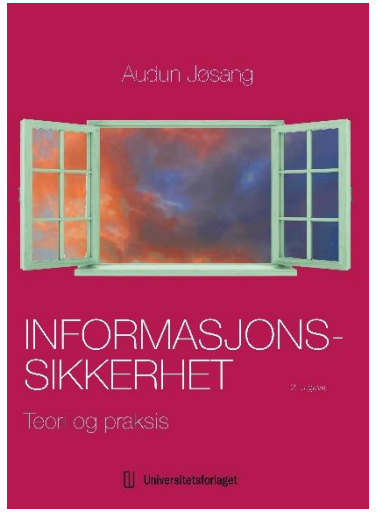
Kapittel 7:
Trådløs sikkerhet

Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utg. 2023

Universitetsforlaget



Oversikt

- Radiokommunikasjon
- Sikkerhet i wifi
- Sikkerhet i blåtann
- Sikkerhet i mobilnett

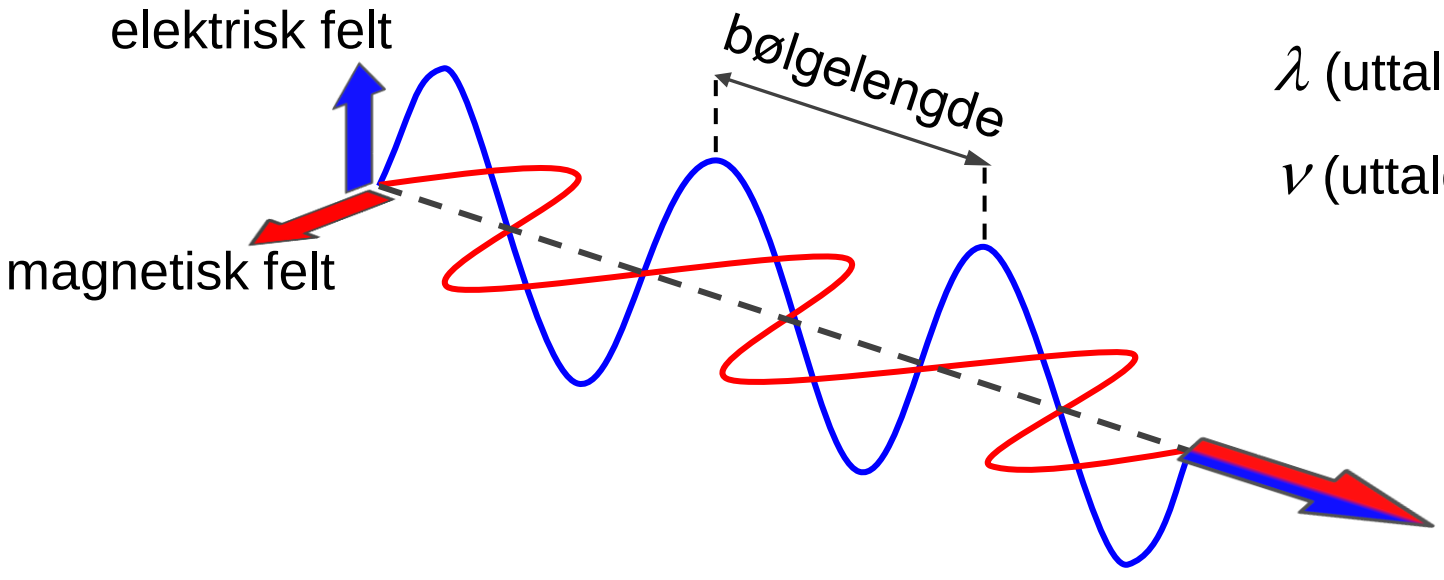
Radiokommunikasjon

$c = \lambda \cdot \nu$

$c = 300\ 000\ \text{km/s} = 3 \times 10^8\ \text{m/s}$ er lysets hastighet

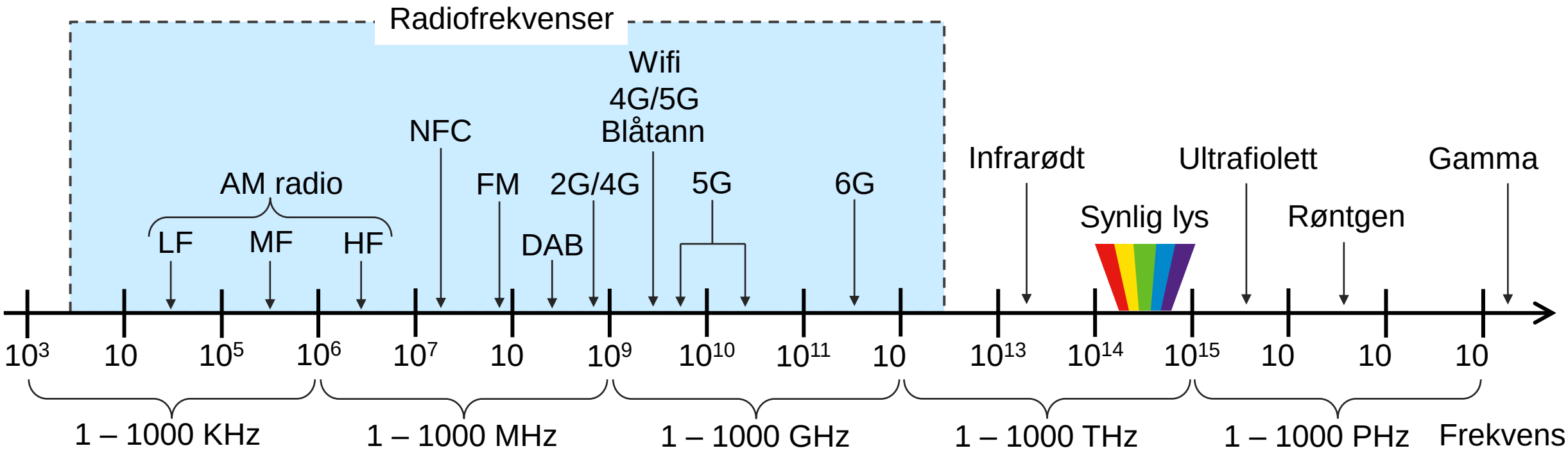
λ (uttales «lambda») er bølgelengden

ν (uttales «ny») er bølgens frekvens



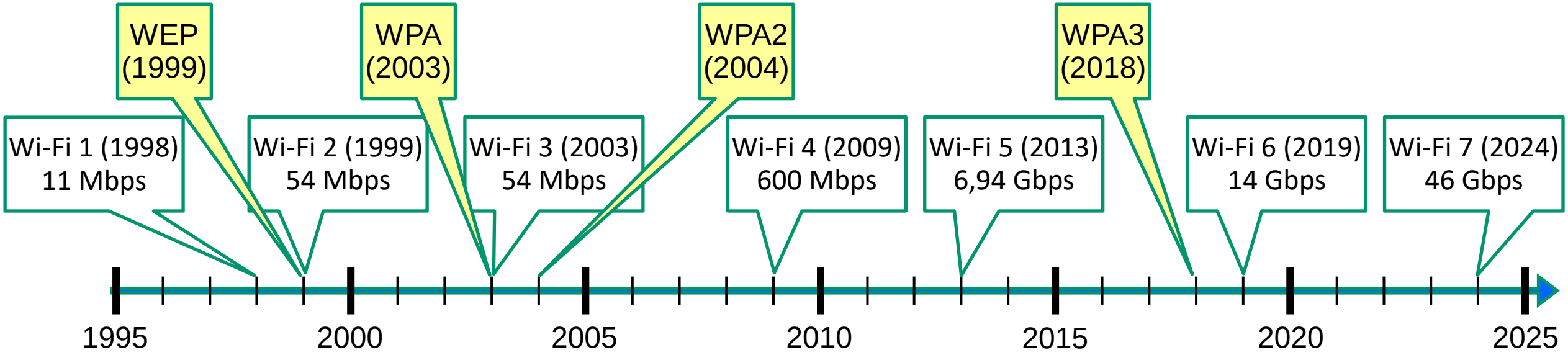
- Radiosignaler er elektromagnetiske bølger av elektriske og magnetiske felt
- Radiobølger og lys er samme fysiske fenomen, bare med ulik frekvens
- Frekvens $\nu = 3$ GHz $= 3 \times 10^9$ (brukes f.eks. i 4G/5G-nettet) gir bølgelengde 10 cm
- Elektromagnetiske bølger dannes ved bevegelse av elektriske partikler, f.eks. ved å koble elektriske signaler (som er bevegelse av elektroner) til en antenne

Spektret av elektromagnetiske bølger



- Jo høyere frekvens, desto større overføringskapasitet
- Jo høyere frekvens, desto lavere gjennomtrengingsevne
  - Signaler med lave frekvenser kan gå gjennom vegger og andre materialer
  - Signaler med høy frekvens stoppes (absorberes) av vegger og materialer slik at kommunikasjon krever fri sikt og relativt kort avstand. Det gjelder de høyeste frekvenser i 5G og 6G.

