

5G Standards and Security

Hank Kafka

April 12, 2018

ITU's IMT-2020 Use Cases & 3GPP's 5G-NR Vision

Enhanced Mobile Broadband

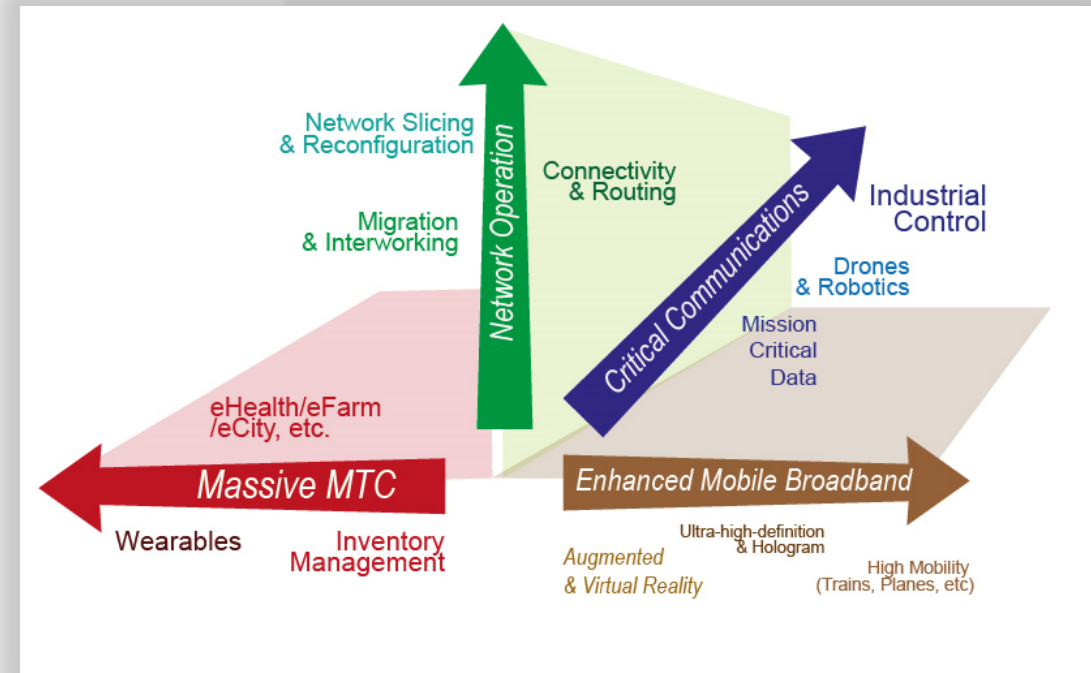
- Ultra high bandwidth
- High spectral efficiency
- Ultra dense network
- Energy efficient

Ultra-reliable and Low Latency Communications

- Ultra low latency
- Low network access and synchronization time
- High reliability

Massive Machine Type Communications

- Ultra high density
- Long battery life
- High system gain and efficiency



Source: 3GPP

One Global Standard

Global Specifications

- Interoperability between networks
- Economies of global scale – significant advantage in device and equipment cost
- Worldwide service wherever operators deploy the technology
- Global roaming
- Device portability
- Case in point is the worldwide adoption of 3GPP-based 4G LTE standard (170 countries)
- Forward compatibility



A GLOBAL INITIATIVE



3GPP Working Procedures



Source: Qualcomm

Work Items

Supported by at least four Members
Rapporteur is named
Worked through contributions and drafting process

Approval Process

Approval by a TSG is normally by consensus

- Where consensus cannot be achieved a vote may be taken
- 71% required to approve

