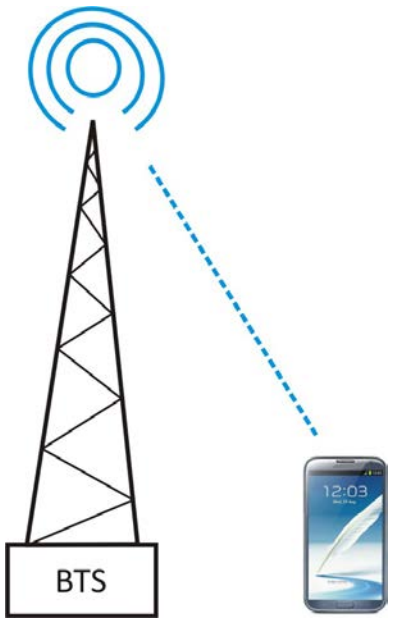
Gezgin Sistemlerde Güvenlik

Prof. Dr. Eşref ADALI

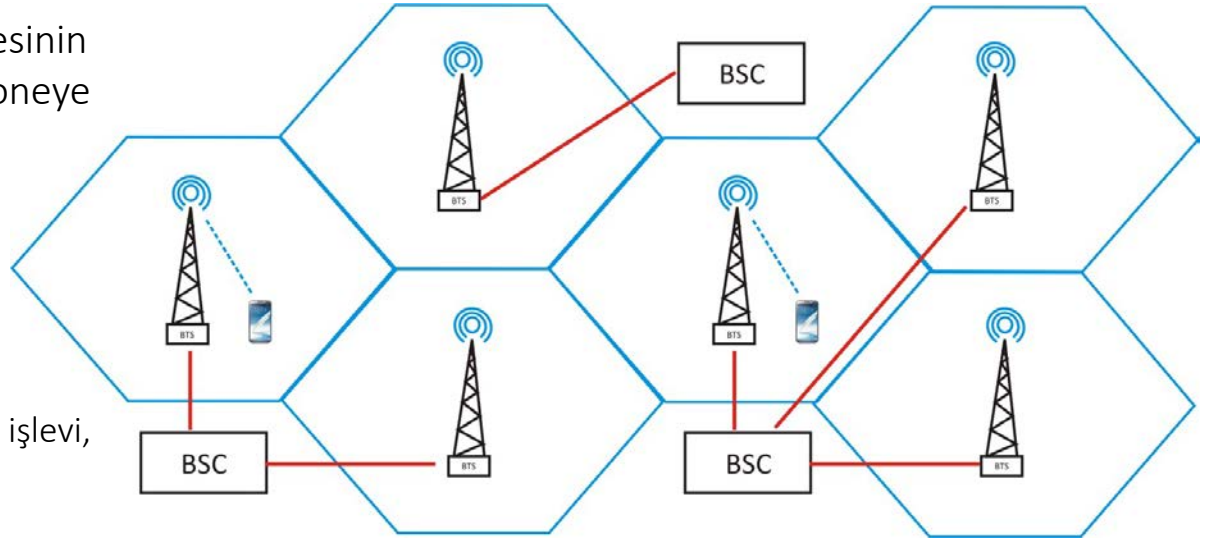
www. Adalı.net

Gezgin Sistemlerin Bileşenleri

- MS (Mobile Station – Gezgin Aygıt) : İçinde SIM kartı barındıran aygıtlara verilen addır.
- BTS (Base Transmitter Station - Alıcı Verici Yer İstasyonu) : Gezgin aygıtın telsiz bağlantısı kurduğu yer istasyonudur.
- BSC (Base Station Controller – Yer İstasyonu Denetçisi) : Yer istasyonunu denetleyen birimdir. Yer istasyonları, belli bir alanı kapsayacak biçimde yerleştirilirler. Dolayısıyla bir yerleşim yerinde, birbirine komşu hücreler oluştururlar. Bir yer istasyonu denetçisi bir ya da daha çok yer istasyonunu denetleyebilir.
- MSC (Mobile Switching Center – Gezgin Telefon Santralı) : Gezgin aygıtlar için telefon santralı görevini gören birimdir.

