ÖZET

MOBİL İMZA SERVİSİ SUNULMASINI SAĞLAYAN BİR SİSTEM

Bu buluş, bir mobil iletişim şebekesi operatörü tarafından mevcut yapıda operatör SMS (Short Message Service – Kısa Mesaj Servisi) altyapısı üzerinden sağlanan mobil imza servisinin, IP (İnternet Protokolü) altyapısı üzerinden sunulmasını sağlayan bir sistem ile ilgilidir. Buluş konusu sistem (1), mobil imza servis platformu (2), IP iletişim birimi (3), mobil cihaz (4), SIM kart (41) içermektedir.

İSTEMLER

1. Mobil imza servisi sunulmasını sağlayan;

- abonelerden (A) mobil imza isteme yetkisi olan ve mobil imza servisine entegre olan firma ya da kurum gibi kullanıcıların (K) abone (A) bilgileri ve imzalanacak açık metin özetini girişi ile birlikte söz konusu mobil imza isteğini göndermek için kullandıkları, tercihen bir istemci cihaz üzerinde görüntülenen bir ara yüz üzerinden erişilerek üzerinde işlemler gerçekleştirilebilen bir sunucu olan en az bir mobil imza servis platformu (2),
- kullanıcıların (K) mobil imza servis platformunda (2) oluşturdukları mobil imza isteklerinin bir veri protokolü üzerinden aktarıldığı ve bu mobil imza isteklerinin bir veri iletim ağı (N) üzerinden aboneye (A) iletilmesi için gereken işlemleri yerine getiren, benzer şekilde abonenin (A) söz konusu mobil imza isteğine istinaden girişini yaptığı mobil imza şifresi ile imzalanmış özet bilgisinin mobil imza servis platformuna (2) iletilmesi için gereken işlemleri yerine getiren en az bir IP iletişim birimi (3),
- abonenin (A) mobil imza isteklerini görüntülemesini ve bu isteklere istinaden mobil imza şifresi girişi yapabilmesini sağlayan, bir veri iletim ağı (N) üzerinden IP iletişim birimi (3) ile iletişim kurabilen en az bir mobil cihaz (4),
- mobil cihazın (4) mobil iletişim şebekesi operatörünün sağladığı hizmetlere erişebilmek için kullandığı, en temel halinde bir IP altyapısı üzerinden gelen komutları alabilecek ve bu komutlara uygun aksiyonları gerçekleştirebilecek şekilde yapılandırılmış en az bir SIM kart (41) **içeren** ve
- kullanıcıların (K) mobil imza servis platformunda (2) oluşturdukları mobil imza isteklerinin bir veri protokolü üzerinden aktarıldığı ve bu mobil imza isteklerinin bir veri iletim ağı (N) üzerinden aboneye (A) iletilmesi için gereken işlemleri yerine getiren, benzer şekilde

abonenin (A) söz konusu mobil imza isteğine istinaden girişini yaptığı mobil imza şifresi ile imzalanmış özet bilgisinin mobil imza servis platformuna (2) iletilmesi için gereken işlemleri yerine getiren en az bir IP iletişim birimi (3),

- mobil cihazın (4) mobil iletişim şebekesi operatörünün sağladığı hizmetlere erişebilmek için kullandığı, en temel halinde bir IP altyapısı üzerinden gelen komutları alabilecek ve bu komutlara uygun aksiyonları gerçekleştirebilecek şekilde yapılandırılmış en az bir SIM kart (41) ile **karakterize edilen** bir sistem (1).

2. En temel halinde bir servis geçidi, bir servis IP altyapısı ve bir istemci veri tabanı içeren IP iletişim birimi (3) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

3. Mobil iletişim şebekesi operatörüne ait bir donanım güvenlik modülü ile veri alışverişi yapabilecek şekilde yapılandırılmış IP iletişim birimi (3) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

4. Mobil imza servis platformu (2) ile mobil imza servisine ilişkin veri alışverişini mobil imza servis platformu (2) tarafından desteklenen bir iletim protokolü üzerinden gerçekleştiren IP iletişim birimi (3) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

5. Mobil cihaza (4) takılı olan SIM kart (41) ile SIM kart (41) tarafından desteklenen bir iletim protokolü üzerinden iletişim gerçekleştiren IP iletişim birimi (3) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

6. Mobil cihaza (4) takılı olan SIM kart (41) ile HTTP üzerinden iletişim gerçekleştiren IP iletişim birimi (3) ile karakterize edilen İstem 5'teki gibi bir sistem (1).

