik bilgilerini birbirine bağlayan kayıttır. Elektronik sertifikalar herkes tarafından güvenilen ve Elektronik Sertifika Hizmet Sağlayıcısı denilen kurumlar tarafından tahsis edilir [12].

Bir elektronik sertifikanın içerisinde sertifika sahibinin kimlik bilgisi, sertifika seri numarası, sertifikanın geçerlilik süresi, sertifika sahibinin açık anahtarı, sertifika hizmet sağlayıcısının elektronik imzası gibi bilgiler bulunmaktadır.

Şekil 2.8'de bir elektronik sertifikanın oluşturulması aşaması anlatılmıştır. Kullanıcı, kendi kişisel bilgilerini ve açık anahtarını Sertifika Hizmet Sağlayıcıya gönderdikten sonra Sertifika Hizmet Sağlayıcı veriyi kendi gizli anahtarıyla şifreleyerek kullanıcının sertifikasını üretmektedir.



Şekil 2.8: Elektronik Sertifikanın Oluşturulması.

2.8.5. Elektronik İmza

Elektronik imza, bir elektronik veriye eklenen ve verinin kimden geldiğini kanıtlamak amacıyla kimlik doğrulaması için kullanılan elektronik veridir [12]. Elektronik imza kullanılan bir veride elektronik sertifikaya dayanarak imza sahibinin kimliğinin inkar edilemez şekilde tespiti yapılır. Şekil 2.9'da Elektronik imzanın ve elektronik sertifikanın kullanımı detaylı olarak verilmiştir.

2.8.6. Güvenli Giriş Katmanı

Güvenli Giriş Katmanı (SSL: Secure Sockets Layer), verilerin Internet üzerinden güvenli bir şekilde iletilmesini sağlamak amacıyla geliştirilmiş olan bir protokoldür. Günümüzde SSL'in 1996 yılında geliştirilen 3.0 versiyonu kullanılmaktadır [13].

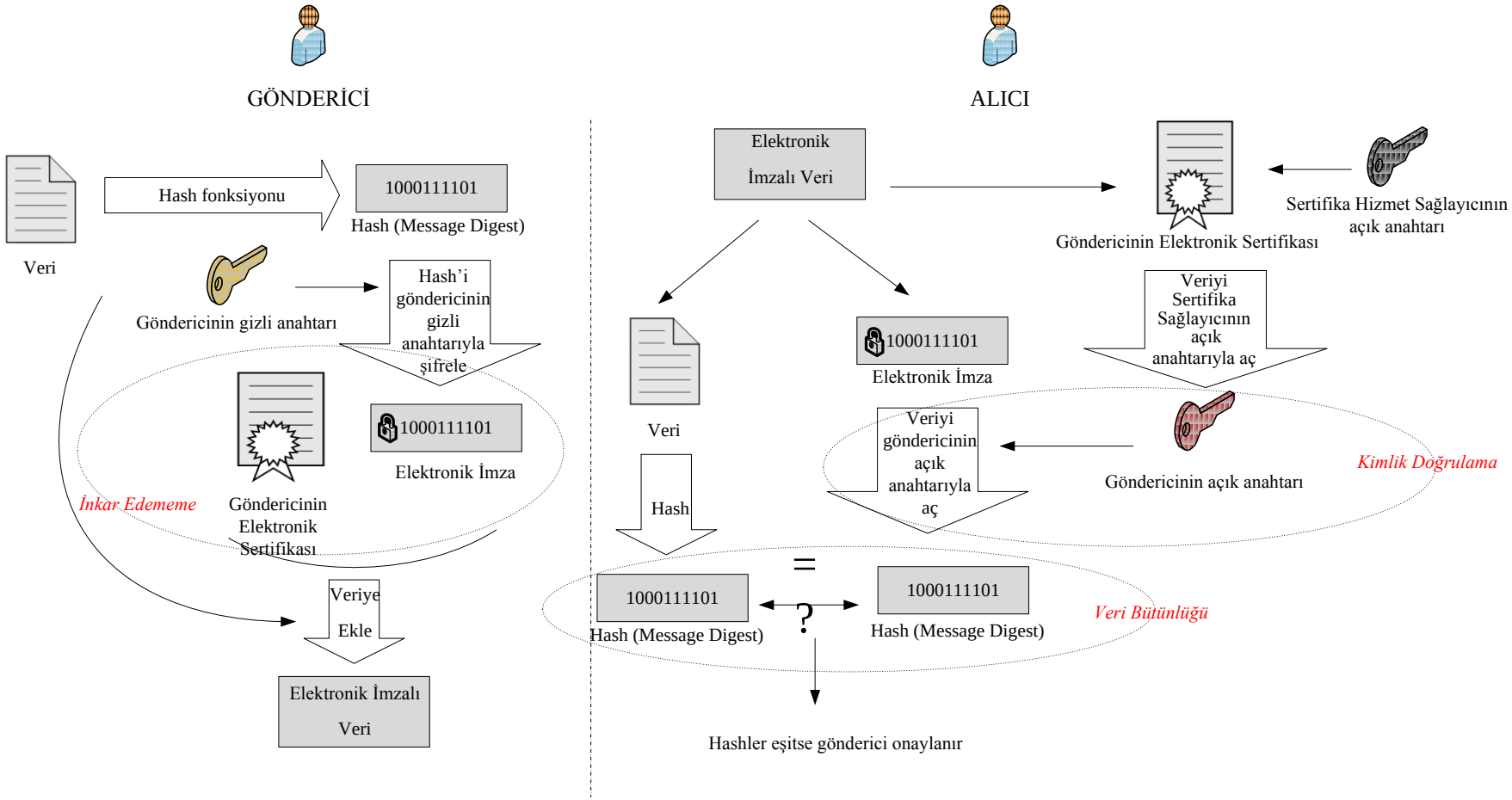
SSL protokolünün kullanımı Şekil 2.10'da detaylı olarak verilmiştir.

2.8.7. Rivest-Shamir-Adleman (RSA) Algoritması

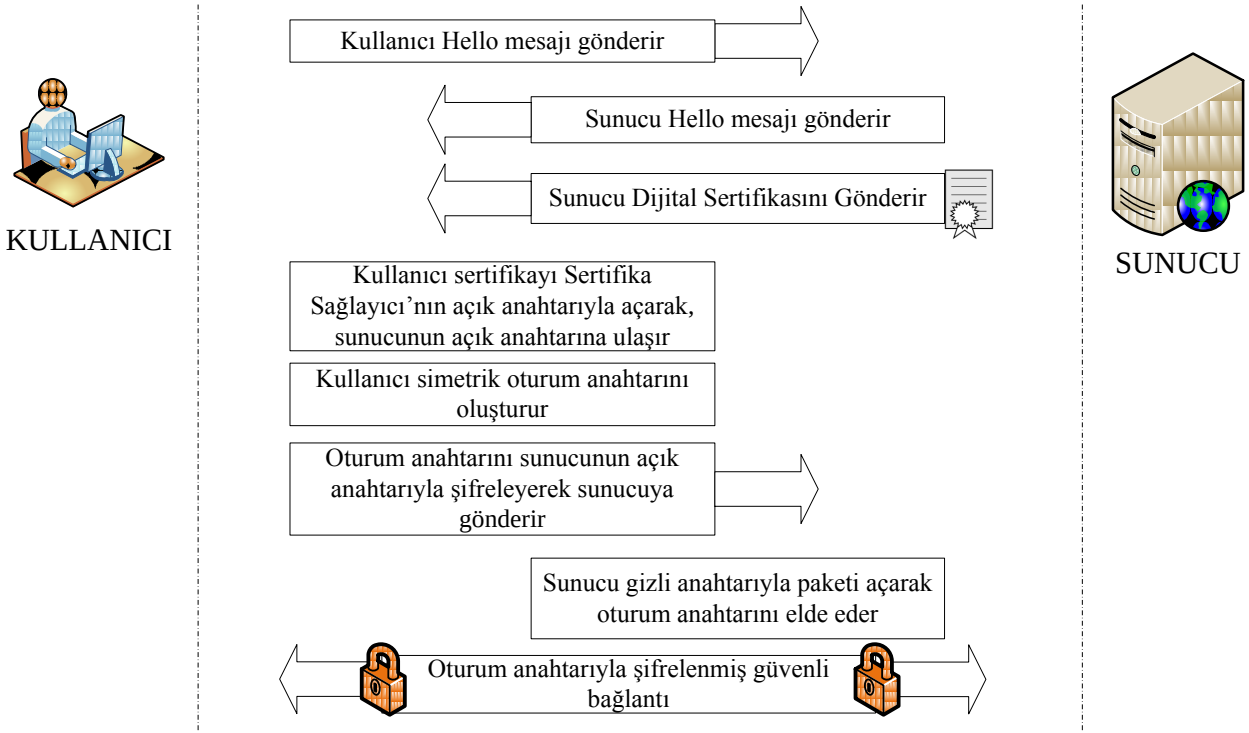
RSA güvenli veri iletişimi için yaygın olarak kullanılan bir açık anahtarlı şifreleme sistemidir. RSA sistemi oluşturmak isteyen bir kullanıcı öncelikle şifreleme gizli anahtarı (K_r) ve şifre çözme açık anahtarını (K_u) oluşturur. Oluşturulan K_r bu kullanıcıda saklı kalıp, K_u ise herkese açık olarak ilan edilir. Herhangi bir kişi K_u kullanarak bir metni şifrelediğinde, bu metnin şifresi sadece K_r anahtarına sahip olan kullanıcı tarafından elde edilebilir.. RSA protokolü kullanılarak anahtar oluşturma süreci Şekil 2.11'de verilmektedir. Şekil 2.12'de ise oluşturulan açık ve gizli anahtarların şifreleme ve şifre çözme işlemlerinde kullanımı gösterilmiştir.

2.8.8. Anahtar Değişim Protokolleri

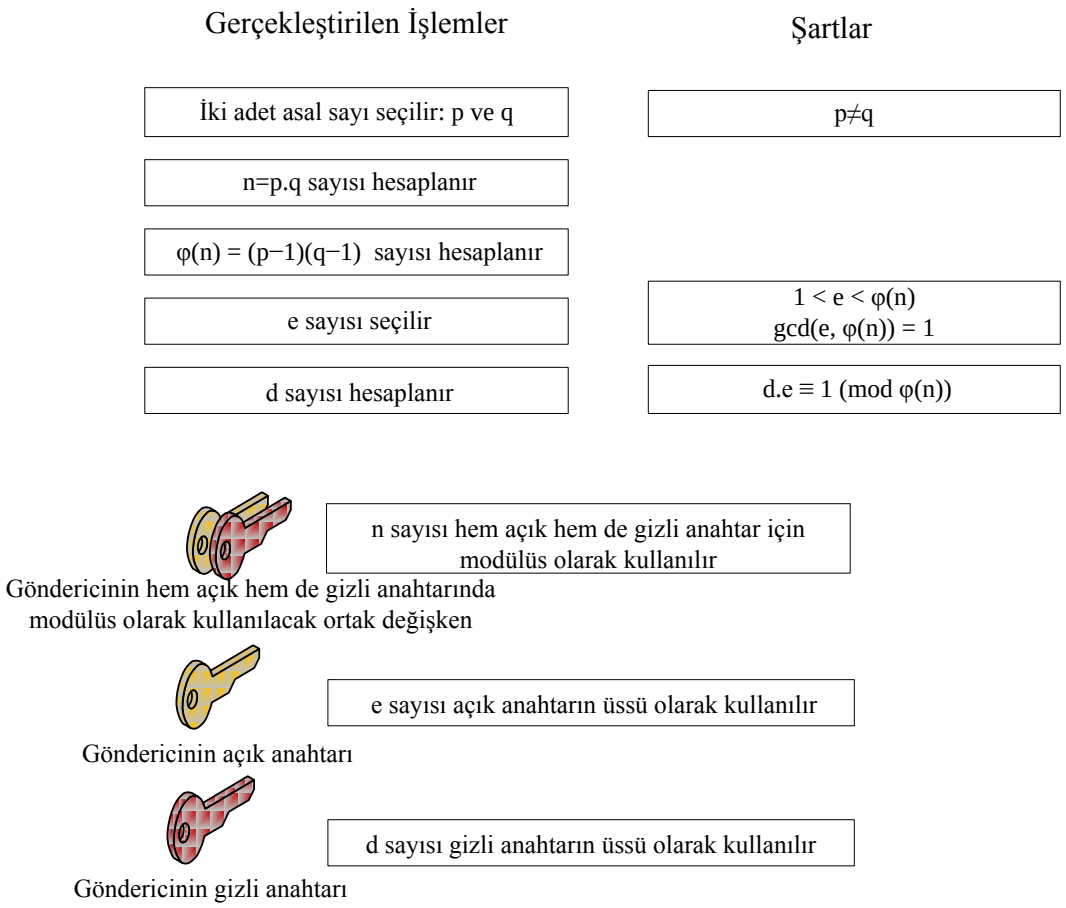
Gönderici ile Alıcı arasında belirli bir güvenlik gereksinimini sağlamak üzere şifreleme yapmak gerektiğinde, eğer taraflarda arzu edilen seviyede güvenlik sağlayacak anahtar(lar) mevcut değil ise, bu anahtar(lar)ı oluşturmak için bir Anahtar Değişim Protokolü uygulanır. Anahtar Değişim Protokolleri herkesin erişebildiği açık kanal üzerinde çalışmak üzere tasarlanırlar. Diffie - Hellman Anahtar Değişim algoritması, bu alandaki kayda değer ilk örnektir [14]. İki kullanıcının karşılıklı olarak matematiksel işlemler gerçekleştirerek gizli anahtar oluşturduğu bu algoritmanın detayları Şekil 2.13'de gösterilmiştir.



Şekil 2.9: Elektronik İmzanın ve Elektronik Sertifikanın Kullanımı.



Şekil 2.10: SSL Protokolü.



Şekil 2.11: RSA ile Anahtar Oluşturma.

Alice

Açık Anahtar: n,e

Gizli anahtar: d

Bob gönderilecek mesaj M'i dolgu şeması(padding scheme) adı verilen yöntemle integer m'e dönüştürür
0 <= m < n

Şifrelenmiş mesajı hesaplar: $c = m^e \pmod n$

Bob c mesajını Alice'e iletir

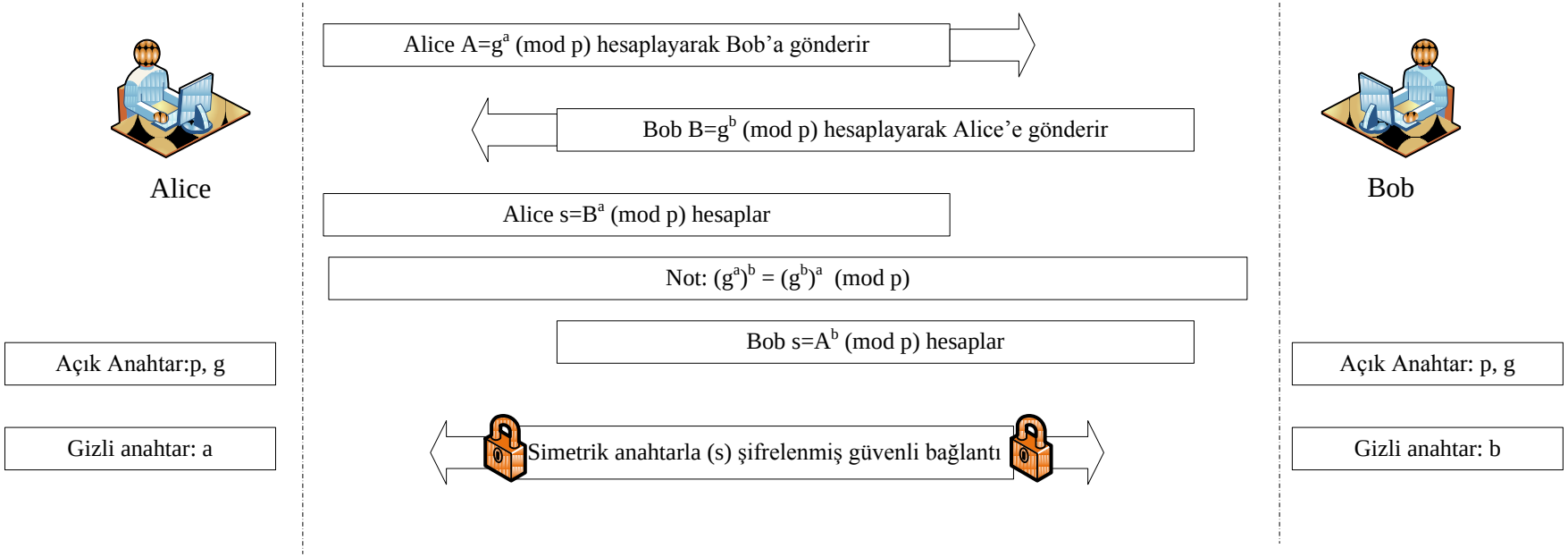
Alice m değerini hesaplar: $m = c^d$

Bob

Açık Anahtar: n,e

Gönderilecek Mesaj: M

Şekil 2.12: RSA ile Şifreleme ve Şifre Çözme İşlemleri.



Şekil 2.13: Diffie - Hellman Anahtar Değişim Protokolü.

Diffie - Hellman Anahtar Değişim Protokolü, iki aktörün (A ve B) açık bir iletişim kanalı üzerinden gizli anahtar oluşturmasını sağlamaktadır. Protokolde p ve g değerleri her iki kullanıcının bildiği iki değerdir. Ayrıca A kullanıcısı sadece kendi bildiği gizli a değerini, B kullanıcısı da yine sadece kendi bildiği gizli b değerini oluşturmaktadır. A kullanıcısı g^a (mod p) değerini hesaplayarak B kullanıcısına göndermekte, o da g^b (mod p) değerini hesaplayarak A kullanıcısına göndermektedir. Daha sonra A ve B'nin hesaplayacakları $(g^a)^b$ (mod p) ve $(g^b)^a$ (mod p) değerleri birbirine eşit olacağından, kullanılacak ortak anahtar üretilmiş olmaktadır. Sistemin güvenliği; a değerinin sadece A, b değerinin de sadece B tarafından bilinmesinden ve diğer kişilerin bu anahtarı elde etmek üzere çözmek zorunda oldukları ayrık logaritmik probleminin zorluğuna dayanmaktadır.