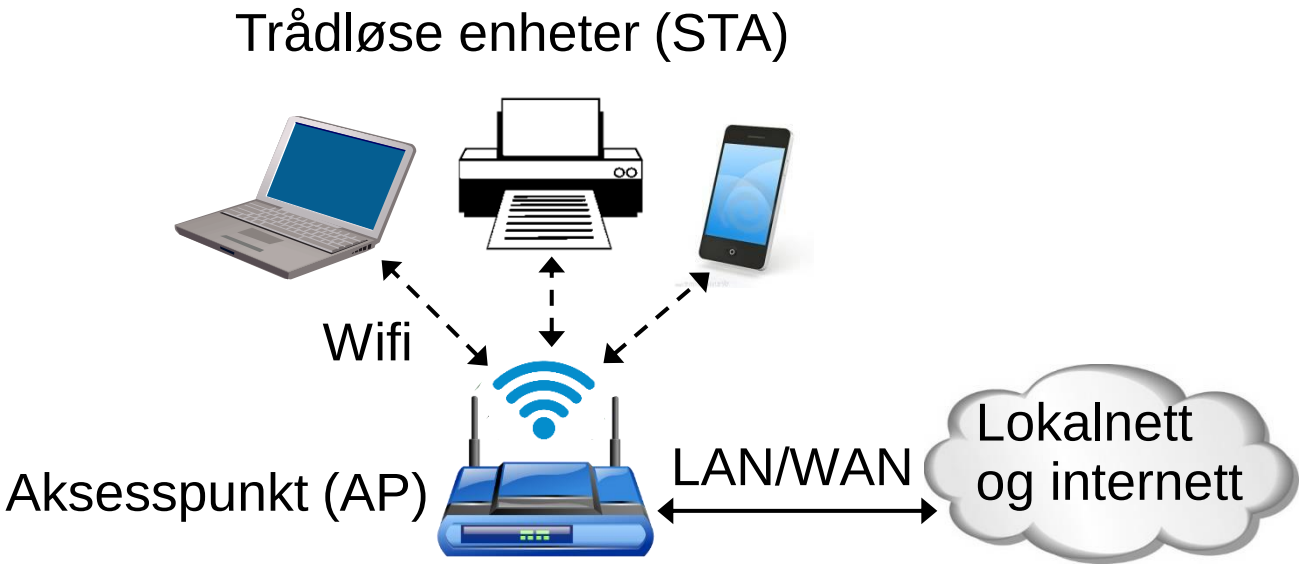
Utvikling av sikkerhet i wifi



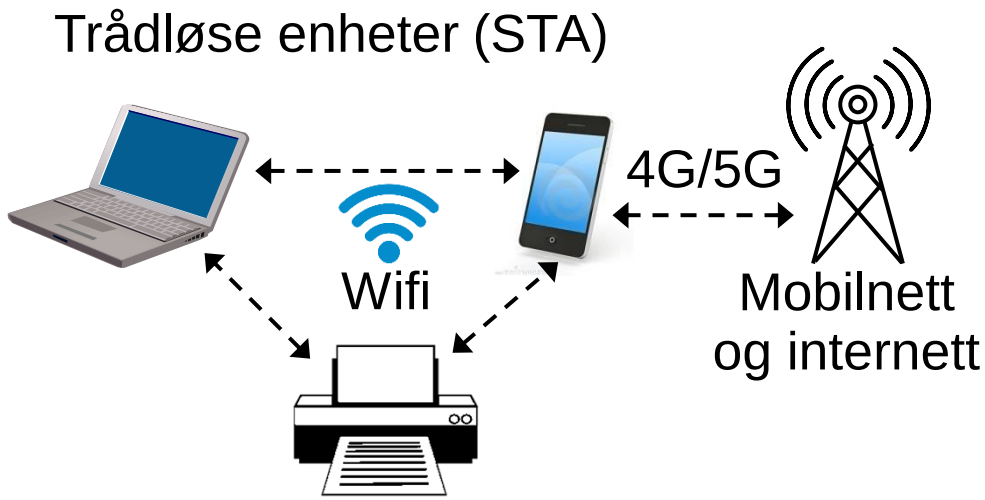
- Wifi kalles Wi-Fi på engelsk. Standardiseres av IEEE 802.11-standardene.
- WEP (Wireless Equivalent Privacy) hadde alvorlige sårbarheter
- WPA (Wi-Fi Protected Access) var litt bedre, men fremdeles alvorlige sårbarheter
- WPA2 var enda bedre, men fremdeles med sårbarheter.
- WPA3 har god sikkerhet. Fra 2020 kreves WPA3 i alt nytt wifi-utstyr som selges.

Wifi-arkitekturer

1) Wifi i infrastrukturmodus

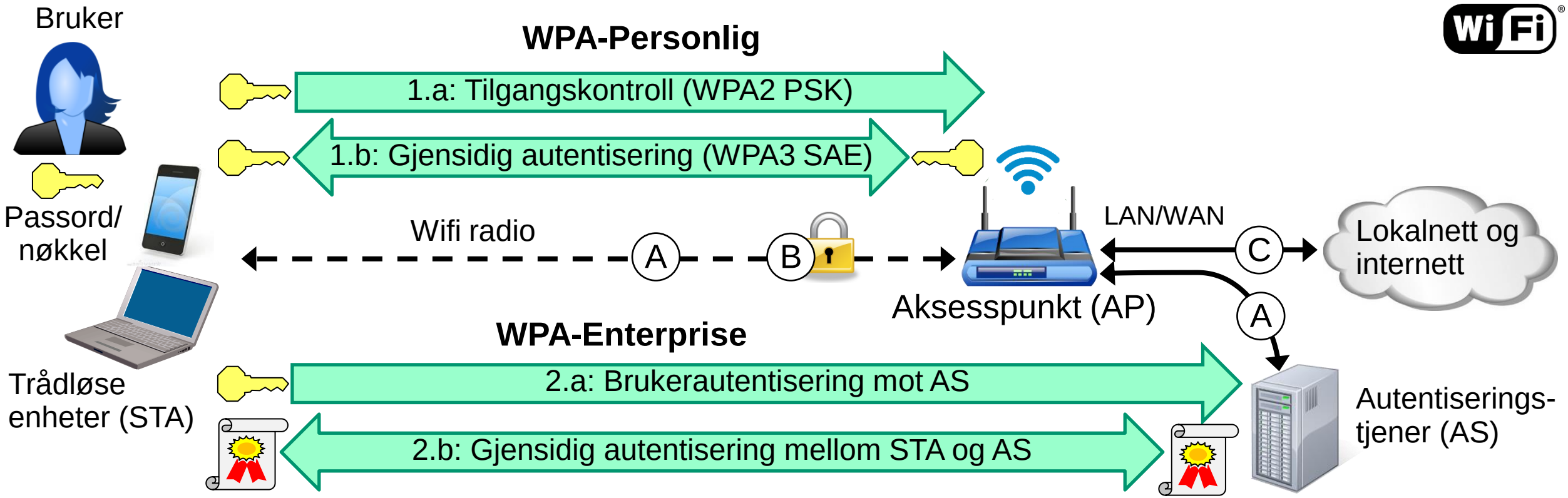


2) Wifi i ad-hoc-modus



- Infrastrukturmodus
  - Krever et aksesspunkt (AP) (ruter) som gir videre forbindelse til datanett/internett
  - Benyttes i kontorlandskap og hjemme-installasjoner
- Ad-hoc modus
  - Støtter kommunikasjon på kort avstand mellom enheter, der én enhet kan ha internettforbindelse

