ÖZET

BİR MOBİL TERMİNAL CİHAZINDA BİR ABONELİK PROFİLİNİN HAZIRLANMASI İÇİN METOT VE CİHAZ

Buluş, bir mobil kablosuz ağ üzerinden iletişim için bir mobil terminal cihaz (30) üzerinde bi abonelik profilinin (SP2) hazırlanması için metot olup, birinci mobil terminal cihazın (20) bir birinci abonelik profili (SP1) ile bir mobil kablosuz ağ şebekesi (50) içine kaydedilmesi olup, içerisinde birinci abonelik profili (SP1) birinci mobil terminal cihazın (20) mobil kablosuz ağ şebekesine (50) karşı tanımlanması ve yetkilendirilmesi için abonelik yetki verilerini içermesi; ikinci abonelik profilinin (SP2) mobil kablosuz ağ şebekesi (50) üzerinden birinci mobil terminal cihaza (20), mobil kablosuz ağ şebekesinin (50) içine başarılı bir şekilde kaydedilmesinden sonra indirilmesi olup, içerisinde ikinci abonelik profili (SP2) bir mobil kablosuz ağ şebekesine (50) ya da bir diğer kablosuz ağ şebekesine karşı bir ikinci mobil terminal cihazın (30) açıkça tanımlanması ve yetkilendirilmesi için abonelik yetki verilerini içermesi; ve İkinci abonelik profilinin (SP2) birinci mobil terminal cihazdan (20) bir iletişim kanalı (40) üzerinden ikinci mobil terminal cihaza (30) aktarılması adımları içermesi ile ilgilidir.

İSTEMLER

1. Bir mobil kablosuz ağ üzerinden iletişim için bir mobil terminal cihaz (30) üzerinde bir abonelik profilinin (SP2) hazırlanması için metot olup, **özelliği**; içerisinde metodun aşağıdaki adımları içermesidir:

   birinci mobil terminal cihazın (20) bir birinci abonelik profili (SP1) ile bir mobil kablosuz ağ şebekesi (50) içine kaydedilmesi olup, içerisinde birinci abonelik profili (SP1) birinci mobil terminal cihazın (20) mobil kablosuz ağ şebekesine (50) karşı tanımlanması ve yetkilendirilmesi için abonelik yetki verilerini içermesi; ikinci abonelik profilinin (SP2) mobil kablosuz ağ şebekesi (50) üzerinden birinci mobil terminal cihaza (20), mobil kablosuz ağ şebekesinin (50) içine başarılı bir şekilde kaydedilmesinden sonra indirilmesi olup, içerisinde ikinci abonelik profili (SP2) bir mobil kablosuz ağ şebekesine (50) ya da bir diğer kablosuz ağ şebekesine karşı bir ikinci mobil terminal cihazın (30) açıkça tanımlanması ve yetkilendirilmesi için abonelik yetki verilerini içermesi; ve

   İkinci abonelik profilinin (SP2) birinci mobil terminal cihazdan (20) bir iletişim kanalı (40) üzerinden ikinci mobil terminal cihaza (30) aktarılması.

2. İstem 1'e göre metot olup, **özelliği**; içerisinde metodun ikinci abonelik profilinin (SP2) birnci mobil terminal cihazdan (20) iletişim kanalı (40) üzerinden ikinci mobil terminal cihaza (30) iletilmesi adımından sonra ikinci mobil terminal cihazın (30) ikinci abonelik profili (SP2) ile mobil kablosuz ağ şebekesinin (50) içine ya da diğer mobil kablosuz ağ şebekesinin içine kaydedilmesini içermesidir.

3. İstem 2'ye göre metot olup, **özelliği**; içerisinde, içinde ikinci mobil terminal cihazın (30) ikinci abonelik profili (SP2) ile birlikte kaydedilmiş olduğu mobil kablosuz ağ şebekesinin, ikinci abonelik profilinin (SP2) birinci mobil terminal cihaza (20) indirilmiş olduğu mobil kablosuz ağ şebekesi (50) olmasıdır.

4. Önceki istemlerden birisine göre metot olup, **özelliği**; içerisinde iletişim kanalının (40) birinci mobil terminal cihaz (20) ve ikinci mobil terminal cihaz (30) arasında bir NFC-iletişim kanalı, bir WiFi- iletişim kanalı, bir Bluetooth iletişim kanalı, bir optik iletişim kanalı ve/ veya bir akustik iletişim kanalı olmasıdır.

5. Önceki istemlerden birisine göre metot olup, **özelliği**; içerisinde ikinci abonelik profilinin (SP2) bir sunucudan (60) mobil kablosuz ağ şebekesi (50) üzerinden birinci mobil terminal cihaza (20) indirilmesidir.

6. İstem 5'e göre metot olup, **özelliği**; içerisinde sunucu (60) ve ikinci mobil terminal cihaz (30) arasında bir iletişim kanalının kriptografik olarak güvenliğinin temin edilmiş olmasıdır.

