BEVEILIGING VAN MOBIELE NETWERKEN

beveiliging in GSM

Fabian van den Broek

Radboud University Nijmegen
CodeYard

24 April 2010

Beveiliging van Mobiele Communicatie Netwerken

Wat wil je allemaal beveiligen in mobiele communicatie?

Beveiliging van Mobiele Communicatie Netwerken

Wat wil je allemaal beveiligen in mobiele communicatie?

- geheimhouding van de communicatie
- geheimhouding verkeersgegevens (wie belt wie?)
- alleen toegang als je betaald hebt
- garantie dat je de juiste persoon spreekt
- ...

Beveiligingsmethoden

- Authenticatie
- Encryptie

GSM

GSM feiten

GSM feiten

- $ 600 Miljard

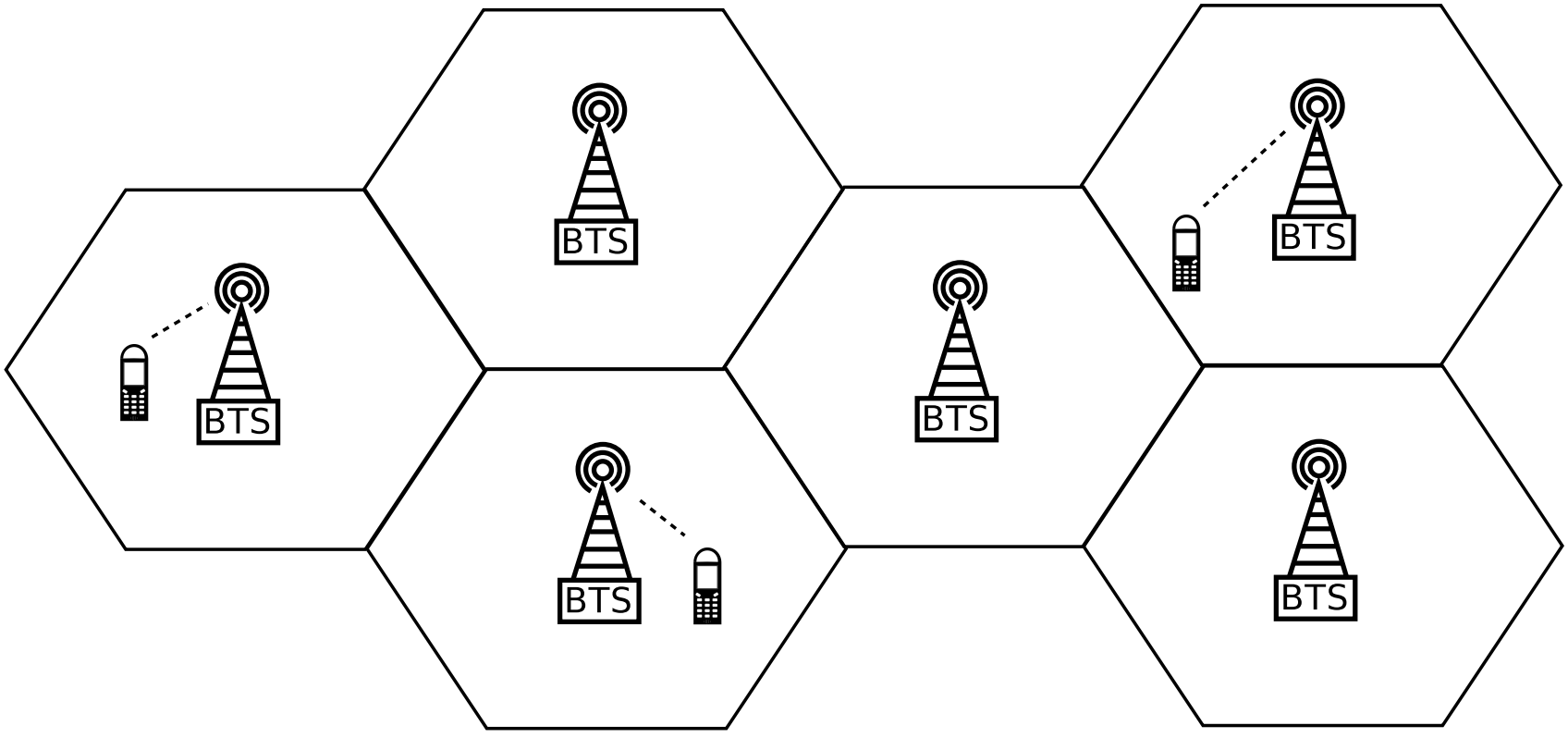
GSM feiten

- $ 600 Miljard
- 90% van de wereldbevolking heeft bereik

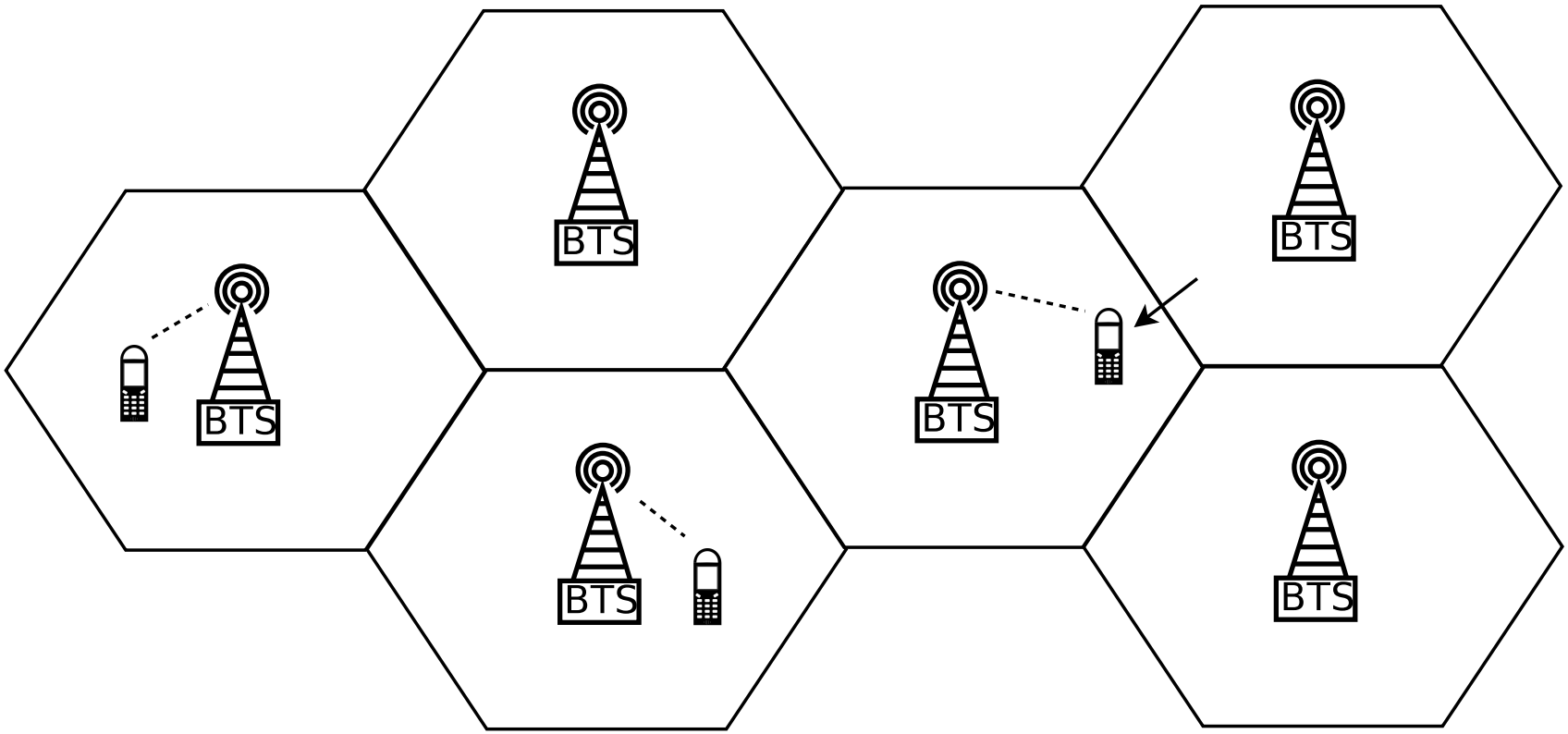
GSM feiten

- $ 600 Miljard
- 90% van de wereldbevolking heeft bereik
- 4.1 Miljard gebruikers