7. Abonelere (A) gönderilen mobil imza isteği sonucunda SIM kart (41) üzerinde yer alan uygulamanın tetiklenmesi ile mobil cihaz (4) ekranında gösterimi sağlanan mobil imza menüsünde abonenin (A) mobil imza şifresi girişi yapması sonrasında imzalanmış hale gelen açık metin özetini, mobil imza isteğinin abone (A) mobil cihazına (4) iletildiği oturum (session) üzerinden mobil imza servis platformuna (2) ileten IP iletişim birimi (3) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

8. Abonenin (A) bir mobil imza isteğine istinaden, imzalanacak açık metin özetini ve mobil imza şifresi giriş alanını içeren mobil imza menüsünü görüntüleyebilmesini ve bu menü üzerinden mobil imza şifresinin girişini yapabilmesini sağlayan görüntüleme ve girdi birimlerine sahip olan mobil cihaz (4) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

9. IP iletişim birimi (3) tarafından gönderilen ve veri iletim ağı (N) üzerinden aldığı komutlar sonrasında çalışması tetiklenecek bir uygulamayı üzerinde barındıran SIM kart (41) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

10. Abone (A) mobil cihazında (4) kullanımda olan SIM kartın (41) dinlemede olduğu IP ve porta herhangi bir iletim protokolü üzerinden söz konusu mobil imza isteğine ilişkin mobil imzalama işleminin yapılabilmesi için gereken menünün mobil cihazda (4) görüntülenmesi ve abonenin (A) girişini yapacağı mobil imza şifresinin alınması için gereken komutu gönderen IP iletişim birimi (3) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

11. Hangi IP adresi ve porta doğru gönderilen komutları alabileceği bilgisini periyodik aralıklarla IP iletişim birimine (3) bildiren SIM kart (41) ile karakterize edilen İstem 10'daki gibi bir sistem (1).

12. SIM kartın (41) hangi IP adresi ve porta doğru gönderilen komutları alabileceği bilgisini tutan IP iletişim birimi (3) ile karakterize edilen İstem 10'daki gibi bir sistem (1).

13. IP iletişim birimi (3) ile şifreli bir biçimde iletişim gerçekleştirmek için kullanılan gömülü (SIM kartın (41) üretimi sırasında SIM karta (41) gömülmüş olan) bir anahtar ve daha sonra güvenli bölgede üretilen bir mobil imza anahtar çiftine sahip olan SIM kart (41) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

14. SIM kart (41) ile gerçekleştirdiği iletişim için, güvenlik ve kimlik doğrulama mekanizmalarını barındıran IP iletişim birimi (3) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

15. Üzerinde yer alan uygulamanın IP iletişim birimi (3) ile kurulacak iletişimde ilk güvenlik kontrolünü geçebilmesi amacıyla kullanılan bir uygulama şifresini içeren SIM kart (41) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

16. Üretimi aşamasında, hafızasına Servis Geçidi modülünün IP/DNS (Domain Name Server – Alan Adı Sunucusu) erişim bilgileri eklenmiş olan SIM kart (41) ile karakterize edilen İstem 2'deki gibi bir sistem (1).

17. Yalnızca IP iletişim biriminden (3) gelecek olan istekleri kabul edecek şekilde bir IP filtrelemesi yapan SIM kart (41) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

18. SIM kartın (41) ilk kayıt aşamasını gerçekleştirmesi sonrasında SIM karta (41) erişim için gerekli olan IP adresi ve anahtar bilgilerini edinmiş olan IP iletişim birimi (3) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

TARİFNAME

MOBİL İMZA SERVİSİ SUNULMASINI SAĞLAYAN BİR SİSTEM

Teknik Alan

Bu buluş, bir mobil iletişim şebekesi operatörü tarafından mevcut yapıda operatör SMS (Short Message Service – Kısa Mesaj Servisi) altyapısı üzerinden sağlanan mobil imza servisinin, IP (İnternet Protokolü) altyapısı üzerinden sunulmasını sağlayan bir sistem ile ilgilidir.

Önceki Teknik

Mobil imza servisi, GSM (Global System for Mobile Communications – Mobil İletişim İçin Küresel Sistem) operatörlerinin sunduğu ve elektronik imza servisinin bir SIM kart kullanılarak mobil cihazlar üzerinden sağlanması temeline dayanan bir servistir. Elektronik imza ile ilgili şifreleme işlemleri SIM karta dışarıdan müdahale edilemeyen güvenli bir alanda saklanmaktadır. Söz konusu bu uygulama, mobil iletişim şebekesi üzerinden yalnızca SMS altyapısı üzerinden komut alarak işlem yapan bir uygulamadır. Bu SMS altyapısı üzerinden komut iletim süresi, SMS gönderim süresiyle doğru orantılıdır ve uzun bir süredir. Ayrıca, SMS altyapısı üzerinden gönderilen komutlar için komutların iletimindeki başarım oranı da düşüktür. Bu durumlar, mevcut SMS altyapıları üzerinden ilerletilen elektronik imza süreç ve çözümlerinin kullanışlılıklarının düşük olduğunu göstermektedir.