7. İstem 6'ya göre metot olup, **özelliği**; içerisinde sunucu (60) ve ikinci mobil terminal cihaz

(30) arasındaki iletişim kanalının, ikinci abonelik profilinin (SP2) sunucu (60) tarafından bir şifre ile şifrelenmiş olması, bunun da sunucuda (60) ikinci mobil terminal cihazın (30) bir tanımlayıcısı ile ve/ veya ikinci mobil terminal cihazı (30) bir güvenlik elemanı (32) ile bağlantılı olarak kaydedilmesi suretiyle kriptografik olarak güvenliğinin temin edilmiş olmasıdır.

8. İstem 1'e göre bir metodun uygulanması için yapılandırılmış olan bir güvenlik elemanı (22) olup, böylece ikinci abonelik profili (SP2) güvenlik elemanında (22) hazırlanmakta olup, **özelliği**, içerisinde kaydetme ve ve indirme adımları birinci mobil terminal cihazın güvenlik elemanını (22) yardımı ile uygulanmasıdır.

9. İstem 8'e göre bir güvenlik elemanına (22) sahip olan mobil terminal cihaz (20).

10. Bir mobil kablosuz ağ şebekesi üzerinden iletişim için bir mobil terminal cihazda (30) bir abonelik profilinin (SP2) hazırlanması için sistem olup, **özelliği**; sistemin aşağıdakileri içermesidir:

Bir birinci abonelik profili (SP1) ile bir mobil kablosuz ağ şebekesi (50) içine kaydedilmek üzere yapılandırılmış olan bir birinci mobil terminal cihaz olup, içerisinde birinci abonelik profili (SP1) abonelik yetki verilerini birinci mobil terminal cihazın (20) mobil kablosuz ağ şebekesine (50) karşı açıkça tanımlama ve yetkilendirme için içermekte olup, mobil kablosuz ağ şebekesinin (50) içine başarılı bir şekilde kaydedildikten sonra birinci mobil terminal cihaza (20) mobil kablosuz ağ şebekesi (50) üzerinden bir ikinci abonelik profilinin (SP2) indirilmesi için bir sunucuyu (60) içermekte olup; içerisinde ikinci abonelik profili (SP2) bir ikinci mobil terminal cihazın (30) mobil kablosuz ağ şebekesine (50) ya da bir diğer kablosuz ağ şebekesine karşı açıkça tanımlanması ve yetkilendirilmesi için abonelik yetki verilerini içermesi, ve

İkinci mobil terminal cihazın (30), ikinci abonelik profilinin (SP2) birinci mobil terminal cihazdan (20) bir iletişim kanalı (40) üzerinden ikinci mobil terminal cihaza (30) iletilmesi için, ve ikinci abonelik profili ile mobil kablosuz ağ şebekesinin içine kaydedilmesi için donatılmış olmasıdır.

TARİFNAME

BİR MOBİL TERMİNAL CİHAZINDA BİR ABONELİK PROFİLİNİN HAZIRLANMASI İÇİN METOT VE CİHAZ

BULUŞUN ALANI

Mevcut buluş, genel olarak mobil kablosuz ağlar üzerinden iletişim ile ve özelikle bir mobil kablosuz ağ üzerinden iletişim için bir mobil terminal cihazda bir abonelik profilinin hazırlanması için metot ve tertibatlar ile ilgilidir.

BULUŞUN ARKA PLANI

Bir mobil terminal cihazı vasıtası ile, örneğin bir mobil telefon vasıtası ile, bir ağ işleticisi (MNO [Mobile Network Operator] olarak da tanımlanır) tarafından işletilen bir mobil kablosuz ağ (PLMN [Public Land Mobile Network] olarak da tanımlanır) üzerinden iletişim normal olarak mobil terminal cihazının bir güvenlik elemanı ya da bir katılımcı tanımlama modülü ile, örneğin bir SIM kart şeklinde, abonelik yetki verilerinin ("Subscription Credentials") emniyetli bir şekilde alınması için donatılmış olmalarını gerektirir, bunlar da normal olarak bir abonelik profilinin parçasıdırlar ve kullanıcıyı mobil terminal cihazının mobil kablosuz ağına karşı açıkça tanımlarlar ve yetkilendirirler. Bu tip abonelik yetki verileri, örneğin bir IMSI (International Mobile Subscriber Identity) ve bir yetkilendirme şifresi (K_i,) geçmişte normal olarak bir "kişiselleştirme" çerçevesi içerisinde güvenlik elemanı üreticisinin emniyetli çevresi içinde emniyet elemanında kaydedilmiştir.

Geçmişte SIM kartlar şeklindeki güvenlik elemanlarının büyük bir kısmı bir mobil terminal cihazı içerisinde basit bir şekilde değiştirilebilirlerken, bir süreden beri, gittikçe artan bir şekilde bir mobil terminal cihazı içerisine sabit bir şekilde monte edilen güvenlik elemanları bulunmaktadır. Bir mobil terminal cihazı içine sabit bir şeklide monte edilmiş olan, teknikte uzman bir kişi tarafından "Embedded SIM" ya da "Embedded UICC (eUICC)" olarak bilinen bu tip bir güvenlik elemanı normal olarak güvenlik elemanının üreticisinin bir güvenlik çevresi içerisinde artık kişiselleştirilemez, çünkü özellikle güvenlik elemanının kullanım alanı önceden bilinmemektedir.