Orijinal Diffie - Hellman Anahtar Değişim Protokolünde zaman içerisinde bazı güvenlik açıkları bulunmuş olup bunlardan en önemlisi Aradaki Adam Saldırısı'dır (Man in the Middle Attack). Ortaya çıkan güvenlik açıklarını yok etmek üzere, Diffie-Hellman protokolünün farklı versiyonları geliştirilmiştir. Bu çalışmalardan bir tanesi "Password-Authenticated Key Exchange" (PAK) protokolüdür. Bu protokol aynı zamanda "RFC 5683" [15] ve "ITU-T Recommendation X.1035" [16] olarak da standartlaşmıştır. Bu protokol Diffie-Hellman protokolünü kullanıcının da hatırlayabileceği bir şifre yardımıyla geliştirmektedir. Protokolde aktörler karşılıklı olarak birbirlerinin şifrelerini doğrulamaktadırlar. Protokolün pasif ve aktif tüm ataklara karşı güvenli olduğu belirtilmiştir ve ayrıca iletme gizliliği (forward secrecy) de sağlanmaktadır. Protokolün detayları Şekil 2.14'de verilmiştir. PAK protokolü işlem gücü düşük olan akıllı kartlar için tasarlanmadığından dolayı akıllı mevcut hali ile kartlarda uygulanması mümkün değildir. Bununla beraber, geliştireceğimiz protokolde kısmi olarak kullanılabileceği görülmüştür.

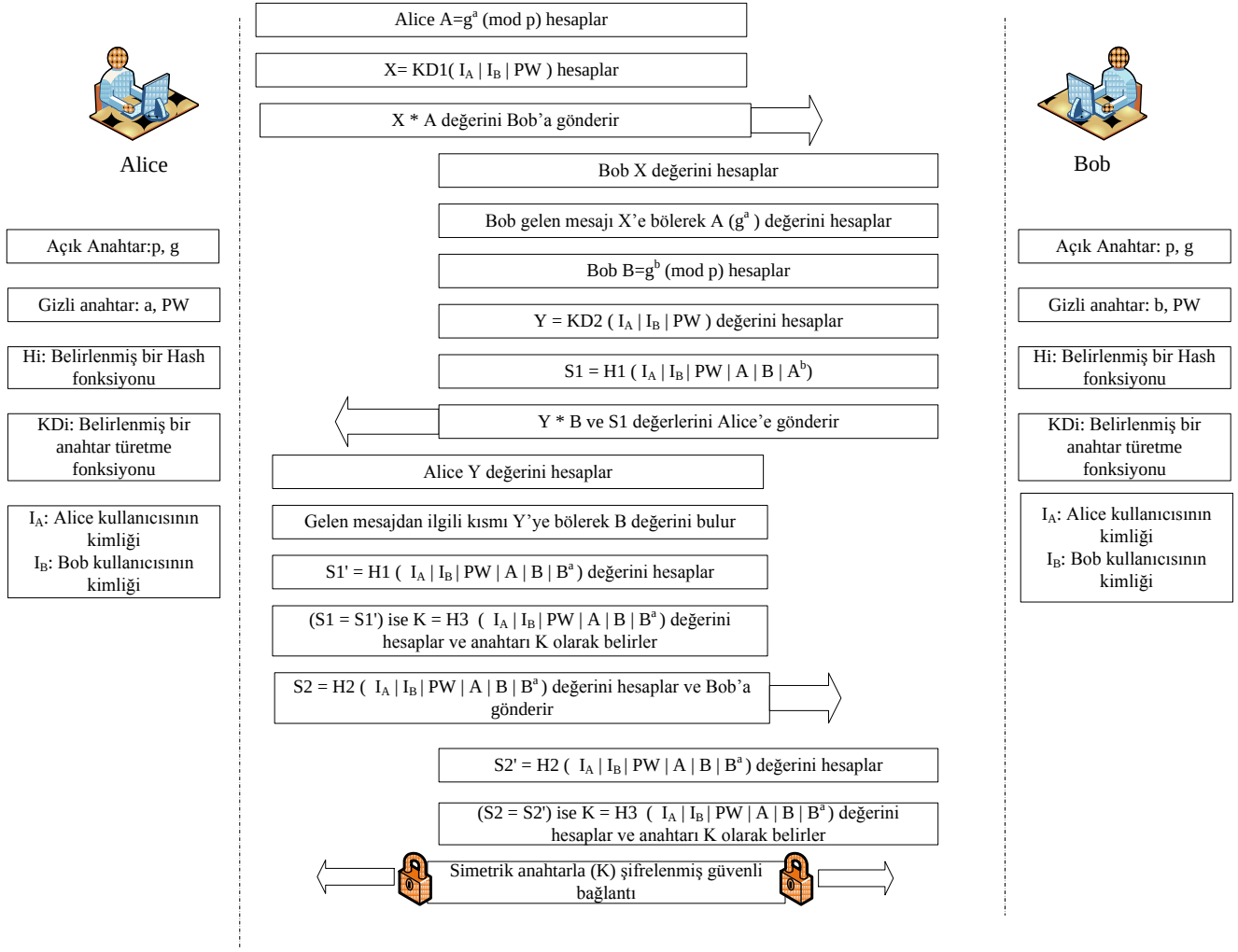
Bir diğer anahtar oluşturma algoritması da RFC 6539 olarak standartlaşan "IBAKE: Identity-Based Authenticated Key Exchange" protokolüdür [17]. Bu protokol kimlik tabanlı (identity based) bir anahtar oluşturma algoritması kullanıp iki aktör arasında kimlik bilgilerine ve açık-gizli anahtar eşlerine göre Eliptik Eğri Şifrelemesi (ECC: Elliptic Curve Cryptography) de kullanarak simetrik anahtar üretmektedir. Bu algoritmayı kullanan aktörlerin açık ve gizli anahtar çiftlerinin önceden oluşturulmuş

olması gerekmektedir. Algoritmanın detayları Şekil 2.15'de verilmiştir. ECC algoritmasında anahtar üretecek olan iki kullanıcı önceden oluşturulmuş açık-gizli anahtar çiftlerine sahip olmaları gerekmekte; hedeflenen Akıllı Kartlarda ise böyle bir olanak mümkün olmadığından dolayı geliştirilen protokolden tez kapsamında yararlanılması mümkün görülmemiştir. Bununla beraber eliptik eğri şifrelemesinin bir uygulaması olmasından dolayı, protokolümüzü geliştirirken kısmen faydalı olabileceği görülmüştür.

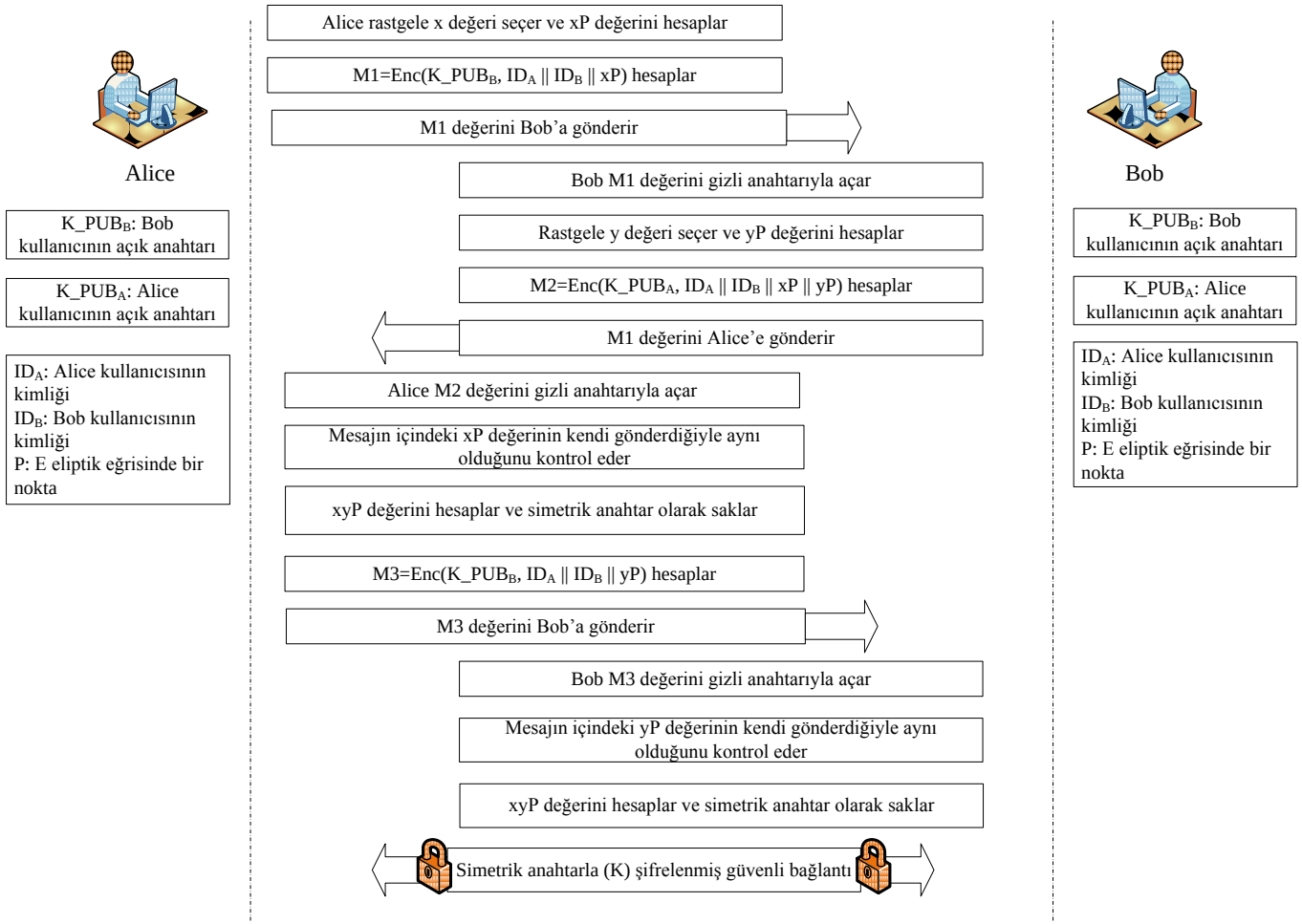
2.9. AKILLI KARTLARDA VE AKILLI KARTLARLA İLETİŞİMDE GÜVENLİK

Literatürde akıllı kartların güvenlikleri ile ilgili bir takım çalışmalar bulunmaktadır. Bununla beraber, SIM kart ile MNO dışındaki bir aktör ile uçtan uca iletişim güvenliğine yönelik sınırlı sayıda çalışma bulunmakta olup, bu çalışmalar aşağıda irdelendiği şekilde problemimizin çözümünde kullanılabilir özelliklere sahip değillerdir.

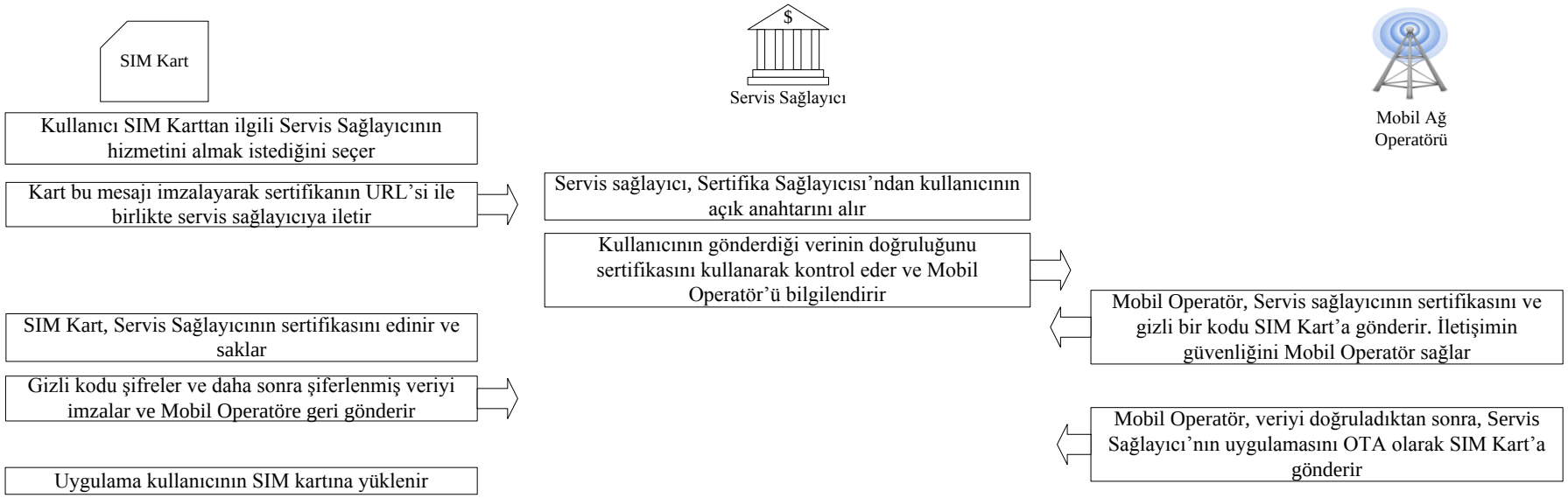
Yapılan bir çalışmada [18], fabrika üretim aşamasında gizli anahtar yüklenmiş olan SIM kartların servis sağlayıcı ile güvenli bir şekilde iletişim kurması için uçtan uca güvenlik modeli tasarlanmıştır. Protokoldeki iletişim, şifrelenmiş SMS mesajları ile gerçekleştirilmiştir ve üç aşamadan oluşmaktadır. Birinci aşama kullanıcının talep ettiği servise kaydolma aşamasını, ikinci aşama kullanıcı ile servis sağlayıcının karşılıklı olarak kimliklerini doğrulama aşamasını, üçüncü aşama ise güvenli anahtar oluşturma aşamasını içermektedir. Çalışmanın detaylı incelenmesinin ardından üç aşama da Şekil 2.16, 2.17, ve 2.18'de özetlenmiştir. Söz konusu çalışmada [18], SIM kart ile Servis Sağlayıcı arasında uçtan uca güvenli iletişim sağlanmış olsa da, bu işlem ancak fabrika aşamasında SIM karta yüklenmiş olan gizli anahtar üzerinden güvenlik sağlanarak gerçekleştirebilmiştir. Gerçekleştirdiğimiz tez çalışmasına konu olan düşük kapasiteli SIM kartlara fabrika aşamasında yüklenmiş herhangi bir gizli anahtar bulunmadığından, bahse konu çalışma amacımıza dönük olarak kullanılamayacaktır.



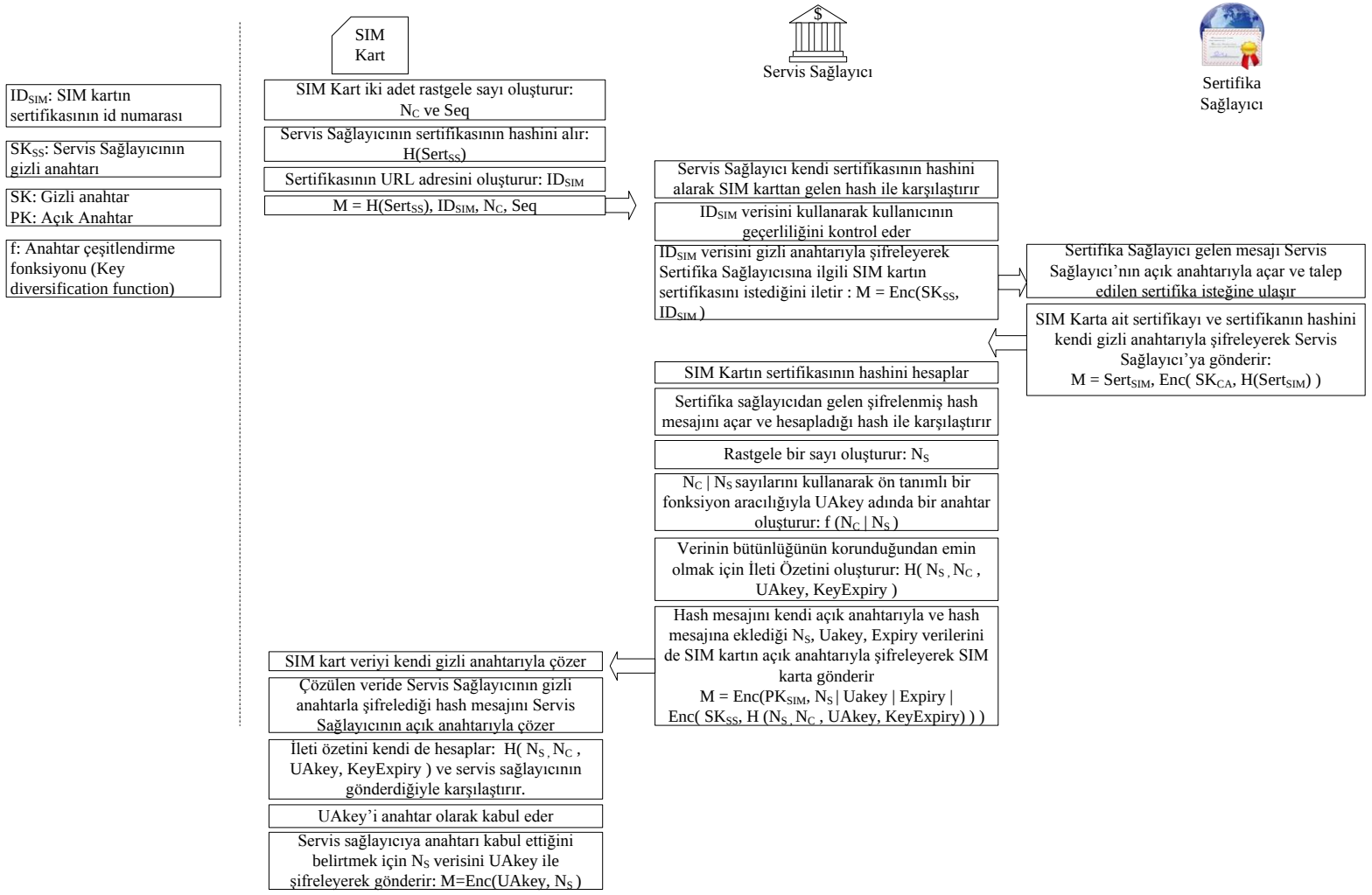
Şekil 2.14: Password-Authenticated Key Exchange Protokolü.



