

Evolution of wireless technology

Mark Pecen,
University of Pennsylvania EMTM Alumnus
(School of Engineering and Applied Sciences
and Wharton School of Business)

Mark Pecen – who am I ?



MARK PECEN is a senior technology executive and head of a specialised technology advisory group, Approach Infinity, Inc. and Vice Chair, Board of Directors of a multi-national cyber security and quantum technology firm, EigenQ, Inc., with a focus on research, standardisation, intellectual property and commercialisation of advanced technologies.

A recognized thought leader with 35+ years in the ICT industry, Pecen has been quoted in the Wall Street Journal, Forbes, Bloomberg, Daily Telegraph, Cybersecurity Magazine and others, and is the author of numerous articles, papers and co-author of Quantum Proofing the Economy (493 pages, available on Amazon : <https://www.amazon.com/dp/B0FSYVQ7G9>)

Pecen is a pioneer in wireless technology and inventor on more than 100 fundamental patents in wireless communication, networking and computing, and is a graduate of the University of Pennsylvania, Wharton School of Business and the School of Engineering and Applied Sciences.

He was awarded the titles of Distinguished Innovator and Science Advisory Board member by Motorola for his foundational research and standardization work on GSM, GPRS and EDGE cellular technologies at the European Telecommunication Standards Institute (ETSI) in France during the 1990s.

Led the work in 3GPP for Motorola on UMTS 3G cellular technology until 2005. As Senior Vice President, R&D for BlackBerry, he and his division contributed substantially to the work on 4G-LTE cellular technology and standards and critical wireless spectrum management in the International Telecommunications Union (ITU) in Geneva.

In 2015, Pecen co-founded the ETSI Technical Committee Cyber, Working Group for Quantum Safe Cryptography (TC Cyber WG QSC) and served as Chair for the first 5 years of its existence, producing some of the very earliest global standards on the topic. He further served as Chair of the Canadian government's task force on GDPR and served as president and executive advisor for Quantum Valley Ideas Lab in Canada, focusing on quantum radio frequency sensors using Rydberg atoms.

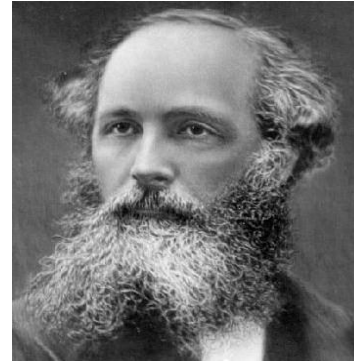
Pecen has served on over 20 advisory and governance boards for public and private companies over the years, including the University of Waterloo (CANADA) Institute for Quantum Computing, and Wilfred Laurier University Institute for Business and Economics (CANADA). He is an investor and advisor to several technology companies and venture funds, and is a general partner of a Canadian venture fund.



History and Standardization

The idea of wireless emerges: around 1861

- By the year 1850, most electrical phenomenon had been investigated by academic researchers
- James Clerk Maxwell (1831-1879), Professor of Experimental Physics at Cambridge introduced a new model for examining both electrical and magnetic phenomena
- His new mathematical model, today referred to as Maxwell's equations, predicted that there might be the existence of electromagnetic waves



$$\oint \mathbf{E} \cdot d\mathbf{A} = \frac{q_{enc}}{\epsilon_0}$$

$$\oint \mathbf{B} \cdot d\mathbf{A} = 0$$

$$\oint \mathbf{E} \cdot d\mathbf{s} = -\frac{d\Phi_B}{dt}$$

$$\oint \mathbf{B} \cdot d\mathbf{s} = \mu_0 \epsilon_0 \frac{d\Phi_E}{dt} + \mu_0 i_{enc}$$

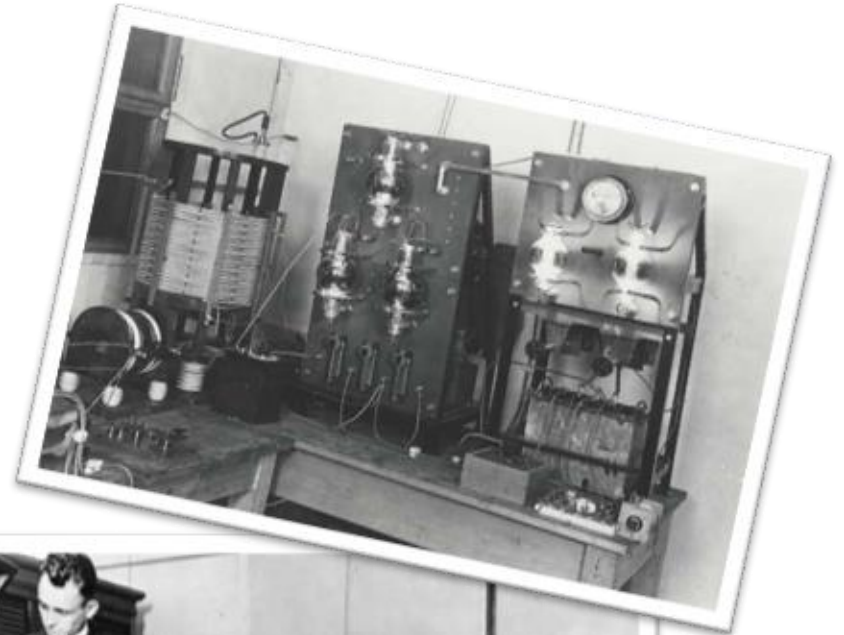
Early Wireless



- **Hertz** and **Popov** did lab experiments circa 1891
- Nikola Tesla filed patents on radio starting in 1892
- First commercial wireless technology deployments
 - Based on the work of **Guglielmo Marconi** (filed first patent for wireless telegraph system in the UK in 1896)
- First broad commercial application was ship-to-shore telegraphy
 - International Yacht Races held off New York Harbour in 1899