Günümüzde yapılan kimi çalışmalar ile birlikte İnternet üzerinden IP altyapısı ile komut alabilen, yani gelişmiş OTA (Over-the-Air – Havadan İletişim) özelliğine sahip olan SIM kartlar geliştirilmiştir. Bu geliştirilme ile SIM kart içerisindeki tanımların hızlı ve yüksek başarımla değiştirilebilmesi hedeflenmiştir. Mobil imza servisini mevcut SMS altyapısı üzerinden sunulması nedeniyle yaşanan sorun ve

verimsizlikler ile birlikte SIM kartlardaki bu gelişmeler düşünüldüğünde, mobil imza servisinin IP altyapısı üzerinden sunulmasını ve böylece mobil imza işlemlerinin daha hızlı, yüksek başarımlı ve veri kısıtlaması olmadan yapılabilmesini sağlayacak bir çözüme ihtiyaç olduğu anlaşılmaktadır.

Tekniğin bilinen durumunda yer alan KR20080017533 sayılı Kore patent dokümanında, kısa mesaj servisinin IP altyapısına sahip bir ağ üzerinden sağlanmasına olanak tanıyan bir sistem ve yöntemden bahsedilmektedir. Yöntem, şebeke içerisinde kısa mesajların, gönderim sonrasında BSC tarafından tespit edilmesi ve bu mesajların MSC'den geçmesi yerine SMSC'ye bir IP paketi içerisinde gönderilmesi esasına dayanmaktadır.

Tekniğin bilinen durumunda yer alan bir diğer doküman olan US8965419 sayılı Birleşik Devletler patent dokümanında, bir uzak sunucudan, bir kısa mesaj servisi sunucusuna bağlı olan bir mobil cihaza SMS gönderilebilmesini sağlayan bir buluştan bahsedilmektedir. Söz konusu buluşta uzak sunucu, SMS merkezine HTTP (Hyper-Text Transfer Protocol - Hiper-Metin Transfer Protokolü) üzerinden bağlantı gerçekleştirmektedir.

Buluşun Kısa Açıklaması

Bu buluşun amacı, bir mobil iletişim şebekesi operatörü tarafından mevcut yapıda operatör SMS altyapısı üzerinden sağlanan mobil imza servisinin, IP altyapısı üzerinden sunulmasını sağlayan bir sistem gerçekleştirmektir.

Buluşun Ayrıntılı Açıklaması

Bu buluşun amacına ulaşmak için gerçekleştirilen "Mobil İmza Servisi Sunulmasını Sağlayan Bir Sistem" ekli şekilde gösterilmiş olup, bu şekil;

Şekil-1 Buluş konusu sistemin şematik bir görünüşüdür.

Şekillerde yer alan parçalar tek tek numaralandırılmış olup, bu numaraların karşılıkları aşağıda verilmiştir.

1. Sistem
2. Mobil imza servis platformu
3. IP iletişim birimi
4. Mobil cihaz
   41. SIM kart

A. Abone

N. Veri iletim ağı

K. Kullanıcı

Buluş konusu, mobil imza servisi sunulmasını sağlayan bir sistem (1);

- abonelerden (A) mobil imza isteme yetkisi olan ve mobil imza servisine entegre olan firma ya da kurum gibi kullanıcıların (K) abone (A) bilgileri ve imzalanacak açık metin özetini girişi ile birlikte söz konusu mobil imza isteğini göndermek için kullandıkları, tercihen bir istemci cihaz üzerinde görüntülenen bir ara yüz üzerinden erişilerek üzerinde işlemler gerçekleştirilebilen bir sunucu olan en az bir mobil imza servis platformu (2),
- kullanıcıların (K) mobil imza servis platformunda (2) oluşturdukları mobil imza isteklerinin bir veri protokolü üzerinden aktarıldığı ve bu mobil imza isteklerinin bir veri iletim ağı (N) üzerinden aboneye (A) iletilmesi için gereken işlemleri yerine getiren, benzer şekilde abonenin (A) söz konusu mobil imza isteğine istinaden girişini yaptığı mobil imza şifresi ile imzalanmış özet bilgisinin mobil imza servis platformuna (2) iletilmesi için gereken işlemleri yerine getiren en az bir IP iletişim birimi (3),