Autentisering og tilgangskontroll for wifi i infrastrukturmodus

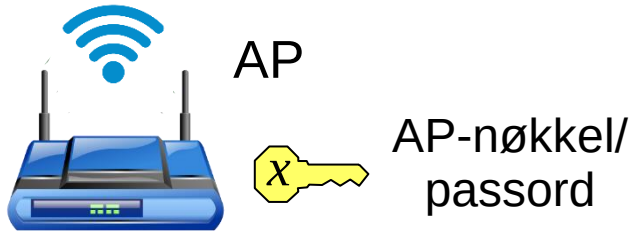


Trinn oppkobling til wifi-nett. Type “Personlig” og “Enterprise” har hver sine protokoller.

A. Autentisering og øktetablering
B. Kryptert radioforbindelse til AP
C. AP åpner for tilgang til datanett/internett

SAE-protokollen for å etablere øktnøkkel med WPA-Personlig

SAE-protokollen



STA og AP deler en felles offentlig elliptisk kurve EC

STA og AP har felles hemmelige nøkkel/passord x

STA og AP beregner et felles hemmelig punkt G på EC ut ifra x og andre parametere

STA velger egen hemmelig parameter a

AP velger egen hemmelig parameter b

STA sender til AP → $a * G$, som er et punkt på EC

$b * G$, som er et punkt på EC ← AP sender til STA

STA beregner hemmelig nøkkel $K = a * b * G$

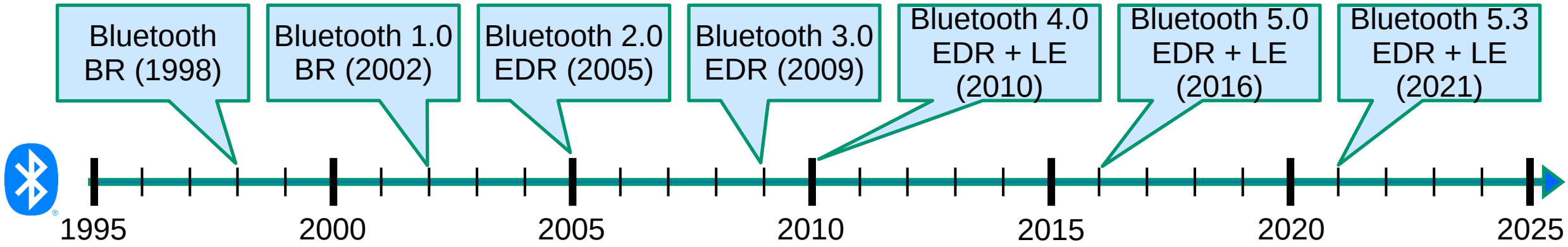
AP beregner hemmelig nøkkel $K = b * a * G$

STA og AP har etablert en autentisert felles hemmelig øktnøkkel K

Trusler relater til wifi

- Evil twin
  - Falske wifi-rutere med spoofet navn kan lure folk til å koble seg på.
  - Overførte data kan stjeles og endres hvis forbindelsen går ukryptert, f.eks. med http (ikke https)
  - Vanligvis tvinges nettleser til å bruke https (med HSTS – http strict transport security), se kapittel 6 om nettverkssikkerhet
  - Man er trygg hvis det benyttes VPN eller ende-til-ende-kryptering
- Cracking av passord for ulovlig tilgang til nettverk
  - Svake wifi-passord kan crackes
  - Sørg alltid for sterke passord for tilgang til wifi-nett.

Utvikling av blåtannteknologier



- Bluetooth Classic (BR: Basic Rate og EDR: Enhanced Data Rate)
  - Brukes av enheter som trenger stor overføringskapasitet (og over relativt stor avstand)
  - Strømforsyning eller stort batteri (f.eks. laptop og mobilbatteri)
  - Høyttalere, mobiltelefoner, laptopper
- Bluetooth Low Energy (LE)
  - Brukes av enheter som bare trenger liten overføringskapasitet (og over relativt liten avstand)
  - Lite batteri (f.eks. i myntstørrelse)
  - Sensorer, smarte enheter (og mobiltelefoner og laptopper som støtter både classic og LE)