1920s: Voice Radio

- ❑ Reliable systems for transmitting and receiving voice information developed
- ❑ Vacuum tube technology was the relevant art
- ❑ One-way commercial radio broadcasting
- ❑ Two-way commercial and military communication systems
- ❑ Rapid adoption during the 1920s through 1940s
- ❑ Radio was the *Internet of the 1920s*



1950s and 1960s: 1st mobile telephones



MTS: Operator-assisted dialing



IMTS deployed in the USA in 1969

1970s to 1983

- **IMTS 1st Generation Telephony**
- Rapid adoption during the 1970s
- Everyone wanted one!
- Execs underestimated the demand
- Insufficient capacity
- Only a few phone numbers
- By 1980, 5-year waiting list in major cities in Europe and North America



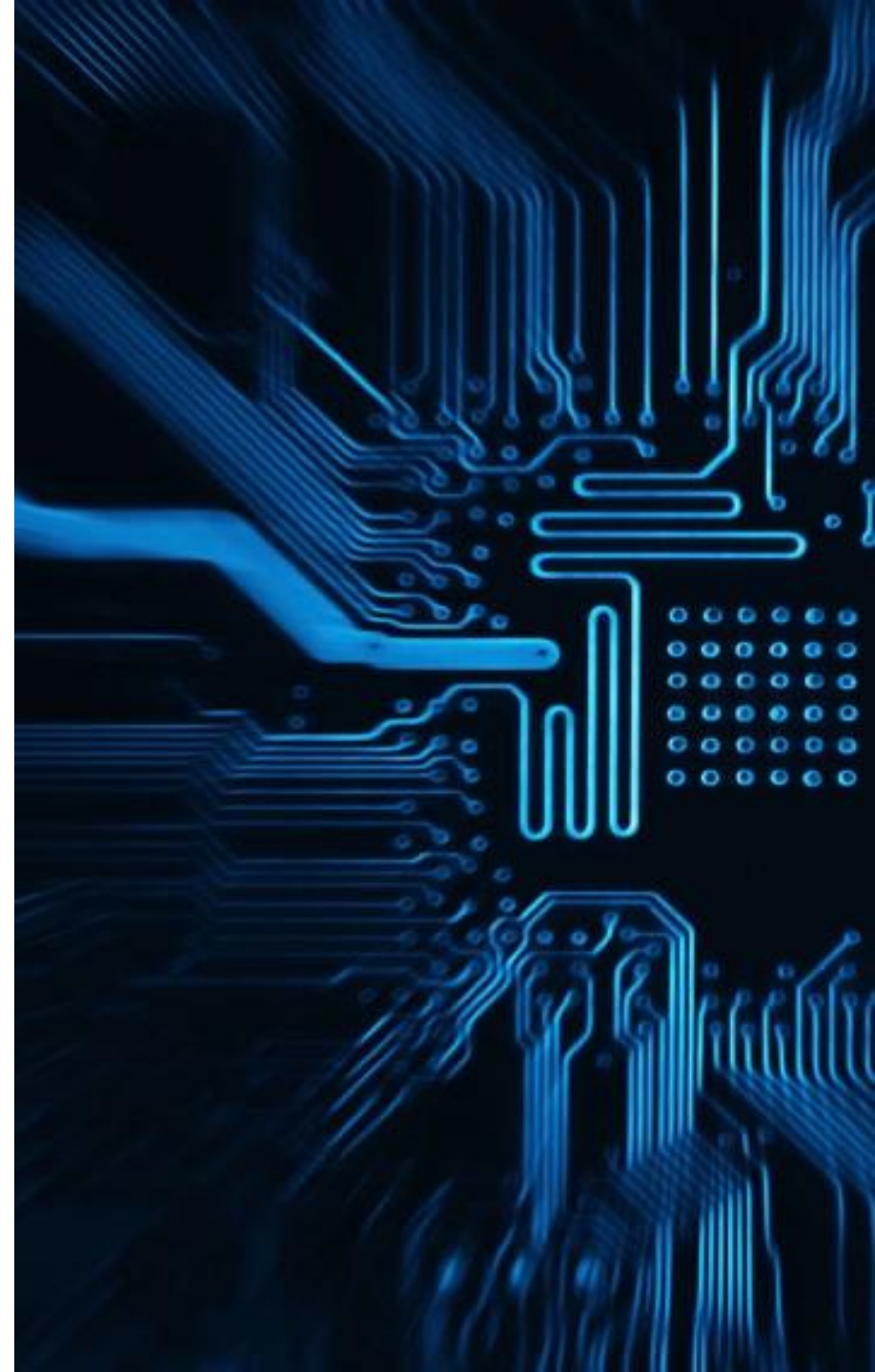
1G Analogue Cellular Technology

- New technologies: mobility management, handover
- 1983 - AMPS launched in Chicago
- Business and professional market segments
- 666 analogue channels
- Lots of phone numbers
- Almost no security – anyone could listen in