- abonenin (A) mobil imza isteklerini görüntülemesini ve bu isteklere istinaden mobil imza şifresi girişi yapabilmesini sağlayan, bir veri iletim ağı (N) üzerinden IP iletişim birimi (3) ile iletişim kurabilen en az bir mobil cihaz (4),
- mobil cihazın (4) mobil iletişim şebekesi operatörünün sağladığı hizmetlere erişebilmek için kullandığı, en temel halinde bir IP altyapısı üzerinden gelen komutları alabilecek ve bu komutlara uygun aksiyonları gerçekleştirebilecek şekilde yapılandırılmış en az bir SIM kart (41) içermektedir. (Şekil 1)

Mobil imza servis platformu (2), abonelerden (A) mobil imza isteme yetkisi olan ve mobil imza servisine entegre olan firma ya da kurum gibi kullanıcıların (K) abone (A) bilgileri ve imzalanacak açık metin özetini girişi ile birlikte söz konusu mobil imza isteğini göndermek için kullandıkları, tercihen bir istemci cihaz üzerinde görüntülenen bir ara yüz üzerinden erişilerek üzerinde işlemler gerçekleştirilebilen bir sunucu birimdir.

IP iletişim birimi (3), kullanıcıların (K) mobil imza servis platformunda (2) oluşturdukları mobil imza isteklerinin bir veri protokolü üzerinden aktarıldığı ve bu mobil imza isteklerinin bir veri iletim ağı (N) üzerinden aboneye (A) iletilmesi için gereken işlemleri yerine getiren, benzer şekilde abonenin (A) söz konusu mobil imza isteğine istinaden girişini yaptığı mobil imza şifresi ile imzalanmış özet bilgisinin mobil imza servis platformuna (2) iletilmesi için gereken işlemleri yerine getiren birimdir.

IP iletişim birimi (3), en temel halinde bir servis geçidi, bir servis IP altyapısı ve bir istemci veri tabanı içermektedir. IP iletişim birimi (3), ayrıca mobil iletişim şebekesi operatörüne ait bir donanım güvenlik modülü ile veri alışverişi yapabilecek şekilde yapılandırılmış bir birimdir.

Buluşun farklı uygulamalarında IP iletişim birimi (3) ile mobil imza servis platformu (2) arasında mobil imza servisine ilişkin veri alışverişi tekniğin bilinen durumunda yer alan ve IP iletişim birimi (3) ile mobil imza servis platformu (2) tarafından desteklenen herhangi bir iletim protokolü (örneğin HTTP, Telnet gibi) üzerinden gerçekleştirilebilmektedir.

Buluşun farklı uygulamalarında, IP iletişim birimi (3) ile mobil cihaza (4) takılı olan SIM kart (41) arasında gerçekleştirilen iletişim, SIM kart (41) tarafından desteklenen herhangi bir iletim protokolü (örneğin HTTP, Telnet gibi) üzerinden gerçekleştirilebilmektedir. Buluşun tercih edilen uygulamasında bu protokol, HTTP'dir.

IP iletişim birimi (3), abonelere (A) gönderilen mobil imza isteği sonucunda SIM kart (41) üzerinde yer alan uygulamanın tetiklenmesi ile mobil cihaz (4) ekranında gösterimi sağlanan mobil imza menüsünde abonenin (A) mobil imza şifresi girişi yapması sonrasında imzalanmış hale gelen açık metin özetini, mobil imza isteğinin abone (A) mobil cihazına (4) iletildiği oturum (session) üzerinden mobil imza servis platformuna (2) ileten birimdir.

Mobil cihaz (4), abonenin (A) mobil imza isteklerini görüntülemesini ve bu isteklere istinaden mobil imza şifresi girişi yapabilmesini sağlayan, bir veri iletim ağı (N) üzerinden IP iletişim birimi (3) ile iletişim kurabilen bir cihazdır.

Mobil cihaz (4), SIM kartın (41) takılı ve kullanımda olduğu cihazdır. Mobil cihaz (4), abonenin (A) bir mobil imza isteğine istinaden, imzalanacak açık metin özetini ve mobil imza şifresi giriş alanını içeren mobil imza menüsünü görüntüleyebilmesini ve bu menü üzerinden mobil imza şifresinin girişini yapabilmesini sağlayan görüntüleme ve girdi birimlerine sahip olan bir cihazdır.