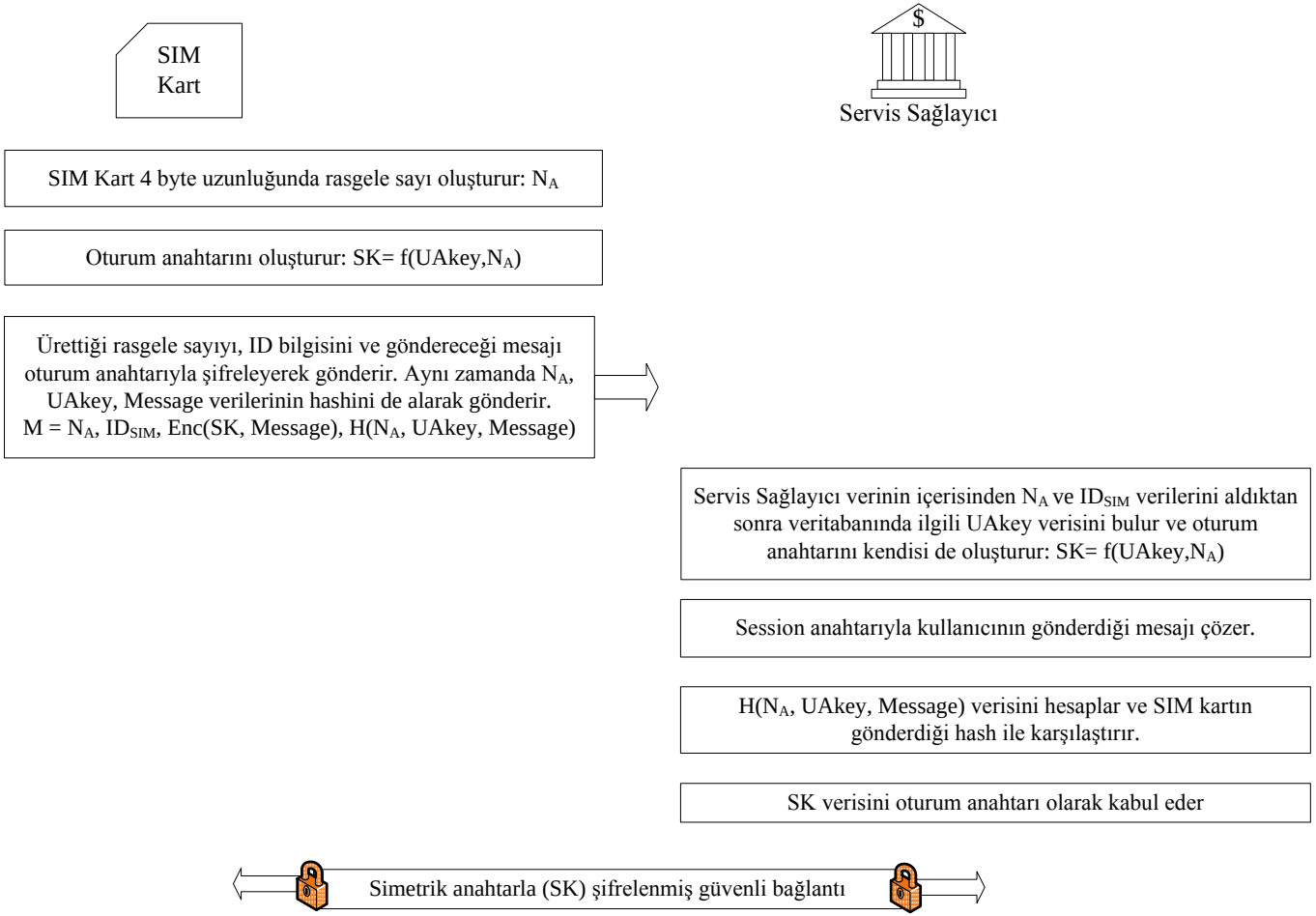
Şekil 2.15: IBAKE: Identity-Based Authenticated Key Exchange Protokolü.



Şekil 2.16: Birinci Aşama - Servise Kaydolma Aşaması.



Şekil 2.17: İkinci Aşama - Kimlik Doğrulama Aşaması.



Şekil 2.18: Üçüncü Aşama - Oturum Anahtarı Oluşturma Aşaması.

SIM kartlardaki güvenlik konusunda gerçekleştirilen bir başka çalışma [19], katma değer katan SIM uygulamalarının güvenliği konusunda incelemelerde bulunmuştur. Bu çalışmada yazarlar SMS üzerine kurgulanmış geleneksel uygulama modelinin güvenliğini analiz etmişlerdir. Ayrıca üretim aşamasında üzerlerine yüklenmiş gizli anahtar içeren SIM kartlar için mobil ticarette kullanılabilecek bir güvenlik modeli tasarlanmıştır. Modelde kimlik doğrulama süreci, SIM kart ile güvenli erişim sunucusu arasındaki iletişim süreci, ve güvenli erişim sunucusunun iç iletişim süreci olmak üzere üç aşama bulunmaktadır. Geliştirilen model yazarlar tarafından güvenilir ve uygulanabilir bir model olarak belirtilmiştir. Model açık-gizli anahtar çiftleri üretim esnasında üzerlerine yüklenmiş olan SIM kartlar üzerinde çalıştığı için, çalışma amacımıza dönük olarak kullanılamamıştır.

Diğer bir çalışmada [20], yazarlar SIM kartlarda uçtan uca oturum anahtarı (session key) değişimi için SSL protokolü öneren bir çalışma gerçekleştirmişlerdir. Çalışmada SSL kullanımının amacı SIM kart ile OTA platformu arasında açık olarak gönderilen SMS mesajlarının şifrelenerek, güvenli bir şekilde iletilmesini sağlamaktır. Mesajların içeriğinin herhangi bir saldırgan tarafından değiştirilemeyerek mesajların veri bütünlüğü ve mesajların ağdaki hiç bir aktör tarafından okunamayacak şekilde veri gizliliği sağlanmıştır. İncelenen protokolde OTA platformu ve SIM kart arasında güvenli iletişim incelenmiş ve tez çalışması için değerlendirilmiştir. Fakat protokol iletişim başlamadan önce SIM kartın üzerine gizli anahtar yüklenmesi varsayımına dayandığı için protokoldeki unsurlar tez çalışmasında kullanılamamıştır.

2.10. BÖLÜM SONUCU

Tez çalışması ile ilişkili olan akıllı kartlar, güvenlik, ve anahtar değişim protokolleri konularında ön bilgiler ile konumuz ile ilgili olarak bugüne kadar yapılmış olan çalışmalar bu bölümde verilmiştir. Yapılan araştırmalar sonucunda, geliştireceğimiz protokolün Diffie-Hellman Key Exchange protokolünü temel alan, fakat SIM kart donanımına bağlı olan gereksinimleri de tatmin eden bir içeriğe sahip olması gerektiği ön görülmüştür.

3. MALZEME VE YÖNTEM

Tezin amacı, üretim esnasında şifreleme anahtarı yüklenmemiş olan SIM kartlar ile Servis Sağlayıcı arasında güvenli iletişimi mümkün kılacak altyapıyı hazırlamaktır. Bu doğrultuda tez çalışması kapsamında; Servis Sağlayıcı ile SIM kart arasında uçtan uca güvenli iletişimi mümkün kılacak olan ve SIMSec ismi verilen protokol tasarlanmış, protokole ait SIM kart yazılımı geliştirilmiş ve protokolün güvenlik testleri gerçekleştirilmiştir. Tez dokümanının bu bölümünde; tez çalışmasında uygulanan yöntem, sistem gereksinimleri, analiz çalışması ve protokolün sağlaması gereken güvenlik gereksinimleri detaylandırılmıştır.

3.1. TEZ ÇALIŞMASININ YÖNTEMİ

İlk olarak, SIMSec protokolüne temel teşkil eden konulardaki literatür çalışması gerçekleştirilmiştir. Bu doğrultuda günümüze kadar yapılmış olan akademik çalışmaların yanında; National Institute of Standards and Technology (NIST), The Internet Engineering Task Force (IETF), International Telecommunication Union (ITU) standartları da incelenmiştir.

Yapılan literatür çalışması sonucunda; geliştirilecek olan protokolün Diffie-Hellman metodolojisini temel almasına karar verilmiştir. Bununla beraber Diffie-Hellman metodolojisindeki güvenlik açıklarının kapatılması ile ilgili çalışmalar da incelenmiş ve uygun olanların SIM kart platformunda da çalışabilecek şekilde uyarlanmasına karar verilmiştir.

Var olan sistemin ve geliştirilecek protokolün analizi için ayrıca hedeflenen sistemin özellikleri ortaya çıkarılmıştır. Çalışmaya ait Birleşik Modelleme Dili (UML: Unified Modeling Language) dilinde, kullanım senaryosu diyagramı ve buna bağlı olarak olay tablosu ile etkinlik diyagramı oluşturulmuştur. Diyagramların çiziminde Microsoft® Visio programı kullanılmıştır.

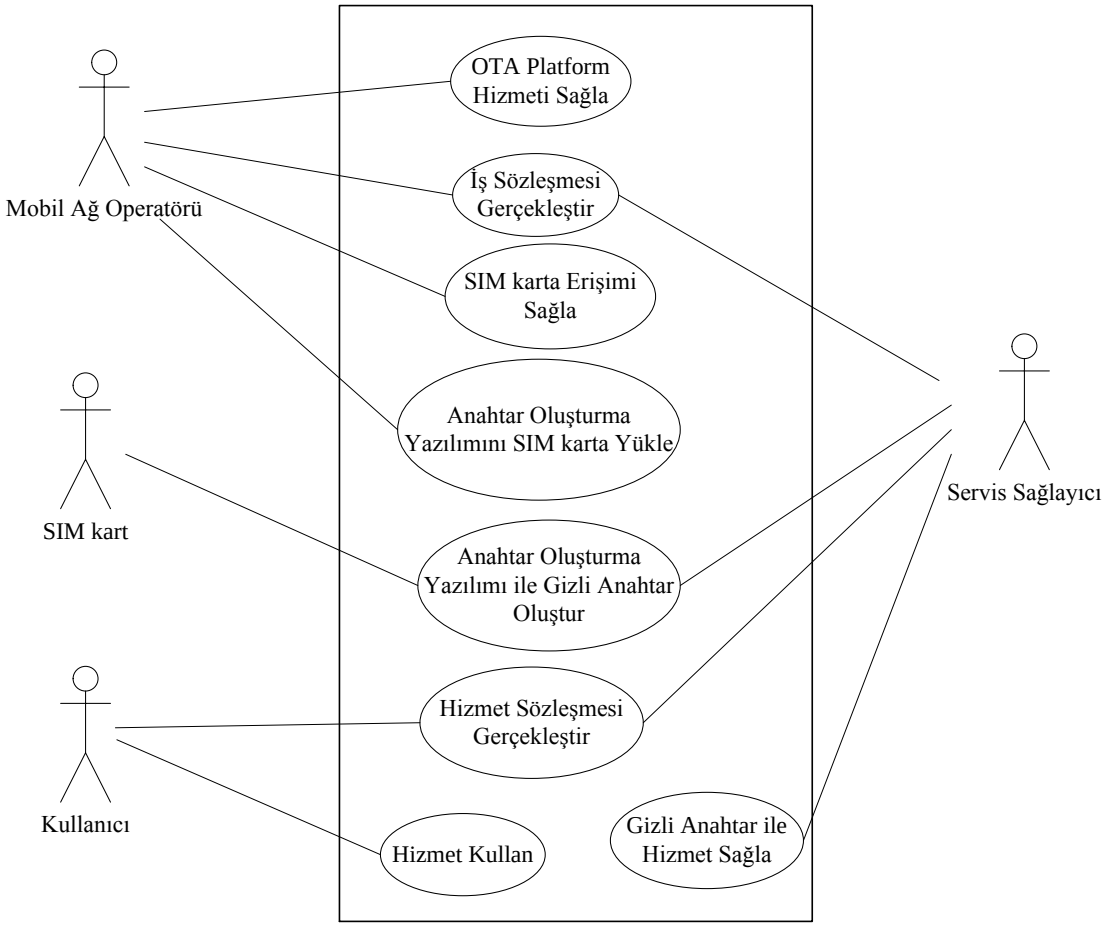
Uçtan uca güvenli iletişim işlevini gerçekleştirecek olan SIM kart yazılımı Java Card programlama dili ve ortamı kullanılarak geliştirilmiştir. Bu kapsamda kullanılan programlar ve araçlar aşağıda yer almaktadır:

- Java Card Yazılım Geliştirme Aracı (Java Card Development Kit): Java Card dilinde yazılım geliştirmek için ihtiyaç duyulan kütüphaneleri bulunduran yazılım geliştirme aracıdır.
- Yazılım Geliştirme Ortamı:
    - Netbeans: SIM kart yazılımının simülatörde test edilmesi için kullanılan yazılım geliştirme ortamıdır.
    - Izy NFC: SIM kart yazılımının geliştirilmesi için kullanılan yazılım geliştirme ortamıdır.
- SIM kart: Yazılımın test edilmesi için kullanılmıştır.
- Omnikey SIM Kart okuyucu: Bilgisayar ile SIM kart arasında bağlantı kuran SIM kart okuma aracıdır.
- Jload uygulaması: SIM kart için geliştirilecek Java card yazılımını SIM kart üzerine yükleyebilmek için ihtiyaç duyulan programdır.
- Casper Güvenlik Aracı: Geliştirilmiş olan protokol, gereksinimleri sağlayıp sağlamadığını belirlemek için kullanılmıştır.

3.2. SİSTEM ANALİZİ

Bu bölümde, geliştirilecek olan SIMSec protokolü için gerekli olan analiz çalışmaları anlatılmaktadır. Aktörlerin sistem ile olan etkileşimini ortaya koymak için kullanım senaryosu diyagramı, olayların detaylarını ortaya koymak için olay tablosu ve olayların zamanlamasını ortaya koymak için ise etkinlik diyagramı UML dili kullanılarak oluşturulmuştur.

Kullanım Senaryosu Diyagramı, ilgili sistem sınırları içerisinde gerçekleşebilecek olan tüm davranış seçeneklerini gösterir ve aktörler ile kullanım senaryoları arasındaki ilişkilerin oluşturulması sağlanır. Böylece sistemden beklenen temel gereksinimler tespit edilebilir. SIMSec protokolünün gerçekleştirilebilmesi için gerekli olan kullanım senaryosu diyagramı Şekil 3.1'de gösterilmektedir.



Şekil 3.1: Kullanım Senaryosu Diyagramı

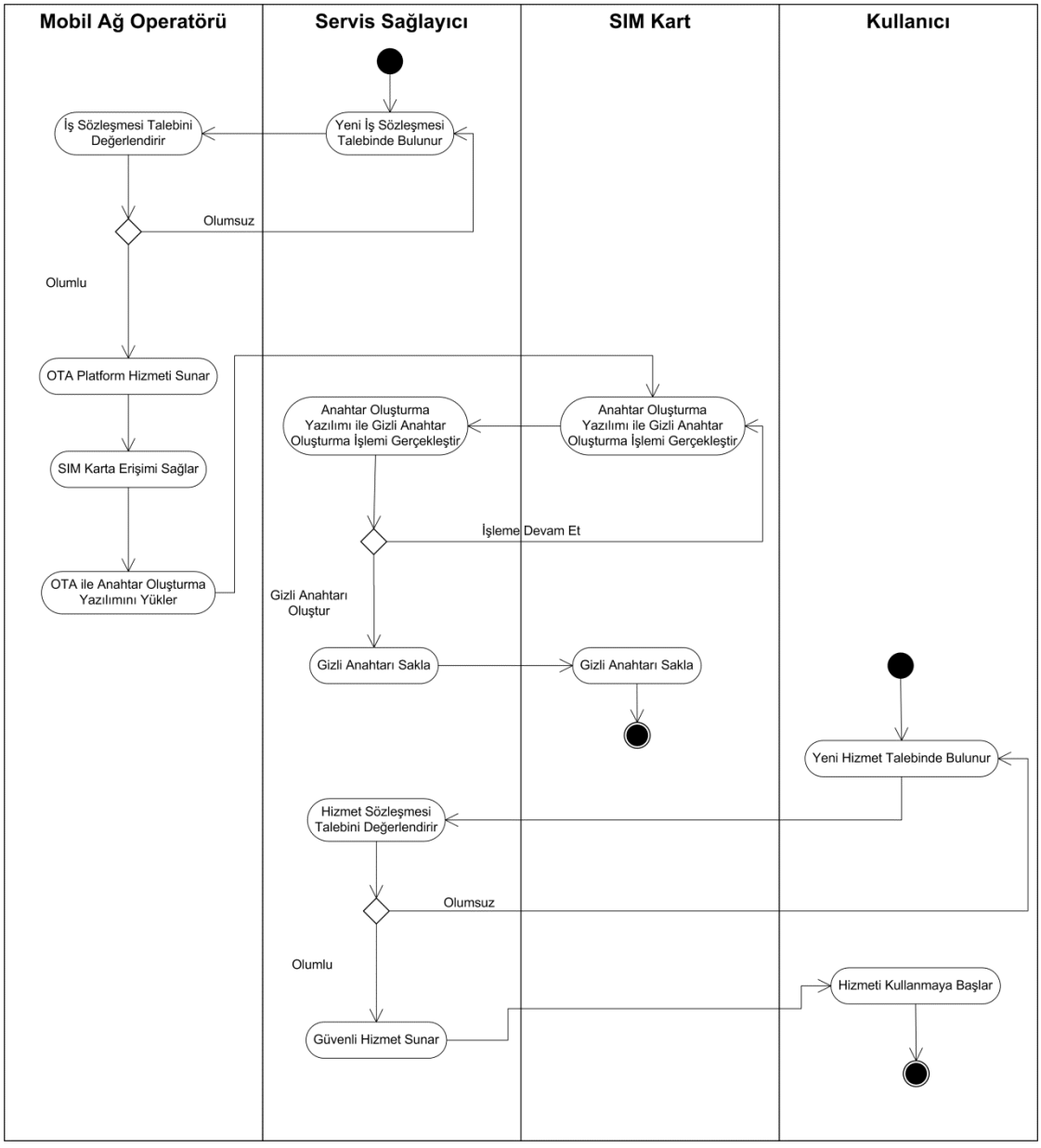
Olay Tablosu, Kullanım Senaryosu Diyagramında bulunan her senaryonun altı parametre (olay, kaynak, tetikleyici, kullanım senaryosu, cevap, hedef) çerçevesinde detaylı olarak açıklanmasına olanak sağlamaktadır ve analiz çalışmasının önemli unsurlarından biridir. Olay Tablosu, kullanım senaryolarının hangi aktör tarafından başlatıldığını ve sonlandırıldığını, sistemdeki tetikleyici unsurların ve oluşacak çıktıların neler olduğunu, ilgili kullanım senaryosunun sistemdeki genel olarak işleyişini anlatır.