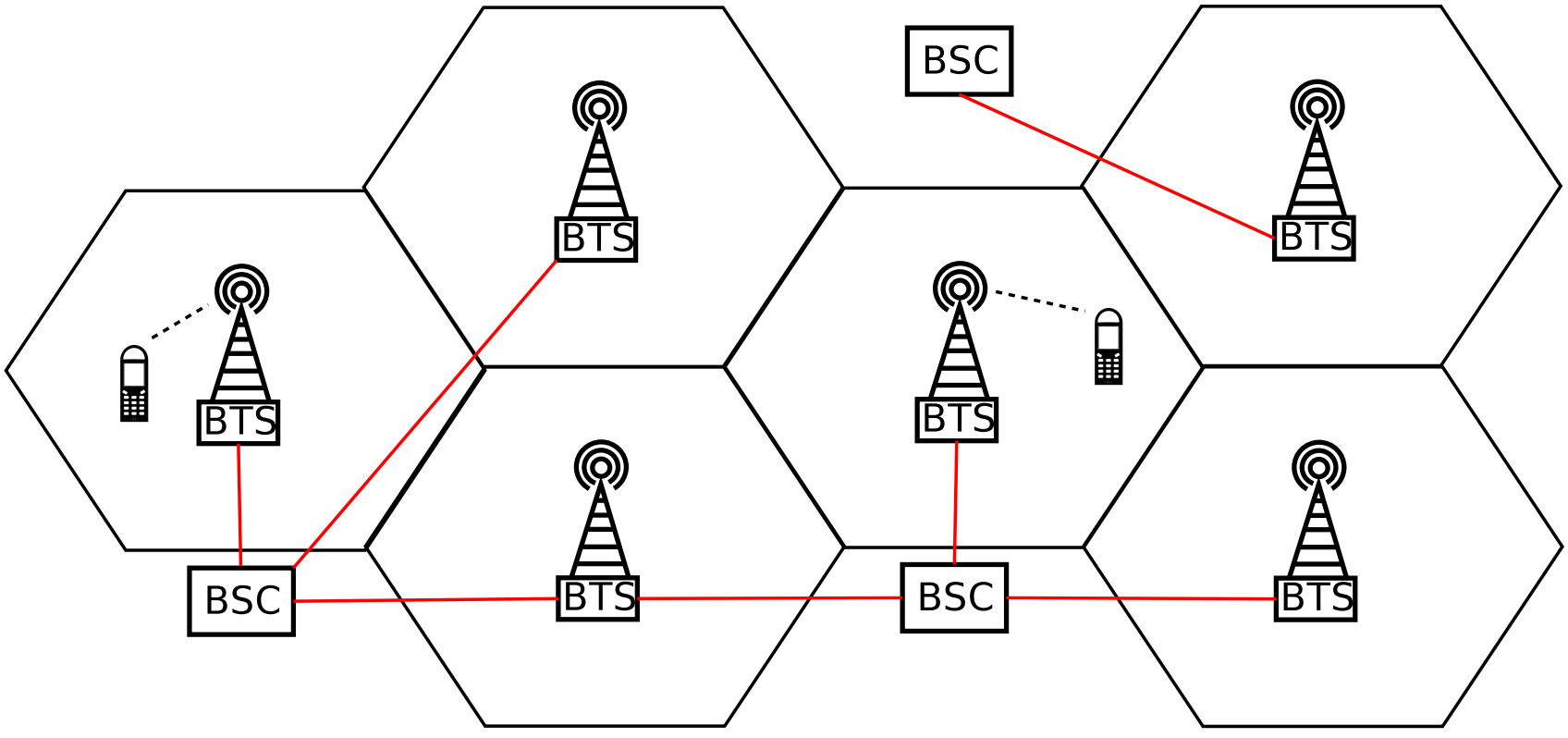
Cellular technology



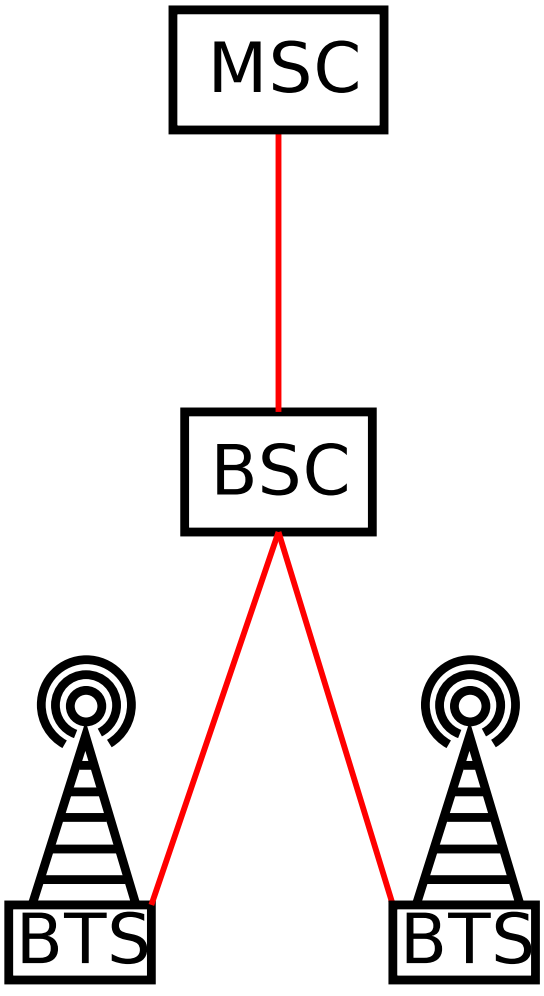
Cellular technology

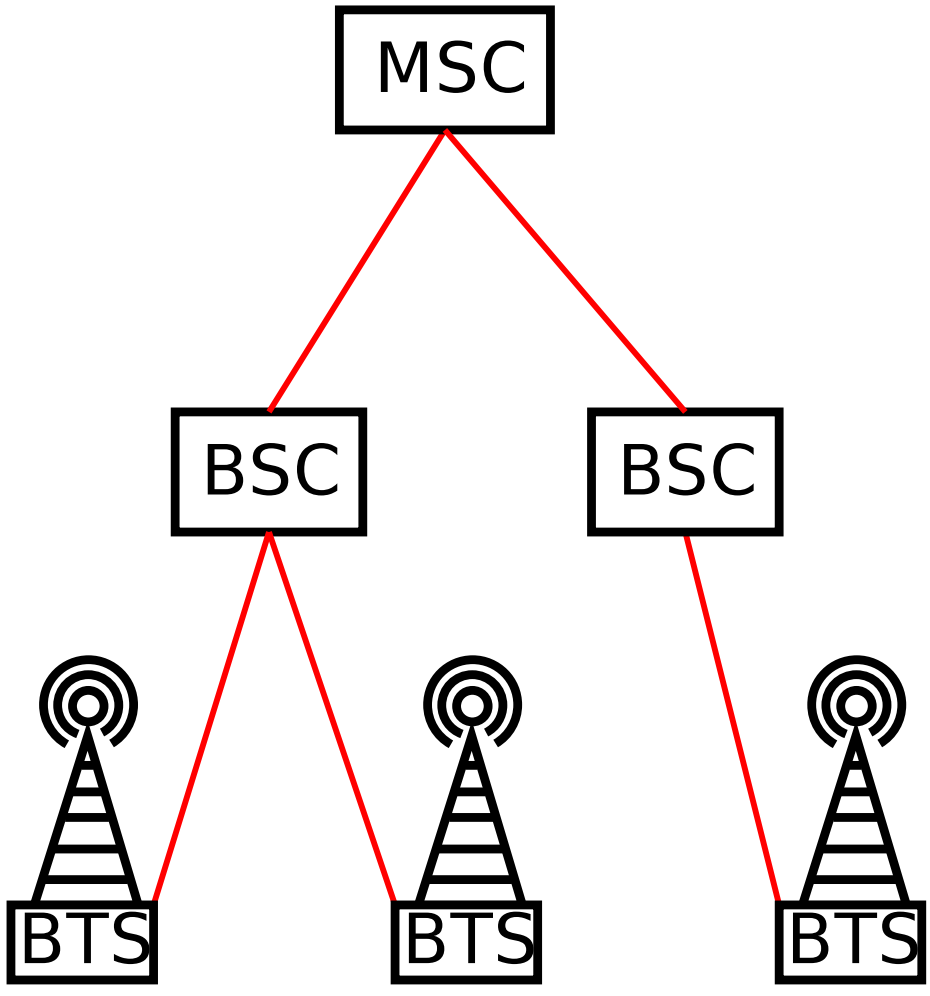


GSM system overview

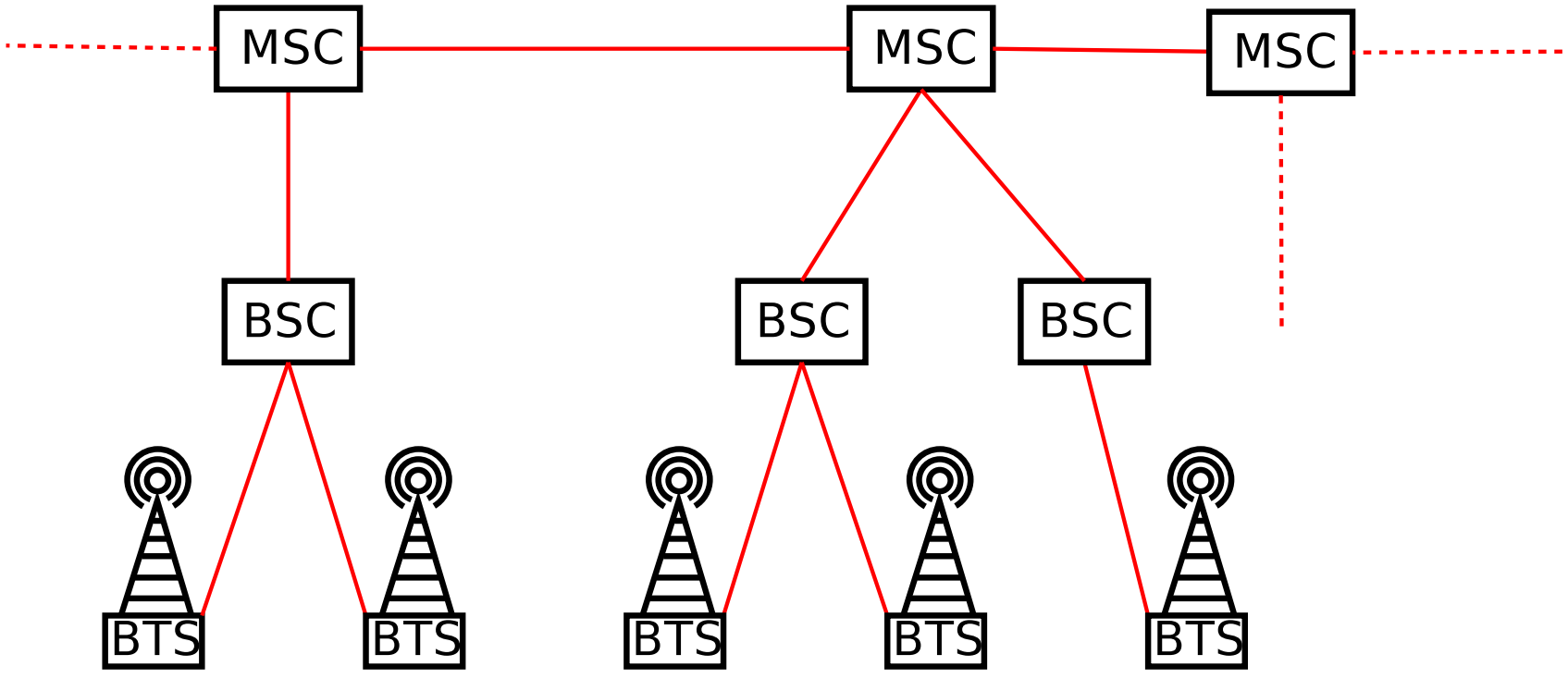


GSM system overview

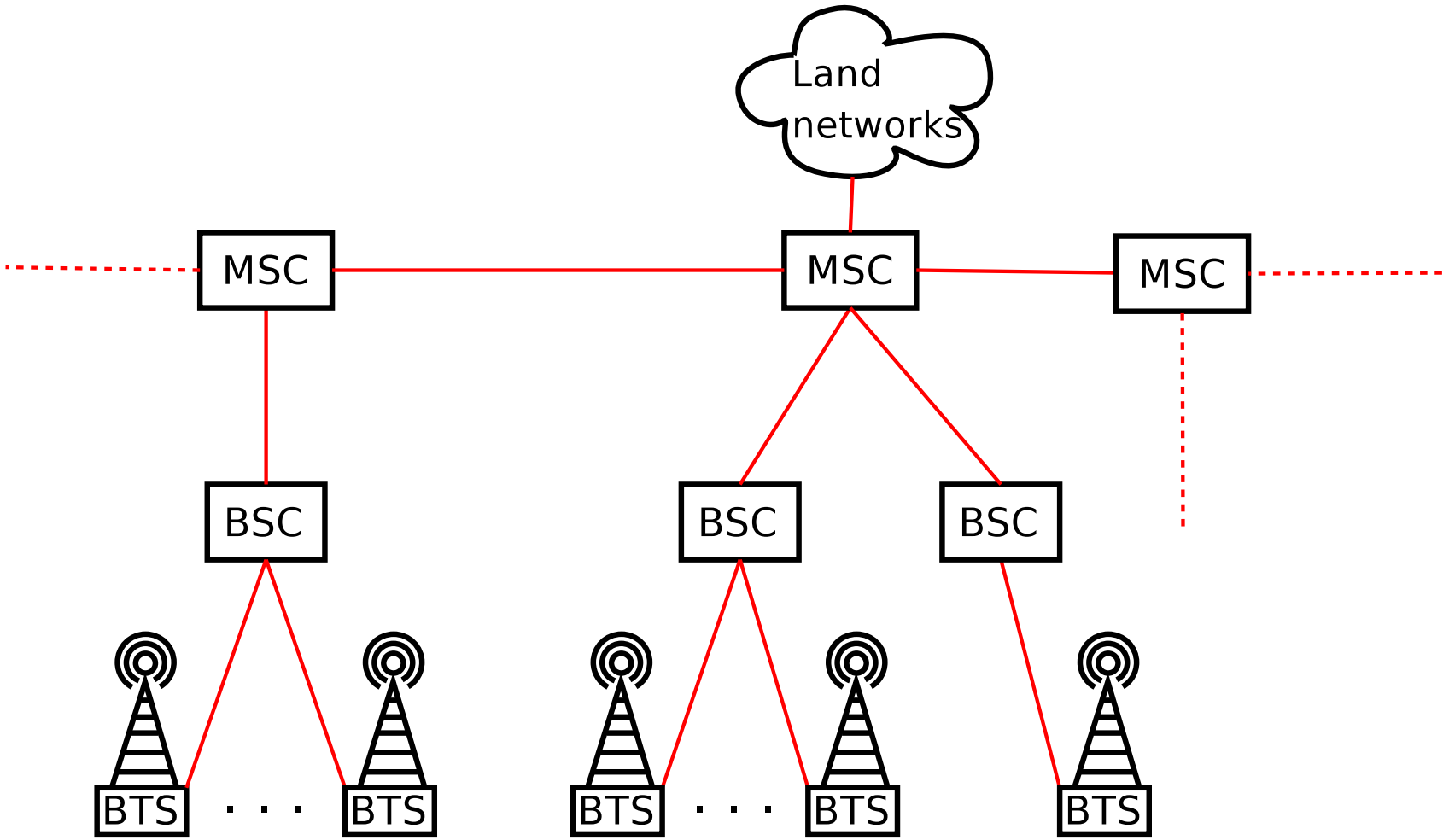




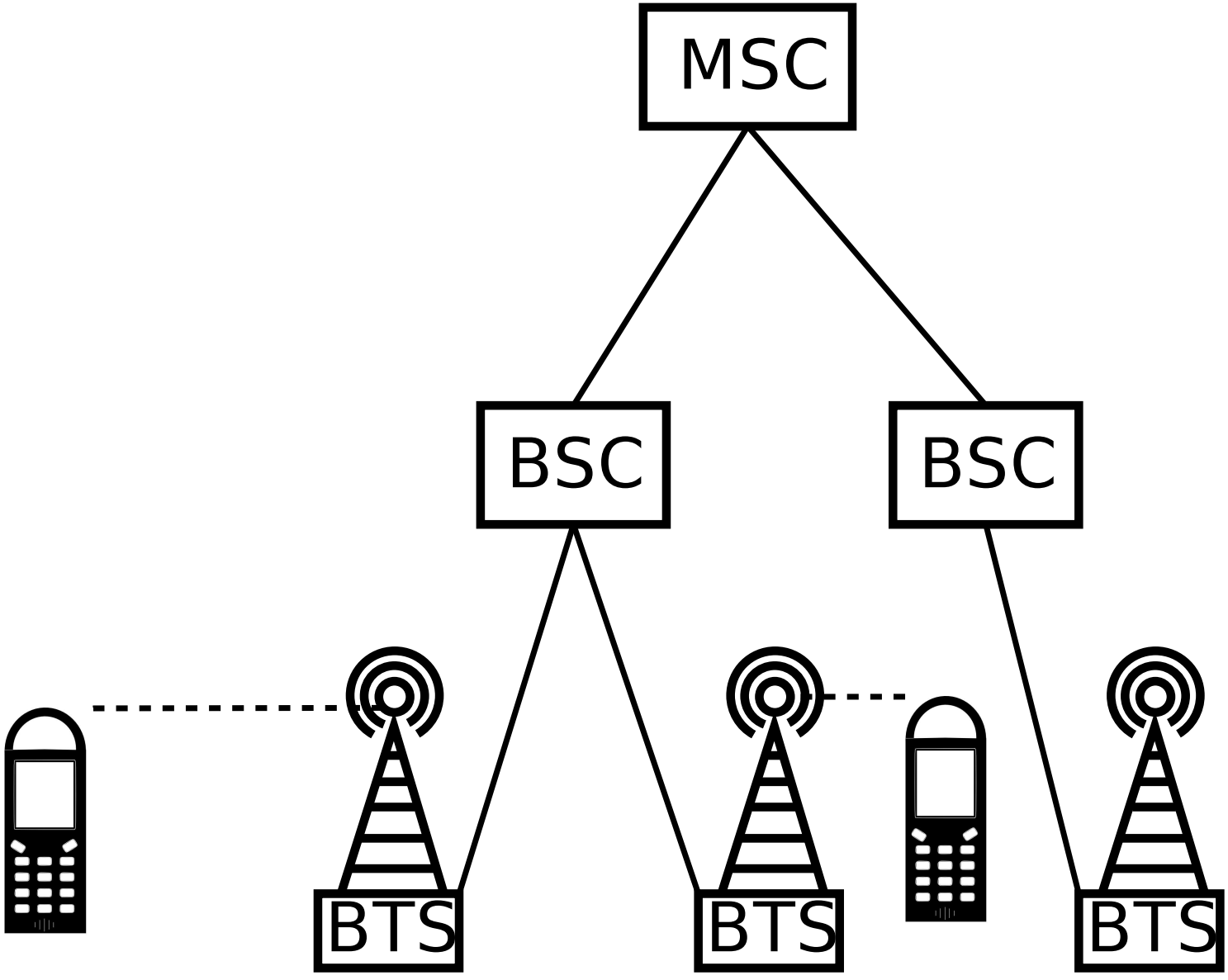
GSM system overview



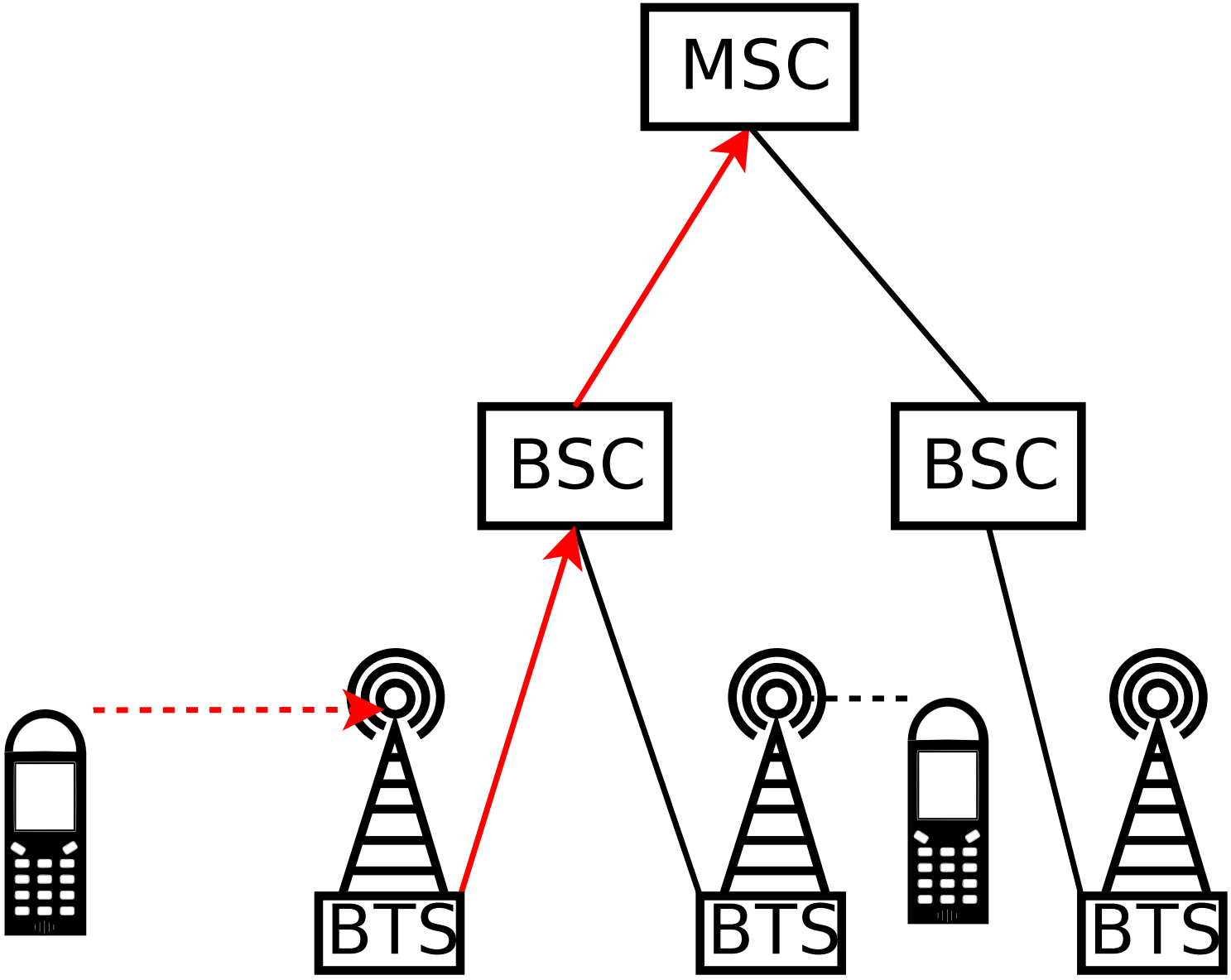
GSM system overview



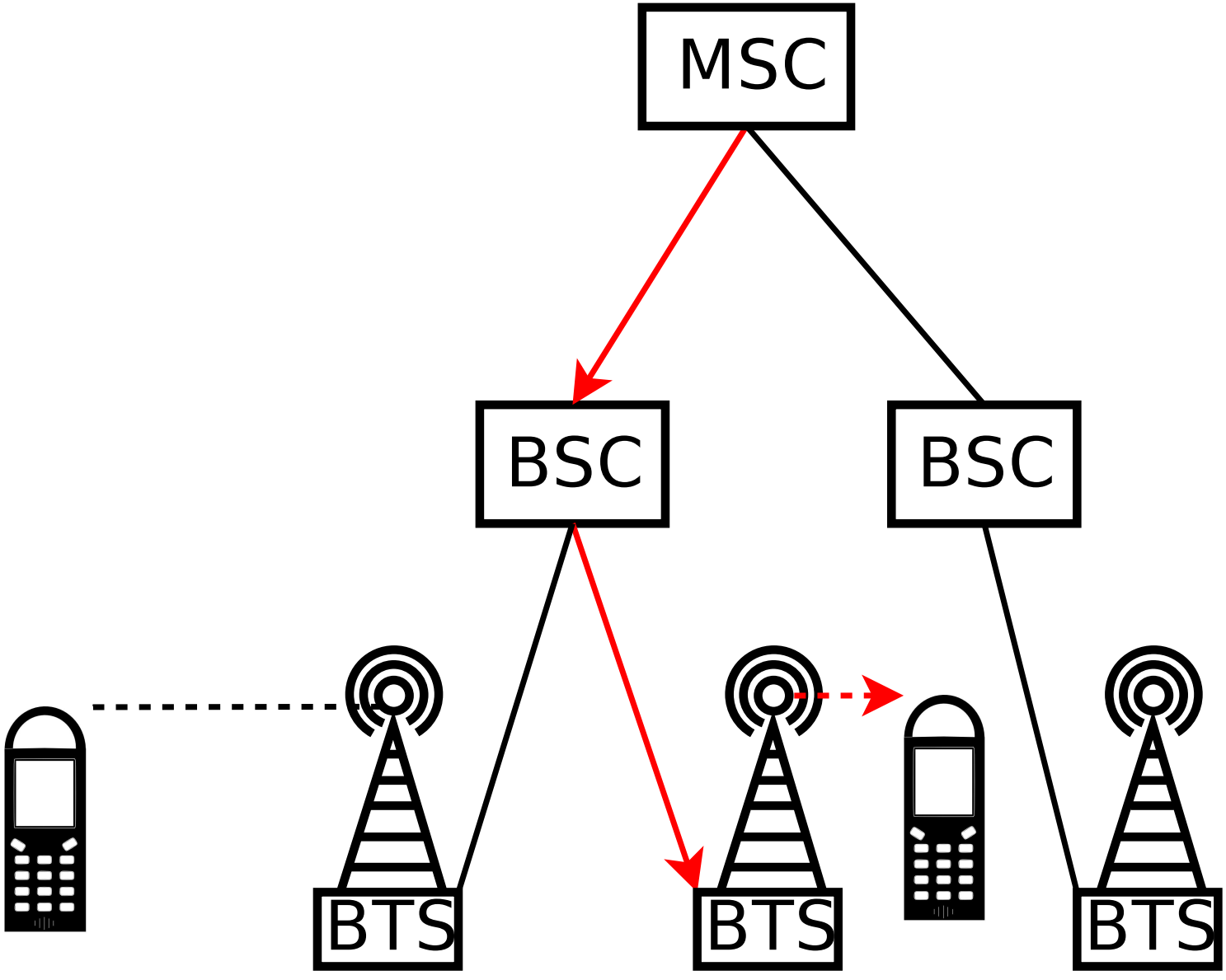
GSM system overview



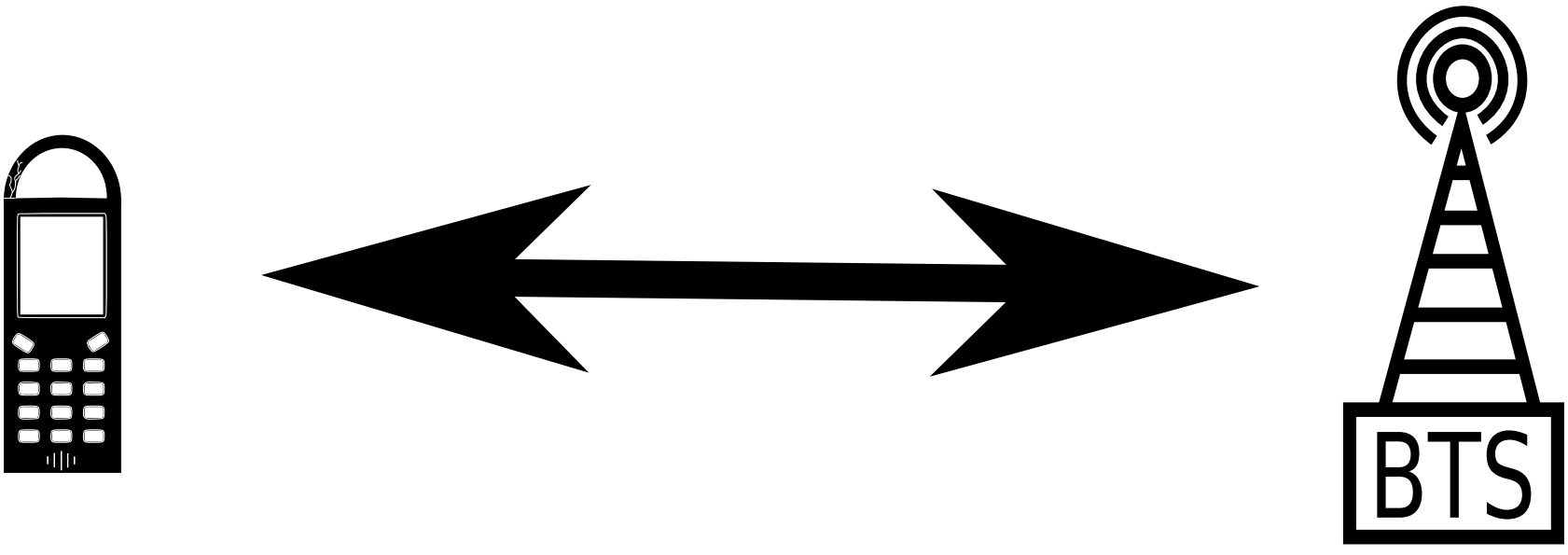