Böylece bir mobil terminal cihazının kişiselleştirilmesi için, yani bir mobil terminal cihazı, özellikle bunun güvenlik elemanında bir abonelik profilinin hazırlanmasına yönelik bir iyileştirilmiş metot ve tertibatlar için ihtiyaç bulunmaktadır.

EP 2 701 359 A1 sayılı belgeden katılımcı tanımlama verileri ile bir kişiselleştirilmemiş terminal cihazının kişiselleştirilmesi için bir metot ortaya çıkmakta olup, içerisinde indirilen katılımcı tanımlama verileri terminal cihaz üzerinde kalır.

US 2014/0057558 A1 sayılı belge aynı SIM verilerinin bir birinci terminal cihazından bir ikinci

terminal cihazına aktarılması ile ilgilidir. SIM verileri bu sırada değişmez ve aktarmadan sonra birinci terminal cihazı tarafından silinir.

BULUŞUN ÖZETİ

Yukarıda belirtilmiş olan amaca mevcut buluşa göre bağımsız istemlerin ilgili konusu ile ulaşılır. Buluşun tercih edilen yapılanmaları bağımlı istemlerde tanımlanır.

Buluşun bir birinci bakış açısına göre bir mobil kablosuz ağ üzerinden iletişim için bir mobil terminal cihazı üzerinden bir abonelik profilinin hazırlanması için bir metot hazırlanmaktadır. Burada metot aşağıdaki adımları içerir: Bir birinci mobil terminal cihazının bir birinci abonelik profili ile bir mobil kablosuz ağ içinde kaydedilmesi; mobil kablosuz ağ üzerinden bir ikinci abonelik profilinin birinci mobil terminal cihazına indirilmesi; ve ikinci abonelik profilinin birinci mobil terminal cihazından bir iletişim kanalı üzerinden bir ikinci mobil terminal cihazına iletilmesi.

Tercihen cihaz ikinci abonelik profilinin birinci mobil terminal cihazından iletişim kanalı üzerinden ikinci mobil terminal cihazına iletilmesi adımından sonra ikinci mobil terminal cihazının ikinci abonelik profili ile birlikte bir mobil kablosuz ağ içine kaydedilmesini içerir.

Buluşun tercih edilen uygulama şekillerine göre, içerisinde ikinci mobil terminal cihazının ikinci abonelik profili ile kaydedildiği mobil kablosuz ağ, ikinci abonelik profilinin birinci mobil terminal cihazına indirilmiş olduğu mobil kablosuz ağdır.

Tercihen birinci mobil terminal cihazı ve ikinci mobil terminal cihazı arasındaki iletişim kanalı bir NFC- iletişim kanalıdır, bir WiFi- iletişim kanalıdır, bir Bluetooth- iletişim kanalıdır, bir optik iletişim kanalıdır ve/ veya bir akustik iletişim kanalıdır.

Buluşun tercih edilen uygulama şekillerine göre ikinci abonelik profili bir sunucudan mobil kablosuz ağ şebekesi üzerinden ikinci mobil terminal cihazına indirilir.

Tercihen lojik iletişim kanalı sunucu ve ikinci mobil terminal cihazı arasında kriptrografik olarak güvenliği sağlanmıştır.

Buluşun tercih edilen uygulama şekillerine göre lojik iletişim kanalı sunucu ve ikinci mobil terminal cihazı arasında, ikinci abonelik profilinin sunucudan bir şifre ile şifrelenmiş olması, bunun da sunucuda ikinci mobil terminal cihazının bir tanımlayıcısı ile ve/ veya ikinci mobil terminal cihazının bir güvenlik elemanı ile bağlantılı olarak kaydedilmiş olması suretiyle kriptorgrafik olarak güvenliği sağlanmıştır.

Buluşun bir ikinci bakış açısına göre, bir mobil kablosuz ağ şebekesi üzerinden iletişim için bir ikinci mobil terminal cihazı üzerinde bir abonelik profilinin hazırlanması için bir sistem hazırlanır. Burada sistem aşağıdakileri içerir: bir mobil kablosuz ağ şebekesi içerisinde bir birinci abonelik profili ile kaydedilmesi için donatılmış olan bir birinci mobil terminal cihaz;

birinci mobil terminal cihazına mobil kablosuz ağ şebekesi üzerinden bir ikinci bir ikinci abonelik profilinin indirilmesi için bir sunucu; ikinci abonelik profilinin birinci mobil terminal cihazından bir iletişim kanalı üzerinden ikinci mobil terminal cihazına iletilmesi için donatılmış olan bir ikinci mobil terminal cihaz.

Teknikte uzman kişinin de gördüğü gibi, yukarıda tarif edilmiş olan tercih edilen yapılanmalar hem buluşun birinci bakış açısı çerçevesi içerisinde, yani bir mobil kablosuz ağ şebekesi üzerinden iletişim için bir mobil terminal cihaza bir abonelik profilinin hazırlanması için metot çerçevesi içerisinde, hem de buluşun ikinci bakış açısı çerçevesi içerisinde yani bir mobil kablosuz ağ şebekesi üzerinden iletişim için bir mobil terminal cihazına bir abonelik profilinin hazırlanması için bir sistem çerçevesi içerisinde avantajlı olarak yerleştirilebilir.