SIM kart (41), mobil cihazın (4) mobil iletişim şebekesi operatörünün sağladığı hizmetlere erişebilmek için kullandığı, en temel halinde bir IP altyapısı üzerinden

gelen komutları alabilecek ve bu komutlara uygun aksiyonları gerçekleştirebilecek, bu IP altyapısı üzerinden IP iletişim birimine (3) doğru veri ve istek gönderebilecek yapıda bir birimdir. SIM kart (41), veri iletim ağı (N) üzerinden aldığı komutlar sonrasında, çalışması tetiklenecek bir uygulamayı üzerinde barındıran bir birimdir.

Buluş konusu sistem (1) sayesinde, bir mobil iletişim şebekesi operatörü tarafından mevcut yapıda operatör SMS altyapısı üzerinden sağlanan mobil imza servisinin, IP altyapısı üzerinden sunulması işlemi gerçekleştirilmektedir. Söz konusu işlem gerçekleştirilirken ilk olarak, mobil imza isteğinde bulunacak olan kullanıcı (K) durumundaki firma ve kurumlar mobil imza servis platformuna (2) ulaşarak mobil imza isteklerini mobil imzası istenecek abone (A) bilgileri ve imzalanacak açık metin özeti girişi ile oluşturmaktadırlar. Mobil imza servis platformu (2), kullanıcı (K) tarafından oluşturulan bu mobil imza isteğini ve mobil imza isteğine dair bilgileri bir iletim protokolü üzerinden IP iletişim birimine (3) iletmektedir. IP iletişim birimi (3) kendisine iletilen bu mobil imza isteği sonrasında, abone (A) mobil cihazında (4) kullanımda olan SIM kartın (41) dinlemede olduğu IP ve porta herhangi bir iletim protokolü üzerinden söz konusu mobil imza isteğine ilişkin mobil imzalama işleminin yapılabilmesi için gereken menünün mobil cihazda (4) görüntülenmesi ve abonenin (A) girişini yapacağı mobil imza şifresinin alınması için gereken komutu göndermektedir. Gelen komut ile tetiklenen ve SIM kart (41) üzerinde çalışan uygulama, mobil cihaz (4) ekranında söz konusu imzalanacak açık metin özeti ile mobil imza şifresinin girişinin yapılmasını sağlayan menünün gösterimini sağlamaktadır.

Abonenin (A) mobil cihaz (4) ekranında görüntülenen imzalanacak açık metin özetini mobil cihaz ekranında (4) görüntülenen mobil imza menüsü üzerinden mobil imza şifresi girişi yaparak imzalaması sonucunda, imzalanmış olan açık metin özeti yine SIM kart üzerinde çalışmakta olan uygulama tarafından, aynı oturum dahilinde ve yine veri iletim ağı (N) ve bir iletim protokolü üzerinden IP iletişim birimine (3) gönderilmektedir. IP iletişim birimi (3) de yine bir iletim

protokolü üzerinden, bu imzalanmış açık metin özetinin mobil imza servis platformuna (2) aktarılmasını sağlamaktadır. Mobil imza işlemine ilişkin olarak doğruluk kontrolleri mobil imza servis platformu (2) tarafından yapılarak imzalama işleminin sonucu mobil imza servis platformu tarafından mobil imza servisini kullanan bir firma ya kurum olan kullanıcıya (K) iletilmektedir. Teknikte uzman bir kişinin anlayabileceği üzere, söz konusu mobil imza isteğinin iletimi ve abonenin (A) mobil imza şifresi girişi ile imzalanan imzalanmış açık metin özetinin alınarak IP iletişim birimi (3) tarafından mobil imza servis platformuna (2) iletilmesi işlemleri bir oturum içinde ya da farklı oturumlarda birden fazla defa tekrar edilebilmektedir. Bu sayede bir abone (A) için birden fazla mobil imza işleminin art arda ve aynı oturum içinde yapılabilmesi sağlanmaktadır.

Buluş konusu sistemde (1) SIM karta (41) doğru giden tüm iletişimlerde bağlantı IP iletişim birimi (3) tarafından açıldığı için SIM kartın (41) hangi IP adresi ve porta doğru gönderilen komutları alabileceğinin IP iletişim birimi (3) tarafından bilinmesi gerekmektedir. Bu nedenle SIM kart (41), hangi IP adresi ve porta doğru gönderilen komutları alabileceği bilgisini periyodik aralıklarla IP iletişim birimine (3) bildirmektedir. Bu sayede, SIM kartın (41) hangi IP adresi ve porta doğru gönderilen komutları alabileceği güncel olarak IP iletişim biriminde (3) tutulmuş olmaktadır.