GSM system overview



GSM system overview



The Um interface



Beveiliging in GSM

Identificatie VS. Authenticatie

Identificatie / Authenticatie

Identificatie

Geef je indentiteit

- Je naam
- Een nummer

“Fabian van den Broek”

Authenticatie

Bewijs je identiteit

- Toon paspoort
- geef wachtwoord
- scan vingerafdruk

Identificatie / Authenticatie

Identificatie

Geef je indentiteit

- Je naam
- Een nummer

“Fabian van den Broek”

Authenticatie

Bewijs je identiteit

- Toon paspoort
- geef wachtwoord
- scan vingerafdruk

Identificatie / Authenticatie

Identificatie
Geef je indentiteit

- Je naam
- Een nummer

“Fabian van den Broek”

Authenticatie
Bewijs je identiteit

- Toon paspoort
- geef wachtwoord
- scan vingerafdruk

Identificatie / Authenticatie

Identificatie
Geef je indentiteit

- Je naam
- Een nummer

Authenticatie
Bewijs je identiteit

- Toon paspoort
- geef wachtwoord
- scan vingerafdruk

“Fabian van den Broek”

Identificatie / Authenticatie

Identificatie
Geef je indentiteit

- Je naam
- Een nummer

Authenticatie
Bewijs je identiteit

- Toon paspoort
- geef wachtwoord
- scan vingerafdruk

“Fabian van den Broek”

Identificatie / Authenticatie

Identificatie
Geef je indentiteit

- Je naam
- Een nummer

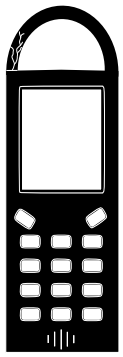
“Fabian van den Broek”

Authenticatie
Bewijs je identiteit

- Toon paspoort
- geef wachtwoord
- scan vingerafdruk

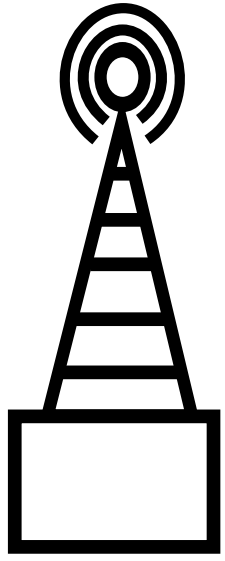
Authenticatie in eerste generatie netwerken

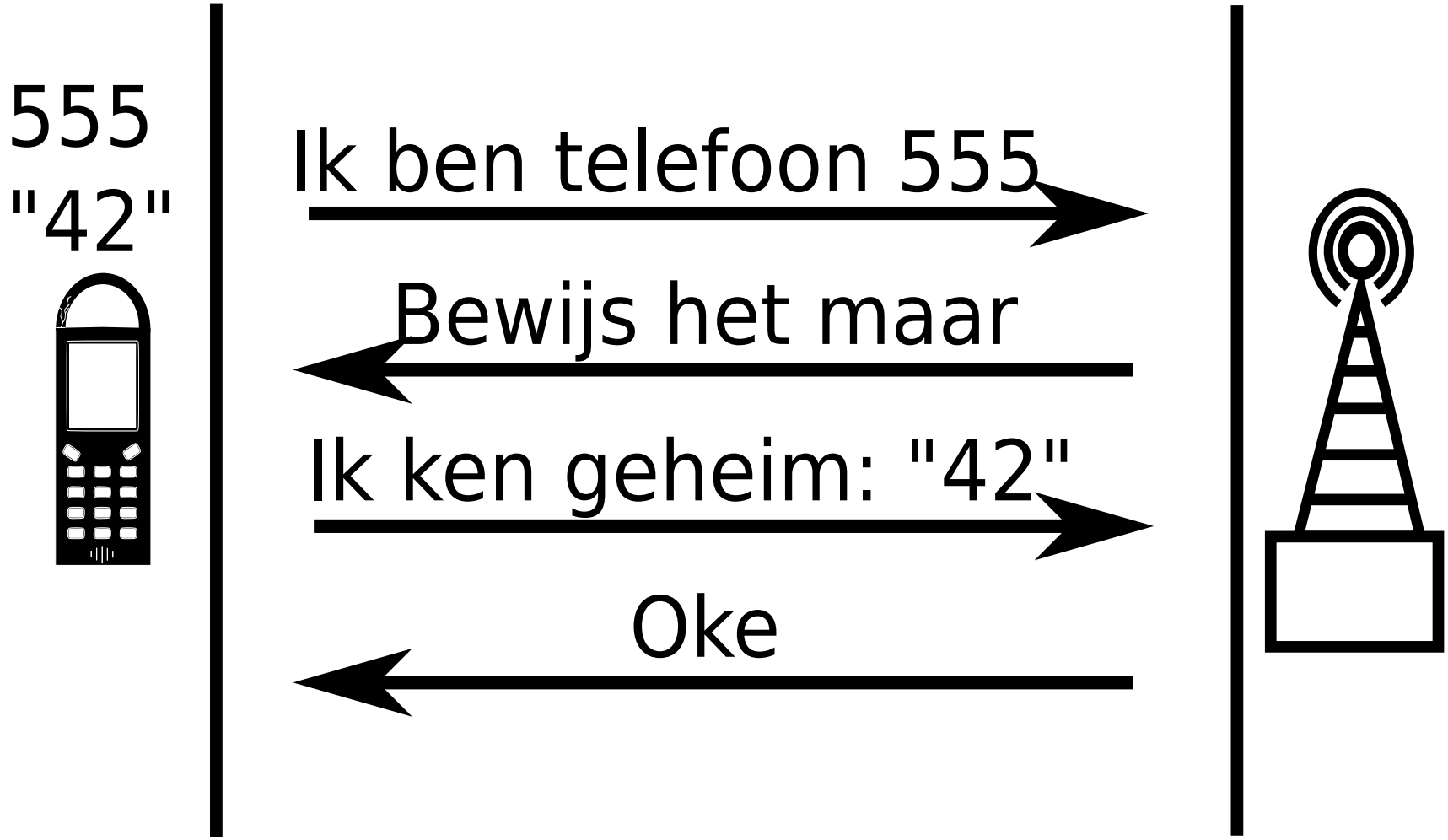
555
"42"