Buluşun diğer özellikleri, avantajları ve amaçları, çok sayıdaki uygulama örneğinin ve uygulama alternatiflerinin aşağıda ayrıntılı olarak tarifinden ortaya çıkar. Çizimler referans olarak verilmekte olup,

Şekil 1, mevcut buluşun farklı bakış açılarını gösteren, bir birinci mobil terminal cihaz ve bir ikinci mobil terminal cihaz ile iletişim içerisinde bir mobil kablosuz sistem ile bir iletişim sisteminin bir şematik görüntüsünü gösterir, ve

Şekil 2, şekil 1'in ikinci mobil terminal cihazı üzerinde bir abonelik profilinin hazırlanması için bir tercih edilen akışın bir şematik görüntüsünü gösterir.

Şekil 1, mevcut buluşun farklı bakış açılarını gösteren, bir iletişim sisteminin (10) bileşenlerinin bir şematik görüntüsünü ve bu komponentlerin arasındaki bazı iletişim bağlantılarını gösterir. Aşağıdaki ayrıntılı tarifte bir "mobil" terminal cihazı referans olarak alınmasına rağmen, teknikte uzman kişi mevcut buluşun avantajlı olarak, bir mobil ya da hücresel iletişim şebekesi ağı ile iletişim üzerinden, yani kuruluş yeri pratikte değişmeyen terminal cihazları ile iletişimde bulunmak üzere donatılmış olan terminal cihazlarının her türü ile kullanılabilir olduğunu görür. Diğer bir deyişle: burada kullanılan "mobil" özelliği bir mobil ya da hücresel iletişim ağı şebekesi üzerinden terminal cihazının iletişim kabiliyeti hakkındadır.

Şekil 1'de örnek olarak bir birinci mobil terminal cihazı (20) ve bir ikinci mobil terminal cihazı (30) gösterilmiştir. Tercihen birinci mobil terminal cihazı (20) ve ikinci mobil terminal cihazı (30), örneğin birinci mobil terminal cihazını (20) ve ikinci mobil terminal cihazını (30) bir mobil kablosuz ağ içerisinde açıkça tanımlayan verilerin güvenilir bir şekilde kaydedilmesi ve işlenmesi için birer güvenlik elemanına ("Secure Element") (22 ya da 32) sahiptirler. Şekil 1'de belirtilmiş olduğu gibi, birinci mobil terminal cihazında (20) tercihen bir akıllı telefon söz konusudur ve ikinci mobil terminal cihazında (30) bir tablet bilgisayar söz konusudur. Teknikte uzman kişi ise, birinci mobil terminal cihazının (20) ve ikinci mobil terminal cihazının (30) mevcut buluşa göre yine, bir mobil kablosuz ağ şebekesi üzerinden iletişimde bulunmak

üzere yapılandırılmış olan, örneğin bir notebook, bir TV sistemi, bir Set- Top box, bir satış otomatı, bir motorlu araç, bir güvenlik kamerası, bir sensör tertibatı ve benzeri gibi diğer cihazlar içine yerleştirilebilir olacağını görür.

Buluşun tercih edilen uygulama şekillerine göre güvenlik elemanı (22) ve güvenlik elemanı (32) bir eUICC (embedded Universal Integrated Circuit Card) olarak, bunun üzerine yerleştirilmiş olan bir SIM aplikasyonu ile donatılmışlardır, yani birinci mobil terminal cihazının (20) ya da ikinci mobil terminal cihazının (30) bir sabit bileşeni olan ve bir mobil kablosuz ağ şebekesi içerisinde kullanıcının ya da katılımcının açıkça ve emniyetli tanımlanması için ve farklı işlevlerin ve çoklu veri hizmetlerinin hazırlanması için bir güvenlik elemanı olarak kullanılır. Alternatif olarak güvenlik elemanı (22) ve/ veya güvenlik elemanı (32) bir UICC (Universal Integrated Circuit Card) ya SIM- Kart (Subscriber Identity Module) olarak donatılmış olabilirler, bunlar da teknikte uzman kişi tarafından bir emniyet elemanının şu anda en sık kullanılan şekilleri olarak bilinirler. Teknikte uzman kişi ise, USIM, R-UIM, ISIM ve benzeri olarak tanımlanan esas alınan mobil kablosuz standardın tipine ve türüne göre tanımlanan güvenlik elemanlarının türlerinin de yine mevcut buluş içerisinde kapsanmış olduğunu görür.

Buluşun diğer tercih edilen uygulama şekillerine göre güvenlik elemanı (22) ve/ veya güvenlik elemanı (32) donanım ve yazılım bileşenlerinden oluşan bir kombinasyon olarak birinci mobil terminal cihazının (30) ya da bir ikinci mobil terminal cihazının (30) bir merkezi işlemci ünitesinin bir işletme sisteminin güvenlik parçası içerisinde yapılandırılmış olabilir, bu da teknikte uzman kişi tarafından güvenliği sağlanmış çalışma süresi çevresi ("Trusted Execution Environment"; TEE) olarak bilinir. Güvenlik elemanı (22) ve/ veya güvenlik elemanı (32) o zaman örneğin birinci mobil terminal cihazının (20) ya da ikinci mobil terminal cihazının (30) bu tip bir güvenliği sağlanmış çalışma süresi çevresi içerisinde akan programlar, yani Trustlets® şeklinde yapılandırılmış olabilirler.