Geliştirilecek olan sistemin olay tablosu, Şekil 3.1'deki kullanım senaryosu diyagramı ile ilişkili olarak Tablo 3.1'de verilmiştir. 3, 4 ve 5 numaralı olaylar proje kapsamında gerçekleştirilecek ve uygulanacaktır. Diğer olaylar/kullanım senaryoları (1, 2, 6, 7, 8) sistemin genel işleyişini anlatmak amaçlı detaylandırılmıştır.

Tablo 3.1: Olay Tablosu.

	Olay	Kaynak	Tetikleyici	Kullanım Senaryosu	Cevap	Hedef
1	MNO, OTA servisi sunar	MNO	OTA Platform Hizmeti	OTA Platform Hizmeti Sağlama	Hizmet Gerçekleştirme	Servis Sağlayıcı
2	Servis Sağlayıcı, MNO ile iş sözleşmesi imzalar	Servis Sağlayıcı	Yeni İş Sözleşmesi	İş Sözleşmesi Gerçekleştirme	İş Sözleşmesi Detayları	MNO & Servis Sağlayıcı
3	MNO, SIM Karta erişimi sağlar	MNO	SIM Karta Erişim	SIM Karta Erişim Sağlama	Erişimi Doğrulama	MNO
4	MNO, OTA platformu ile anahtar yazılımı ilgili SIM Karta yükler	MNO	Anahtar Yazılımı Yükleme	Anahtar Oluşturma Yazılımını SIM Karta Yükleme	Yüklemeyi Doğrulama	MNO
5	SIM Kart ve Servis Sağlayıcı karşılıklı gizli anahtar oluşturur	SIM Kart & Servis Sağlayıcı	Yeni Gizli Anahtar	Anahtar Oluşturma Yazılımı ile Gizli Anahtar Oluşturma	Gizli Anahtar	SecSIM64 Servis Sağlayıcı
6	Kullanıcı, Servis Sağlayıcı ile hizmet sözleşmesi yapar	Kullanıcı	Yeni Hizmet Sözleşmesi	Hizmet Sözleşmesi Gerçekleştirme	Hizmet Sözleşmesi Detayları	Kullanıcı & Servis Sağlayıcı
7	Kullanıcı Servis Sağlayıcı sayesinde ilgili hizmeti kullanır	Servis Sağlayıcı	Yeni Hizmet Sunma	Hizmet Kullanma	Hizmet Detayları	Kullanıcı
8	Servis Sağlayıcı, oluşturduğu gizli anahtar ile güvenli hizmet sunar	Servis Sağlayıcı	Güvenli Hizmet Sunma	Gizli Anahtar ile Hizmet Sağlama	Güvenli Hizmeti Doğrulama	Servis Sağlayıcı

Etkinlik Diyagramı, sistemin akış yönünden davranışını anlatan iş akış diyagramıdır. Şekil 3.2, geliştirilecek olan sistemin etkinlik diyagramını göstermektedir.



Şekil 3.2: Etkinlik Diyagramı

3.3 PROTOKOLDE SAĞLANMASI GEREKEN GÜVENLİK ŞARTLARI

Literatür Araştırması kısmında da anlatıldığı gibi, bugüne kadar bilgisayar gibi yüksek depolama ve işlem kapasitesine sahip iki aktör arasında anahtar değişiminde kullanılmak üzere geliştirilmiş olan genel amaçlı algoritmalar yanında, Akıllı kartlara

özel bazı çalışmalar da mevcuttur. Oysa üretim esnasında kişisel anahtar yüklenmemiş olan düşük kapasitelik kartlarda kullanılabilecek herhangi bir çalışma mevcut değildir.

Üretim esnasında gizli anahtar yüklenmemiş olan SIM kartların sağlayabildiği düşük seviyeli güvenlik şartları şu şekildedir:

- IMSI numarasının kullanımı sayesinde SIM kart kimliğinin hücresel ağ üzerinde tanımlanması
- K_i anahtarının kullanımı sayesinde SIM kart kimliğinin hücresel ağ üzerinde doğrulanması

SIM kart ile Servis Sağlayıcı arasında güvenli veri transferi gerçekleştirilebilmesi için SIMSec protokol sürecinin ve sonrasında oluşturulacak anahtarın sahip olması gereken güvenlik gereksinimleri ise aşağıdaki şekildedir, ve şu anda mevcut olan yeterlikten daha kapsamlıdır:

- Anahtar gizliliği,
- Oluşturulacak anahtarın güvenli iletişim için yeterli uzunlukta olması,
- İki aktörün de birbirinin kimliklerini doğrulaması,
- Veri bütünlüğünün korunması,
- Aradaki adam saldırısına karşı konulması,
- Tekrar gönderme saldırısına karşı konulmasıdır.

3.3.1. Anahtar Gizliliği

SIMSec protokolü sonrasında oluşturulacak olan anahtar sadece SIM kart ve Servis Sağlayıcı tarafından bilinmelidir. Anahtar oluşturma sürecindeki veri iletişimi Mobil Ağ Operatörünün kontrolündeki kanallardan gerçekleştirilecek olmasına rağmen, Mobil Ağ Operatörü de anahtar hakkında bilgi sahibi olmamalıdır.

3.3.2. Anahtar Uzunluğu

SIMSec protokolü sonrasında oluşturulacak olan anahtarın, veri güvenliğini yeterli ölçüde sağlayacak uzunlukta olması gerekmektedir. Oluşturulacak olan anahtar ele geçirilememeli, kaba kuvvet saldırısı ile kırılamayacak ölçüde de güçlü olmalıdır.

3.3.3. Servis Sağlayıcının SIM Kartın Kimliğini Denetlemesi

Servis Sağlayıcı tarafından SIM kartın kimlik doğrulaması gerçekleştirilerek, birlikte anahtar oluşturduğu aktörün doğru aktör olduğunu bilmesi gerekmektedir.

3.3.4. SIM Kartın Servis Sağlayıcının Kimliğini Denetlemesi

SIM kart tarafından Servis Sağlayıcının kimlik doğrulaması gerçekleştirilerek, birlikte anahtar oluşturduğu aktörün doğru aktör olduğunu bilmesi gerekmektedir.

3.3.5. Veri Bütünlüğü

Protokol kapsamında Servis Sağlayıcı ile SIM Kart arasında iletilen verilerin bu süreçte bir saldırgan tarafından değiştirilmesi önlenmelidir. İletilen veride bir saldırgan tarafından herhangi bir değişiklik yapılırsa, bu değişiklik alıcı tarafından saptanmalı ve dolayısıyla verinin bütünlüğünün bozulduğu anlaşıldığından anahtar oluşturma protokolü sonlandırılmalıdır.

3.3.6. Aradaki Adam Saldırısına Karşı Koruma

Aradaki adam saldırısı, iletilen verinin bir saldırgan tarafından elde edilmesi ve değiştirmesi yolu ile saldırganın birbiriyle iletişim gerçekleştirdiğini düşünen iki aktör arasında iletilen tüm veriye ulaşabilmesi amacıyla yapılan bir saldırı çeşididir. SIMSec anahtar oluşturma protokolü de, yetkisiz bir aktör tarafından gerçekleştirilecek olası bir Aradaki Adam Saldırısına karşı güvenli olmalıdır.

3.3.7. Tekrar Gönderme Saldırısına Karşı Koruma

Tekrar gönderme saldırısı, bir saldırganın bir aktörün gönderdiği veriyi ele geçirerek, bekletmesi ve belirli bir süre geçtikten sonra alıcıya göndermesi ya da veriyi ele geçirerek aynı veriyi alıcıya tekrardan göndermesi yoluyla yapılan bir saldırıdır. SIMSec anahtar oluşturma protokolü, bir saldırgan tarafından gerçekleştirilecek olası bir Tekrar Gönderme Saldırısına karşı güvenli olmalıdır.

3.4. BÖLÜM SONUCU

Tezin bu bölümünde tez çalışmasında uygulanan yöntem detaylandırılmış, gerçekleştirilen sistem analiz çalışması sunulmuş ve SIMSec protokolü sürecinde sağlanması gereken güvenlik şartları ortaya konulmuştur. Bir sonraki bölüm, geliştirilen SIMSec protokolünü detaylı olarak sunmakta, SIMSec protokolünün güvenlik testlerini

ortaya koymakta ve geliştirilen SIM kart uygulaması hakkında kapsamlı bilgiler sunmaktadır.

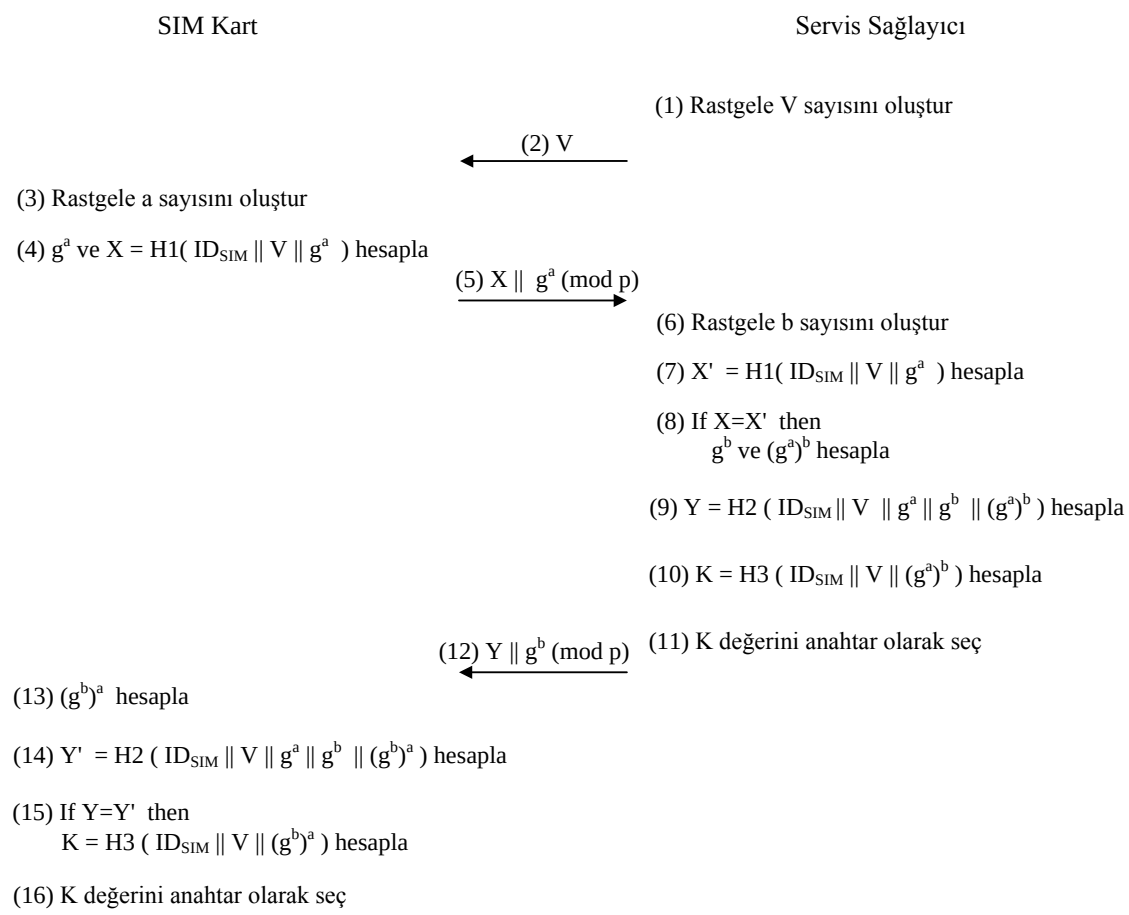
4. BULGULAR

Tez kapsamında literatür taraması, ilgili çalışmaların incelenmesi, ve analiz aşamalarından sonra SIMSec protokolünün tasarım sürecine geçilmiştir. Önceden yüklenmiş bir anahtar içermeyen SIM kartlar ile Servis Sağlayıcı arasında uçtan uca güvenli iletişim altyapısında kullanmak üzere anahtar oluşturulması protokolünü hedef alan tez çalışmamızda, akıllı kartların bellek ve işlem kapasitelerinin düşük olması dikkate alınmıştır. Dolayısıyla Java Card programlama dilindeki özel tanım ve komutlar kullanılarak etkin bir şekilde programa dönüştürülebilecek bir tasarım gerçekleştirilmekle beraber protokolün uyması gereken güvenlik şartları da dikkate alınmıştır.

Bu bölümde öncelikle geliştirilen SIMSec protokolü tanımlanmış ve protokolün detayları anlatılmıştır. Daha sonra protokolün 3. Bölüm'de detayları verilen güvenlik şartlarına uygunluğu denetlenmiştir. Son olarak da SIM kart üzerinde çalışmak üzere geliştirilen SIMSecApp yazılımıyla ilgili detaylar ve protokolün Casper aracı ile gerçekleştirilen güvenlik analizi ortaya konulmuştur.

4.1. SIMSEC PROTOKOLÜ

SIMSec protokolünün amacı, üretim esnasında gizli anahtar yüklenmemiş olan SIM kartlar ile Servis Sağlayıcı arasında güvenli iletişimi mümkün kılacak altyapıyı hazırlamaktır. SIMSec protokolü temel alınarak Java Card programlama dili ile geliştirilecek SIMSecApp yazılımı SIM karta yüklendikten sonra Servis Sağlayıcı ile etkileşimli olarak simetrik anahtar üretilecektir. Gerekli olan güvenlik altyapısı sağlandıktan sonra Servis Sağlayıcılar kullanıcılara SIM kart üzerinden katma değerli servisler sunabileceklerdir. İlgili gereksinim ve kısıtlar dikkate alınarak geliştirilmiş olan SIMSec protokolünün esasları Şekil 4.1'de verilmiştir.



Şekil 4.1: SIMSec Protokolü.

4.1.1. SIMSec Protokolünün Detayları

Şekil 4.1'de verilen SIMSec protokolünden de görüldüğü üzere:

- Servis Sağlayıcı 10 karakter uzunluğundaki V adı verilen rastgele bir değişkeni (1)'de üreterek (2) de SIM karta gönderir. V değişkeni ve kullanılan diğer değişkenler ile ilgili detaylar aşağıda değişkenlerin ve fonksiyonların anlatıldığı bölümde verilmiştir.
- (3)'de SIM kart Diffie-Hellman işleminde kullanılacak olan a sayısını rastgele oluşturur.
- a değerini oluşturduktan sonra (4)'de g^a (mod p) değerini ve ayrıca ID_{SIM}, V, ve g^a değerlerinin hash'ini hesaplar ve bunları (5)'de Servis Sağlayıcıya gönderir.

- Servis Sağlayıcı, V değerini SIM karta gönderdikten sonra, önceden belirlenen süre içerisinde, SIM karttan veri paketi kendine ulaşırsa işlemlere devam eder. Aksi halde protokolü sonlandırır.
- Eğer bu süre içerisinde paket kendisine ulaşırsa (6)'da Diffie-Hellman işleminde kullanılacak olan b sayısını rastgele oluşturur.
- (7)'de ise SIM kartın (4)'de hesapladığı X değerinin aynısı olan X' değerini hesaplar. Eğer iki sonuç birbirine eşit ise (V değerini sadece Servis Sağlayıcı ile SIM kart bildiği için) Servis Sağlayıcı SIM kartın kimliğini doğrular.
- Servis Sağlayıcı (8)'de g^b (mod p) ve $(g^a)^b$ (mod p) değerlerini hesaplar.
- Servis Sağlayıcı (9)'da SIM karta göndermek üzere V, g^a (mod p), g^b (mod p), ve $(g^a)^b$ (mod p) değerlerinin hash'ini hesaplar ve bu değeri (12)'de g^b (mod p) değeri ile birlikte SIM karta gönderir.
- Bu değerleri göndermeden önce (11)'de anahtar olarak belirleyeceği K değerini hesaplamak için (10)'da ID_{SIM}, V, ve $(g^a)^b$ (mod p) değerlerinin hash'ini hesaplar ve (11)'de bu değeri anahtar olarak seçer.
- SIM kart, (12)'de Servis Sağlayıcının gönderdiği paketi aldıktan sonra Servis Sağlayıcı'nın hesapladığı $(g^a)^b$ (mod p) ile aynı sonucu verecek olan $(g^b)^a$ (mod p) değerini (13)'de hesaplar.
- (14)'de Servis Sağlayıcının (9)'da hesapladığı Y değerinin aynısı olan Y' değerini hesaplar. Y' değerini hesaplarken bulunan tek fark hash fonksiyonuna $(g^b)^a$ (mod p) değerinin yerine $(g^a)^b$ (mod p) değerinin verilmesidir. Bu iki değer aynı olduğu için sonuçları da hash fonksiyonunun sonuçları da aynı olacaktır.
- SIM kart (15)'de K değerini ID_{SIM}, V, ve $(g^a)^b$ (mod p) değerlerinin hash'ini hesaplayarak elde eder ve (16)'da bu değeri anahtar olarak seçer.

4.1.2. SIMSec Protokolünde Kullanılan Değerler

Verilen protokol tanımında kullanılan değerlerin detayları şu şekildedir.

4.1.2.1. p Değeri

p değeri herkese açık bir değerdir. Diffie-Hellman üs alma işlemlerinde mod değeri olarak kullanılmaktadır. Örnek kullanımı (4.1)'de verilmiştir.

$$g^a \text{ (mod p)} \tag{4.1}$$

Güvenli bir anahtar değişimi için en az 1024 bit uzunluğunda bir asal sayı seçilmelidir. [21] standardına bağlı kalınarak, p değeri için EK 1'de verilen sayının seçilmesi güvenli görülmüştür.

4.1.2.2. g Değeri

g değeri herkese açık bir değerdir. Diffie-Hellman üs alma işlemlerinde taban değeri olarak kullanılmaktadır.

Güvenlik standardına [21] bağlı kalınarak "00001101" aşağıdaki sayının seçilmesi uygun görülmüştür.

4.1.2.3. a Değeri

Sadece SIM Kartın bildiği, protokolde SIM Kart tarafından rastgele oluşturulan bir değerdir. Üs alma işleminde üst değeri olarak kullanılmaktadır. Uzunluğu [16] standardına bağlı kalınarak 384 bit olarak belirlenmiştir.