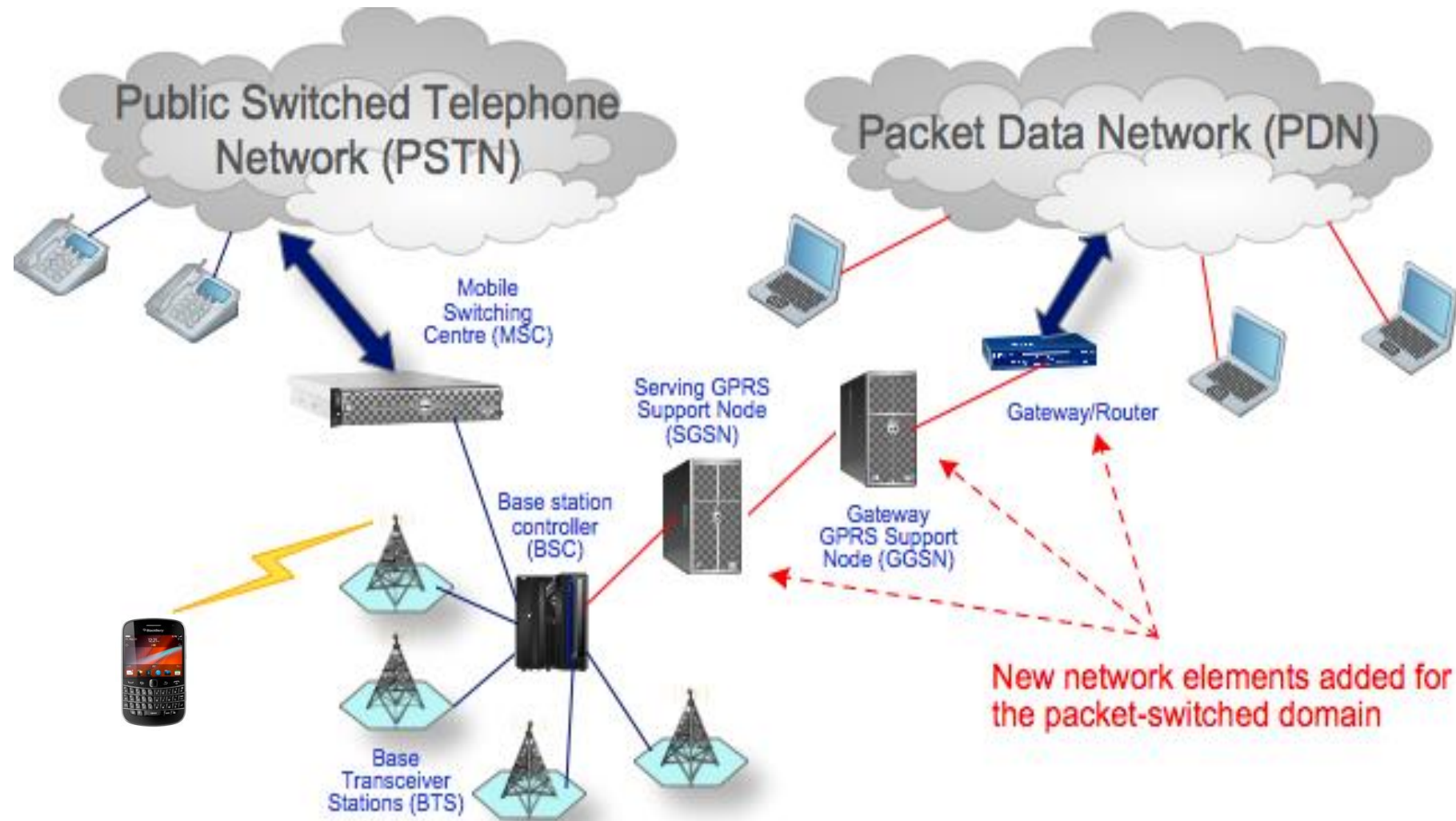


2G Digital Cellular

- Members of European Telecommunication Standards Institute (ETSI) in France developed the first standards in the late 80s, early 90s
- **First digital cellular standard in the world**
- System turned on in Europe in 1992
- GSM Phase 1 supported voice and SMS



GSM enhanced in 90s with GPRS and EDGE



The Evolution of Standards

0G

MTS, IMTS



1946, 1965

1G

AMPS, NMT,
TACS



1983

2G

GSM, D-AMPS (IS-54, IS-136),
cdmaOne (IS-95, IS-95A)



1992

2.5G

GPRS,
IS-95B,
EDGE



1998

3G

IMT-2000:
UMTS,
cdma2000
(IS-2000)