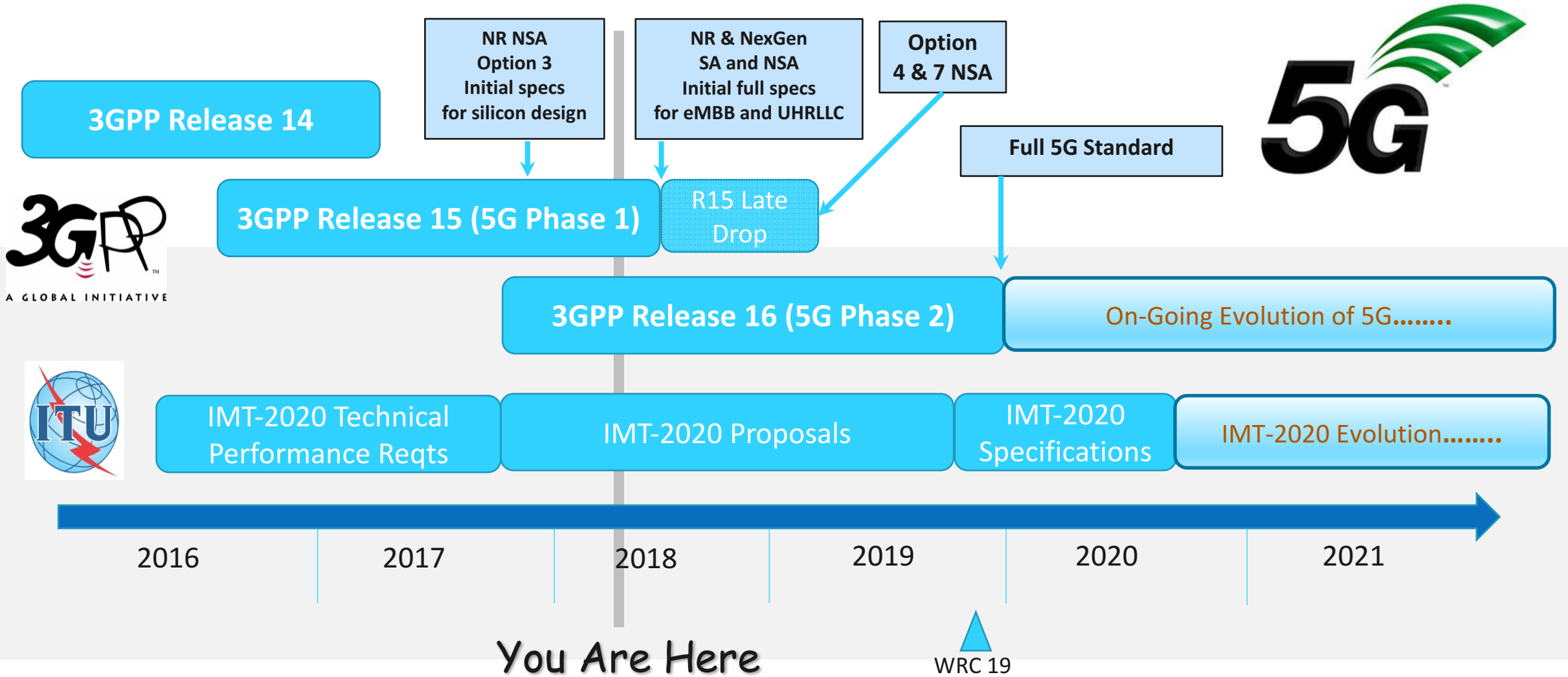
IPR Policy

Individual Members are bound by the IPR Policy of their respective Organizational Partner

Declare essential, or potentially essential, to any work ongoing within 3GPP

Source: 3GPP Working Procedures

Expected Timeline for Industry 5G



Overview of Cellular Security per Generation

1G

Threats: Analog, fraud, eaves dropping

2G

Improvements: Digital, air-link encryption
Threats: Attacks on encryption

3G

Improvements: Mutual mobile/network authentication, open algorithms
Threats: Exploit clear transmission of IMSI, hacking in/out going calls

4G LTE

Improvements: Strong encryption, built-in security mechanisms
Threats: Internet IP-based attacks (DDoS, etc.)

3GPP 5G Security Examples

- **Increased Home Network Control for Authentication**
 - Home network verifies the UE is present and requesting service
- **Unified Authentication Framework**
 - Same authentication for 3GPP and non-3GPP access
- **Introduction of Security Anchor Function (SEAF)**
 - Re-authentication of UE as it moves between access networks
- **Subscriber Identity Privacy**
 - Use of home network key to encrypt subscriber identity (e.g., IMSI)
- **Introduction of Security Edge Protection Proxy at PLMN border**
 - Application layer security for information exchanged between Network Functions in different PLMNs

Drivers for 5G Security

- **New service delivery models**
- **Evolving threat landscape**
- **Increased focus on privacy**
- **New Trust Models**



AT&T