Blåtann-arkitekturer

a. -arkitektur med Classic (EDR) teknologi

b. -arkitektur med Low Energy (LE) teknologi

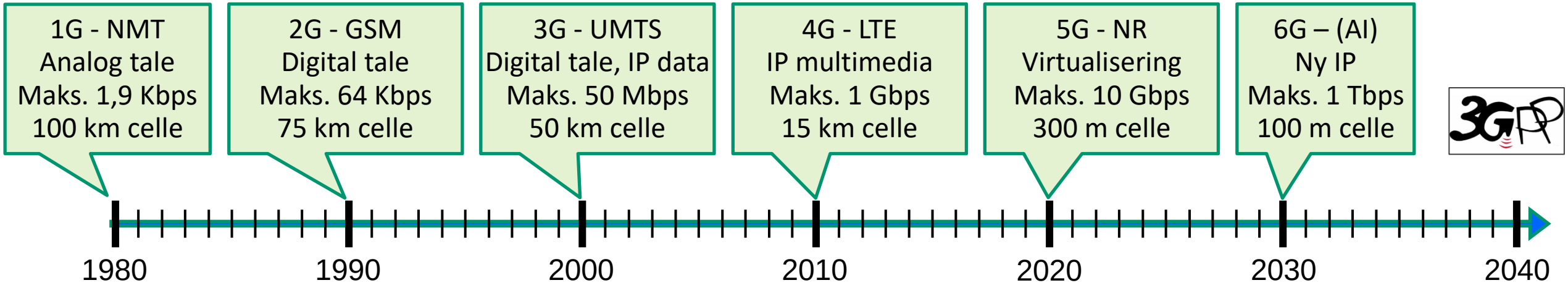
- I en blåtann-tilkobling er det alltid én master-enhet og én eller flere slave-enheter.
- Classic (EDR) lar master-enheten ha tilkoblet maks 7 slave-enheter
- LE lar master-enheten ha et ubegrenset antall tilkoblede slave-enheter.
- LE er tenkt brukt i smarte omgivelser for å styre og kommunisere med et vilkårlig antall ulike sensorer og smarte apparater.

SSP (Secure Simple Pairing) mellom blåtann-enheter

Ulike metoder for paring mellom blåtann-enheter:

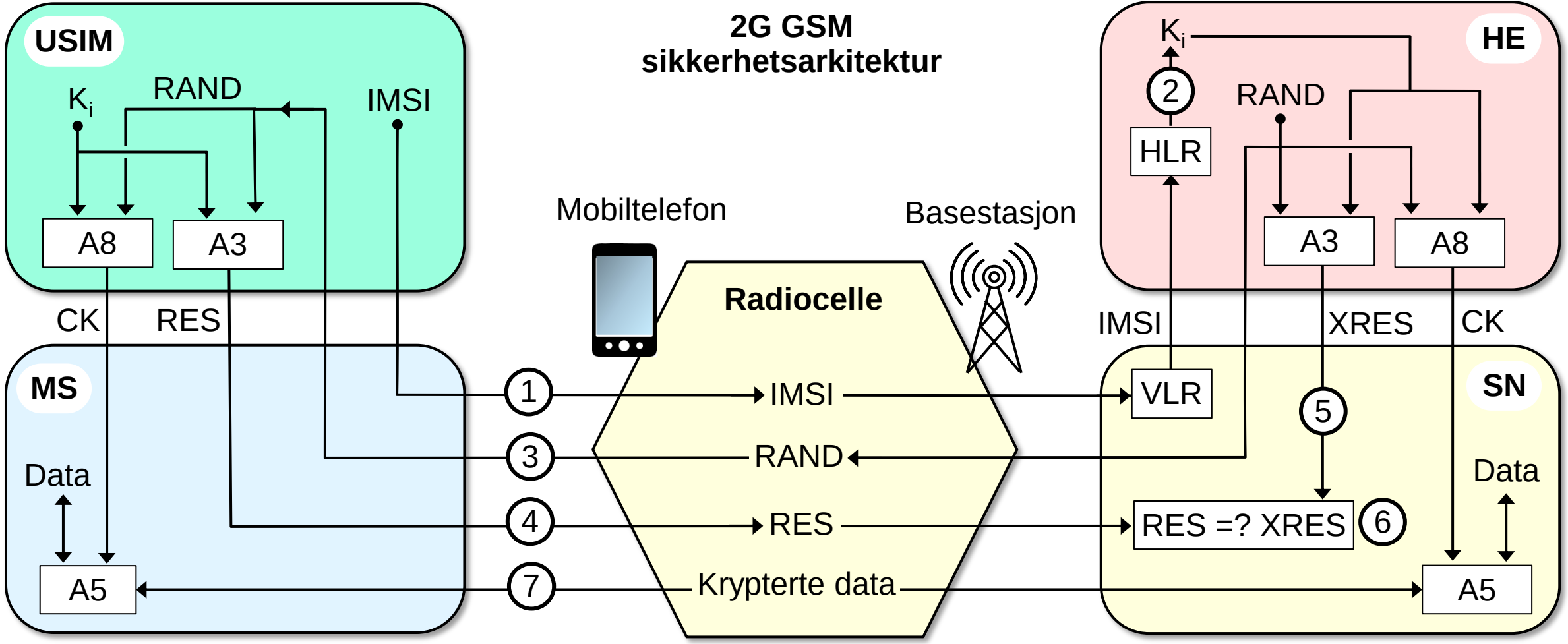
- Numerisk sammenligning er at begge blåtann-enhetene viser et sekssifret tall på et display og lar bruker velge «ja» eller «nei» hvis tallene er like.
- Passkey Entry er at én blåtann-enhet kan ta input fra brukeren (f.eks. med tastatur), mens den andre enheten har en skjerm. Enheten med bare skjerm viser et sekssifret tall som brukeren skriver inn på enheten med input.
- Just Works kan brukes når minst én av enhetene hverken har display eller tastatur (f.eks. headset). Brukeren godtar paring uten eksplisitt autentisering.
- Out of Band (OOB) betyr at autentisering foregår gjennom en sekundærkanal, altså ikke gjennom blåtann. En slik sekundærkanal kan for eksempel være NFC (Near Field Communication) eller kabel. Paring med NFC skjer enkelt ved å legge blåtann-enhetene mot hverandre, etterfulgt av at brukeren godtar tilkoblingen med et enkelt tastetrykk. Autentisering med OOB er basert på direkte fysisk nærhet eller kabelforbindelse.