Birinci mobil terminal cihazı (20) ve ikinci terminal mobil cihazı (30), hava ara yüzü üzerinden bir mobil kablosuz ağ şebekesi (50) (kısaca “mobil kablosuz ağ” olarak ya da "Public Land Mobile Network" [PLMN] olarak tanımlanır) ile iletişim sağlamak üzere donatılmıştır. bunun için birinci mobil terminal cihaz (20) ve ikinci mobil terminal cihaz (30) normal olarak bir uygun donatılmış antene (şekil 1'de gösterilmemiştir) radyo dalgalarının alınması ve gönderilmesi için sahiptirler.

Aşağıda buluşun tercih edilen uygulama şekilleri GSM standardına ("Global Standard for Mobile Communications") göre bir mobil kablosuz ağ şebekesi (50) ile bağlantılı olarak tarif edilmekte olup, bu da çok sayıda ETSİ spesifikasyonları ile spesifize edilmiştir. Teknikte uzman kişi ise, mevcut buluşun diğer mobil kablosuz ağlar ile birlikte avantajlı olarak

kullanılabileceğini görür. Bu tip şebekeler üçüncü nesil (3GPP) mobil kablosuz ağları, örn UMTS (Universal Mobile Telecommunications System), dördüncü nesil mobil kablosuz ağları (4G), örneğin LTE (Long Term Evolution), ve diğer mobil kablosuz ağları, örn. CDMA ve benzerlerini içerir.

Teknikte uzman kişinin de bildiği gibi, GSM standardına göre kurulmuş bir mobil kablosuz ağ ya da PLMN genel olarak, PLMN'nin ilgili telsiz hücrelerini tanımlayan ve bir BSC ("Base Station Controller") ile bağlanmış olan çok sayıda BTS ("Base Transceiver Station") 'den meydana gelen bir BSS ("Base Station Subsystem") içerir. Normal olarak BSC'de bir ortak MSC ("Mobile Switching Center") ile iletişim içerisinde bulunan çok sayıda BSC'ler söz konusudur. Anlık olarak, bir MSC tarafından beslenen (yani MSC tarafından örtülmüş olan bir alandan) telsiz hücreleri içerisinde bulunan mobil kablosuz katılımcılar üzerinden bilgilerin tutulması için genellikle VLR ("Visitor Location Register") olarak adlandırılan bir lokal veri bankası MSC'nin parçasıdır. MSC esas olarak sabit şebeke (publicswitched telephone network; PSTN) içerisinde bir aracılık yeri gibi aynı işlevselliğe sahiptir ve bir HLR ("Home Location Register"), ile iletişim içerisinde olup, bunda da içerisinde mobil kablosuz katılımcının başvurusu ya da yetkilendirilmesi için bilgilerin depolandığı PLMN'nin primer veri bankası söz konusudur. Bunun için HLR normal olarak bir AUC'ye ("Authentication Center") ulaşım yetkisi vardır. Teknikte uzman kişi tarafından bilindiği gibi, yukarıda tarif edilmiş olan bir PLMN'nin komponentlerinin arasındaki iletişim bağlantıları mülkiyet ve/ veya açık standart bazında olabilir. Kullanılan protokoller örneğin SS7- ya da IP-bazlı olabilir. Ağ şebeke komponentlerinin ayrı ya da birleştirilmiş üniteler olarak nasıl yapılandırılmış oldukları ve bu komponentlerin arasındaki ara yüzlerin nasıl yapılandırılmış oldukları MNO'nun konusudur, böylece yukarıdaki tarifname yalnızca örnek olarak anlaşılmalıdır.

Teknikte uzman kişi, yukarıda tarif edilmiş olan bir bilinen mobil kablosuz ağın işlev ünitelerinin GSM standardına göre diğer ya da gelecekteki mobil kablosuz sandartlarda başka isimlere sahip olabilmelerine rağmen, esaslı prensipler esas olarak aynıdırlar ve bunlar bu nedenle buluş tarafından da kapsanırlar. Görünüşlülük açısından yukarıda tarif edilmiş olan bir mobil kablosuz ağın komponentlerinden yalnızca aşağıda şekil 1'de şematik görüntüde gösterilmiştir: bir örnek BTS 52 ve bir HLR 54 mobil kablosuz ağ (50) için.

Şekil 1'den de görülebileceği üzere, mobil kablosuz ağ (50) en azından kısmen, tercihen bir uygun yapılandırılmış "Subscription Management" Servers (SM Server) şeklinde bir arka plan sistemi (60) ile, aşağıda ayrıntılı olarak tarif edildiği gibi iletişim içerisindedir.