2003

3.5G

HSDPA,
HSUPA



2005

4G

IMT-A: LTE,
IEEE 802.16m



2013

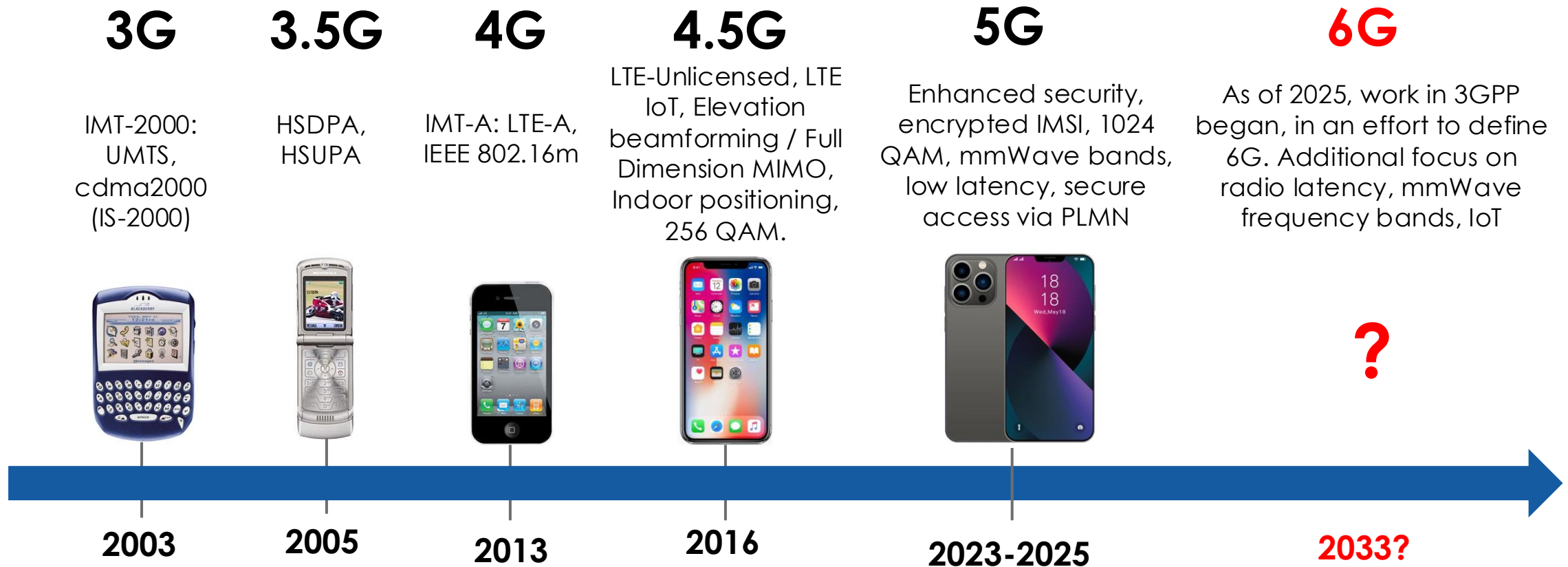
4.5G

LTE-Unlicensed, LTE
IoT, Elevation
beamforming / Full
Dimension MIMO,
Indoor positioning,
256 QAM.



2016

Forward to 5G and 6G...



Difference between 1G and 2G...

- The key difference between 1G and 2G was that 2G moved cellular communications to digital technology.

• Feature	1G	2G
• Main service	Voice	Voice + SMS + limited data
• Signal type	Analog	Digital
• Typical technologies	AMPS, NMT, TACS	GSM, IS-95/CDMAOne
• Voice quality	More noise/interference	Generally clearer and more consistent
• Security	Very weak	Digital encryption/authentication
• Capacity	Relatively low	Much higher
• Text messaging	No	Yes, especially SMS
• Data	Essentially none	Low-speed data, later GPRS/EDGE
• Spectral efficiency	Low	Much better

Difference between 2G and 3G...

- The key difference is that 2G was designed primarily for digital voice and messaging, while 3G was designed to make mobile data a major service alongside voice.

• Feature	2G	3G
• Main purpose	Digital voice + SMS	Voice + mobile Internet
• Typical technologies	GSM, IS-95/CDMAOne	UMTS/WCDMA, CDMA2000
• Typical data speed	~10–100 kbit/s; EDGE > 100 kb/s	~0.5–5+ Mbit/s; HSPA 10s or Mbit/s
• Latency	Often several hundred ms or more	Typically ~100–300 ms
• Voice	Circuit-switched	Usually still circuit-switched
• Data	Added with GPRS/EDGE	Designed around packet data
• Multimedia	Very limited	Web, email, video calling, streaming

Difference between 3G and 4G...

- The key difference is that 3G was designed to add practical mobile data to voice-centric cellular networks, while 4G was designed as a broadband, all-IP packet network capable of supporting high-speed Internet applications.

• Feature	3G	4G
• Typical technologies	UMTS/WCDMA, HSPA, CDMA2000	LTE, LTE-Advanced
• Typical user speeds	~0.5–10 Mbit/s	~10–100+ Mbit/s
• Peak speeds	Tens of Mbit/s with advanced HSPA	Hundreds of Mbit/s to 1 Gbit/s class
• Typical latency	~100–300 ms	~20–50 ms
• Radio access	Wideband CDMA / CDMA	OFDMA downlink, SC-FDMA uplink
• Voice architecture	Traditionally circuit-switched	Primarily packet/IP, e.g. VoLTE
• Core network	Mixed circuit + packet switching	Essentially all-IP
• Main goal	Voice + usable mobile Internet	Mobile broadband

Difference between 4G and 5G...

- The key difference is that 4G was designed primarily for fast mobile broadband, while 5G was designed for broadband plus very low latency, high device density, industrial connectivity, and much more flexible radio/network operation.

• Feature	4G / LTE	5G / NR
• Main purpose	Mobile broadband	Broadband + IoT + low-latency/industrial
• Typical user speeds	~10–100+ Mbit/s	~100 Mbit/s to 1+ Gbit/s in good conditions
• Peak theoretical rate	About 1 Gbit/s class for advanced LTE	Up to ~20 Gbit/s theoretical target
• Latency	~20–50 ms end-to-end	~10–20 ms; potentially much lower
• Spectrum	Mostly below ~6 GHz	Low band, mid-band, and mmWave
• Channel bandwidth	Typically up to 20 MHz per LTE carrier	Up to 100 MHz < 6 GHz, 400 MHz > 6 GHz
• Antennas	MIMO, few antennas	Massive MIMO and beamforming
• Core network	LTE EPC	Newer 5G Core architecture
• Device density	High	Designed for much larger IoT populations
• Network slicing	Not native	Major architectural feature

Difference between 5G and 6G...

- The key difference is that 5G is primarily a high-performance communications network, whereas 6G is being designed as a communications + sensing + computing + AI platform. 5G is deployed today; 6G is still under development and is expected to begin deployment around 2030. The ITU calls the 6G framework IMT-2030.

• Characteristic	5G	6G / IMT-2030
• Status	Commercially deployed	Research/standardization
• Approx. introduction	~2019–2020	~2030
• Peak data rate target	~20 Gbit/s	Research targets ~50–200 Gbit/s
• Radio latency	~1 ms target for URLLC	~0.1–1 ms research target
• Frequencies	Sub-1 GHz, mmWave	Those bands plus potentially >100 GHz
• AI	Mainly for network optimization	AI designed more deeply into the core
• Sensing	Primarily communications	Integrated sensing + communications
• Coverage	Mainly terrestrial, satellite	Ubiquitous terrestrial/non-terrestrial
• IoT	Massive machine connectivity	More device density, very-low-power devices
• Primary goal	Fast, reliable mobile connectivity	Connectivity, sensing, intelligence, computing