Buluş konusu sistemde (1), mobil imza servisi kullanımı ile aboneye (A) iletilen imzalanacak özet bilgisi, imza içeriği hakkında bilgi vermediği için hassas bir bilgi değildir. Aynı şekilde, abonenin (A) imzaladığı özet bilgisi, şifrelenmiş özet bilgisi içerdiğinden ötürü, ayrıca bir şifreleme yapılmasına gerek bulunmamaktadır. Mobil imza servisinin kullanımı amacıyla zaten oluşturulmuş olan mobil imza anahtar çifti, aynı zamanda güvenlik amaçlı olarak da kullanılabilmektedir. Bu nedenle buluş konusu sistemde (1) yer alan SIM kartta (41) IP iletişim birimi (3) ile şifreli bir biçimde iletişim gerçekleştirmek için kullanılan gömülü (SIM kartın (41) üretimi sırasında SIM karta (41) gömülmüş olan) bir anahtar ve daha sonra güvenli bölgede üretilen bir mobil imza anahtar

çifti mevcuttur. Böylece ek anahtar çifti kullanımının ve SIM kartın (41) sınırlı alanında yer işgal edilmesinin önüne geçilmiş olmaktadır. Bunların yanı sıra kimlik doğrulama ve mesaj içeriğinin değiştirilmemiş olması önemini korumaktadır. Dolayısıyla, buluş konusu sistemde (1) yer alan IP iletişim birimi (3), güvenlik ve kimlik doğrulama mekanizmalarını barındıran bir birimdir.

Buluş konusu sistem (1) dahilinde IP iletişim birimi (3) ile mobil cihaz (4) arasında yüksek güvenlikli iletişimin gerçekleştirilmesi 4 ayrı aşamada sağlanmaktadır. Bu aşamalar, SIM kartın (41) üretim aşaması, SIM kartın (41) mobil iletişim şebekesi ve IP iletişim birimi (3) nezdinde ilk kayıt işlemi aşaması, SIM kart (41) tetiklemeli iletişim aşaması ve mobil iletişim şebekesi tetiklemeli yani IP iletişim birimi (3) tetiklemeli iletişim aşamalarıdır. Bu aşamalarda mobil cihaz (4) ve SIM kart (41) ile iletişimde olan IP iletişim biriminin (3) kullandığı alt birimler SIB (Service IP Backbone – Servis IP Altyapısı), SG (Service Gateway – Servis Geçidi) ve HSM (Hardware Security Module – Donanım Güvenlik Modülü) birimleridir. Bu aşamalarda çeşitli güvenlik anahtarları da kullanılmaktadır. Buluş konusu sistem (1) dahilinde kullanılan güvenlik anahtarları şu şekildedir:

ES_K: SIM kartın (41) Servis Geçidi ya da Servis IP Altyapısına erişirken SSL/TLS gibi bir protokol aracılığıyla belirlediği ortak tek kullanımlık simetrik anahtardır.

SIM_K: SIM kartın (41) üretimi esnasında kart içerisine eklenen simetrik anahtardır. Bu anahtar aynı zamanda Donanım Güvenlik Modülüne kaydedilmiş bir anahtardır.

$MSIGN_{pub}$: Mobil imza kullanımı için SIM karttaki (41) güvenli bölgede yer alan anahtar çiftinden açık anahtar olanıdır.

$MSIGN_{pri}$: Mobil imza kullanımı için SIM karttaki (41) güvenli bölgede yer alan anahtar çiftinden gizli anahtar olanıdır.

SIM kartın (41) üretim aşamasında SIM kart (41) içerisindeki güvenli alana gömülü olarak simetrik anahtar SIM_K eklenmektedir. Bu simetrik anahtar, SIM

karta (41) özel bir anahtar olup aynı zamanda Donanım Güvenlik Modülünde de kayıtlı olan bir anahtardır. Buluşun bir uygulamasında SIM kart (41), üzerinde yer alan uygulamanın ilk güvenlik kontrolünü geçebilmesi amacıyla kullanılacak bir uygulama şifresini de içeren bir karttır. Aynı zamanda, SIM kart (41), üretimi aşamasında, hafızasına Servis Geçidi modülünün IP/DNS (Domain Name Server – Alan Adı Sunucusu) erişim bilgileri de eklenmiş olan bir karttır.