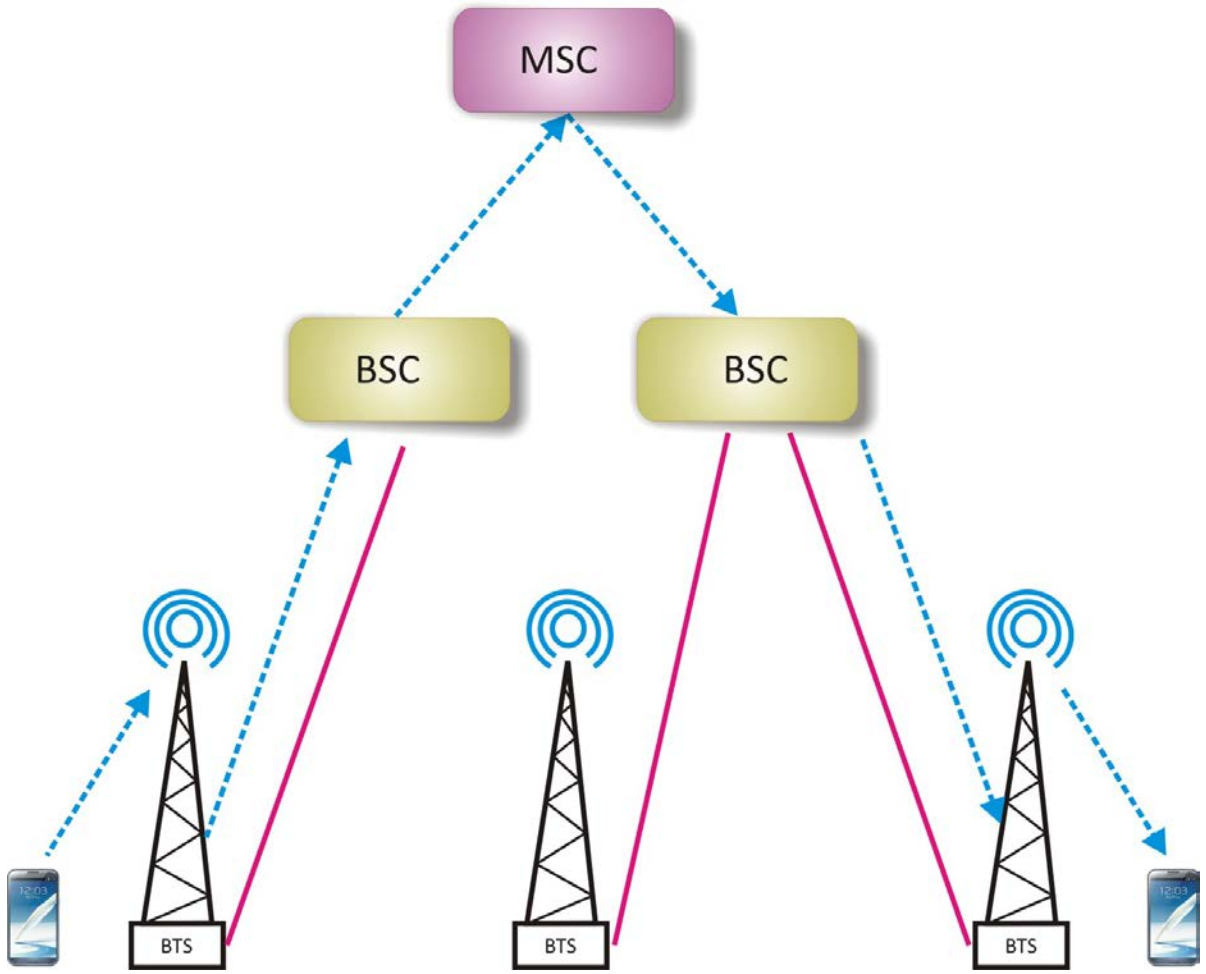


- HLR (Home Location Register – Ana Kütük) : Bir telefon abonesinin kaynak bilgilerini içeren veri tabanıdır. Bu veri tabanında, aboneye ilişkin şu bilgiler yer alır:
  - Kimlik (IMSI ve MSISDN),
  - Numarası,
  - O anda bulunduğu yer,
  - Ek hizmetler,
  - Abonenin durumu (kayıtlı olup olmadığı)
  - Kimlik doğrulama anahtarı ve Kimlik Doğrulama Merkezi (AUC) işlevi,
  - Abonenin dolaşım numarası.



Gezgin Aygıtların Bağlantısı

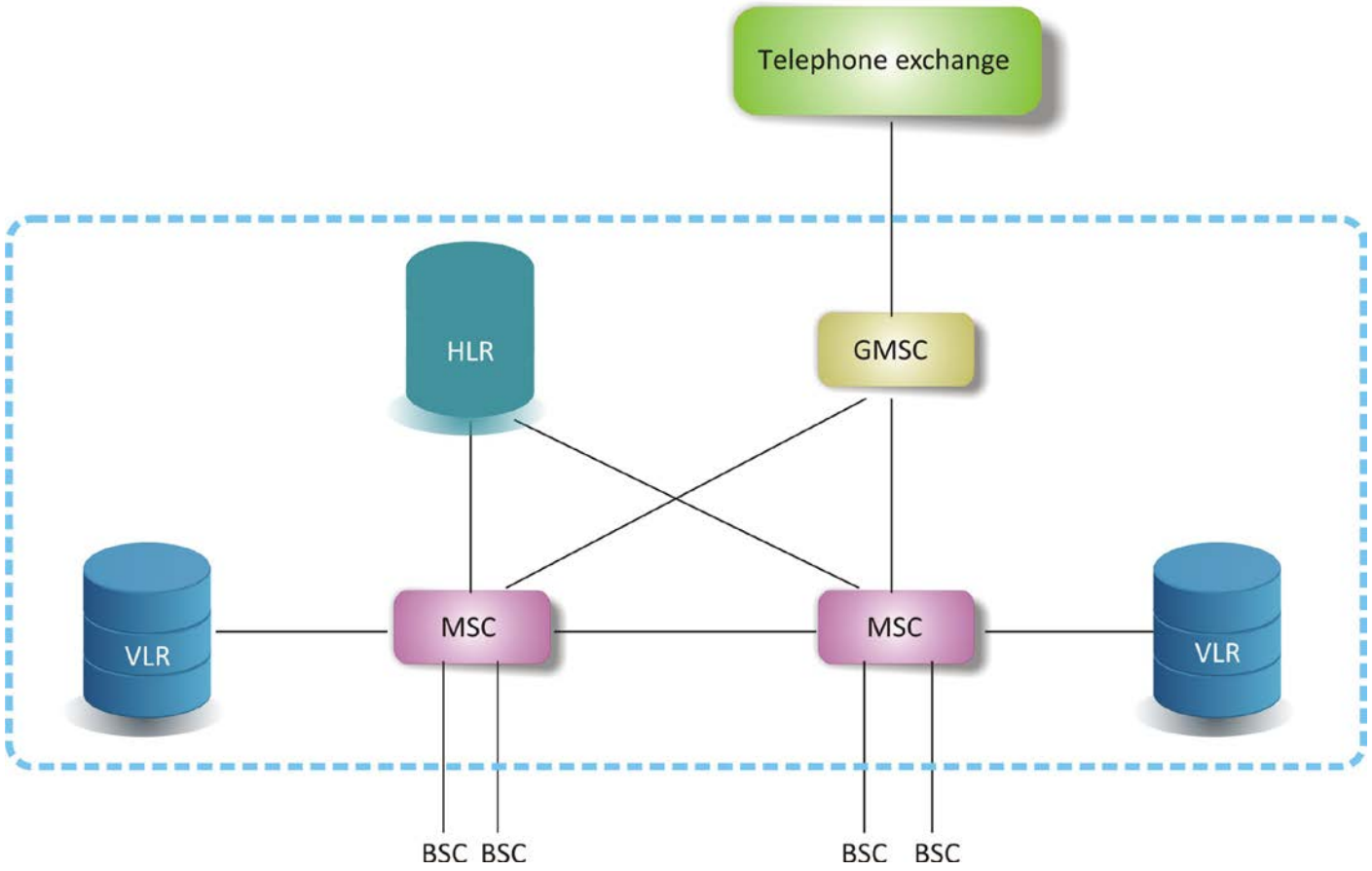
- VLR (Visitor Location Register – Konuk Yeri Kütüğü) : Abonenin telefonunun çalışır durumda olduğu bölgeyi kapsayan Konuk Yeri Kütüğüdür. Bu kütük içerisinde, aboneye ilişkin, Ana Kütükte bulunan çoğu bilgiler yer alır; ancak bunlar, telefon, kapsama alanı içinde kaldığı sürece tutulur, sonra silinir. Konuk Yeri Kütüğü içinde aşağıda belirtilen bilgiler yer alır:
  - Kapsama alanı kimliği (LAI)
  - Abonenin geçici kimliği (TMSI)
  - Gezgin istasyon dolaşım numarası (MSRN)
  - Gezgin aygıtın durumu (Uygun, meşgul, yanıtlamadı)
- GMSC (Gateway MSC – Ağ Geçidi) : Gezgin telefon santralının, sabit telefon santralları ile bağlantısını sağlayan birimdir.
- OMC (Operation and Management Centre – İşletme ve Yönetim Merkezi) : Telsiz ve ağ alt sistemini denetleyen birimdir.