Şekil 1'de güvenlik elemanlarının (22 ve 32) ilgili büyütülmüş görüntülerinden de görülebileceği üzere, bunlar tercihen birer merkezi işleme ünitesini ya da bir merkezi işlemciyi ("central processing unit"; CPU) (25 ya da 35) içerirler. Tercihen işlemci (25 ya da 35),

uygulamaların, aşağıda şekil 2 ile bağlantılı olarak tarif edileceği gibi ikinci mobil terminal cihazında (30) bir abonelik profilinin hazırlanması için en azından özelliklerin bazılarını hazırlayan işlemci (25 ya da 35) üzerinde uygulanabileceği şekilde yapılandırılmıştır. Bu tip uygulamalar tercihen Java Applets formunda yerleştirilmişlerdir.

Güvenlik elemanı (22) ve güvenlik elemanı (32) tercihen ayrıca, tercihen geçici olmayan, tekrar yazılabilir, örneğin bir Flash Bellek formunda bellek ünitesi olarak yerleştirilmiş olan birer bellek ünitesini (26 ya da 36) içerirler. Burada bellek ünitesi (26 ya da 36), örneğin şekil 1'de şematik olarak gösterilmiş olduğu gibi abonelik profili SP1 ya da SP2 gibi en azından bir abonelik profilini bulundururlar.

Şekil 1'in şematik görüntüsünde abonelik profili (SP1) birinci mobil terminal cihazın (20) güvenlik elemanının (22) bellek ünitesi (26) içerisinde yerleştirilmiş olup, bu da özellikle, örneğin güvenlik elemanının (22) CPU 25'inin abonelik profiline SP1 müdahale edebileceği anlamını taşır. Tercihen abonelik profili SP1, güvenlik elemanının (22) ve birinci mobil terminal cihazının (20) mobil kablosuz ağ (50) içine kaydedilmesini ve bunun üzerinden iletişim kurulmasını mümkün kıldığı verileri, yani abonelik izin verileri ("Sub-scription Credentials"), gibi verileri, bir MNO'ya özel yetkilendirme algoritması ve/veya benzerlerini içerir.

Şekil 1'in şematik görüntüsünde ikinci mobil terminal cihazının (30) güvenlik elemanının (32) bellek ünitesi (36) abonelik profilinin (SP2) alınması için hazırdır, bu da aşağıda şekil 2 referans alınarak ayrıntılı olarak tarif edilmektedir. Tercihen abonelik profili (SP2), güvenlik elemanına (32) ve ikinci mobil terminal cihazına (30) mobil kablosuz ağ (50) içine kaydolmasını ve bunun üzerinden iletişimde bulunmasını mümkün kılan verileri içerir, yani aboneliğe yetkili veriler ("Subscription Credentials"), bir MNO'ya özel yetkilendirme algoritması ve/ veya benzerleri gibi verileri içerir. Alternatif olarak abonelik profili (SP2), güvenlik elemanına (32) ve ikinci mobil terminal cihazına (30) mobil kablosuz ağdan (50) farklı olan bir diğer mobil kablosuz ağa, örneğin bir diğer mobil kablosuz ağ işletmecisinin mobil kablosuz şebekesinin içine kaydolmasını mümkün kılan verileri içerebilir.

Şekil 2 ikinci mobil terminal cihazı (30) üzerinde abonelik profilinin (SP2) hazırlanması sırasında buluşa uygun tercih edilen bir akışı gösterir.

Şekil 2'nin adımında (S1) birinci mobil terminal cihaz (20) mevcut abonelik profili (SP1) ile mobil kablosuz ağ (50) içine kaydolur. Bu da, örneğin bir IMSI ve/ veya bir yetkilendirme şifresi (K_i) gibi abonelik profilinin (SP1) parçası olan abonelik yetki verileri kullanılarak bir yetkilendirme işlemi çerçevesi içerisinde meydana gelir.

Birinci mobil terminal cihazı (20) başarılı bir şekilde mobil kablosuz ağ (50) içine kaydolduktan sonra ve bununla iletişim sağlayabilmesinden sonra birinci mobil terminal cihazı (20) şekil 2'nin S2 adımında mobil kablosuz ağ (50) üzerinden SM sunucusunda (60)

ikinci mobil terminal cihaz (30) için bir abonelik profilini (SP2) sorar. Buluşa göre, birinci mobil terminal cihaz (20) üzerinde çalışan bir uygulama vasıtası ile bir kullanıcının bir grafik kullanıcı yüzeyi ile bu işlemi uygulayabilmesi ve özelikle ikinci mobil terminal cihaz (30) için abonelik profilini (S2) seçebilmesi de düşünülebilir.

Bu talep üzerine SM sunucusu (60) şekil 2'nin S3 adımında kullanıcı tarafından ikinci mobil terminal cihaz (30) için seçilmiş olan abonelik profilini (SP2) mobil kablosuz ağ (50) üzerinden birinci mobil terminal cihaza (20) yükler. Bu sırada SM sunucusu (60) birinci mobil terminal cihaza (20) güvenebilir, çünkü bu da mobil kablosuz ağ şebekesine (50) karşı yetkilendirilmiştir.

