UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

# ATTACCO DI TIPO DENIAL OF SERVICE ALLE RETI CELLULARI

**Relatore: Prof. Mauro Migliardi**

**Laureando: Stefano Leggio**

**ANNO ACCADEMICO: 2020-2021**

**Data di laurea: 20/09/2021**

# Indice

# Elenco delle figure

# 1 Sistema di autenticazione

Il meccanismo di autenticazione è la procedura per verificare che un determinato dispositivo è abilitato a connettersi alla rete. Questo procedimento avviene tramite il riconoscimento dell'identificativo del cellulare (IMSI) e Successivamente avviene l'*Authentication and key agreement* (AKA), procedimento in cui il *core network* abilita un dispositivo a connettersi.
In questo capitolo verranno trattati le procedure di autenticazione per le generazioni dal 2G al 5G, il 1G è stato escluso poiché ha un funzionamento completamente analogico.

## 1.1 2G

Il sistema di autenticazione di seconda generazione utilizza principalmente due codici univoci della SIM e del MS:

- IMSI ovvero un codice identificatvo della SIM
- IMEI ovvero un codice identificativo del MS

Questi due codici saranno necessari anche per le prossime generazioni fino al 4G.
La procedura di autenticazione di un MS segue questi passaggi:

1. Il MS invia l'IMSI alla BTS di riferimento che lo inoltra al *Core Network*, questo avviene ogni volta che il MS vuole connettersi al *network* e non risulta già risultato presso la rete di riferimento. In caso lo fosse, verrà utilizzato il TMSI *Temporary MobileSubscriber Identity* per preservare il suo anonimato.
2. L'AuC cerca la chiave Ki associata all'IMSI e insieme a un numero casuale RAND genera un codice SRES che verrà salvato nel VLR.
3. Viene inviato al MS il RAND generato.
4. La stessa procedura viene fatta dal MS, che genera quindi il suo SRES e lo invia al VLR
5. Il VLR confronta se l'SRES ricevuto corrisponde a quello generato dall'AuC, se corrispondono l'autenticazione risulta effettuata con successo e viene generato,salvato e inviato il TMSI.

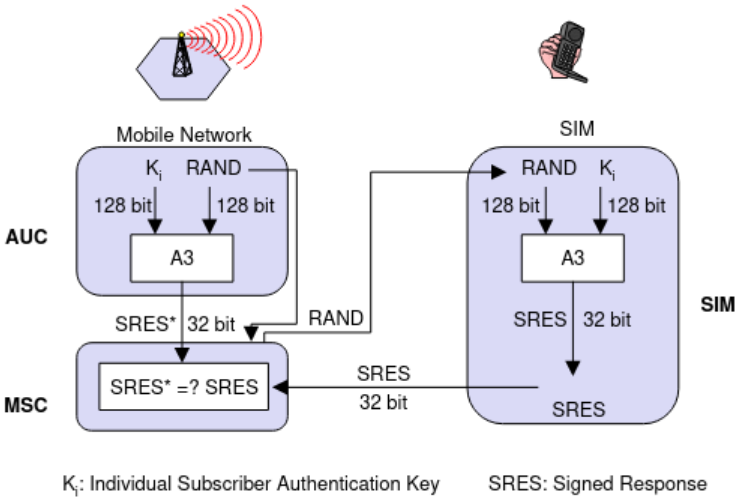


Figura 1: Autenticazione nelle reti 2G

## 1.2 3G

L'autenticazione nell'architettura di terza generazione è molto simile a quella precedente salvo i seguenti miglioramenti:

- Viene introdotta l'autenticazione mutua per prevenire l'autenticazione a false *Base stations*.
- La lunghezza della chiave Ki viene incrementata da 64 a 128 bit.

## 1.3 4G

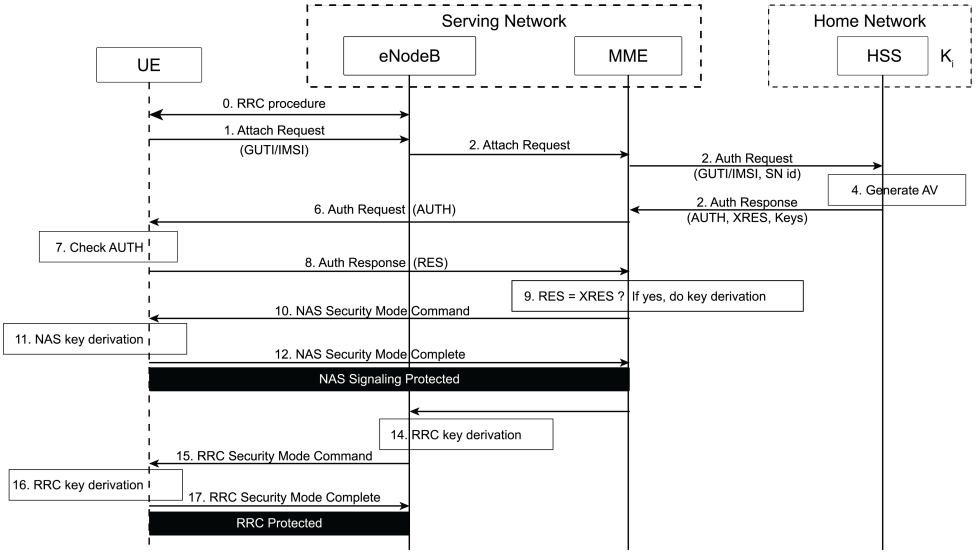


Figura 2: Autenticazione nelle reti 4G

## 1.4 5G

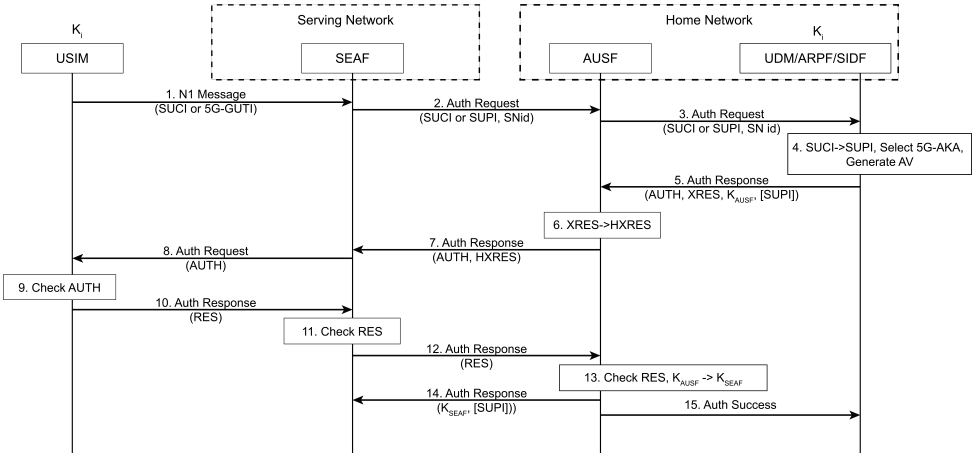


Figura 3: Autenticazione nelle reti 5G