GSM Ağının Yapısı - I

- AuC (Authentication Centre – Kimlik Doğrulama Merkezi) : Güvenlik birimi olarak çalışır. Gezgin aygıtın kimliğini doğrulama ve iletişimi güvenli kılmak için şifreleme işlemini yapar. Bu amaçla;
  - Ki : Abonenin özel kimlik doğrulama anahtarını kullanır,
  - A3 : Kimlik doğrulama algoritmasını kullanır,
  - A8 : şifreleme anahtarı üretimini sağlar.
- EIR (Equipment Identity Register – Aygıt Kimlik Kütüğü) : Gezgin aygıt kayıt işlemini sürdürür. Bu kütük içinde üç türlü liste bulunur:
  - Beyaz liste : Beyaz listede yer alan gezgin aygıtlara bağlantı için yol verilir.
  - Siyah liste : Siyah listede yer alan gezgin aygıtlara bağlantı için yol verilmez. Bunlar çalıntı aygıt olabilir.
  - Gri Liste : Gözetimde olan aygıtlardır.

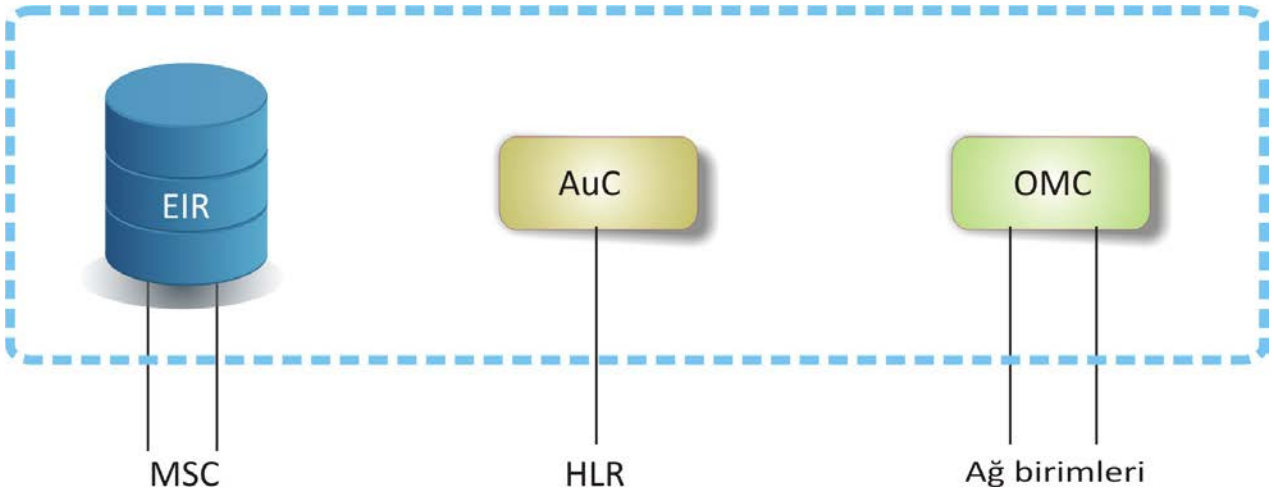
  OMC, AuC ve EIR birlikte işletme Alt Sistemini (Operation Subsystem - OSS) oluştururlar;