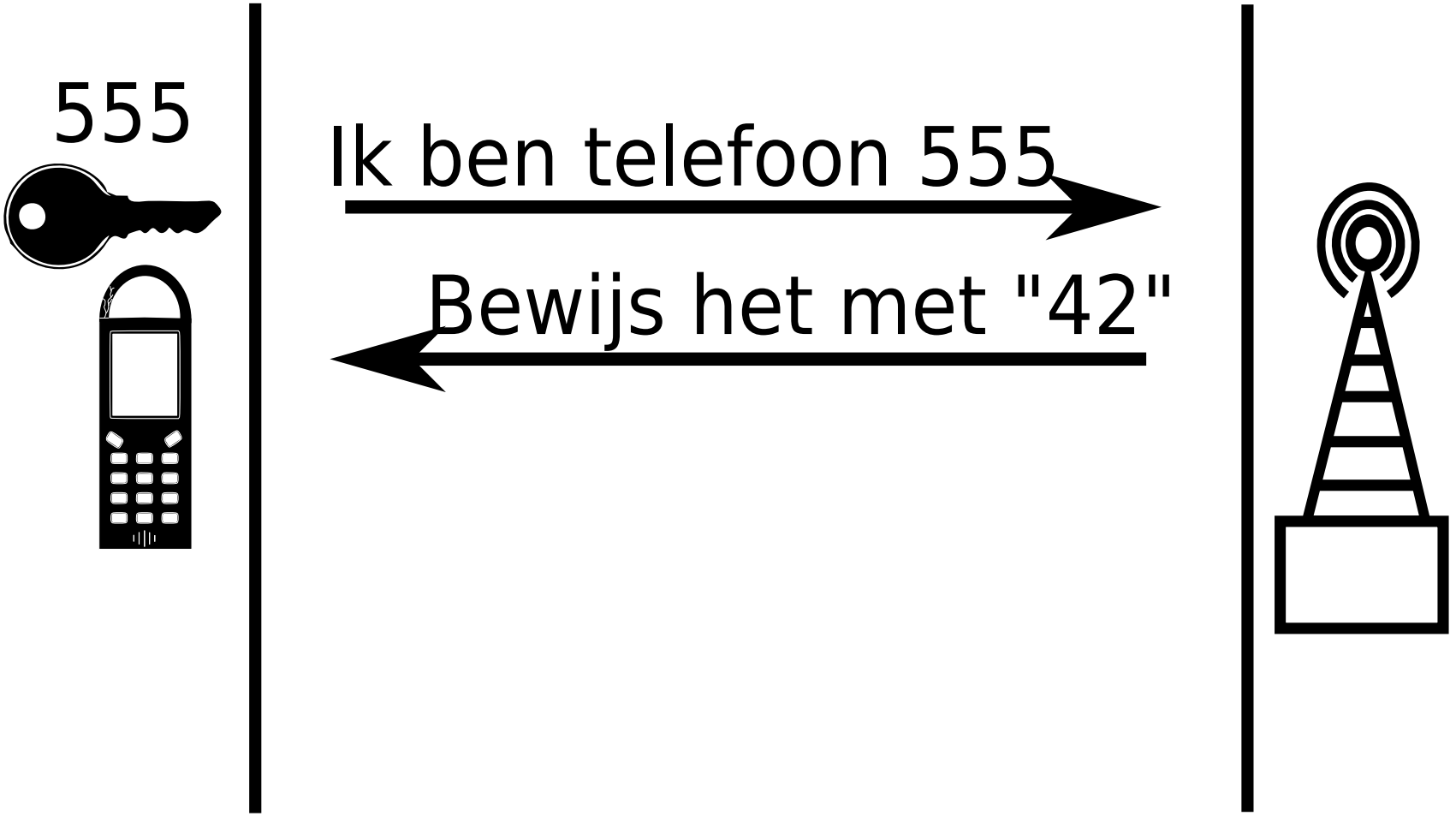
Ik ben telefoon 555

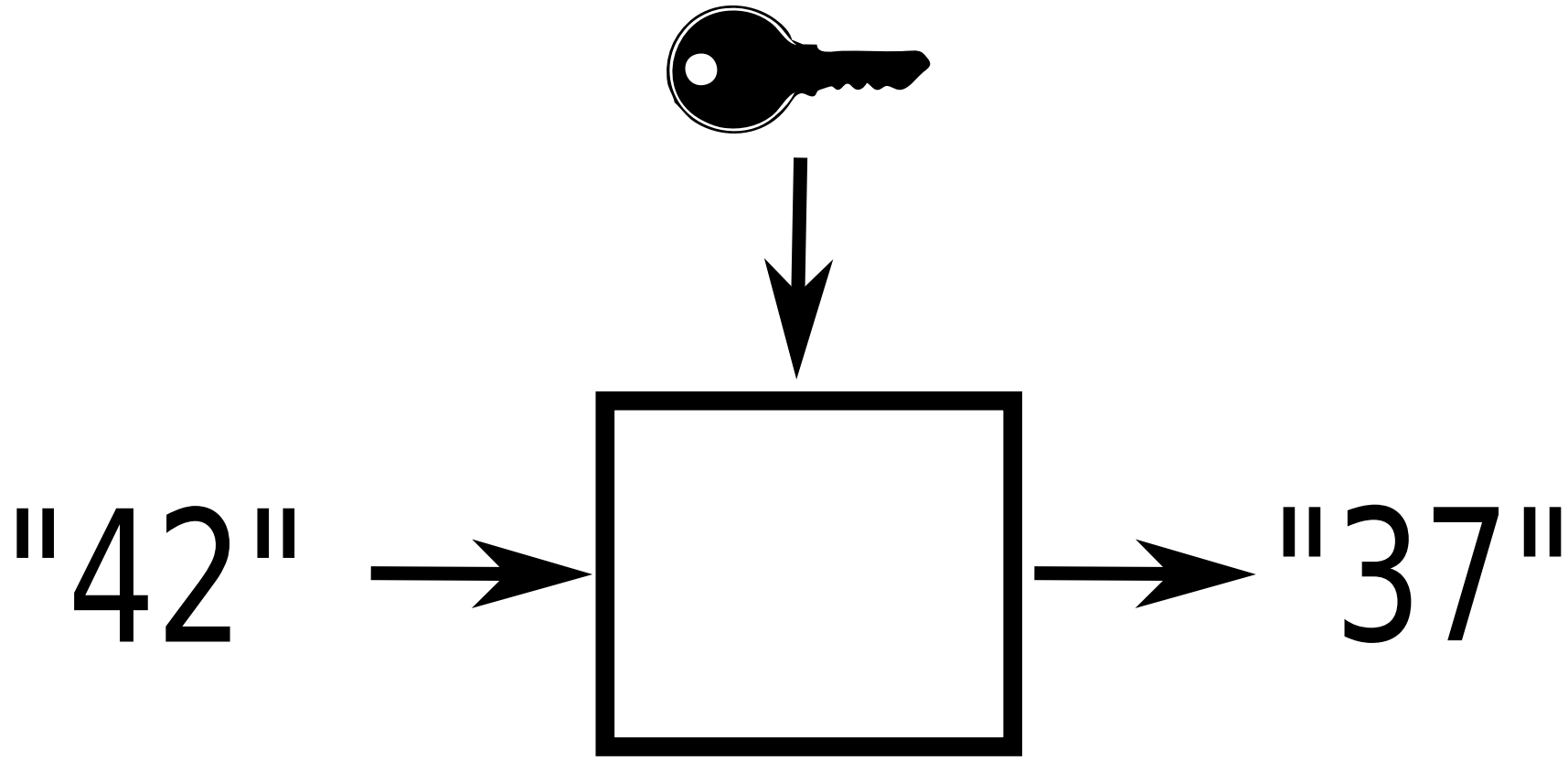
Bewijs het maar




555
"42"
Ik ben telefoon 555
Bewijs het maar
Ik ken geheim: "42"
Oke

Authenticatie in tweede generatie netwerken (GSM)


555
Ik ben telefoon 555
Bewijs het met "42"


"42"
"37"