4.1.2.4. b Değeri

Sadece Servis Sağlayıcının bildiği, protokolde Servis Sağlayıcı tarafından rastgele oluşturulan bir değerdir. Üs alma işleminde üst değeri olarak kullanılmaktadır. Uzunluğu [16] standardına bağlı kalınarak 384 bit olarak belirlenmiştir.

4.1.2.5. V Değeri

V değerinin uzunluğu 10 karakterlik alfa nümerik bir veridir. Her karakter için 64 seçenek (alfa nümerik değeler ve ek işaretler) kullanılmıştır. Bu değer Servis Sağlayıcı tarafından protokolün başlangıcında rastgele üretilecek olup, tek kullanımlıktır ve Kaba Güç (Brute force) saldırısına karşı savunmayı güçlendirmek üzere kısa bir kullanım süresi bulunmaktadır (Örnek: 5 dakika).

SIMSec protokolünde, SIM kart ile Servis Sağlayıcı arasındaki (5) ve (12) numaralı iletişimler SMS kanalı üzerinden, (2) numaralı V değerinin paylaşıldığı iletişim ise alternatif bir kanal üzerinden gerçekleştirilmektedir. Bu değişim için https veya benzeri güvenli bir Internet iletişim protokolü kullanılmalıdır. Güvenli anahtar oluşumu sağlamak için Servis Sağlayıcının ve kullanıcının karşılıklı kimlik doğrulama gerçekleştireceği İnternet şubesi gibi bir kanal idealdir. Alternatif olarak Servis Sağlayıcı bu değeri kullanıcıya bir şubesinde kimlik doğrulaması yaparak fiziksel olarak

da teslim edebilir. Kullanıcı elde edeceği bu veriyi SIM karta yüklenmiş olan Servis Sağlayıcının SIM kart uygulamasına elle girmesi gerekmektedir.

V değeri böylece, Servis Sağlayıcının ürettiği ve daha sonra da SIM karta kullanıcıya iletmek yoluyla aktardığı bir değer olmaktadır. SIM Kart ile Servis Sağlayıcının bütün iletişimleri Mobil Ağ Operatörü üzerindeki SMS kanalında olacağından dolayı, V değeri de alternatif bir kanal üzerinden karşılıklı kimlik doğrulaması yoluyla paylaşıldığı için, SMS kanalına saldırı yapan bir kişinin elde edemeyeceği bir veri olarak tasarlanmıştır.

4.1.2.6. ID_{SIM} Değeri

ID_{SIM}, SIM Karta özel olan IMSI ve ICCID verileri kullanılarak oluşturulan 96 bit uzunluğunda bir değerdir. IMSI ve ICCID verilerinin detayları tezin 2. bölümünde anlatılmıştır. Servis Sağlayıcı SIM Karta ilişkin IMSI ve ICCID verilerini MNO'dan temin ederek hesaplar. SIM kart ise IMSI ve ICCID verilerini verileri kendi dosya sisteminden okuyarak hesaplar.

4.1.2.7. H_1 Fonksiyonu

Hash fonksiyondur. Hash sonucunun 128 en önemsiz bitleri (LSB: Least Significant Bit) kullanılmaktadır. H_1 fonksiyonuna şu girdiler belirtilen sırada verilmelidir:

1. 32 bit uzunluğunda fonksiyon numarası (H_1 için 1)
2. 32 bit uzunluğunda olan ve aşağıda içeriği tanımlanan temel girdinin bit olarak uzunluğunu içeren bilgi
3. ID_{SIM}, V, ve g^a (mod p) değerlerinden oluşan temel girdi: $ID_{SIM} \| V \| g^a \pmod p$

4.1.2.8. H_2 Fonksiyonu

Hash fonksiyondur. Hash sonucunun LSB 128 biti kullanılmaktadır. H_2 fonksiyonuna şu girdiler belirtilen sırada verilmelidir:

1. 32 bit uzunluğunda fonksiyon numarası (H_2 için 2)
2. 32 bit uzunluğunda olan ve aşağıda içeriği tanımlanan temel girdinin bit olarak uzunluğunu içeren bilgi

3. ID_{SIM}, V, g^a (mod p), g^b (mod p), ve $(g^b)^a$ (mod p) değerlerinden oluşan temel girdi:
   ID_{SIM} || V || g^a (mod p) || g^b (mod p) || $(g^a)^b$ (mod p)

4.1.2.9. H_3 Fonksiyonu

168 bit çıktı üreten bir hash fonksiyondur. H_3 fonksiyonuna şu girdiler belirtilen sırada verilmelidir:

1. 32 bit uzunluğunda fonksiyon numarası (H_3 için 3)
2. 32 bit uzunluğunda olan ve aşağıda içeriği tanımlanan temel girdinin bit olarak uzunluğunu içeren bilgi
3. ID_{SIM}, V, ve $(g^b)^a$ (mod p) değerlerinden oluşan temel girdi: ID_{SIM} || V || $(g^a)^b$ (mod p)

4.2. SIMSEC PROTOKOLÜNÜN GÜVENLİK ANALİZİ

SIMSec protokolüne saldırıda bulunabilecek üç farklı saldırgan tipi bulunmaktadır:

(a) Sadece herkese açık değerleri bilen bir saldırgan,
(b) MNO'da çalışan bir saldırgan, ve
(c) Başka bir Servis Sağlayıcıda çalışan bir saldırgan.

Verilen liste içinde (a) tipi bir saldırgan, SMS kanalına sadece herkese açık olan g ve p değerlerini bilerek anahtar değişim protokolü üzerine saldırı gerçekleştirebilir.

Diğer taraftan; MNO, Servis Sağlayıcı tarafından kurumsal olarak güvenilir bir kuruluş kabul edilmektedir. Fakat MNO'da çalışan personelin bireysel olarak saldırgan olma riski vardır ve MNO çalışanlarına bireysel olarak güvenilemez. Bu nedenle (b) tipi bir saldırgan ID_{SIM} verisine ulaşabilir, SMS kanalını dinleyebilir ve hatta SMS kanalı üzerine saldırı yaparak paketleri değiştirmeye çalışabilir.

Başka bir Servis Sağlayıcı daha önce MNO ile anlaşma gerçekleştirmiş ve SIM kart ile anahtar oluşturma protokolünü çalıştırmış olabilir. Bu durumda, bu Servis Sağlayıcı ID_{SIM} verisini bilmekte ve dolayısıyla (c) tipi bir saldırgan ID_{SIM} değerini ve herkese açık olan g ve p değerlerini bilerek anahtar değişim protokolü üzerine saldırı gerçekleştirebilir.

Bu bölümün devamında SIM kart ve Servis Sağlayıcı arasında güvenli veri transferi gerçekleştirilebilmesi için SIMSec protokolünün ve protokol sonucu oluşturulacak anahtarın yerine getirmesi gereken güvenlik şartlarının değerlendirilmesi yapılacaktır.

4.2.1. Anahtar Güvenliği

SIMSec protokolünde, MNO dahil herhangi bir aktörün SIM kart ile Servis Sağlayıcı arasında gerçekleşen iletişimi dinleyememesi ve dolayısıyla MNO dahil herhangi bir aktörün anahtar oluşturma protokolünde oluşturulan anahtarı elde edememesi gerekmektedir.

SIMSec temelinde Diffie-Hellman algoritması kullanılmıştır. Bu algoritmada yer alan $(g^b)^a$ (mod n) ve $(g^a)^b$ (mod n) sayılarının a ya da b sayılarını bilmeyenler tarafından hesaplanması mümkün değildir. Aynı anahtarı oluşturabilmek için saldırganın bu iki sayıdan birini elde edebilmesi gerekmektedir, dolayısıyla SIMSec anahtar oluşturma protokolünde SIM kart ve Servis Sağlayıcı arasındaki anahtar gizliliği sağlanmaktadır.

4.2.2. Anahtar Uzunluğu

SIMSec protokolünde oluşturulan anahtarın, verileri güvenli bir şekilde şifrelemede kullanılabilmesi için yapılan çalışmalara göre 168 bit uzunluğunda olması gerekmektedir. 168 bit anahtarlı 3DES algoritmasının 2030 yılına kadar güvenli olduğu NIST tarafından varsayılmaktadır [22]. SIMSec kullanılarak oluşturulacak 168 bit uzunluğunda bir anahtarın 3DES algoritmasında kullanılması durumunda Servis Sağlayıcı ile SIM kart arasında güvenli iletişim sağlanmış olacaktır.

4.2.3. Servis Sağlayıcı tarafından SIM Kart Kimliğinin Doğrulanması

SIMSec protokolünde Servis Sağlayıcı SIM kartın kimlik denetimini V değerini kullanarak gerçekleştirmektedir. Servis Sağlayıcı V değerini SIM karta karşılıklı kimlik doğrulama gerçekleştirdiği alternatif bir kanaldan gönderdiği ve V değerini sadece SIM kart ve Servis Sağlayıcı bildiği için, Servis Sağlayıcı SIM kartın kimliğini V değerini kullanarak doğrulayabilmektedir.

İkincil bir kimlik denetimi ise ID_{SIM} değeri üzerinden gerçekleştirilmektedir. SIM kartın Servis Sağlayıcıya (5) adımında gönderdiği hash değeri de ID_{SIM} değerini içermekte ve Servis Sağlayıcı bu değeri (8) adımında kontrol ederek ikincil bir doğrulama daha gerçekleştirmektedir.

4.2.4. SIM Kart Tarafından Servis Sağlayıcının Kimliğinin Doğrulanması

SIMSec anahtar oluşturma protokolünde SIM kart Servis Sağlayıcının kimlik denetimini V değerini kullanarak gerçekleştirmektedir. Servis Sağlayıcı V değerini SIM karta karşılıklı kimlik doğrulama gerçekleştirdiği alternatif bir kanaldan gönderdiği ve V değerini sadece SIM kart ve Servis Sağlayıcı bildiği için, Servis Sağlayıcı SIM kartın kimliğini V değerini kullanarak doğrulayabilmektedir.

4.2.5. Veri Bütünlüğü

SIMSec protokolünde veri bütünlüğünü sağlamak için karşı tarafa (5) ve (12) adımlarında gönderilen hash değerleri alıcı tarafından da (8) ve (15) adımlarında hesaplanmaktadır. Gelen hash değerinin hesaplanan hash değerinden farklı olduğu saptandığında ise veri üzerinde bir değişiklik yapıldığı anlaşılmakta ve protokol sonlandırılmaktadır.

4.2.6. Aradaki Adam Saldırısına Karşı Koruma

SIMSec protokolü, Aradaki Adam Saldırısına karşı korunaklı olarak geliştirilmiştir. Protokolde V değeri Servis Sağlayıcı tarafından tek kullanımlık olarak üretilmektedir ve belirli bir süre için geçerlidir. Bu değer Servis Sağlayıcı ve SIM kartın karşılıklı kimlik doğrulama gerçekleştirdiği alternatif bir kanaldan paylaşılmaktadır.

Şekil 4.1'deki SIMSec protokolünden de görüleceği üzere, SIM kartın ve Servis Sağlayıcının (5) ve (12) adımlarında birbirlerine gönderdikleri hash fonksiyonlarının içerisinde V değeri kullanılmıştır. Yetkisiz bir aktör Aradaki Adam Saldırısı gerçekleştirmek istediğinde, V değerini tahmin etmesi gerekmektedir. Toplamda ise 2^{60} adet olası V değeri bulunmaktadır (10 karakter uzunluğunda ve her karakter için 64 olası değer). V değeri tek kullanımlık olduğu ve (8) ve (15) adımlarında SIM kart ve Servis Sağlayıcı eşit hash sonuçlarına ulaşamadıkları takdirde protokolü sonlandıracakları ve protokolden baştan başlatılacağı için, V değeri protokolü olası bir Aradaki Adam Saldırısından korumaktadır.

4.2.7. Tekrar Gönderme Saldırısına Karşı Koruma

SIMSec protokolünde Tekrar Gönderme Saldırısını engellemek için Nonce kullanılmaktadır. V değeri tek kullanımlık olduğu için aynı zamanda Nonce değeri olarak kullanılmaktadır. V değeri tek kullanımlık olduğu için paketi tekrar göndermek

suretiyle gerçekleştirilecek olan Tekrar Gönderme Saldırısı alıcı tarafından paket reddedileceğinden, başarılı olamayacaktır. Paketi geciktirmek sureti ile yapılacak olan Tekrar Gönderme Saldırısı ise V değeri sadece belirli bir kısa periyot için geçerli olduğu için, bu periyot sona erdikten sonra gönderilen paketler reddedilecektir.

4.3. SIMSEC AKILLI KART YAZILIMI

Bu bölümde, geliştirilmiş olan SIMSec protokolüne uygun olarak SIM kart üzerinde çalışacak olan yazılımın geliştirilme konusu anlatılacaktır. SIM kartın depolama ve işlem kapasitelerinin düşük olmalarından dolayı, bu süreç de oldukça yoğun ve kapsamlı bir çalışmayı gerekli kılmıştır. Anahtar oluşturma sürecinin, daha önce belirtilmiş olan gereksinimleri karşılayacak şekilde gerçekleştirilmesi için de bu hassas çalışma tez çalışmasının önemli bir aşaması olmuştur.

SIMSecApp, SIMSec protokolünün SIM kart üzerinde gerçekleştirilmesini sağlayacak olan akıllı kart uygulamasıdır. SIMSecSP ise, SIMSec protokolünde Servis Sağlayıcının sunucusunda yapılması gerektiği belirtilen işlemlerin gerçekleştirilmesi sağlanacaktır. Tez kapsamında SIMSecApp akıllı kart uygulaması geliştirilmiştir. Uygulamaya ait kodlar ise bu bölümde anlatılmıştır.

4.3.1. Hash İşlemi

Hash alma SIMSec protokolünün önemli bir bölümünü oluşturmaktadır. Hash alma fonksiyonu protokolün birden fazla yerinde bulunduğu ve dolayısıyla uygulamanın da bir çok yerinde kullanılacağı için hash alma işlemi için ayrı bir fonksiyon tanımlanmış olup, hash alınacağı zaman bu fonksiyon çağırılmaktadır. Hash işleminin sonucu `hashBuffer` adlı `byte` dizisine kayıt edilmektedir. SIMSecApp içinde hash alma fonksiyonu ile ilgili kısım Şekil 4.2'de gösterilmiştir.

```
private MessageDigest md =
   MessageDigest.getInstance(MessageDigest.ALG_SHA, true);
public void calculateHash(byte[] source, short offset,
   short dataLength) {
/* Clear the hashBuffer byte array*/
Util.arrayFillNonAtomic(hashBuffer, (short)0,
   (short) hashBuffer.length, (byte) 0);
md.doFinal(source, offset, dataLength, hashBuffer, (short) 0);
}
```

Şekil 4.2: SIMSecApp Uygulamasında Hash Alma.

4.3.2. Debug İşlemleri

Geliştirilen yazılımda, yazılan kodların başarılı bir şekilde çalışıp çalışmadığını görebilmek için yazılım parçacıklarının arasına debug mesajları eklenmektedir. Bu şekilde yazılımın hangi parçalarının çalıştığını ya da yeni geliştirilen bir kod parçasının çalışıp çalışmadığı görülebilmektedir. Şekil 4.3'de kullanılan bir debug kodu görüntülenmektedir.

```
private static byte[] DEBUG_MSG_1 = new byte[] { 'H', 'A', 'S', 'H',
' ', 'B', 'A', 'S', 'A', 'R', 'I', 'L', 'I' };
ProactiveHandler proHdlr = ProactiveHandler.getTheHandler();
proHdlr.initDisplayText((byte) 0, DCS_8_BIT_DATA, DEBUG_MSG_1,
   (short) 0, (short) DEBUG_MSG_1.length);
proHdlr.send();
```

Şekil 4.3: SIMSecApp Uygulamasında Debug İşlemi.

4.3.3. Sonuçların Görüntülenmesi

Hash alma, şifreleme, birleştirme vb. gibi işlemlerin sonuçlarını ekranda görüntülenmesi istendiğinde sonuç `byte` dizisi ekrana bastırıldığında, sonuç ekranda düzgün bir şekilde görüntülenememektedir. Bunun nedeni `byte` dizisinin içerisindeki her `byte` değerinin Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi (ASCII: American Standard Code for Information Interchange) tablosunda otomatik olarak karşılığının aranıp onun ekranda görüntülenmeye çalışılmasıdır. Bu nedenden dolayı bir `byte` dizisinin (örnek olarak kontrol amaçlı hash işleminin sonucu) ekranda görüntülenebilmesi için sonuç dizisindeki her `byte` değerinin ASCII olarak karşılığı yine `byte` olarak kodlanmalı ve bu şekilde ekrana basılmalıdır ki bu karakterlerin ASCII karşılığı gösterildiğinde karakterler ekranda görüntülenebilsin. Aşağıda verilen

iki metot bir `byte` dizisini ekranda görüntüleyebilmek için bu `byte` dizisinin ASCII karşılığına çevirerek yeni bir `byte` dizisine kayıt etmektedir. Geliştirilen uygulamada uygulanan kod parçası Şekil 4.4'de verilmiştir.

```
public static short hexArray2AscArray( byte[] in,
   short inOffset, byte[] out, short outOffset, short inLen)
{
  short retVal = (short)(outOffset + (short)(inLen*2));
  outOffset = (short)(retVal - 1);
  while(inLen > 0)
  {
    short tempInOffset = (short)(inOffset + inLen - 1);
    out[outOffset--] =
       Hex2Asc_byte((byte)(in[tempInOffset]&0x0F));
    out[outOffset--] =
      Hex2Asc_byte((byte)(in[tempInOffset]>>4));
    inLen--;
  }
  return retVal;
}
public static byte Hex2Asc_byte(byte b)
{
  b = (byte)(b&0x0F);
  if ( b < (byte)0x0A )
    return (byte)(b+0x30);
  else
    return (byte)(b+0x37);
}
```

Şekil 4.4: SIMSecApp Uygulamasında İşlem Sonuçlarını Ekranda Görüntüleme.

4.3.4. ICCID ve IMSI Okuma

SIM Kart üzerinde gerçekleştirilen işlemlerden bir tanesi de SIM kart üzerindeki IMSI ve ICCID verilerinin uygulama tarafından okunmasını sağlamaktır. Uygulamanın bu verilere erişmesi için SIMSecApp uygulaması SIM karta yüklenirken GSM'e özel "Access Domain" yetkisinin "00" değerine ayarlanarak uygulamanın IMSI ve ICCID verilerine ulaşılmasına yetki verilmesi gerekmektedir.