Utvikling av mobilnett, standardisert av 3GPP (fra 3G)



- 1G NMT (Nordisk mobiltelefon) sendte ukryptert tale, var sårbar for avlytting og tyveri av mobilkonto.
- 2G GSM (Global System for Mobile Communication, opprinnelig Grope Spécial Mobile) sender tale som en strøm av bits, med svak kryptering.
- 3G UMTS (Universal Mobile Telecommunications System) sender tale som strøm av bits og data som pakker. 3G-teknologi er faset ut av de fleste teleoperatører.
- 4G LTE (Long Term Evolution) sender tale, video og alle typer data som datapakker, med god utnyttelse av radiofrekvensspekteret.
- 5G har nytt radiogrensesnitt (NR New Radio) og modularisert arkitektur med bruk av skytjenester.
- 6G vi antagelig ta i bruk AI og innføre nye nettverksprotokoller som erstatning for TCP/IP.

2G GSM sikkerhetsarkitektur



Forklaring:

USIM:	Unversal Subscriber Identity Module
MS:	Mobile Station (mobiltelefon)
K_i :	Individuell autentiseringsnøkkel for abonnenten
CK:	Cipher Key (krypteringsnøkkel for forbindelsen)
IMSI:	International Mobile Subscriber Identity

A3, A5 og A8 er kryptoalgoritmer

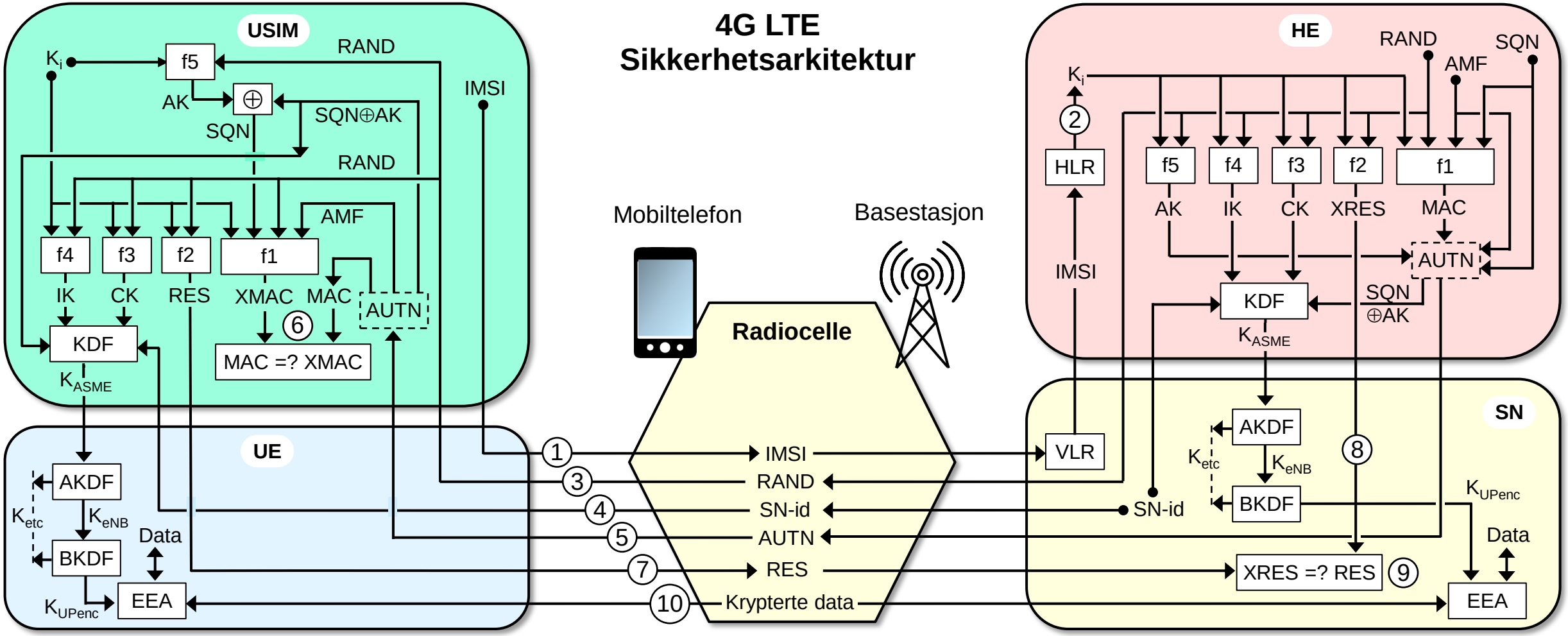
HE:	Home Environment (abonnentens operatør)
SN:	Serving Network (mobilnett og basestasjon)
HLR/VLR:	Home/Visited Location Register
RES:	Response
XRES:	Expected Response
RAND:	Random Number

2G sikkerhet - forklaring

1. USIM (SIM-brikken) sender IMSI (via mobiltelefon og VLR) til HLR
2. Oppslag med IMSI i HLR finner K_i for abonnenten
3. HE (abonnentens teleoperatør) genererer og sender RAND til USIM
4. USIM beregner RES som sendes til SN
5. HE beregner XRES som sendes til SN
6. SN sammenligner RES og XRES (som er autentisering av abonnenten)
7. Hvis RES = XRES kan kryptert forbindelsen settes opp