Şekil 2'nin S4 adımında bir iletişim kanalı (40) birinci mobil terminal cihaz (20) ile ikinci mobil terminal cihaz (30) arasında oluşturulur. Kullanıcıya normalde hem birinci mobil terminal cihaz (20) hem de ikinci mobil terminal cihaz (30) kullanıma sunulmuş olduğundan dolayı ve iki terminal cihazı da (20, 30) birleştirebilmesi nedeniyle, iletişim kanalında (40) kısa erişim mesafesine sahip olan bir iletişim kanalı söz konusu olabilir. Tercihen bu iletişim kanalında (40) bir NFC kanalı, Bluetooth- Kanalı, WiFi- Kanalı ya da benzerleri söz konusudur. Alternatif olarak bir optik ya da bir akustik veri aktarımı şeklinde bir iletişim kanalı (40) birinci mobil terminal cihaz (20) ve ikinci mobil terminal cihaz (30) arasında düşünülebilir. Örneğin veriler birinci mobil terminal cihazın (20) bir ekranı üzerinde, örneğin bir QR kodu şeklinde gösterilebilir, ve ikinci mobil terminal cihazın (30) bir kamerası vasıtası ile algılanabilir.

Şekil 2'nin S4 adımında iletişim kanalı birinci mobil terminal cihaz (20) ve ikinci mobil terminal cihaz (30) arasında oluşturulduktan sonra, şekil 2'nin S5 adımında abonelik profili (SP2) birinci mobil terminal cihazdan (20) iletişim kanalı (40) üzerinden ikinci mobil terminal cihaza (30) aktarılır.

Bunun üzerine şekil 2'nin S6 adımında ikinci mobil terminal cihaz ya da bunun güvenlik elemanı (32) abonelik profili (SP2) ve bunun içinde içerilmiş olan abonelik yetki verileri, örneğin bir İMSI ve/ veya bir yetkilendirme şifresi (K_i) ile birlikte mobil kablosuz ağ (50) içine kaydedebilir. Yukarıda da bahsedildiği gibi buluş tarafından, abonelik profilinin (SP2) abonelik yetki verilerinin bir diğer mobil kablosuz ağa giririşi, örneğin bir diğer mobil kablosuz ağ işletmecisinin mobil kablosuz ağına girişi mümkün kılması da içerilmiştir.

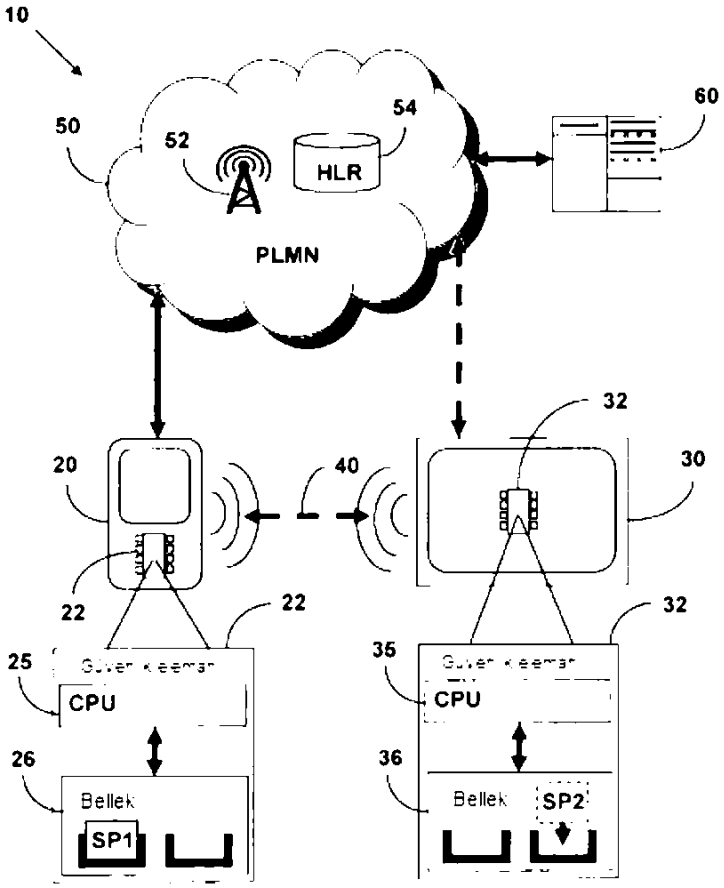
S6 adımında mobil terminal cihaz (30) başarılı bir şekilde mobil kablosuz ağ (50) içine kaydedilmiş ise, şekil 2'nin S7 adımında ikinci mobil terminal cihaz (30) mobil kablosuz ağ (50) üzerinden SM sunucusuna (60) bir uygun onayı gönderebilir.