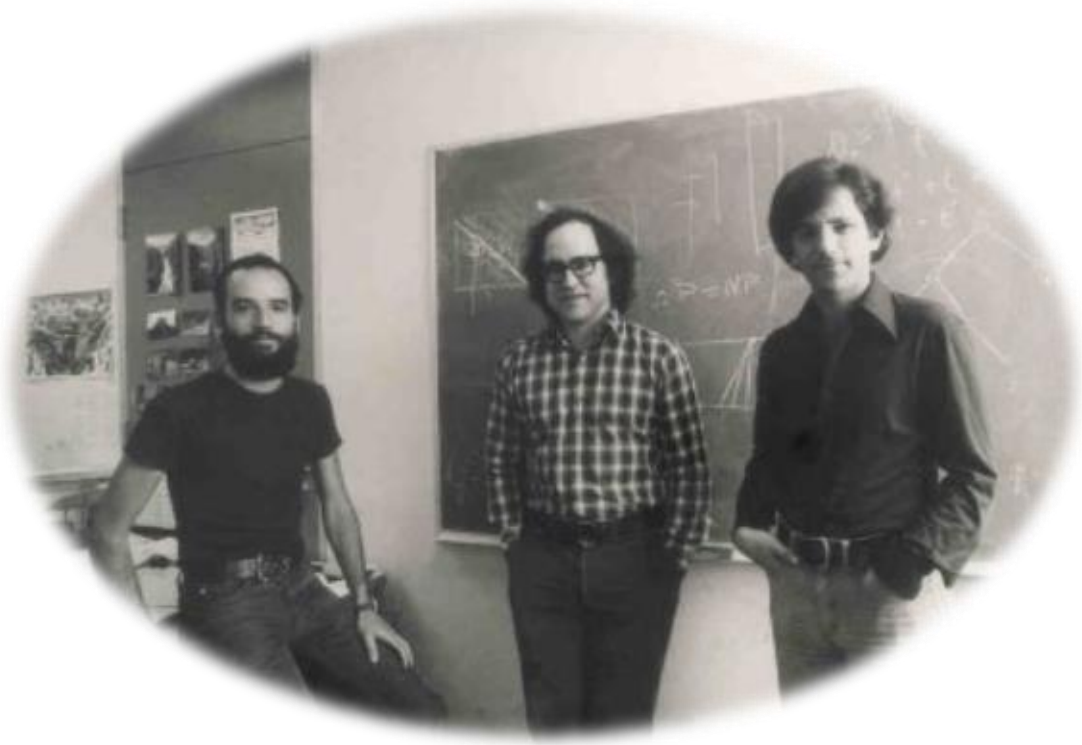
Wireless Security

Wireless Security

- Cryptography is a key component of wireless security
- Includes public-key and symmetric key technology
- Provides the following:
 - Data authentication
 - Entity authentication
 - Confidentiality (through encryption)
 - Non repudiation (through digital signatures)

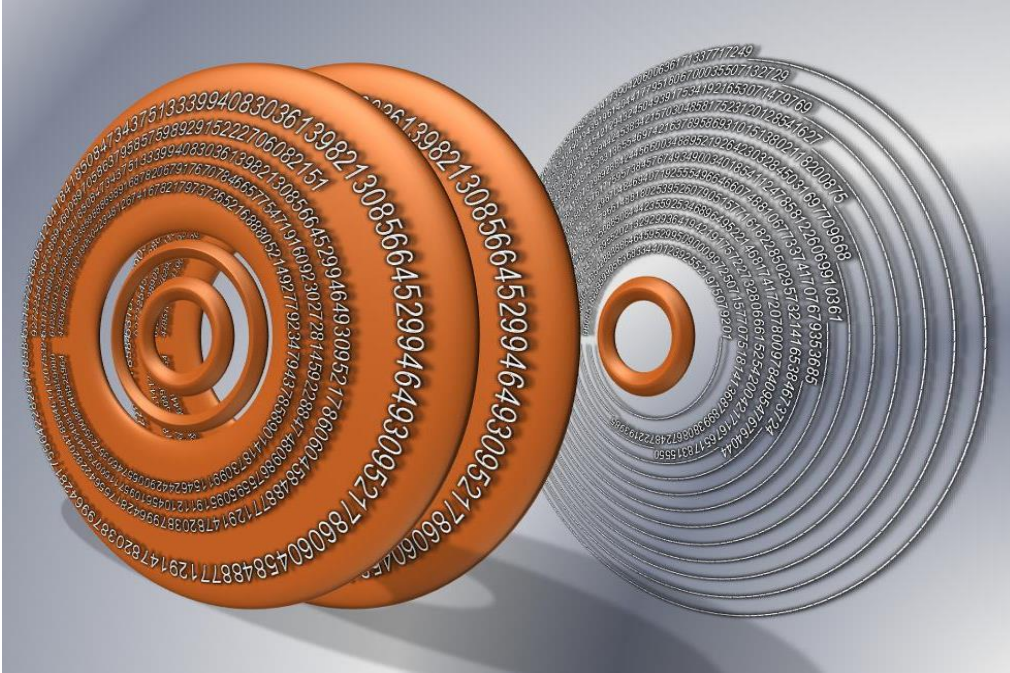

$$\begin{aligned} & (y f(2) + 2015^2) y_1 + e_2(x) y_2 + e_3(x) y_3 \\ & (x+1) = \left(\frac{x(x-2)}{2} \right) 1 + (x(x-1)) 0 + \left(\frac{x(x-1)}{2} \right) \\ &)^2 = \left(\frac{(x-1)(x-2)}{2} \right) 1 + (x(x-1)) 0 + \left(\frac{x(x-1)}{2} \right) \\ &)^2 (y + 6x + 2)^4 (y + 8x + 2)^4 (y + 9x + 6)^4 (y + 10x + 8)^4 \\ & 1)(x+6)^4 (x+9)^4 x(x+1)(x+2)^4 (y+8x+2)^4 \\ & -9b + \sqrt{3} \sqrt{4a^3 + 27b^2} (y+6x)^2 (y+10x+8)^2 x+1 \\ & 2^{1/3} 3^{2/3} x(x+6)^2 (y+8x+2)^2 \\ & (1-i\sqrt{3})(-9b + \sqrt{3} \sqrt{4a^3 + 27b^2})^{1/3} (y+8x+2)^2 (y+7x+4)^4 (y+9x+6)^4 \end{aligned}$$