GSM Ağının Yapısı - II

- IMSI (International Mobile Subscriber Identity - Gezgin Abone Kimliği) : IMSI'nin içeriğinde sırasıyla şu bilgiler bulunur:
  - Gezgin Ülke Kodu (MCC)
  - Gezgin Ağ Kodu (MNC)
  - Gezgin Abonenin Numarası (MSIN)

  Bu şekilde, abonenin SIM kartını tekil olarak tanımlar.
- TMSI (Temporary Mobile Subscriber Identity – Abone Geçici Kimliği) : Konuk veri kütüğündeki bilgileri içerir. IMSI bilgisini saklar, onun yerine TMSI'yi iletir.
- MSRM (Mobile Station Roaming Number – Dolaşım Numarası) : MSRM'nin içeriğinde sırasıyla aşağıdaki bilgiler yer alır. Bu bilgi VLR tarafından her aygıt için üretilir. HLR için konum bilgisi üretir. IMSI bilgisini gizler.
  - Konuk Ülke Kodu (VCC)
  - Konuk Erişim Kodu (VNDC)
  - O anda Bağlı Olunan Gezgin Santral Kodu
  - Abonenin Geçici Numarası

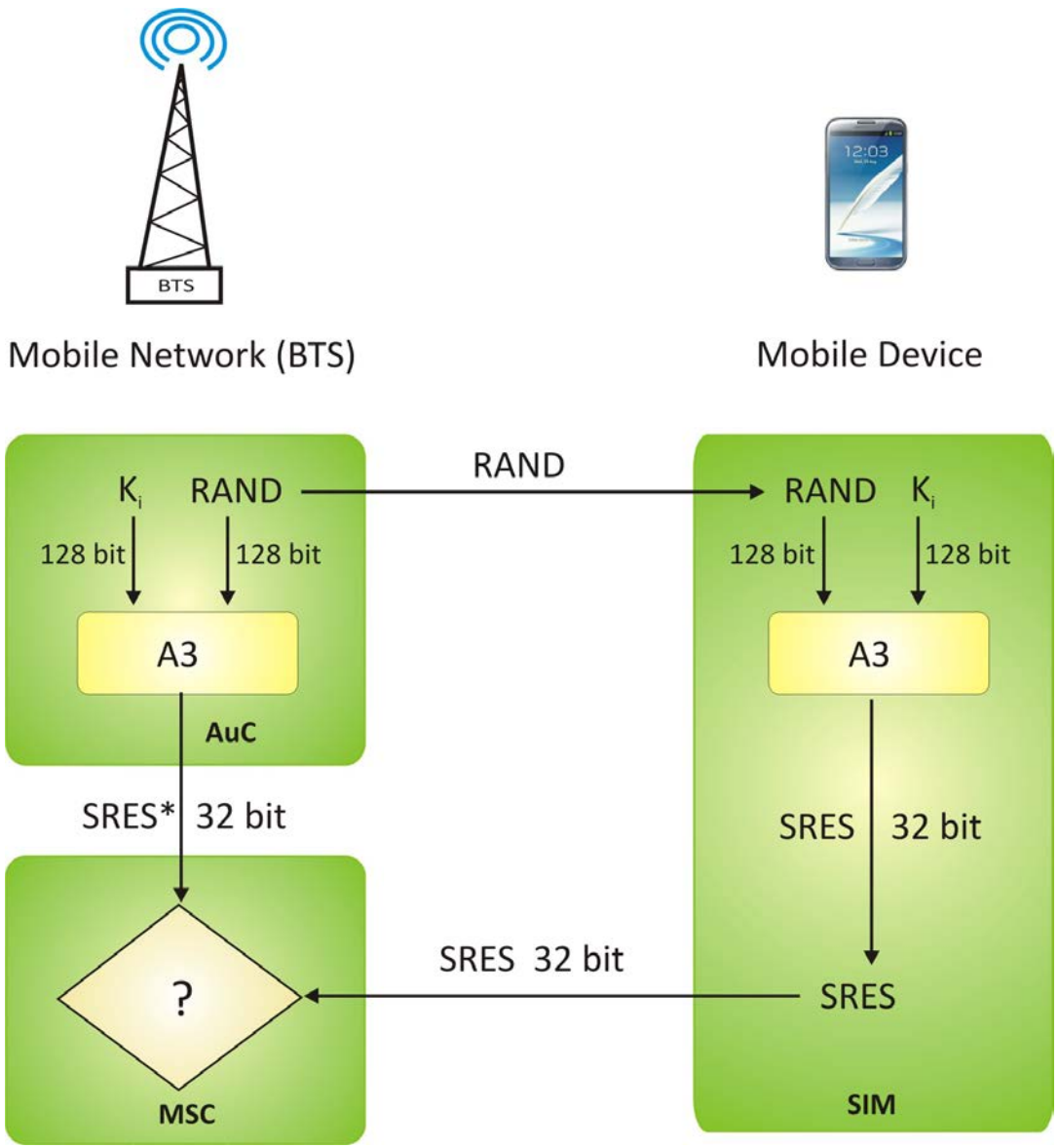


GSM'in Güvenliği

Erişim Güvenliği ve Kimlik Doğrulama : Aygıt sahibi, PIN numarasını girerek, SIM kartını etkinleştirir. SIM kartı, abone olunan GSM ağına bağlanmayı sağlar.

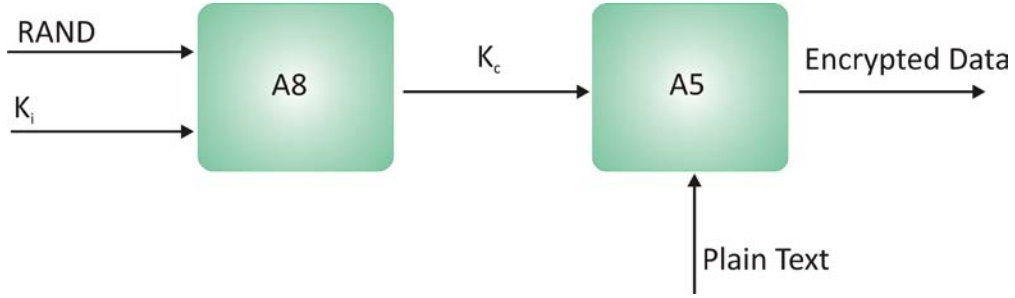
Gizlilik : Telsiz iletişimi sırasında, ses şifrelenerek gizlenmeye çalışılır.