SIM kartın (41) ilk kayıt aşamasında ilk olarak, mobil cihaza (4) takılı halde bulunan SIM kartta (41) yer alan güvenli alanda mobil cihazın (4) aktive edilmesi ile birlikte SIM kart (41) tarafından $MSIGN_{pub}$ ve $MSIGN_{pri}$ 'den oluşan bir mobil imza açık anahtar çifti oluşturulmaktadır. Daha sonra SIM kart (41) Servis Geçidi'ne doğru bir protokol üzerinden erişim gerçekleştirmekte ve Servis Geçidi'nin açık anahtarı ile şifrelenmiş olarak tek kullanımlık bir şifre belirlenmektedir. Uygulama şifresi ve SIM kart (41) vasıtasıyla kullanılacak MSISDN (Mobile Station International Subscriber Directory Number – Mobil İstasyon Uluslararası Abone Dizin Numarası) bilgisi SIM karttan (41) Servis Geçidi'ne doğru bu tek kullanımlık şifre ile şifrelenerek iletilmektedir. Bu noktada Servis Geçidi bir istemci veri tabanı üzerinden kullanıcı adı, şifre doğrulamasını gerçekleştirerek abone (A) mobil cihazına (4) belirteç (token), Servis IP Altyapısına ait URL ve Servis IP Altyapısı çıkış bilgisini iletmektedir. Bu noktada SIM kart (41), yalnızca Servis IP Altyapısından, yani IP iletişim biriminden (3) gelecek olan istekleri kabul edecek şekilde bir IP filtreleme tanım eklemesini yapmaktadır. Servis IP Altyapısına ait URL bilgisini edinen SIM kart (41), bu URL adresine doğru SSL, TLS benzeri bir protokolle bir bağlantı başlatmakta ve tek kullanımlık şifre belirlenmiş olmaktadır. Daha sonra, SIM kart (41) tarafından üretilmiş olan $MSIGN_{pub}$ açık anahtarı SIM kart (41) dahilinde bulunan $MSIGN_{pri}$ ile şifrelenmekte ve şifrelenmiş $MSIGN_{pub}$, şifresiz $MSIGN_{pub}$, belirteç ve SIM kartın dinleme IP ve port bilgileri Service IP Altyapısına iletilmektedir. Servis IP Altyapısı, aldığı mesajın belirteç bilgisini doğruladıktan sonra, şifrelenmiş mobil imza açık anahtarını $MSIGN_{pub}$ ile çözüp içeriğin değiştirilmediğini ve SIM kartın (41) kimliğini doğrulamaktadır. Ayrıca, SIM kart

(41), IP, MSISDN ve mobil imza açık anahtar bilgileri bir istemci veri tabanına Service IP Altyapısı tarafından eklenmektedir.

SIM kartın (41) ilk kayıt aşamasının gerçekleştirilmesi sonrasında IP iletişim biriminde (3) SIM karta (41) erişim için gerekli olan IP adresi ve anahtar bilgileri kaydedilmiş olmaktadır.

Mobil cihazda (4) takılı bulunan SIM kart (41) ile IP iletişim birimi (3) arasında gerçekleşen yüksek güvenlikli iletişimde bir aşama da SIM kart (41) tetiklemeli iletişimdir. SIM kart (41) tetiklemeli iletişimde ilk olarak SIM kart (41) Servis Geçidine doğru SSL/TLS gibi bir protokol üzerinden iletişim kurmaktadır. Daha sonra, Servis Geçidinin açık anahtarı ile şifrelenmiş olarak tek kullanımlık şifre belirlenmektedir. MSISDN ve uygulama şifresi bilgileri bu tek kullanımlık şifre ile şifrelenerek SIM karttan (41) Servis Geçidine doğru iletilmektedir. Servis Geçidi, bir istemci veri tabanına erişerek kullanıcı adı ve şifre doğrulaması gerçekleştirdikten sonra doğrulama başarılı ise SIM kartın (41) kullanımda olduğu mobil cihaza (4) belirteç (token), Servis IP Altyapısına ait URL ve Servis IP Altyapısı çıkış bilgisini iletmektedir. Bu noktada SIM kart (41), yalnızca Servis IP Altyapısından, yani IP iletişim biriminden (3) gelecek olan istekleri kabul edecek şekilde bir IP filtreleme tanım eklemesini yapmaktadır. Daha sonra SIM kart (41) Servis IP Altyapısı URL adresi ile SSL, TLS gibi bir protokol üzerinden iletişim kurmakta ve bu iletişim ile birlikte tek kullanımlık bir şifre belirlenmektedir. SIM kart (41) imzalanmış içeriği ve imzalama isteğini Servis IP Altyapısına gönderdikten sonra Servis IP Altyapısı istemci veri tabanına erişerek ilgili SIM kartın (41) güvenli bölgede üretmiş olduğu mobil imza açık anahtarına ait bilgiye erişir ve bu mobil imza açık anahtarı ile, mobil imza gizli anahtarı ile şifrelenmiş durumda bulunan açık anahtar bilgisini çözerek çözülmüş açık anahtarın, istemci veri tabanından alınan açık anahtar ile aynı olup olmadığını kontrol etmektedir. Bu iki açık anahtar uyuşuyor ise, Servis IP Altyapısı, SIM kartın (41) iletmiş olduğu istek içeriğine uygun şekilde isteği işlemeye başlamaktadır.