Aşağıda verilen kodda SIM kart üzerinden ICCID verisi okunmakta ve bu verinin 7 LSB `byte` değeri saklanmaktadır. Çünkü her SIM karta özel olan ICCID verisi aslında son 7 `byte` içerisinde bulunmaktadır. ICCID verisini okumak için kullanılan kod parçası Şekil 4.5'de verilmiştir.

```
//ICCID Okuma
private SIMView gsmFile;
gsmFile.select(SIMView.FID_MF);
gsmFile.select(SIMView.FID_EF_ICCID);
// ICCID değerinin LSB 7 byte değeri
gsmFile.readBinary((short)3, IDSim ,(short) 0, (short)7);
```

Şekil 4.5: SIMSecApp Uygulmasında ICCID Okuma.

Şekil 4.6'da verilen kodda SIM kart üzerinden IMSI verisi okunmakta ve bu verinin 5 LSB `byte` değeri saklanmaktadır. Çünkü her SIM karta özel olan IMSI verisi aslında son 5 `byte` içerisinde bulunmaktadır.

```
//IMSI Okuma
private SIMView gsmFile;
gsmFile.select(SIMView.FID_MF);
gsmFile.select(SIMView.FID_DF_GSM);
gsmFile.select(SIMView.FID_EF_IMSI);
// IMSI değerinin LSB 5 byte değeri
gsmFile.readBinary((short) 4, IDSim, (short) 7, (short) 5);
```

Şekil 4.6: SIMSecApp Uygulamasında IMSI Okuma.

4.3.5. Diffie-Hellman değerlerinin hesaplanması

Akıllı kartta Diffie-Hellman'a ait g^a (mod p) hesaplanmalı ve bilinen g^b (mod p) değeri kullanılarak $(g^b)^a$ (mod p) değeri de hesaplanmalıdır. g değerinin 8 bit, a ve b değerlerinin 384 bit ve p değerinin 1024 uzunluğunda olduğundan, belirtilen işlemler oldukça yüksek hesaplama gücü gerektiren işlemlerdir. Ayrıca Java Card programlama dilinin sınırlı özelliklerinden dolayı hesaplamalarda sadece `byte` ve `short` veri tiplerinin kullanılması gerektiği de düşünüldüğünde, bahsedilen hesaplamaların yapılabilmesi için etkin bir algoritma kullanılması halinde bile uygulanabilmesinin mümkün olmadığı anlaşılmaktadır. Bu nedenle akıllı kartlarda üs alma işlemini matematiksel hesaplama yapmadan gerçekleştirecek bir yöntem gerekmektedir. Akıllı

kartlarda yüksek hesaplama gerektiren matematiksel işlemler ancak kart üretiminde yerleştirilmiş devreler aracılığıyla mümkün olduğundan dolayı, üs alma işleminin makul bir süre içerisinde üretilebilmesi için, bu devrelerin kullanılması gerekmektedir. Bu devreleri kullanan kriptografik API'lerin içerisinde bulunan RSA işleminin bu işlem için uygun olduğu saptanmıştır. RSA'in şifreleme fonksiyonunun bir anlamda modüler üs alma operasyonu olduğu, dolayısıyla da Diffie-Hellman üs alma işleminin benzeri olduğu görülerek bu API'nin kullanımını mümkün kılacak olan çalışma gerçekleştirilmiştir.

RSA şifreleme işleminde; A kullanıcısının açık anahtarlarına n ve e; gizli anahtarına ise d adı verilmektedir. B kullanıcısı m adında bir veriyi A kullanıcının okuyabileceği şekilde şifrelemek istediğinde uyguladığı işlem (4.2) de verilmiştir.

$$\text{Şifrelenmiş Mesaj} = m^e \pmod n \tag{4.2}$$

Diffie-Hellman işleminde ise hesaplamak istediğimiz verinin $g^a \pmod p$ olduğu düşünüldüğünde;

- RSA şifrelemesindeki mesaj içeriğinin (m değeri) yerine Diffie-Hellman'da g değeri,
- RSA şifrelemesindeki A kullanıcısının açık anahtarı (e değeri) yerine Diffie-Hellman'da a değeri,
- RSA şifrelemesindeki A kullanıcısının diğer bir açık anahtarı (n değeri) yerine Diffie-Hellman'da p değeri

kullanıldığında RSA şifrelemesi sonucu ortaya çıkan değer $g^a \pmod p$ değeri olmaktadır. RSA Şifreleme işlemi ile Diffie-Hellman hesaplama işlemlerinde kullanılan değerlerin birbiriyle eşleştirilmesi aynı zamanda Tablo 4.1'de verilmiştir.

Tablo 4.1: RSA ile Diffie-Hellman Değerlerinin Eşleştirilmesi

	Taban	**Üs**	**Mod**	**Sonuç**
RSA Şifreleme	M	e	N	$m^e \pmod n$
1. Diffie-Hellman	G	a	P	$g^a \pmod p$
2. Diffie-Hellman	$g^b \pmod p$	a	P	$(g^b)^a \pmod p$

Dolayısıyla tez kapsamında geliştirilen yazılımda Diffie-Hellman değerini hesaplamak için akıllı kartın kriptografik API'sinde bulunan RSA ile ilgili fonksiyonların kullanılması uygun ve verimli bir yol olarak bulunmuştur. SIMSecApp'da g^a (mod p) ve $(g^b)^a$ (mod p) değerleri hesaplanırken RSA fonksiyonları kullanılmaktadır. g^a (mod p) değerini hesaplamak için kullanılan RSA şifreleme kodu Şekil 4.7'de verilmiştir.

```
Cipher cipher =
   Cipher.getInstance( Cipher.ALG_RSA_ISO14888,false );
RSAPublicKey publicKey = ( RSAPublicKey )
   KeyBuilder.buildKey(KeyBuilder.TYPE_RSA_PUBLIC,
   KeyBuilder.LENGTH_RSA_1024, false );
publicKey.setExponent(a, (short) 0,(short) a.length );
publicKey.setModulus(modp, (short) 0,(short) modp.length );
cipher.init( publicKey, Cipher.MODE_ENCRYPT );
cipher.doFinal( g, (short) 0, (short) g.length, ga, (short) 0 );
```

Şekil 4.7: SIMSec Protokolünde RSA şifrelemesi.

SIMSecApp geliştirildikten sonra veriler kullanılarak test edilmiştir. SIMSec uygulamasının bilgisayar üzerinde geliştirildikten sonra SIM kart'a yüklenerek gerçek ortamda çalıştırılması sonucunda ortaya çıkan veriler EK 1'de sunulmuştur.

4.4. CASPER ARACI İLE GÜVENLİK ANALİZİ

Casper güvenlik aracı [23, 24], protokollerin güvenlik analizleri için geliştirilmiş bir araçtır. Casper, kodlanması basit bir kod alarak, bu kodu arka planda otomatik olarak derlemekte ve kodu verilen protokolün güvenlik analizini gerçekleştirmektedir. Casper günümüzde literatürde iletişim ve güvenlik protokollerin kontrol edilmesinde oldukça çok kullanılmaktadır [25].

Casper/FDR aracı ile geliştirilen kod Tablo 4.2'de gösterildiği gibi sekiz ana bölümde toplanmaktadır.

4.4.1. Casper Notasyonu

Casper aracında kod geliştirme literatürde benzerine çokça rastlanabilen ve araştırmacıların aşina olduğu bir sözdizimi kullanmaktadır.

Örnek olarak P aktörünün N aktörüne na adlı nonce değerini N kullanıcısının açık anahtarı ile şifrelemesine ait ifade (4.3)'deki gibi yazılmaktadır:

$$P \rightarrow N : \{na\}_{PK(N)} \tag{4.3}$$

Bu ifade Casper aracında ise (4.4'deki gibi yazılmaktadır:

$$P \rightarrow N : \{na\}\{PK\ (N)\} \tag{4.4}$$

Tablo 4.2: Casper/FDR Aracı için Geliştirilmesi Gereken Kod Bölümleri

Bölüm	**Açıklama**
Serbest Değişkenler (Free Variables)	Protokoldeki değişkenlerin ve fonksiyonların tiplerinin tanımlandığı bölümdür.
Süreçler (Processes)	Her aktörün CSP süreci olarak tanımlandığı bölümdür
Tanımlama (Specification)	Protokolde kontrol edilmesi gereken güvenlik şartlarının belirlendiği bölümdür.
Asıl Değişkenler (Actual Variables)	Sistemdeki asıl değişkenlerin tanımlandığı bölümdür.
Fonksiyonlar (Functions)	Protokolde kullanılan fonksiyonların tanımlandığı bölümdür.
Sistem (System)	Sistemde yer alan aktörlerin parametreleriyle beraber tanımlandığı bölümdür.
Saldırgan Bilgisi (Intruder Information)	Saldırgan bildiklerinin ve yeteneklerinin tanımlandığı bölümdür.
Protokol Tanımı (Protocol Description)	Protokoldeki veri iletişiminin gösterildiği bölümdür.
Kanallar (Channels)	Protokolde aktörler arasında kullanılan kanalın tipinin belirtilebileceği yerdir. ki veri iletişiminin gösterildiği bölümdür.
Eşitlikler (Equivalances)	Protokolde farklı fonksiyon sonuçlarının birbirine eşit olma durumlarının belirtildiği bölümdür.

4.4.2. Casper ile Bir Protokol Örneği

Bu bölümde basit bir protokolün nasıl Casper aracında tanımlandığı gösterilecektir.

Serbest Değişkenler

Örnek bir Serbest Değişkenler bölümü Şekil 4.8'de verildiği gibi tanımlanabilir.

```
#Free variables
A, B, M : Agents
na : Nonce
PK : Agent -> PublicKey
SK : Agent -> SecretKey
InverseKeys = (PK, SK)
```

Şekil 4.8: Casper Aracında Serbest Değişkenler Bölümü.

Verilen koddan da görüleceği üzere, bölümde A, B, ve M adlı üç aktör ve `na` adlı bir nonce tanımlanmıştır. PK ve SK adlı değişkenler ise aktörlerin açık ve gizli anahtarları olarak tanımlanmıştır. Son satırda ise PK ve SK anahtarlarının birbirlerinin karşılığı olan anahtarlar olduğu belirtilmiştir.

4.4.3. Süreçler

Örnek bir `Processes` bölümü Şekil 4.9'da verildiği gibi tanımlanabilir.

```
#Processes
INITIATOR(A, na) knows PK, SK(A)
RESPONDER(B) knows PK, SK(B)
```

Şekil 4.9: Casper Aracında Süreçler Bölümü.

Sistemdeki her aktör bir CSP süreci olarak bu bölümde tanımlanmaktadır ve A ve B aktörlerinin detayları bu bölümde verilmiştir. Satırların başında büyük harflerle yazılan kelimeler CSP sürecinin adı, ilk parantez içerisindeki veriler aktörlerin protokolün başında hangi verilere sahip olduğu ve `knows` kelimesinden sonraki bölüm ise hangi fonksiyonları bildiğidir.

Dolayısıyla birinci satırda, `INITIATOR` adlı süreç `A` aktörünü ve `na` verisini bilmekte, bütün aktörlerin açık anahtarlarını ve B aktörünün gizli anahtarını hesaplayabilmektedir.

4.4.4. Tanımlama

Örnek bir `Specification` bölümü Şekil 4.10'da verildiği gibi tanımlanabilir.

```
#Specification
Secret(A, na, [B])
Agreement(B, A, [y])
```

Şekil 4.10: Casper Aracında Tanımlama Bölümü.

Tanımlama bölümünde verilen "Secret" ile başlayan satırda `na` adlı değişkenin sadece A ve opsiyonel olarak B tarafından bilinmesi gerekmektedir" ifade edilmektedir. Dolayısıyla saldırgan bu değişkeni protokol sırasında elde edememelidir.

"Agreement" ile başlayan ikinci satırda ise "B aktörü A aktörü ile protokolü uyguladığı zaman, y adlı değişken üzerinde anlaşması gerekmektedir" ifade edilmektedir.

4.4.5. Asıl Değişkenler

Örnek bir `Actual variables` bölümü Şekil 4.11'de verildiği gibi tanımlanabilir.

```
#Actual variables
Alice, Bob, Mallory : Agent
Na : Nonce
```

Şekil 4.11: Casper Aracında Tanımlama Bölümü.

Bu bölümdeki bir çok değişken Serbest Değişkenler bölümündekilerle aynı değişkenler olmakla beraber ek olarak saldırgan olan Mallory tanımlanmıştır.

4.4.6. Fonksiyonlar

Örnek bir `Functions` bölümü Şekil 4.12'de verildiği gibi tanımlanabilir.

```
#Functions
symbolic PK, SK
```

Şekil 4.12: Casper Aracında Fonksiyonlar Bölümü.

Bu bölümde fonksiyonlar sembolik olarak gösterilmiştir. Bu sayede Casper aracı fonksiyonların için bir hesaplama yapmadan kendi değer üretecektir.

Sistem

Örnek bir `System` bölümü Şekil 4.13'de verildiği gibi tanımlanabilir.

```
#System
INITIATOR(A, na)
RESPONDER(B)
```

Şekil 4.13: Casper Aracında Sistem Bölümü.

Bu bölümde sistemde bulunması gereken aktörler ilk sahip olduğu değerlerle birlikte belirtilmektedir.

4.4.7. Saldırgan Bilgisi

Örnek bir `Intruder Information` bölümü Şekil 4.14'de verildiği gibi tanımlanabilir.

```
#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Alice, Bob, Mallory, PK, SK(Mallory)}
```

Şekil 4.14: Casper Aracında Saldırgan Bilgisi Bölümü.

Bu bölümde saldırganın kim olduğu tanımlanmış ve saldırganın sahip olduğu bilgiler belirtilmiştir. Casper bu bilgileri kullanarak protokole saldırı yapılıp yapılamayacağını kontrol edecektir. Verilen koddan da görüldüğü üzere saldırgan Mallory, saldırganın bildiği bilgiler de aktörlerin bilgileri, bütün aktörlerin açık anahtarları ve kendi gizli anahtarıdır.

4.4.7. Protokol Tanımı

Örnek bir `Protocol description` bölümü Şekil 4.15'de verildiği gibi tanımlanabilir.

```
#Protocol description
0. -> A : B
1. A -> B : {na, A}{PK(B)}
2. B -> A : {na}{PK(A)}
```

Şekil 4.15: Casper Aracında Protokol Tanımı Bölümü.

Tanımlanan protokol 0. adımda ortamdan N aktörüne gelen bir mesajla başlamaktadır ve bu mesajda M kullanıcısının kimliği bildirilmektedir. Daha sonra 1. adımda A aktür na değişkenini ve kendi kimliğini B aktörünün açık anahtarıyla göndermektedir. B aktörü ise kendi gizli anahtarıyla veriyi açtıktan sonra, 2. adımda veriyi A aktörünün açık anahtarıyla şifreleyerek A kullanıcısına göndermektedir.

4.5. SIMSEC PROTOKOLÜNÜN GÜVENLİK ANALİZİ

SIMSec protokolünün güvenlik analizinin gerçekleştirilmesi için Casper aracı kullanılmıştır. Analiz işlemleri ve sonuçları bu bölümde verilmiştir.

Casper aracında, SIMSec protokolüne ait güvenlik analizlerinden anahtar güvenliği, anahtar bütünlüğü, SIM kartın Servis Sağlayıcı tarafından kimliğinin denetlemesi, ve Servis Sağlayıcının SIM kartın tarafından kimliğinin denetlemesi test edilmiştir.

Protokolde kullanılan anahtarın güvenliği Casper aracında `Specification` bölümü altında Şekil 4.16'da verildiği gibi kodlanmıştır.

```
StrongSecret(SIMcard, key, [SP])
StrongSecret(SP, key, [SIMcard])
```

Şekil 4.16: Casper Aracı İçin Tanımlanan Anahtar Güvenliği.

Verilen tanımlama, oluşturulan anahtarın SIM kart ile Servis Sağlayıcı arasında gizli kalması gerektiğini belirtmektedir. `StrongSecret` tanımlamasıyla Casper, protokoldeki saldırganın anahtarı kırıp kıramayacağını bulmaya çalışmaktadır.

Protokoldeki Servis Sağlayıcı tarafından SIM Kartın kimliğinin doğrulanması süreci, Casper aracında `Specification` bölümü altında Şekil 4.17'de verildiği gibi kodlanmıştır.

```
Agreement(SP, SIMcard, [key])
```

Şekil 4.17: Casper Aracı İçin Tanımlanan SIM Kartın Kimliğinin Denetlemesi.

Verilen tanımlama, SIM kartın Servis Sağlayıcının kimliğini doğrulaması gerektiği ve aynı zamanda bu doğrulamadan sonra iki aktörün de `key` adlı anahtar üzerinde anlaşmaları gerektiği şartını vermektedir.

Protokoldeki SIM Kart tarafından Servis Sağlayıcının kimliğinin doğrulanması süreci, Casper aracında `Specification` bölümü altında Şekil 4.18'de verildiği gibi kodlanmıştır.

```
Agreement(SP, SIMcard, [key])
```

Şekil 4.18: Casper Aracı İçin Tanımlanan Servis Sağlayıcının Kimliğinin Denetlemesi.

Verilen tanımlama, protokolde Servis Sağlayıcının SIM kartın kimliğini doğrulaması gerektiği ve aynı zamanda bu doğrulamadan sonra iki aktörün de `key` adlı anahtar üzerinde anlaşmaları gerektiği şartını vermektedir.