Gerçek Kimliği Saklama : Gezgin geçici kimliği (TMSI) kullanılarak, arayan numaranın kimliği saklanır

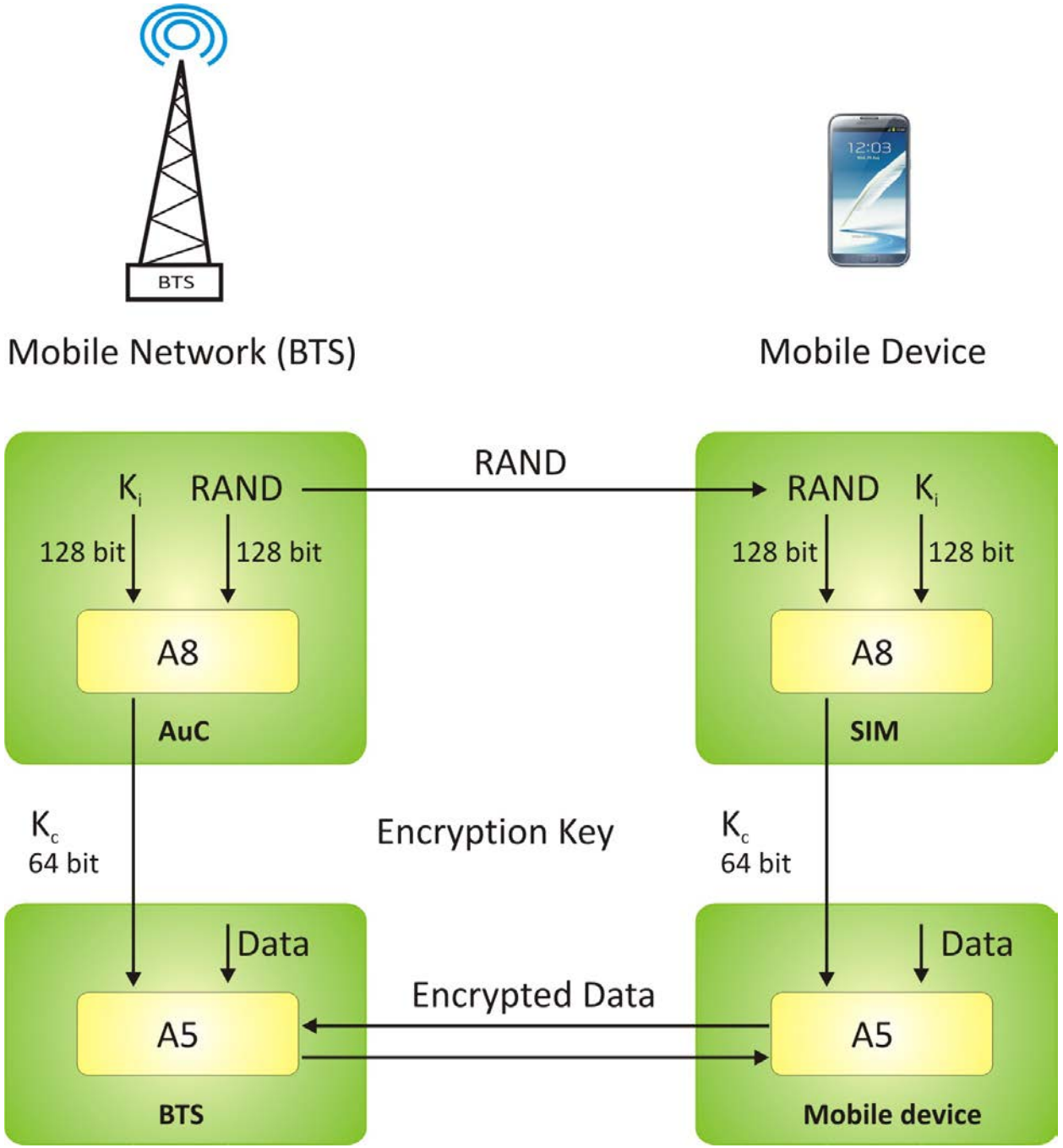


Kimlik doğrulama süreci

Verileri Şifreleme Yöntemi



Verileri şifreleme



GSM’in Algoritmaları

Cep telefonları, dünya genelinde kullanılabilecek biçimde tasarlanmıştır. Bu nedenle, ülkeler arası iletişimde, işletmen kuruluşlar bazı değerleri aralarında takas ederler. Bu değerler RAND, SRES ve Kc dir ve HLR (Ana Kütük)’ten istenir. Dolayısıyla, dolaşılan yerin işletmeni, telefonun SIM kartında bulunan A3 ve A8 algoritmalarını bilemez.