Mobil cihazda (4) takılı bulunan SIM kart (41) ile IP iletişim birimi (3) arasında gerçekleşen yüksek güvenlikli iletişimde bir aşama da IP iletişim birimi (3) tetiklemeli iletişim aşamasıdır. IP iletişim birimi (3) tetiklemeli iletişimde ilk olarak, IP iletişim biriminin (3) bir parçası olan Servis IP Altyapısı, iletişim kuracağı SIM karta (41) ait MSISDN, IP/port ve $MSIGN_{pub}$ (açık anahtar) bilgilerini istemci veri tabanından elde etmektedir. Daha sonra Servis IP Altyapısı, zaman bilgisini Donanım Güvenlik Modülüne göndererek ilgili SIM karta (41) ait SIM_K (gömülü anahtar) ile şifrelemektedir. Daha sonra Servis IP Altyapısı, SIM karta (41) zaman damgası, şifreli zaman damgası, komut ve imzalanacak metin özeti içeriği ve sayaç bilgisini, bu açık anahtar ile şifrelenmiş biçimde göndermektedir. Bu bilgileri alan SIM kart (41) bilgileri, daha önce güvenli bölgede üretmiş olduğu mobil imza gizli anahtarı ile çözmekte, bilgiler içinde yer alan şifrelenmiş zaman damgası bilgisini de gömülü anahtar ile çözerek çözülmüş zaman damgası değeri ile şifresiz zaman damgası değerinin uyuşup uyuşmadığını belirlemektedir.

SIM kart (41) ayrıca bu noktada, sayaç bilgisini de dikkate almaktadır. SIM kart (41) ile IP iletişim birimi (3) arasında gerçekleştirilen her işlem için her iki tarafta da bir arttırılan bu sayaç değeri, SIM kart (41) tarafından her seferinde kontrol edilerek, sayaç değerinin kendindeki sayaç değerinden küçük olarak gelmesi durumunda komutun reddi sağlanmaktadır. Bu sayede SIM karta (41) yapılabilecek olası tekrarlama saldırıları önlenmiş olmaktadır.

Zaman değeri bilgilerinin uyuşması (Servis IP Altyapısının doğrulanması) ve sayaç değerinin uygunluğu hallerinde, SIM kart (41) kendisine gelen komutu, ilgili içeriği de dikkate alarak işleme almaktadır.

Buluş konusu sistemin (1) bir uygulamasında, mobil imza servis platformu (2), kullanıcılardan (K) gelen ve aynı aboneye (A) gönderilecek mobil imza isteklerini, biriktirerek bu imza istekleri belirli bir sayıya ulaştığında ya da ilk imza isteği üzerinden belirli bir süre geçtikten sonra bu imza isteklerini toplu

olarak IP iletişim birimine (3) iletmektedir. IP iletişim birimi (3) de bu toplu imza isteklerini SIM karta (41) yine toplu bir biçimde iletmektedir. Buluşun bu uygulamasında SIM kart (41) da kendisine gelen toplu mobil imza isteklerinin tek bir mobil imza girişi ile toplu olarak imzalanabilmesini sağlayan bir uygulamanın üzerinde çalıştığı bir SIM karttır (41).

Teknikte uzman bir kişinin anlayabileceği üzere SIM kart (41) ile IP iletişim birimi (3) arasında gerçekleşen iletişim, mobil cihazın (4) sahip olduğu donanımsal iletişim yetenekleri sayesinde ve tercihen İnternet olan veri iletim ağı (N) ve tercihen HTTP olan bir protokol üzerinden gerçekleştirilmektedir.

Bu temel kavramlar etrafında, buluş konusu sistem (1) ile ilgili çok çeşitli uygulamaların geliştirilmesi mümkün olup, buluş burada açıklanan örneklerle sınırlandırılamaz, esas olarak istemlerde belirtildiği gibidir.

Şekil 1