555
Ik ben telefoon 555
Bewijs het met "42"
Het antwoord: "37"
Oke

Identificatie / Authenticatie in GSM

Identificatie

- Telefoonnummer
- IMEI
- IMSI
- Netwerkidentiteit

Authenticatie

- Geheime sleutel

Identificatie / Authenticatie in GSM

Telefoon wordt geauthenticeerd
Zendmast wordt geïdentificeerd

KPN system information

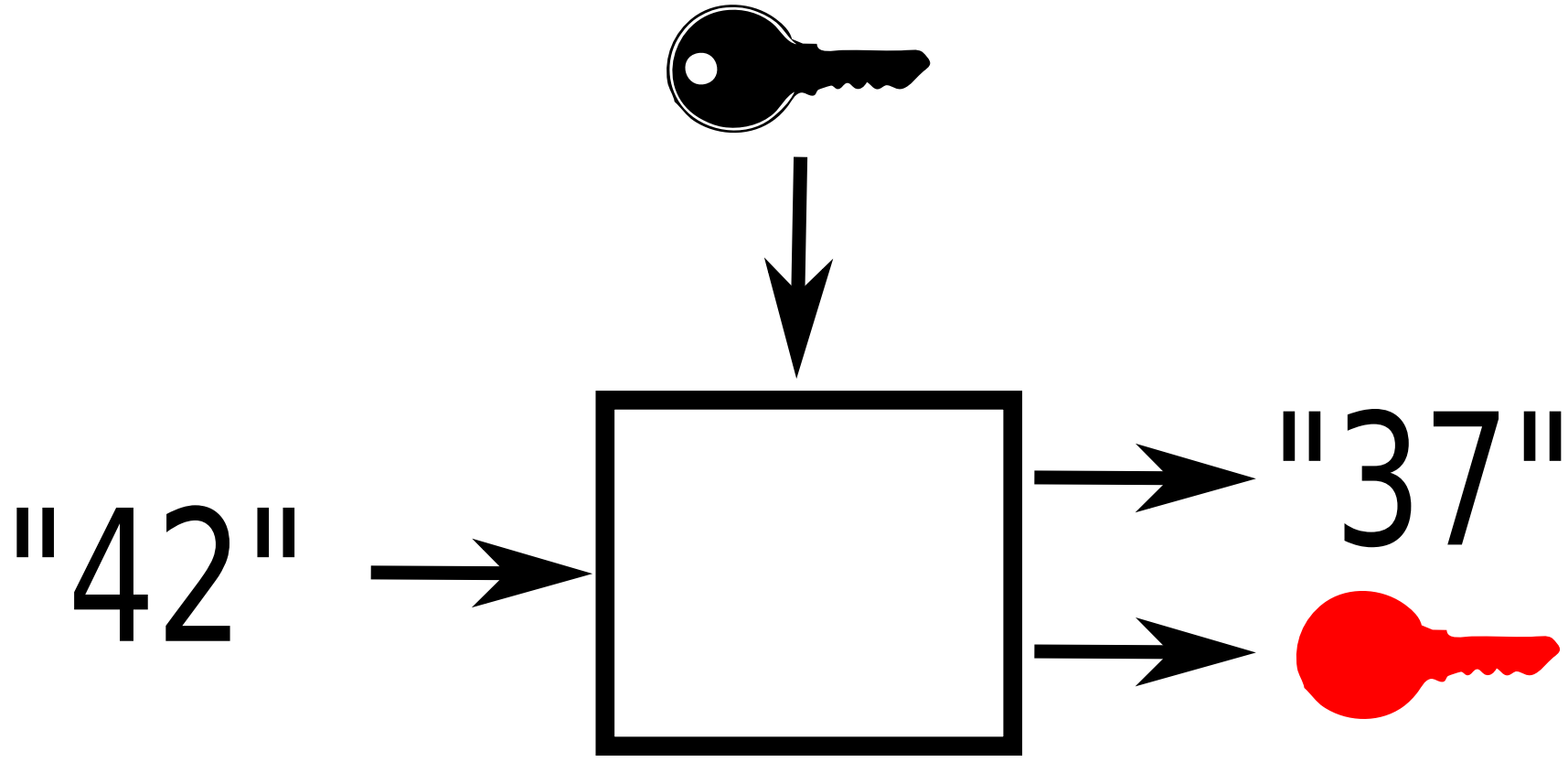
```
1: 49 06 1b 32 22 02 f4 80  – 11 7f d8 04 28 15 65 04 – a9 00 00 1c 13 2b 2b
    0: 49 010010–– Pseudo Length: 18
    1: 06 0––––––– Direction: From originating site
    1: 06 –000–––– 0 TransactionID
    1: 06 ––––0110 Radio Resouce Management
    2: 1b 00011011 RRsystemInfo3C
    3: 32 12834    [0x3222] Cell identity
    5: 02 204      Mobile Country Code (Netherlands)
    6: f4 08f      Mobile Network Code (KPN Telecom B.V.)
    8: 11 4479     [0x117f] Local Area Code
   10: d8 1––––––– Spare bit (should be 0)
   10: d8 –1––––– MSs in the cell shall apply IMSI attach/detach procedure
   10: d8 ––011––– Number of blocks: 3
   10: d8 –––––000 1 basic physical channel for CCCH, not combined with SDCCHs
   11: 04 00000––– spare bits (should be 0)
   11: 04 –––––100 6 multi frames period for paging request
   12: 28 00101000 T3212 TimeOut value: 40
   13: 15 0––––––– spare bit (should be 0)
   13: 15 –0––––– Power control indicator is not set
   13: 15 ––01–––– MSs shall use uplink DTX
   13: 15 ––––0101 Radio Link Timeout: 24
   14: 65 011––––– Cell Reselect Hyst. :  6 db RXLEV
   14: 65 –––xxxxx Max Tx power level: 5
   15: 04 0––––––– No additional cells in SysInfo 7–8
   15: 04 –0––––– New establishm cause: not supported
   15: 04 ––xxxxxx RXLEV Access Min permitted = –110 + 4dB
   16: a9 10––––– Max. of retransmiss : 4
   16: a9 ––1010–– slots to spread TX : 14
   16: a9 ––––––0– The cell is barred  : no
   16: a9 –––––––1 Cell reestabl.i.cell: not allowed
   17: 00 –––––0–– Emergency call EC 10: allowed
   17: 00 00000––– Acc ctrl cl 11–15: 0 = permitted, 1 = forbidden
   17: 00 ––––––00 Acc ctrl cl  8– 9: 0 = permitted, 1 = forbidden
   17: 00 –––––––0 Ordinary subscribers (8)
```

KPN system information

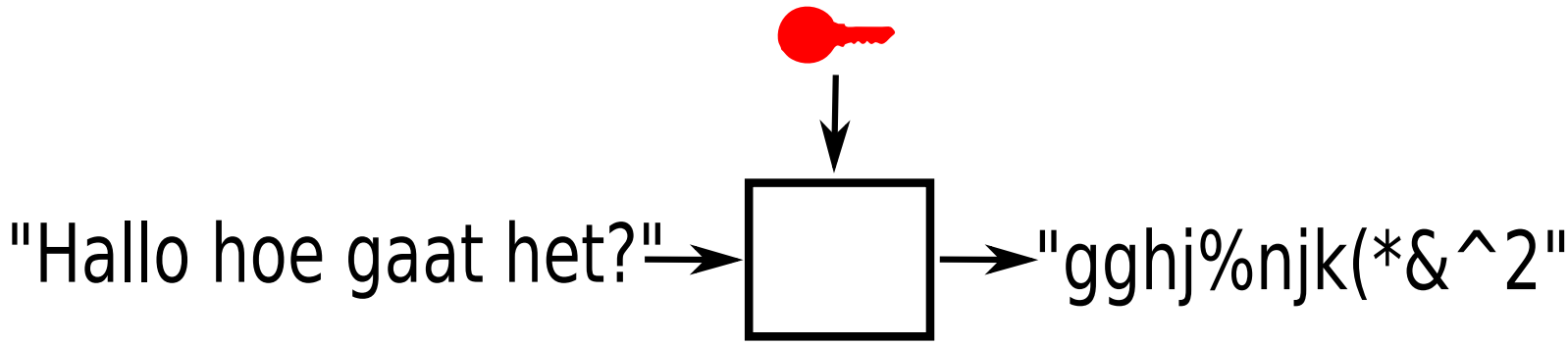
```
12834     [0x3222] Cell identity
02 204       Mobile Country Code (Netherlands)
f4 08f       Mobile Network Code (KPN Telecom B.V.)
11 4479      [0x117f] Local Area Code
```