- A3 Asıllama Algoritması : A3 asıllama algoritması, tek yönlü çalışan bir algoritmadır ve GMS işletmeni tarafından belirlenir. Tek yönlü olması nedeniyle, RAND ve Ki ‘yi kullanarak üreteceği SRES’i hesaplama olanağı vardır, ancak geriye doğru Ki ‘yi ve RAND’ı bulmak çok zordur. GSM sisteminde Ki‘nin gizli tutulması temel ilkedir. Bu nedenle, işletmenler güçlü bir A3 algoritması kullanmak zorundadır. Basit bir A3 algoritması güvenlik açığına neden olur.
- A5 şifreleme Algoritması : şifreleme algoritması olarak, günümüzde A5/0, A5/1 ve A5/2 şifreleme algoritmaları kullanılmaktadır. Bunların içinde A5/1 en güçlü olanıdır ve Avrupa’da yaygın olarak kullanılmaktadır. A5/2 daha çok Asya’da kullanılmaktadır. Birleşmiş Milletlerin yaptırımlarının uygulandığı ülkelerde, şifresiz iletişimin (A5/0) kullanılması zorunlu tutulmaktadır.
- A8 şifreleme Anahtarı Algoritması : Bu algoritma da seçimli bırakılmıştır. Çoğunlukla A3 ve A8 algoritmalarının özetini üreten COMP128 Hash algoritması kullanılmaktadır. COMP128 Kc ve SRES’i aynı anda üretmektedir.

Genel Değerlendirme

- GSM sisteminde kullanılan algoritmalar gizli tutulmaktadır. Genel kural gereği, içeriği bilinmeyen algoritmalar her zaman güvenlik açığına neden olur. Nitekim 1998 yılında, U.C. Berkley'den iki araştırıcı SDA (Smartcard Developer Associaton) ile birlikte SIM kartı içindeki COMP128 algoritmasını çözebildiler. Böylece birkaç saat içinde Ki 'yi bulabildiler. Aynı takım Kc yi de elde ettiklerini gösterdiler. Bu sırada 64 bitlik Kc içinde 54 bitin kullanıldığını geri kalan 10 bitin hepsinin sıfır olduğunu gösterdiler.
- Zayıf anahtar kullanılmasının nedeni olarak, hükümetlerin bu yönde istekleri olduğu anlaşıldı. Hükümetler, gerektiğinde şifrelenmiş konuşmaları kolayca çözebilmeleri için böyle kolay bir şifreleme anahtarı seçilmiş olabileceği sonucuna varıldı.
- Söz konusu deney, laboratuvar ortamında gerçekleştirilmiştir. Ortam dinlemesi yöntemiyle de yapılabileceği açıktır. 1999'da bir grup Amerikalı araştırmacı Asya'da kullanılan A5/2 algoritmasını çözdüler.
- 1999'da ortam dinleme yöntemiyle A5/1'in de İsrailli uzmanlarca kısa sürede çözüldüğü görülmüştür.
- Hatırlanacağı gibi, A5/0 güvensiz iletişim ortamı sunmaktadır. Bu özellikte bir yer istasyonunu kurmanın bedeli 30.000,-TL dolayındadır. Böyle bir istasyonu, gezgin biçimde oluşturup, konuşmasını dinlemek istenen kişinin yakınına gidildiğinde, aradaki adam yöntemiyle, telefon konuşmasını dinlemek olasıdır.
- GSM'in bilinen bu güvenlik açıklarını gidermek amacıyla ilk olarak COMP128-2 kullanılmaya başlanmıştır. Ardından A5/3 algoritması A5/2'nin yerini almıştır. Güvenlik konusundaki önlem çalışmaları halen devam etmektedir.