- Det er lett for en IMSI-fanger å motta IMSI, som gjør at abonnenten kan spores
- Det skjer ingen autentisering av SN, som betyr at abonnenten/USIM ikke kan vite om nettverket er en ekte teleoperatør, eller en IMSI-fanger.
- A5-algoritmen er relativt svak og kan knekkes i sanntid

4G LTE Sikkerhetsarkitektur



Forklaring

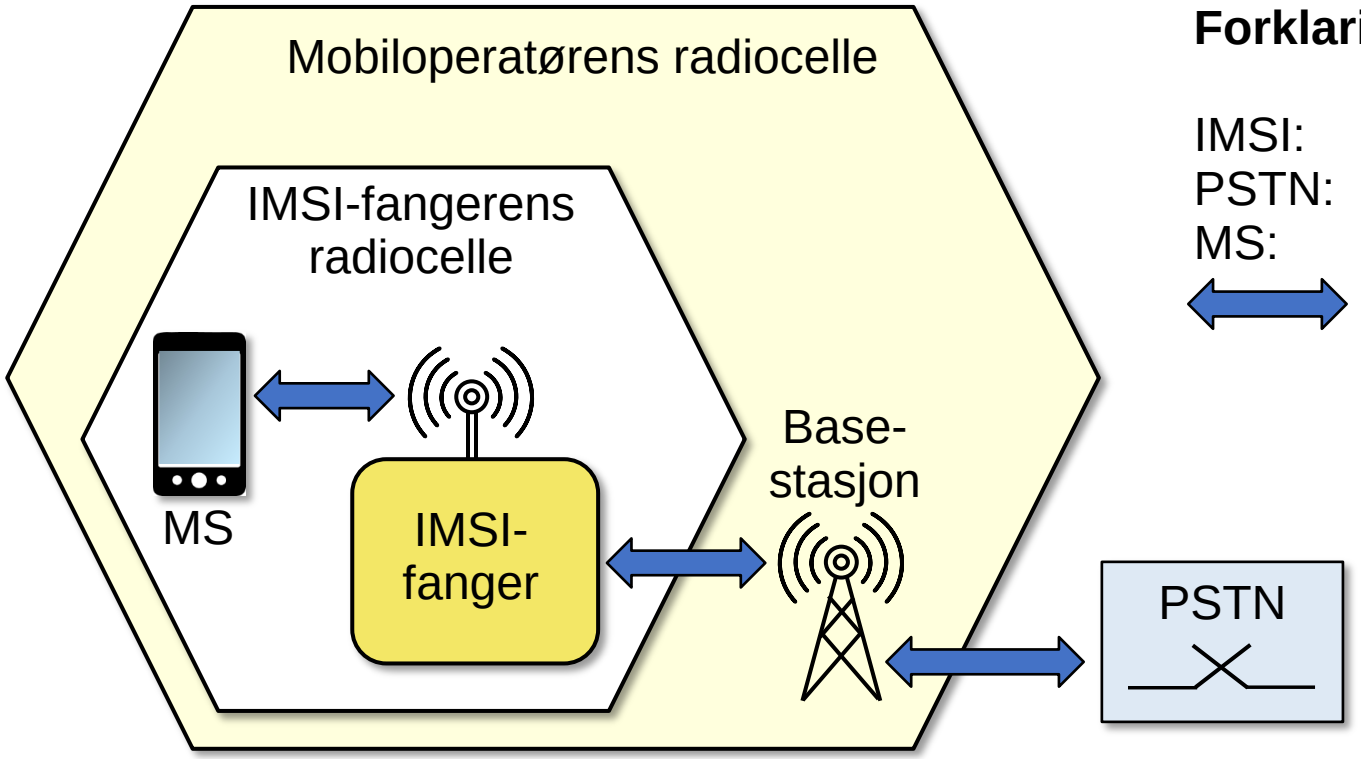
K_i :	Individuell autentiseringsnøkkel for abonnenten
CK:	Cipher Key
K_{ASME}:	Access Security Management Entity Key
K_{eNB}:	Enhanced Node B Key (for Base Station)
K_{UPenc}:	User Plane Encryption Key
K_{etc}:	Various Keys in the LTE Key Hierarchy
HE:	Home Environment
(X)MAC:	(Expected) Message Authentication Code
IMSI	International Mobile Subscriber Identity
SN:	Serving Network
SN-id:	Serving Network Identifier
SQN	Sequence Number
(X)RES:	(Expected) Response
IK:	Integrity Key
AK:	Anonymity Key
AMF:	Authentication Management Function
AUTN:	Network Authentication Token
HLR:	Home Location Register
USIM:	Universal Subscriber Identity Module
UE:	User Equipment (phone handset)
KDF:	Key Derivation Function
AKDF:	ASME Key Derivation Function
BKDF:	Base Station Key Derivation Function
EEA:	EPS Encryption Algorithm
EPS:	Evolved Packet System
RAND:	Random Number
VLR:	Visited Location Register
f1, f2, f3, f4, og f5 er kryptoalgoritmer	

4G sikkerhet - forklaring

1. USIM (SIM-brikken) sender IMSI (via mobiltelefon og VLR) til HLR
2. Oppslag med IMSI i HLR finner K_i for abonnenten
3. HE (abonnentens teleoperatør) genererer og sender RAND til USIM
4. SN sender SN-id til både USIM og HE
5. HE genererer AUTN (inneholder AK, MAC, AMF og SQN) som sendes til USIM
6. USIM beregner XMAC og sammenligner med mottatt MAC
7. Hvis MAC = XMAC genereres RES som sendes til SN
8. HE beregner XRES som sendes til SN
9. SN sammenligner RES og XRES (som er autentisering av abonnenten)
10. Hvis RES = XRES kan kryptert forbindelsen settes opp