Casper aracı için geliştirilen kodun tamamı ve kodların hangi amaç için kullanıldığı Şekil 4.19'de verilmiştir.

```
-- SIMSec Protocol

-- Bu bölümde protokolde kullanılan değişkenler, fonksiyonlar, ve
-- aktörler tanımlanmıştır.
(1)   #Free variables
(2)   datatype Field = G | Exp(Field,Num) unwinding 2
(3)   SIMcard, SP  : Agent
(4)   a, b : Num
(5)   InverseKeys = (key,key), (Exp, Exp), (G,G)
(6)   key, ga, gb, cardMsg, spMsg, dhKey, h1Result, h1Result',
         h2Result, h2Result' : Field
(7)   v : SessionKey
(8)   H1 : Agent x SessionKey x Field->Field
(9)   H2 : Agent x SessionKey x Field x Field x Field -> Field
(10)  H3 : Agent x SessionKey x Field -> Field

-- Bu bölümde SIM kartın ve Servis Sağlayıcının protokol
-- başlangıcında bildiği değerler belirtilmiştir. SIM kart Servis a
-- değerini, V değerini, ve hash metotlarını bilmektedir. Servis
-- Sağlayıcı ise b değerini, V değerini, ve hash metotlarını
-- bilmektedir.
(11)  #Processes
(12)  INITIATOR( SIMcard,SP,a,v ) knows H1, H2, H3
(13)  RESPONDER( SP,SIMcard,b,v ) knows H1, H2, H3

-- Bu bölümde protokol kodlanmıştır. 0. adımda SIM karta Servis
-- Sağlayıcının bilgileri gelerk protokol başlamaktadır.
(14)  #Protocol description
(15)  0.   -> SIMcard : SP
(16)  [SIMcard != SP]

-- 1. adımda SIM kart, X değerini ve g^a değerini hesaplamakta ve
-- bunları Servis Sağlayıcıya göndermektedir.
(17)  < cardMsg := Exp(G,a); h1Result:= H1(SIMcard,v,cardMsg) >
(18)  1. SIMcard -> SP : cardMsg % ga, h1Result
(19)  [SIMcard != SP]

-- 2.adımda ise Servis Sağlayıcı da g^b değerini, X' değerini, Y
-- değerini ve anahtarı hesaplamaktadır. X ve X' değeri birbiriyle
-- eşit olduğu durumda protokole devam ederek  g^b değerini ve Y
-- değerini SIM karta göndermektedir.
(20)  < dhKey := Exp(ga, b); spMsg := Exp(G,b);
         h1Result':= H1(SIMcard, v,ga);
         h2Result := H2(SIMcard,v,ga, Exp(G,b), dhKey);
         key := H3(SIMcard,v, dhKey) >
(21)  2. SP -> SIMcard : spMsg % gb, h2Result
(22)  [h1Result==h1Result']
```

Şekil 4.19: Casper Aracı için Geliştirilen SIMSec Protokol Kodu.

```
-- Son adımda ise SIM kart Y' değerini ve anahtarı hesaplamaktadır.
-- Y ve Y' değeri birbiriyle eşit olduğu durumda protokole devam
-- ederek  anahtarı oluşturduğunu Servis Sağlayıcıya bildirmektedir.

(23)  < dhKey := Exp(gb, a);
        h2Result':= H2(SIMcard, v, Exp(G,a), gb, dhKey);
        key := H3(SIMcard, v, dhKey) >
(24)  3.  SIMcard -> SP   : {key}{key}
(25)  [h2Result==h2Result']

-- Bu bölümde (g^a)^b ve (g^b)^a değerlerinin birbirine eşit olduğu
-- belirtilmektedir.
(26)  #Equivalences
(27)  forall a,b : Num . \
        Exp(Exp(G,b), a) = Exp(Exp(G,a), b)

-- Bu bölümde yukarıda anlatıldığı gibi protokolün güvenlik
-- analizleri gerçekleştirilmiştir.
(28)  #Specification
(29)  Secret( SIMcard, v, [SP]) Secret(SP, v, [SIMcard] )
(30)  Agreement( SP, SIMcard, [key] )
(31)  Agreement( SIMcard, SP, [key] )
(32)  StrongSecret( SIMcard, key, [SP] )
(33)  StrongSecret( SP, key, [SIMcard] )

-- Bu bölümde H1, H2, ve H3 fonksiyonları tanımlanmıştır
(34)  #Functions
(35)  symbolic H1, H2, H3

-- Bu bölümde Casper aracının saldırı sisteminde kullanabilmesi için
-- değerler tanımlanmıştır.
(36)  #Actual variables
(37)  Alice, Bob, Mallory : Agent
(38)  W, A, B : Num
(39)  V, V2 : SessionKey

-- Bu bölümde Casper aracının saldırı sisteminde kullanabilmesi için
-- aktör eşleştirmeleri yapılmıştır. Ayrıca aktörlerin #Actual
-- Variables bölümünde tanımlanan değişkenlerden hangilerini bildiği
-- de tanımlanmıştır.
(40)  #System
(41)  INITIATOR( Alice, Bob, A, V )
(42)  RESPONDER( Bob, Alice, B, V )

-- Bu bölümde saldırgan tanımlanmış ve saldırganın bilebeleceği
-- değerler belirtilmiştir.
#Intruder Information
(43)  Intruder = Mallory

IntruderKnowledge = { Alice, Bob, Mallory, W, V2, H1,
   H2, H3 }
```

Şekil 4.19 (devam): Casper Aracı için Geliştirilen SIMSec Protokol Kodu.

Casper, Şekil 4.19'da da verilen kod üzerinde çalıştırıldığında SIMSec protokolünü analiz ederek Şekil 4.20'de yer alan analiz sonuçlarını üretmiştir.

```
Checking assertion SECRET_M::SECRET_SPEC
[T= SECRET_M::SYSTEM_S
No attack found

Checking assertion SECRET_M::SEQ_SECRET_SPEC
[T= SECRET_M::SYSTEM_S_SEQ
No attack found

Checking assertion
AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_key
[T= AUTH1_M::SYSTEM_1
No attack found

Checking assertion
AUTH2_M::AuthenticateINITIATORToRESPONDERAgreement_key
[T= AUTH2_M::SYSTEM_2
No attack found

Done
```

Şekil 4.20: Casper Aracının Çıktısı.

Çıktılardan da görüleceği üzere, test sonucunda herhangi saldırı başarılı olamamış, netice olarak SIM kart ve Servis Sağlayıcı arasında anahtar değişiminin güvenli bir şekilde gerçekleştirildiği anlaşılmıştır.

4.6. BÖLÜM SONUCU

Tezin bu bölümünde ilk olarak SIMSec protokolü detaylı olarak anlatılmış, ardından da protokolün güvenliğini değerlendirmek ve test etmek için gerçekleştirilen güvenlik çalışmalarına ve geliştirilen SIMSecApp yazılımına ilişkin bilgiler sunulmuştur. Bir sonraki bölümde ise gerçekleştirilen tez kapsamında yapılan çalışmalar özetlenecek ve literatürdeki diğer çalışmalar değerlendirilecektir.

5. TARTIŞMA VE SONUÇ

Tezin bir önceki bölümünde tez çalışmasında gerçekleştirilen çalışmalar detaylı olarak verilmiştir. Bu bölümde ise tez kapsamında yapılan çalışmalar değerlendirilmiştir.

Tez çalışmasının amacı, üretim esnasında gizli anahtar yüklenmemiş olan düşük depolama ve işlem kapasitesi olan 64K SIM kartlar ile Servis Sağlayıcılar arasında uçtan uca güvenli iletişimi mümkün kılacak altyapıyı oluşturmaktır. Bu işlem için ise SIM kart ile Servis Sağlayıcının işbirliği içinde anahtar oluşturmasına ilişkin bir protokol geliştirilmesi hedeflenmiştir. Geliştirilecek olan protokolün, düşük bellek kapasitesi ile işlem gücü olan 64K SIM kartlar üzerinde çalışacak şekilde programlanabilir olması gerekmektedir. Tez çalışması sonrasında SIMSec protokolüne bağlı kalarak geliştirilecek olan SIM kart programı ve Servis Sağlayıcı için Sunucu programı MNO'nun sağladığı servisleri kullanarak güvenli bir şekilde anahtar oluşturacaklardır. Oluşturulacak olan anahtar, 3DES ya da benzeri güvenli bir simetrik model ile şifrelemede kullanılarak SIM Kart ile Servis Sağlayıcı arasında uçtan uca güvenli iletişim altyapısı oluşturulmuş olacaktır.

Literatürde iki bilgisayar arasında anahtar paylaşımına olanak sağlayan modeller mevcuttur [6, 14-17, 26-31]. Fakat bu protokoller sadece yüksek hesaplama kabiliyeti olan bilgisayara uygun olup, SIM kartlara uygulanamaz. Bir anahtar değişim protokolünün problemimizin çözümünde kullanılabilmesi için, SIM kartların düşük bellek kapasiteleri ile düşük işlem güçlerinin yeterli olacağı bir programa dönüştürülebilir olması gerekmektedir.

Literatürde yapılan çalışmalar SIM kartlara uygunluk açısından ele alındığında ise, mevcut olan bir kaç modelin [18, 19, 20, 32] sadece üretim esnasında üzerlerine kişisel anahtar yüklenmiş olan ve aynı zamanda bellek kapasitesi ile işlem gücü yüksek olan 512K ve 256K SIM kartlarda çalışabilir oldukları görülmektedir.

SIMSec protokolüne ait performans ölçüm detayları Tablo 5.1'de verilmiştir. Verilen sonuçlardan görüldüğü üzere protokolün bir saniyeden daha az bir sürede tamamlandığı

görülmektedir. Tablodaki veriler, programın kart üzerinde çalışma süresini içermekte, buna karşın SIM kart işletim sistemi tarafından mesajların protokole göre birleştirilmesi vb. işlemleri ve verilerin EEPROM ile RAM arasında ve tam tersi yönde kopyalanması süreçlerini kapsamamaktadır. Veriler değerlendirildiğinde uygulamada en uzun süre alan işlemin Diffie-Hellman üs alma işlemi (SIMSec protokolündeki 4. ve 13. adımlardaki üs alma işlemleri - Şekil 4.1) olduğu görülmekle beraber toplamda 250 ms süre tutmuştur. Ayrıca hash alma işlemleri ortalama 50 ms'de gerçekleştirilmiştir.

Tablo 5.1: SIMSec Protokolünün Performansı.

İşlem	**SIMSec protokolündeki (Şekil 4.1) adım**	**SIMSec Protokolüne ait Ortalama Süre**	**[32] Protokolüne ait Ortalama Süre**
Rastgele Sayı Oluşturma	3	~30 ms	~30 ms
Diffie-Hellman üs alma işlemi (g^{ab})	4 ve 13	~250 ms	~300 ms
H1 fonksiyonunun hesaplanması	4	~50 ms	-
H2 fonksiyonunun hesaplanması	14	~50 ms	-
H3 fonksiyonunun hesaplanması	15	~50 ms	-
Simetrik Şifreleme		~10 ms	~10 ms
Diğer işlemler	14 ve 15	~200 ms	~490 ms
Toplam	**-**	**~640 ms**	**~830 ms**

Daha önce de belirtildiği gibi, literatürde mevcut çalışmalar değerlendirildiğinde, SIMSec protokolü ile aynı işlevselliği sağlayan bir protokol bulunmamaktadır. Bununla beraber, en yakın benzerliği bulunan protokol [32] ile karşılaştırıldığında, SIMSec protokolünün 200 ms daha hızlı çalıştığı görülmektedir.

SIMSec protokolü güvenlik şartları açısından değerlendirildiğinde de ihtiyaç duyulan bütün güvenlik şartlarını sağladığı görülmektedir. SIMSec protokolü ile aynı işlevselliği

sağlayan bir protokol bulunmadığından dolayı güvenlik şartları literatürdeki bir başka çalışma ile karşılaştırılamamıştır. SIMSec protokolünün sağladığı güvenlik şartları bir önceki bölümde anlatıldığı gibi şunlardır:

- SIM Kartın Kimliğinin Saptanması (Identification of SIM card)
- Servis Sağlayıcının Kimliğinin Saptanması (Identification of Service Provider)
- SIM Kartın Kimliğinin Doğrulanması (Authentication of SIM card)
- Servis Sağlayıcının Kimliğinin Doğrulanması (Authentication of Service Provider)
- Protokoldeki Veri Bütünlüğünün Korunması (Data Integrity)
- Protokolde Aradaki Adam Saldırısına Karşı Koruma (Protection to Man in the Middle Attack)
- Protokolde Tekrar Gönderme Saldırısına Karşı Koruma (Protection to Replay Attack)

Tez çalışması kapsamında özetle şu çalışmalar gerçekleştirilmiştir. Literatür araştırması gerçekleştirildikten ve mevcut hiç bir çalışmanın problemimizin çözümü için yeterli olmadığı görüldükten sonra, Servis Sağlayıcı ile SIM Kart arasında anahtar üretim ve paylaşım protokolünün geliştirilmesine karar verilerek SIM kart ile ilgili bilgiler ve standartlar, Java Card programlama dili ile ilgili bilgiler, konu ile ilgili olan güvenlik algoritmaları ve anahtar değişimi protokolleri incelenmiştir. Ardından geliştirilecek protokolde sağlanması gereken güvenlik şartları Bölüm 3'de verildiği üzerine belirlenmiştir. Bu bilgileri takiben SIMSec protokolü geliştirilmiştir. Protokolün güvenlik değerlendirmelerinin yapılmasının ardından protokolün güvenlik kriterlerine uygunluğu Casper/FDR güvenlik analiz aracı ile incelenmiş ve SIMSec protokolünün evrensel güvenlik kriterlerine uygun olduğu anlaşılmıştır. Son olarak da protokolün SIM kart uygulaması geliştirilmiş ve testleri gerçekleştirilerek çalışma tamamlanmıştır.

KAYNAKLAR

[1]. Lu, C., dos Santos, A. L., Pimentel, F. R., 2002, Implementation of fast RSA key generation on smart cards, *2002 ACM symposium on Applied computing*, 11-14 Mart 2002 Madrid, SPAIN, 214-220.

[2]. Hansmann, U., Nicklous, M. S., Seliger, F., Schack, T., Schneider, A., 2002, *Smart card application development using Java*, Springer, ISBN: 978-3-642-55969-3.

[3]. Smart Card Basics, 2015, *Smart Card Standards*, http://www.smartcardbasics.com/smart-card-standards.html, [Ziyaret Tarihi: 7 Haziran 2015].

[4]. Bichsel, P., Camenisch, J., Groß, T., Shoup, V., 2009, Anonymous credentials on a standard java card, *16th ACM conference on Computer and communications security*, 9-13 Kasım 2009 Chicago, IL, USA, 600-610

[5]. 3GPP, 1999, *3GPP TS 11.11 - Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface*, http://www.3gpp.org/dynareport/1111.htm, [Ziyaret Tarihi: 7 Haziran 2015].

[6]. Komninos, N., Dimitriou, T., 2006, Adaptive authentication and key agreement mechanism for future cellular systems, *15th IST Mobile & Wireless Communications Summit*, 4 - 8 Haziran 2006 Mykonos, GREECE, 1-4.

[7]. Oracle, 2015, *Java Card Technology*, http://www.oracle.com/technetwork/java/, [Ziyaret Tarihi: 7 Haziran 2015].

[8]. Witteman, M., 2003, Java card security, *Information Security Bulletin*, 8, 291-298.

[9]. 3GPP, 2007, *3GPP TS 11.14 - Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface*, http://www.3gpp.org/dynareport/1114.htm, [Ziyaret Tarihi: 7 Haziran 2015].

[10]. ISO/IEC, 2005, *ISO/IEC 7816-12:2005 Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures*, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40604, [Ziyaret Tarihi: 7 Haziran 2015].

[11]. ISO/IEC, 2013, *ISO/IEC 7816-4:2013 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54550, [Ziyaret Tarihi: 7 Haziran 2015].

[12]. *Elektronik İmza Kanunu Kanun No. 5070, Kabul Tarihi: 15.01.2004*, https://www.tbmm.gov.tr/kanunlar/k5070.html, [Ziyaret Tarihi: 7 Haziran 2015].

[13]. Freier, A., Karlton, P., Kocher, P., 2011, *The secure sockets layer (SSL) protocol version 3.0*, http://tools.ietf.org/html/rfc6101, [Ziyaret Tarihi: 7 Haziran 2015].

[14]. Diffie, W., Hellman, M. E., 1976), New directions in cryptography, *IEEE Transactions on Information Theory*, 22(6), 644-654.

[15]. Zeltsan, Z., Patel, S., Faynberg, I., Brusilovsky, A., 2010, *Password-Authenticated Key (PAK) Diffie-Hellman Exchange*, https://tools.ietf.org/html/rfc5683, [Ziyaret Tarihi: 7 Haziran 2015].

[16]. ITU-T, 2007, *X:1035: Password-authenticated key exchange (PAK) protocol, ITU-T Recommendation X.1035*, https://www.itu.int/rec/T-REC-X.1035-200702-I/en, [Ziyaret Tarihi: 7 Haziran 2015].

[17]. Cakulev, V., Sundaram, G., 2012, *IBAKE: Identity-Based Authenticated Key Exchange*, https://tools.ietf.org/html/rfc6539, [Ziyaret Tarihi: 7 Haziran 2015].

[18]. Rongyu, H., Guolei, Z., Chaowen, C., Hui, X., Xi, Q., & Zheng, Q., 2009, A PK-SIM card based end-to-end security framework for SMS. *Computer Standards & Interfaces*, 31(4), 629-641.

[19]. Li, Y., Chen, M., Nie, J., 2011, Mobile commerce security model construction based on sms, *7th International Conference on Wireless Communications, Networking and Mobile Computing*, 23-25 Eylül 2011 Wuhan, CHINA, 1-3.

[20]. Badra, M., Urien, P., 2004, Toward SSL integration in SIM smartcards, *Wireless Communications and Networking Conference*, 21-25 Mart 2004 Atlanta, USA, 889-893

[21]. 3GPP2, 2007, *Wireless Local Area Network (WLAN) Interworking - Access to Internet*,http://www.3gpp2.org/public_html/specs/X.S0028-100-0_v1.0_070405.pdf, [Ziyaret Tarihi: 7 Haziran 2015].

[22]. Polk, W. T., Dodson, D. F., Burr, W. E., Ferraiolo, H., Cooper, D., 2010, *NIST Special Publication 800-78-3 Cryptographic algorithms and key sizes for personal identity verification,* http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf, [Ziyaret Tarihi: 7 Haziran 2015].

[23]. Lowe, G., 2015, *Casper: A Compiler for the Analysis of Security Protocols*, http://www.cs.ox.ac.uk/gavin.lowe/Security/Casper/, [Ziyaret Tarihi: 7 Haziran 2015].

[24]. Lowe, G., Broadfoot, P., Dilloway, C., Hui, M. L., 2009, *Casper: A compiler for the analysis of security protocols-user manual and tutorial Version 1.12*, http://www.cs.ox.ac.uk/gavin.lowe/Security/Casper/manual.pdf, [Ziyaret Tarihi: 7 Haziran 2015].

[25]. Tegeler, F., 2009, *Security Analysis of IKEv2 Session Resumption*, Technical Report No: IFI-TB-2009-01, ISSN: 1611-1044.

[26]. Boyko, V., MacKenzie, P., Patel, S., 2000, *Provably secure password-authenticated key exchange using Diffie-Hellman*, Advances in Cryptology - Eurocrypt, In: Preneel, B. (ed.), Springer, ISBN: 978-3-540-67517-4, 156-171.