Public Key Technologies



- Rivest, Shamir, Adelman (RSA)
- Most well-known public-key technology for conventional wired environments
- Not well-suited for wireless due to constraints of the environment

Public Key Technologies

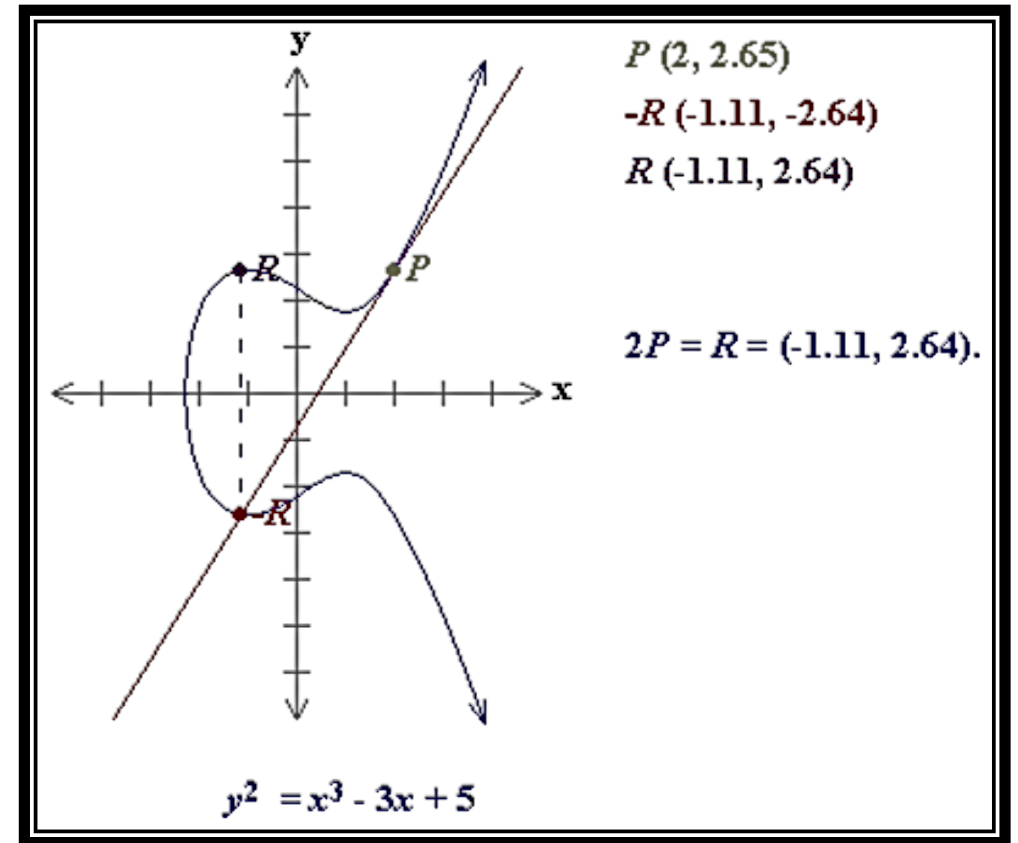


Elliptic Curve Cryptography (ECC)

- Discovered by Neal Koblitz, University of Washington, and independently by Victor Miller, IBM, in 1985
- Provides the most security per bit than any other public-key technology
- Certicom Research realized in the late 90s that ECC is a perfect cryptographic solution for wireless devices

Elliptic Curve Cryptography (ECC)

- Meets the following constraints for wireless:
 - Battery power efficiency
 - Storage/memory requirements low
 - Computation requirements reasonable
 - Bandwidth – key size fairly small
- In all major security standards for wireless and constrained environments



Wireless Security Standards

- ❑ Standards have driven the evolution of wireless security
- ❑ Protocols, algorithms and hardware are subjected to systematic attacks as part of the evolution
- ❑ If vulnerabilities are found, countermeasures are implemented in new revisions of standards
- ❑ Evolution of quantum computers will create additional opportunities for attack, once a cryptographically relevant quantum computer appears



Standards for wireless security

- Three are mature:



- One is relatively new:



Cellular Security Goals

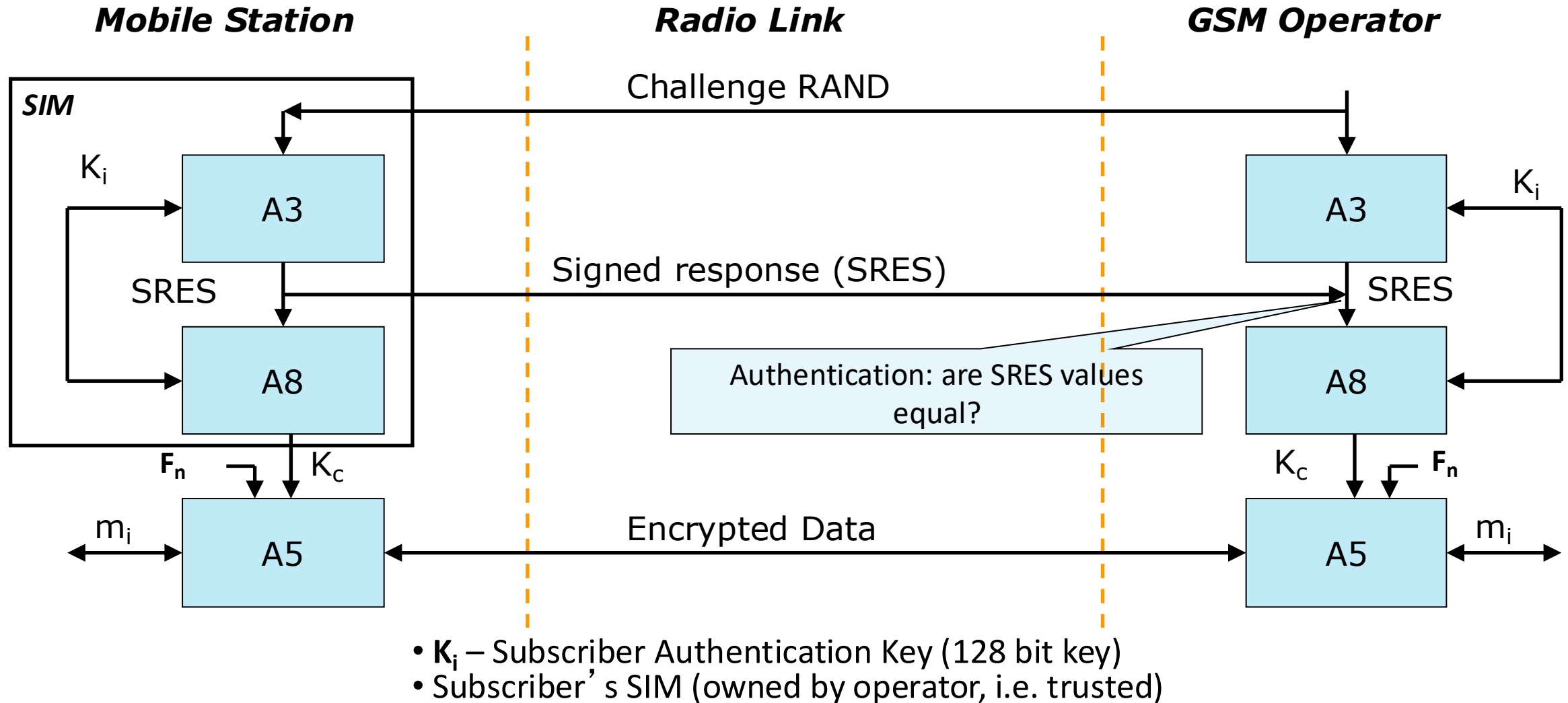
- ❑ Confidentiality and anonymity on the radio path
- ❑ Strong client authentication to protect the operator against billing fraud
- ❑ Prevention of operators from compromising each others' security
 - ❑ Inadvertently
 - ❑ Competition pressure
- ❑ Driven by ETSI (<http://www.etsi.org/>) and 3GPP (<https://www.3gpp.org>)

ANONYMOUS



CONFIDENTIAL

Authentication and Encryption Scheme



WiFi Security Goals

- ☐ Confidentiality on the wireless LAN
- ☐ Strong client authentication to protect the network from unauthorized use
- ☐ Standard algorithms for home and enterprise use
- ☐ Driven by IEEE 802 (<http://www.ieee802.org/>)

	Authentication	Encryption	Suitable for Corp WAN	Suitable for home and small business WLAN
WEP	None	RC4	Poor	Less than good
WPA(PSK)	PSK	TKIP	Poor	Best
WPA2(PSK)	PSK	AES-CCMP	Poor	Best
WPA(full)	802.1x	TKIP	Better	Good (expensive)
WPA2(full)	802.1x	AES-CCMP	Best	Good (expensive)

802.1X Authentication

1. Using Extensible Authentication protocol (EAP) an end-user contacts a wireless access point and requests to be authenticated



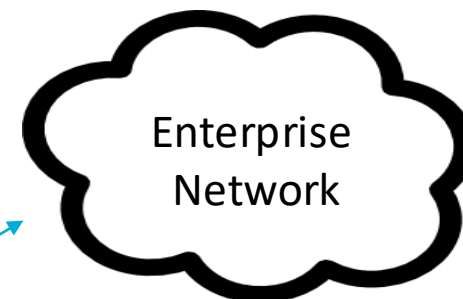
5. User gains access to the Enterprise Network



Wireless Access Point



2. The Access Point passes the EAP request to the Radius Server



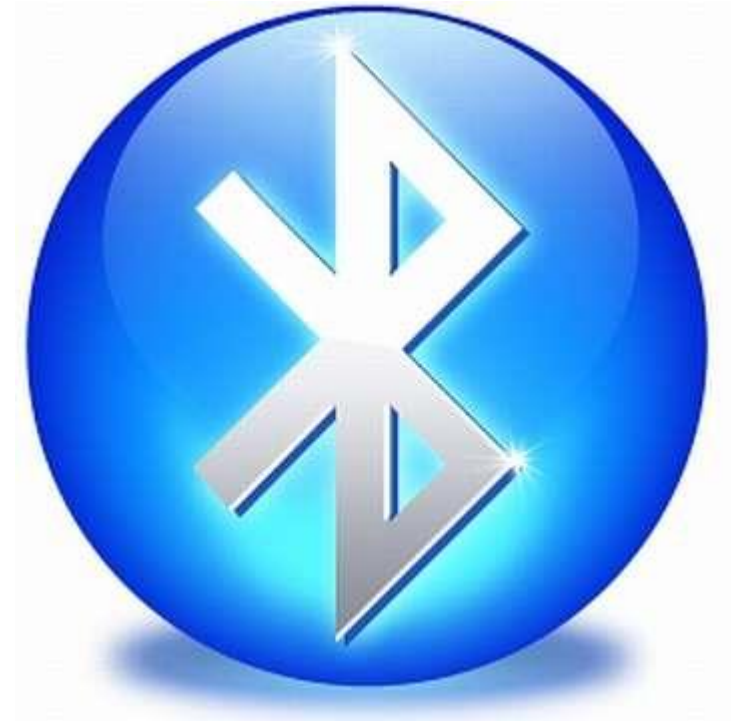
Authentication Server (RADIUS)