Teknikte uzman kişinin de görebileceği gibi, mevcut buluş vasıtası ile oluşturulmuş olan avantajların elde edilmesi için, şekil 2'nin adımlarının orada gösterilmiş olan sırada meydana gelmesi gerekli değildir. Örneğin mevcut buluş çerçevesi içerisinde, birinci mobil terminal

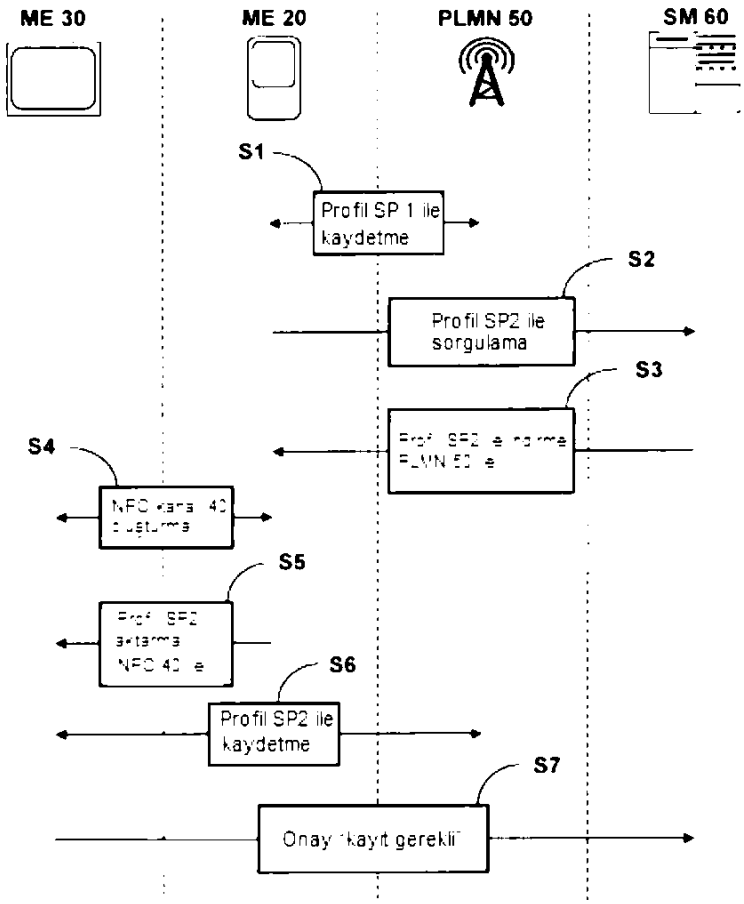
cihaz (20) ve ikinci mobil terminal cihaz (30) arasında iletişim kanalının (40) oluşturulması için S4 adımının abonelik profilinin (SP2) birinci mobil terminal cihaza (20) indirilmesinden önce meydana gelmesi de düşünülebilir.

Şekil 2'rin, mobil kablosuz ağ (50) üzerinden SM sunucusundan (60) birinci mobil terminal cihaza (20) ve birinci mobil terminal cihazdan (20) iletişim kanalı (40) üzerinden ikinci mobil terminal cihaza (30) indirilmesi için S3 ila S5 adımları SM sunucusu (60) ve ikinci mobil terminal cihaz (30) arasında bir lojik iletişim kanalı olarak görülebilir, bunda da birinci mobil terminal cihaz (20) yalnızca verilerin iletilmesine hizmet eder. Tercihen SM sunucusu (60) ve ikinci mobil terminal cihaz (30) arasındaki lojik iletişim kanalı kriptografik olarak güvenliği sağlanmıştır.

SM sunucusu (60) ve ikinci mobil terminal cihaz (30) arasındaki lojik iletişim kanalının kriptografik olarak emniyete alınması örneğin tercihen ikinci mobil terminal cihazın (30) güvenlik elemanı (32) üzerinde bir gizli şifrenin mevcut olması suretiyle elde edilebilmekte olup, bu da yine SM sunucusunda (60) ikinci mobil terminal cihazın (30) ya da güvenlik elemanının (32), örneğin bir Çip- D gibi bir tanımlayıcısı ile kaydedilmiştir. Bu durumda ikinci mobil terminal cihaz (30) bir ilave, şekil 2'de gösterilmemiş olan bir adım içerisinde SM sunucusuna (60) karşı tanımlanabilir ve SM sunucusu (60) abonelik profilini (SP2) bu tanımlayıcı ile bağlanmış olan şifre ile şifrelendirebilir. Teknikte uzman kişinin de görebileceği gibi, bu durumda iletişim kanalı (40) birinci mobil terminal cihaz (20) ve ikinci mobil terminal cihaz (30) arasında, birinci mobil terminal cihaza (20) tanımlayıcının, ikinci mobil terminal cihazın (30) örneğin güvenlik elemanının (32) bir Çip-ID 'sinin bildirilmesi için daha önceki bir zamanda yapılandırılabilir. Burada, birinci mobil terminal cihazın (20) ikinci mobil terminal cihazın (30) ya da güvenlik elemanının (32) tanımlayıcısını ikinci abonelik profili (SP2) sorgusu çerçevesinde mobil kablosuz ağ (50) üzerinden SM sunucusunda (60) (bkz. şekil 2'nin S2 adımı) talep etmesi de düşünülebilir.


10
50
52
54
HLR
60
PLMN
32
20
40
30
22
22
32
25
CPU
35
CPU
26
Bellek
SP1
36
Bellek
SP2

Şekil 1


ME 30
ME 20
PLMN 50
SM 60
S1
Profil SP 1 ile kaydetme
S2
Profil SP2 ile sorgulama
S3
S4
S5
S6
Profil SP2 ile kaydetme
S7

Şekil 2