- Det er lett for en IMSI-fanger å motta IMSI, som gjør at abonnenten kan spores
- Trinn 6 er en slags godkjenning av SN, men lar ikke brukeren autentisere SN

IMSI-fanger

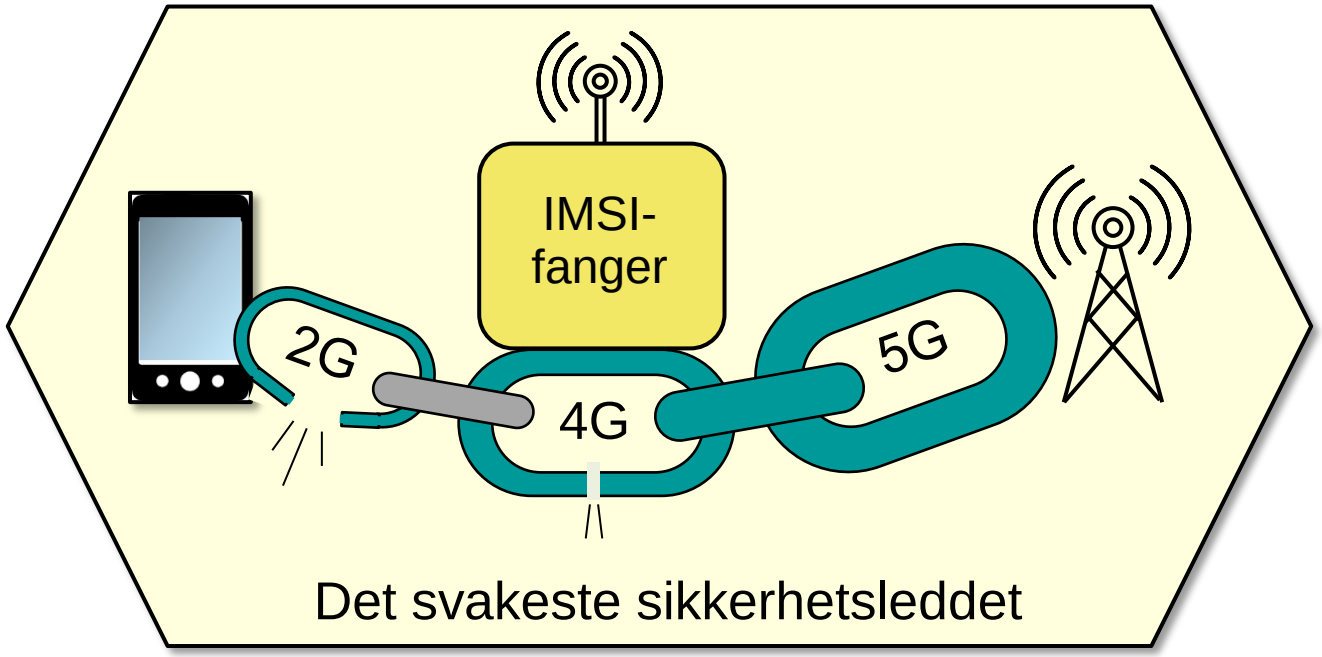


Forklarig:

IMSI: International Mobile Subscriber Identity
PSTN: Public Switched Telephone Network
MS: Mobile Station (mobiltelefon med SIM)
⟷ Mobilnettforbindelse

- IMSI-fangere utnytter sårbarheter i mobilnett for å utføre mellommannsangrep
- En IMSI-fanger kan brukes til:
  - å spore en abonnent
  - å avlytte samtaler og data

Systematisk sårbarhet i mobilnett



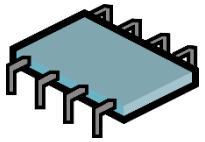
- Selv om 5G i prinsippet ikke er sårbart for IMSI-fangere kan en IMSI-fanger tvinge en mobiltelefon til å benytte 4G som er sårbar.
- Sårbarheten i milliarder av mobilenheter kan ikke fjernes så lenge mobilenheter kan (tvinges til å) benytte 4G eller 2G.

SIM-teknologier

SIM

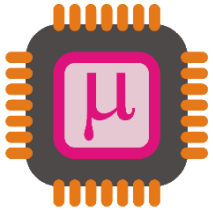
- Separat brikke mottatt fra teleoperatør.
- Manuell installering og utskifting.
- Tar betydelig plass i mobilenhet.

eSIM



- Koprosessor innebygd (embedded) i mobilenhet.
- Konfigureres online.
- Tar liten plass i mobilenhet.

iSIM



- Integrert i mobilenhetens mikroprosessor.
- Konfigureres online.
- Tar ingen plass i mobilenhet.

- Applikasjonen kalles egentlig USIM (Universal Subscriber Identity Module)
- Begrepene SIM, eSIM og iSIM er betegnelser for de ulike fysiske formatene der data og programvare for USIM-applikasjonen er lagret og kjører.
- SIM formatet har vært vanlig siden 1990, mens eSIM er kommet etter 2020
- iSIM vil bli vanlig i IoT-enheter i fremtiden

Slutt på presentasjonen