[27]. Lu, R., Cao, Z., 2007, Simple three-party key exchange protocol, *Computers & Security*, 26(1), 94-97.

[28]. Xie, M., Wang, L., 2012, One-round identity-based key exchange with Perfect Forward Security, *Information Processing Letters*, 112(14), 587-591.

[29]. Abdalla, M., Pointcheval, D., 2005, *Simple password-based encrypted key exchange protocols*, Topics in cryptology–CT-RSA, In: Menezes, A. (ed.), Springer, ISBN: 978-3-540-30574-3, 191-208.

[30]. Shamir, A., 1985, *Identity-based cryptosystems and signature schemes*, Advances in cryptology, In: Blakley, G. R., Chaum, D. (eds.), Springer, ISBN: 978-3-540-39568-3, 47-53.

[31]. Wu, T. Y., Tseng, Y. M., 2009, An ID-based mutual authentication and key exchange protocol for low-power mobile devices, *The Computer Journal*, 53 (7), 1062-1070.

[32]. Markantonakis, K., Mayes, K., 2005, *A Secure Channel protocol for multi-application smart cards based on public key cryptography*, Communications and Multimedia Security Volume 175, In: Chadwick, D., Preneel, B. (eds.), Springer, ISBN 978-0-387-24486-0, 79-95.

EKLER

EK 1. SIMSec Protokolünde Kullanılan Parametreler

İsmi	Uzunluğu	Değeri
g	2 byte	00 0C
p	128 byte	FF FF FF FF FF FF FF FF C9 0F DA A2 21 68 C2 34 C4 C6 62 8B 80 DC 1C D1 29 02 4E 08 8A 67 CC 74 02 0B BE A6 3B 13 9B 22 51 4A 08 79 8E 34 04 DD EF 95 19 B3 CD 3A 43 1B 30 2B 0A 6D F2 5F 14 37 4F E1 35 6D 6D 51 C2 45 E4 85 B5 76 62 5E 7E C6 F4 4C 42 E9 A6 37 ED 6B 0B FF 5C B6 F4 06 B7 ED EE 38 6B FB 5A 89 9F A5 AE 9F 24 11 7C 4B 1F E6 49 28 66 51 EC E6 53 81 FF FF FF FF FF FF FF FF
a	48 byte	0E A9 BB 7A BD 7D 65 40 2B 08 C6 DF C9 4B 09 6A 29 3B C2 42 88 23 44 AF 08 84 21 FE 0B A4 CA F9 7D BC FC 82 4C FF 42 A4 B8 D2 DA CC EE C5 34 ED
g^a (mod p)	128 byte	6A 25 C1 9C 08 85 5F 5A 4A 1F 3A 33 CA 3A 9E E9 53 97 F9 72 02 90 F5 6A DB 88 D9 4F 1A 88 19 F4 85 7C 44 1E 36 0F 59 5F 4C 68 1F 9C 5F 73 7E E1 73 FB F9 B4 C9 DF 47 AC 01 0F 7E AD F4 A1 71 6C 31 85 08 C7 D3 9C 0E 6A 9C 7D 99 C7 97 99 E8 61 9F 50 71 8A 80 00 BB AE 4A D5 70 0F 58 3B E2 DD CA BE 82 6E 29 E1 D5 2A 3E EE 33 EA D5 91 0A E0 56 77 AB 99 30 C9 2B 8B 17 B2 09 DB 51 4B 87 3C
g^b (mod p)	128 byte	6E BC F7 97 D9 96 AD 4E 10 9B 3E 20 6D E8 35 FF F5 06 04 81 B0 C8 D8 9F CA EB 0F 8E BB F8 54 D5 E0 D7 4E 54 B1 F9 6E 31 4A 1A 6C 1B 85 A1 EF 71 1C 0A E6 72 B4 2A A9 7C 0E E0 F4 6E 84 98 DD 39 0C 96 74 7F 00 CB BE 3F E1 E1 F0 B0 98 21 82 3E 98 52 DF 5C 47 C2 9C 20 AE 1E 21 19 29 AC 45 42 E2 DD 23 56 48 6F D4 33 7C E6 81 65 36 17 B8 F0 E7 69 F3 F9 15 D8 F3 F3 FA 57 82 94 62 25 54 0C
g^{ab} (mod p)	128 byte	27 C8 CE CE B4 16 95 23 EA 4D B3 EA B0 37 93 96 D0 B9 EE 5E 9D C2 FB 69 EB A2 F0 9E 26 77 ED 8D EA 30 47 9C E4 63 6B 00 22 80 9E E8 56 E3 6A 12 13 84 88 9F F2 36 38 05 EC B2 49 A1 5F 62 78 7C 70 B9 71 32 F5 C6 AD 66 8A 92 20 A7 D8 0E 35 85 C2 55 3F 47 BE D7 BF 4D 81 44 61 FD 7B 0A F3 54 F2 A2 B9 38 BA 1B 67 EB 43 2F 5C 20 0C 42 E5 39 F6 51 17 4D 43 18 1F 4D 12 DE E0 61 2C C6 2C 07

İsmi	Uzunluğu	Değeri
g^{ba} (mod p)	128 byte	27 C8 CE CE B4 16 95 23 EA 4D B3 EA B0 37 93 96 D0 B9 EE 5E 9D C2 FB 69 EB A2 F0 9E 26 77 ED 8D EA 30 47 9C E4 63 6B 00 22 80 9E E8 56 E3 6A 12 13 84 88 9F F2 36 38 05 EC B2 49 A1 5F 62 78 7C 70 B9 71 32 F5 C6 AD 66 8A 92 20 A7 D8 0E 35 85 C2 55 3F 47 BE D7 BF 4D 81 44 61 FD 7B 0A F3 54 F2 A2 B9 38 BA 1B 67 EB 43 2F 5C 20 0C 42 E5 39 F6 51 17 4D 43 18 1F 4D 12 DE E0 61 2C C6 2C 07
V	6 byte	02 0B BE A6 3B 13
ICCID	LSB 7 byte	31 50 92 00 00 70 F8
IMSI	LSB 5 byte	15 32 62 23 71
ID_{SIM}	12 byte	31 50 92 00 00 70 F8 15 32 62 23 71
H_1 Girdisi	154 byte	00 00 00 01 00 00 00 92 31 50 92 00 00 70 F8 15 32 62 23 71 02 0B BE A6 3B 13 6A 25 C1 9C 08 85 5F 5A 4A 1F 3A 33 CA 3A 9E E9 53 97 F9 72 02 90 F5 6A DB 88 D9 4F 1A 88 19 F4 85 7C 44 1E 36 0F 59 5F 4C 68 1F 9C 5F 73 7E E1 73 FB F9 B4 C9 DF 47 AC 01 0F 7E AD F4 A1 71 6C 31 85 08 C7 D3 9C 0E 6A 9C 7D 99 C7 97 99 E8 61 9F 50 71 8A 80 00 BB AE 4A D5 70 0F 58 3B E2 DD CA BE 82 6E 29 E1 D5 2A 3E EE 33 EA D5 91 0A E0 56 77 AB 99 30 C9 2B 8B 17 B2 09 DB 51 4B 87 3C
X (H_1 sonucu)	16 byte	55 A1 06 68 18 F2 19 ED 81 FB AF 4A E0 43 0A A8
X || g^{a} (mod p)	144 byte	55 A1 06 68 18 F2 19 ED 81 FB AF 4A E0 43 0A A8 6A 25 C1 9C 08 85 5F 5A 4A 1F 3A 33 CA 3A 9E E9 53 97 F9 72 02 90 F5 6A DB 88 D9 4F 1A 88 19 F4 85 7C 44 1E 36 0F 59 5F 4C 68 1F 9C 5F 73 7E E1 73 FB F9 B4 C9 DF 47 AC 01 0F 7E AD F4 A1 71 6C 31 85 08 C7 D3 9C 0E 6A 9C 7D 99 C7 97 99 E8 61 9F 50 71 8A 80 00 BB AE 4A D5 70 0F 58 3B E2 DD CA BE 82 6E 29 E1 D5 2A 3E EE 33 EA D5 91 0A E0 56 77 AB 99 30 C9 2B 8B 17 B2 09 DB 51 4B 87 3C

İsmi	Uzunluğu	Değeri
H_2 Girdisi	410 byte	00 00 00 02 00 00 01 92 31 50 92 00 00 70 F8 15 32 62 23 71 02 0B BE A6 3B 13 6A 25 C1 9C 08 85 5F 5A 4A 1F 3A 33 CA 3A 9E E9 53 97 F9 72 02 90 F5 6A DB 88 D9 4F 1A 88 19 F4 85 7C 44 1E 36 0F 59 5F 4C 68 1F 9C 5F 73 7E E1 73 FB F9 B4 C9 DF 47 AC 01 0F 7E AD F4 A1 71 6C 31 85 08 C7 D3 9C 0E 6A 9C 7D 99 C7 97 99 E8 61 9F 50 71 8A 80 00 BB AE 4A D5 70 0F 58 3B E2 DD CA BE 82 6E 29 E1 D5 2A 3E EE 33 EA D5 91 0A E0 56 77 AB 99 30 C9 2B 8B 17 B2 09 DB 51 4B 87 3C 6E BC F7 97 D9 96 AD 4E 10 9B 3E 20 6D E8 35 FF F5 06 04 81 B0 C8 D8 9F CA EB 0F 8E BB F8 54 D5 E0 D7 4E 54 B1 F9 6E 31 4A 1A 6C 1B 85 A1 EF 71 1C 0A E6 72 B4 2A A9 7C 0E E0 F4 6E 84 98 DD 39 0C 96 74 7F 00 CB BE 3F E1 E1 F0 B0 98 21 82 3E 98 52 DF 5C 47 C2 9C 20 AE 1E 21 19 29 AC 45 42 E2 DD 23 56 48 6F D4 33 7C E6 81 65 36 17 B8 F0 E7 69 F3 F9 15 D8 F3 F3 FA 57 82 94 62 25 54 0C 27 C8 CE CE B4 16 95 23 EA 4D B3 EA B0 37 93 96 D0 B9 EE 5E 9D C2 FB 69 EB A2 F0 9E 26 77 ED 8D EA 30 47 9C E4 63 6B 00 22 80 9E E8 56 E3 6A 12 13 84 88 9F F2 36 38 05 EC B2 49 A1 5F 62 78 7C 70 B9 71 32 F5 C6 AD 66 8A 92 20 A7 D8 0E 35 85 C2 55 3F 47 BE D7 BF 4D 81 44 61 FD 7B 0A F3 54 F2 A2 B9 38 BA 1B 67 EB 43 2F 5C 20 0C 42 E5 39 F6 51 17 4D 43 18 1F 4D 12 DE E0 61 2C C6 2C 07
Y (H_2 sonucu)	16 byte	DA 2F 0C 2F 1E 00 9F 3C FE CC AF B4 A8 9A 1C 61
H_3 Girdisi	154 byte	00 00 00 01 00 00 00 92 31 50 92 00 00 70 F8 15 32 62 23 71 02 0B BE A6 3B 13 27 C8 CE CE B4 16 95 23 EA 4D B3 EA B0 37 93 96 D0 B9 EE 5E 9D C2 FB 69 EB A2 F0 9E 26 77 ED 8D EA 30 47 9C E4 63 6B 00 22 80 9E E8 56 E3 6A 12 13 84 88 9F F2 36 38 05 EC B2 49 A1 5F 62 78 7C 70 B9 71 32 F5 C6 AD 66 8A 92 20 A7 D8 0E 35 85 C2 55 3F 47 BE D7 BF 4D 81 44 61 FD 7B 0A F3 54 F2 A2 B9 38 BA 1B 67 EB 43 2F 5C 20 0C 42 E5 39 F6 51 17 4D 43 18 1F 4D 12 DE E0 61 2C C6 2C 07
Z (H_3 sonucu)	21 byte	7D 9A 04 83 35 0F 89 AE 67 EF 24 D6 61 27 65 44 33 0A 1F 9F 02

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı	Kerem Ok
Uyruğu	TC
Doğum tarihi, Yeri	02.11.1984, İstanbul
Telefon	(533) 651 0823
E-mail	okkerem@gmail.com

Eğitim

Derece	**Kurum/Anabilim Dalı/Programı**	**Yılı**
Doktora	İ.Ü. Fen Bilimleri Enstitüsü / Enformatik Anabilim Dalı / Enformatik Doktora Programı	2015
Yüksek Lisans	Işık Üniversitesi Fen Bilimleri Enstitüsü / Enformasyon Teknolojileri Anabilim Dalı / Enformasyon Teknolojileri Yüksek Lisans Programı	2010
Lisans	Işık Üniversitesi Fen Edebiyat Fakültesi / Enformasyon Teknolojileri Bölümü	2006
Lise	Vefa Anadolu Lisesi	2002

Makaleler / Bildiriler

SCI ve SCI-E KAPSAMINDA DERGİ YAYINLARI

Ozdenizci B., Coskun V., **Ok K.**, NFC Internal: An Indoor Navigation System, Sensors, Mart 2015, 15(4), pp. 7571-7595, DOI: 10.3390/s150407571

Coskun V., Ozdenizci B., **Ok K.**, A Survey on Near Field Communication (NFC) Technology, Wireless Personal Communications, Ağustos 2013, 71 (3), pp. 2259-2294, DOI: 10.1007/s11277-012-0935-5

Ozdenizci B., **Ok K.**, Coskun V., NFC Loyal for Enhancing Loyalty Services through Near Field Communication, Wireless Personal Communications, Şubat 2013, 68 (4), pp. 1923-1942, DOI: 10.1007/s11277-012-0556-z

Ok K., Coskun V., Ozdenizci B., Aydin M. N., A Role-Based Service Level NFC Ecosystem Model, Wireless Personal Communications, Şubat 2013, 68 (3), pp. 811-841, DOI: 10.1007/s11277-011-0484-3

DİĞER DERGİ YAYINLARI

Ok K., Coskun V., Cevikbas R. C., Challenges and Risks for a Secure Communication between a Smartcard and a Service Provider through Cellular Network, *International Journal of Advances in Computer Networks and Its Security*, 2014, 4 (4), pp. 26-30.

Ozdenizci B., **Ok K.**, Alsadi M., Coskun V., Soylemezgiller F., Development of NFC Enabled Loyalty Application: Technical and Business Opportunities, *Academic Journal of Science (*AJS), 2014, 3 (1), pp. 141-149.

Ozdenizci B., Alsadi M., **Ok K.**Coskun V., Classification of NFC Applications in Diverse Service Domains, International Journal of Computer and Communication Engineering (IJCCE), Eylül 2013, 2 (5), pp.614-620, DOI: 10.7763/IJCCE.2013.V2.260

Ozdenizci B., **Ok K.**, Aydin M. N., Coskun V., Yakın Alan İletişimi Teknolojisi İncelemesi (A Survey on Near Field Communication), *BBM Dergisi*, 2011, 4 (1), pp. 85-92

KONFERANS BİLDİRİLERİ

Ok K., Impact of Customer Culture on Innovations, *2nd International OFEL Conference on Governance, Management and Entrepreneurship*, Dubrovnik, Hırvatistan, 4-5 Nisan, 2014, pp. 1026-1033.

Coskun V., Soylemezgiller F., Ozdenizci B., **Ok K.**, Development and Performance Analysis of Multifunctional City Smart Card System, *ICCSSE 2014: International Conference on Computer Science and Software Engineering*, Rio de Janeiro, Brezilya, 27-28 Şubat 2014, pp. 783-786.

Ok K., Alsadi M., Coskun V., Ozdenizci B., Soylemezgiller F., NFCLoyal: NFC Sadakat Sistemi, *Bilişim 2013 - 30. Ulusal Bilişim Kurultayı,* Ankara, Türkiye, 28-29 Kasım, 2013, pp. 221-224.

Coskun V., Ozdenizci B., **Ok K.**, Alsadi M., Soylemezgiller F., Design and Development of NFC Enabled Loyalty System , *6th International Conference of Advanced Computer Systems and Networks: Design and Application*, Lviv, Ukrayna, 16-18 Eylül 2013, pp. 42-45.

Ok K., Ayhan K, Unal S, Gursul F, A Colleger's Best Friend: MobilePhone or PC?, *4th International Future-Learning Conference on Innovations in Learning for the Future 2012: e-Learning*, Istanbul, Türkiye, 14-16 Kasım 2012, pp. 533-544.

Ok K., Gulsecen S., Kültürel Faktörlerin E-Öğrenme'deki Etkileri, 5th International Computer & Instructional Technologies Symposium, Fırat Üniversitesi, Elazığ, Türkiye, 22-24 Eylül 2011, pp. 541-545.

Ozdenizci B., Coskun V., **Ok K.**, Aydin M. N., Development of an Indoor Navigation System Using NFC Technology, *The Fourth International Conference on Information and Computing Science*, Phuket Island, Tayland 25-27 Nisan 2011, pp. 11-14.

Ozdenizci B., Coskun V., Aydin M. N., **Ok K.**, NFC Loyal: A Beneficial Model to Promote

Loyalty on Smart Cards of Mobile Devices, *2010 International Conference for Internet Technology and Secured Transactions (ICITST-2010)*, Londra, UK, 8-11 November 2010, pp. 134-139.

Ozdenizci B., Aydin M. N., Coskun V., **Ok K.**, Design Science in NFC Research, *2010 International Conference for Internet Technology and Secured Transactions (ICITST-2010)*, Londra, UK, 8-11 November 2010, pp. 158-163.

Ok K., Coskun V., Aydin M. N., Ozdenizci B., Current Benefits and Future Directions of NFC Services, *2010 International Conference on Education and Management Technology (ICEMT 2010)*, Kahire, Mısır, 2-4 November 2010.

Ok K., Aydin M. N., Coskun V., Ozdenizci B., Exploring Underlying Values of NFC Applications, *2010 International Conference on Management Technology and Applications (ICMTA 2010)*, Singapore, Singapore, 10-12 September 2010, pp. 283-287.

Ozdenizci B., Aydin M. N., Coskun V., **Ok K.**, NFC Research Framework: A Literature Review and Future Research Directions, *14th International Business Information Management Association Conference on Global Business Transformation through Innovation and Knowledge Management*, Istanbul, Türkiye, 23-24 June 2010, pp. 2672-2685.

Ok K., Coskun V., Aydin M. N., Usability of Mobile Voting with NFC Technology, *IASTED International Conference on Software Engineering*, Innsbruck, Avusturya, 16-18 February 2010, pp. 151-158.