3. The Radius Server challenges the end user for a password

4. The Radius Server authenticates the end user and the access point opens a port to accept data

Bluetooth Security Goals

- ❑ Secure pairing of devices in a short range
- ❑ Authentication and confidentiality
 - ❑ Protect against eavesdropping and man-in-the-middle
- ❑ **Secure Simple Pairing Protocol (SSP)**
 - ❑ Unlike GSM and WiFi, Bluetooth creates a secure channel first, then authentication
- ❑ Driven by the Bluetooth SIG (<http://www.bluetooth.com>)



Secure Simple Pairing Protocol



Let's Pair

Public Key Exchange: Elliptic Curve Diffie-Hellman

Authentication: Numeric comparison, Just works*,
Out of Band, Passkey Entry

Verification: Verify that key exchange succeeded

Link key calculation: Derive link key for communications

Secure link established

* Just works only protects against passive man-in-the-middle

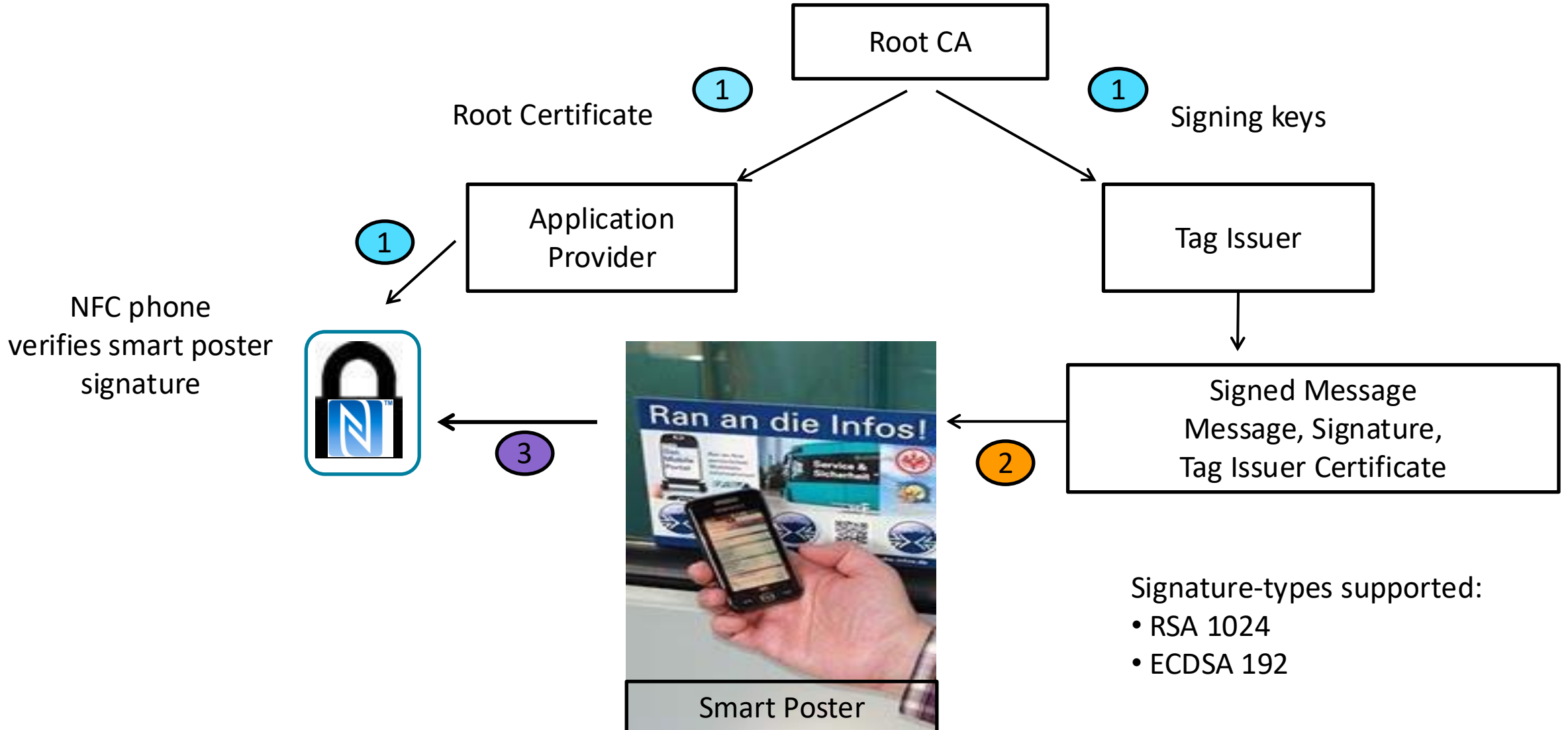
NFC Security Goals

- Near-field communication (NFC) protects authenticity and integrity of messages sent and received using **digital signatures**
 - No explicit goal for confidentiality
 - Hand-off to Bluetooth or WiFi
- Driven by **NFC Forum** (www.nfc-forum.org)



Objects sending/receiving radio signals

NFC Smart Poster



Conclusions: elements of wireless investment strategy

Look for the technological forces that constrain the wireless industry...

- **Radio spectrum** – finite, expensive, scarce in densely populated areas
- **Battery life for mobiles** – more features consume more power
- **User mobility** – uncontrolled users increase uncertainty in the management of wireless systems
- **Greater cyber-attack surface** – due to almost ubiquitous wireless access from PLMN to trusted environments

Look for technologies that ease industry constraints...

- **Research focus** on ubiquitous wireless access and routing
- **Use of mmWave technologies** – force more information through very wide spectrum allocations
- **Information theoretic advances** – push more data over the same spectrum
- **Advanced antenna techniques** – cover more spectrum with less physical space consumption, smart antennas combine signal processing and electromagnetics – smaller mobile devices
- **More intelligent radio systems** – better cope with user mobility and the increasing number of wireless products and users – add more users
- **Security evolution** – quantum-safe security, more advance security architecture

Thank you