Encryptie

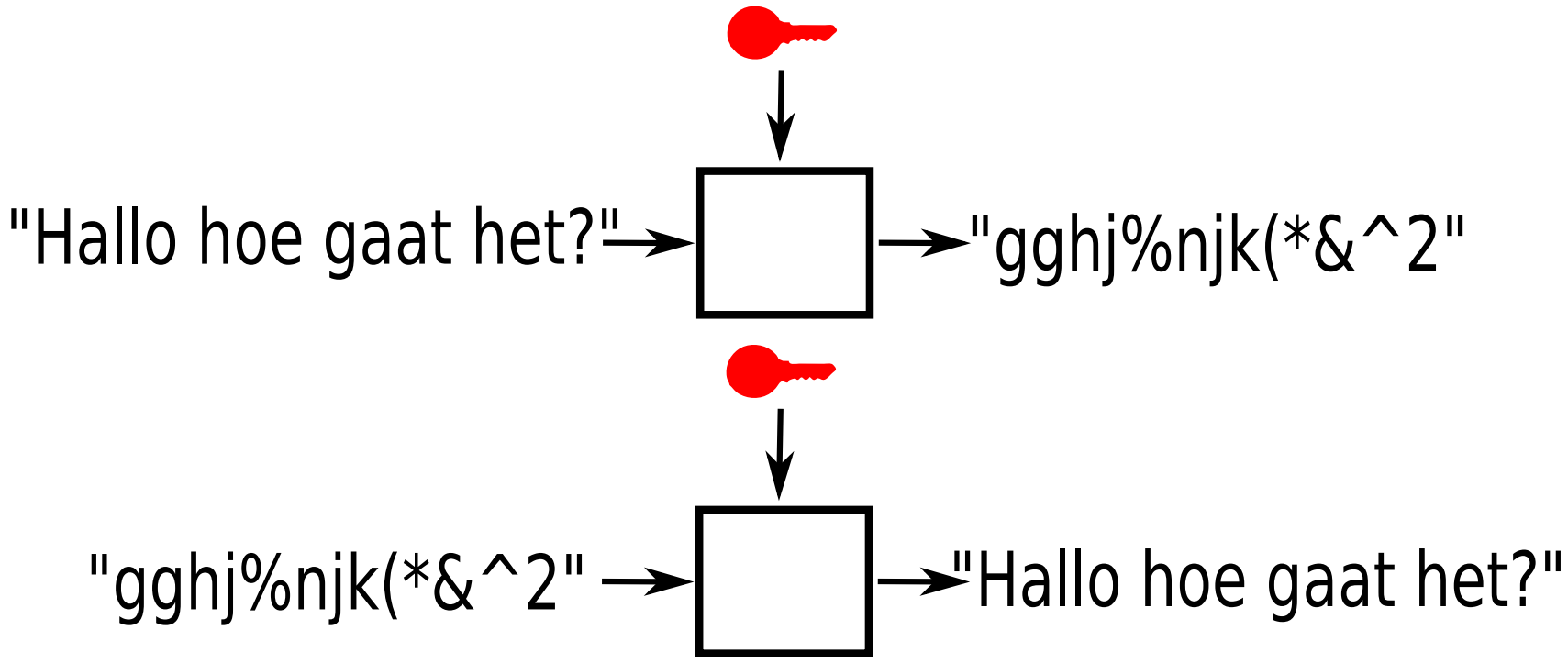
Encryptie



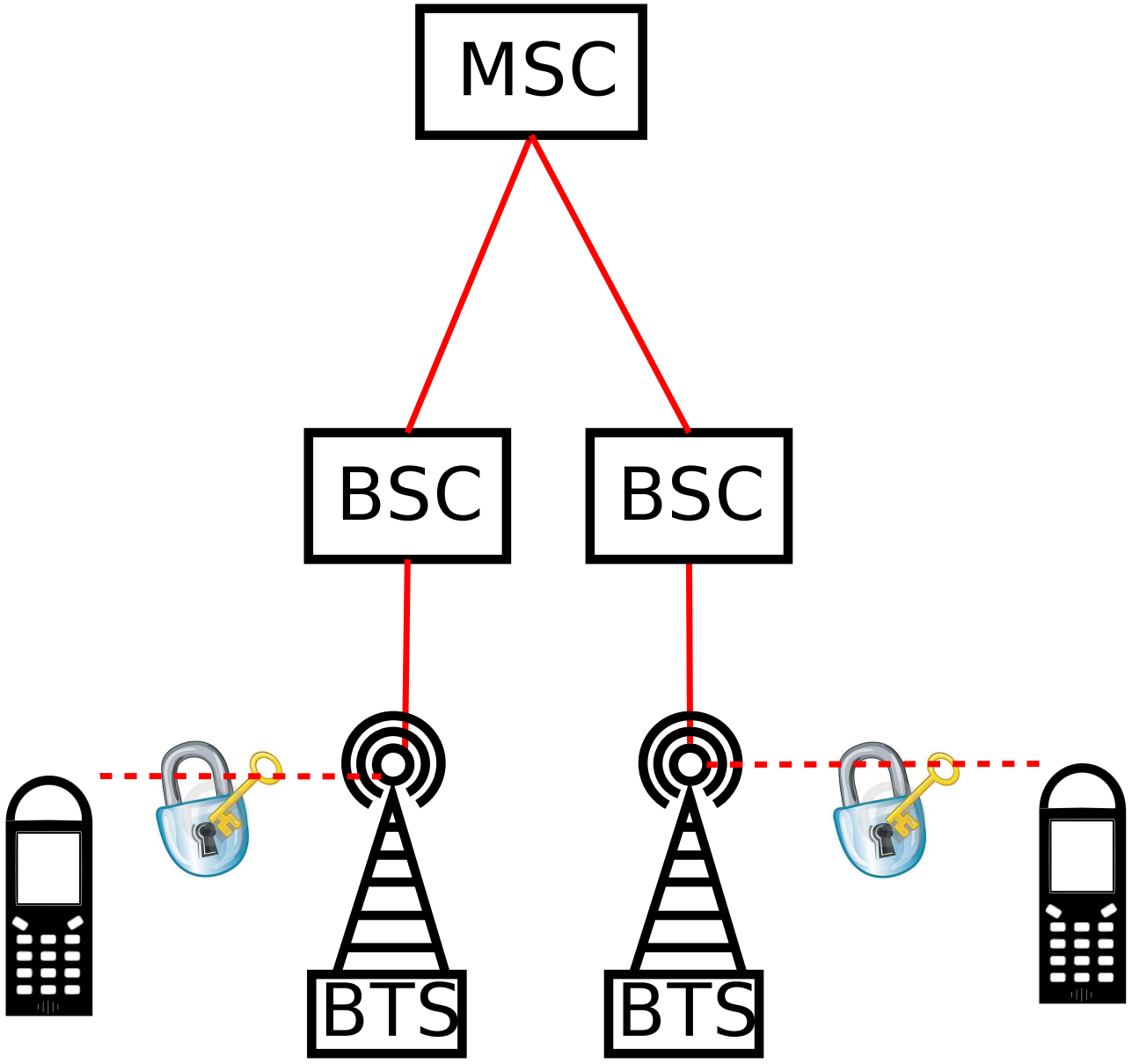
Encryptie



Encryptie



Encryptie tijdens een gesprek



Mogelijke encrypties in GSM

- A5/1
- A5/2
- A5/3
- A5/0

Mogelijke encrypties in GSM

- A5/1
- A5/2
- A5/3
- A5/0

Mogelijke encrypties in GSM

- A5/1 (+/-)
- A5/2 (-)
- A5/3 (+)
- A5/0

Mogelijke encrypties in GSM

- A5/1 (+/-)
- A5/2 (-)
- A5/3 (+)
- A5/0 (- -
  – - - - - - - - - - - - - - - - - – - - - - - - – - - - – - - - - – - - - – - - - - – - - -
  - - – - - – - - – - - – – – - - – - - - – - - - – - - – - - – - - - – - - – - - – - - –
  - -)

Maar hoe zit het nu met die veiligheid?

Gevaren

- Afluisteren
  - Door de overheid
  - Door een “gewone” aanvaller
- Verkeersgegevens verzamelen
- Onbetaald bellen
- Je als iemand anders voordoen

Gevaren

- Afluisteren
  - Door de overheid
  - Door een “gewone” aanvaller
- Verkeersgegevens verzamelen
- Onbetaald bellen
- Je als iemand anders voordoen

Gevaren

- Afluisteren
  - Door de overheid
  - Door een “gewone” aanvaller
- Verkeersgegevens verzamelen
- Onbetaald bellen
- Je als iemand anders voordoen

Gevaren

- Afluisteren
  - Door de overheid
  - Door een “gewone” aanvaller
- Verkeersgegevens verzamelen
- Onbetaald bellen
- Je als iemand anders voordoen

Gevaren

- Afluisteren
  - Door de overheid
  - Door een “gewone” aanvaller
- Verkeersgegevens verzamelen
- Onbetaald bellen
- Je als iemand anders voordoen

Een ander gevaar

Questions