TIA TR-45 and 3GPP2 Security

presented by

Christopher Carroll

Chair, TR-45 Adhoc Authentication Group

Stockholm, Sweden - April 11, 2000

Contact Info

Christopher Carroll

GTE Laboratories Incorporated

+1-781-466-2936

ccarroll@gte.com

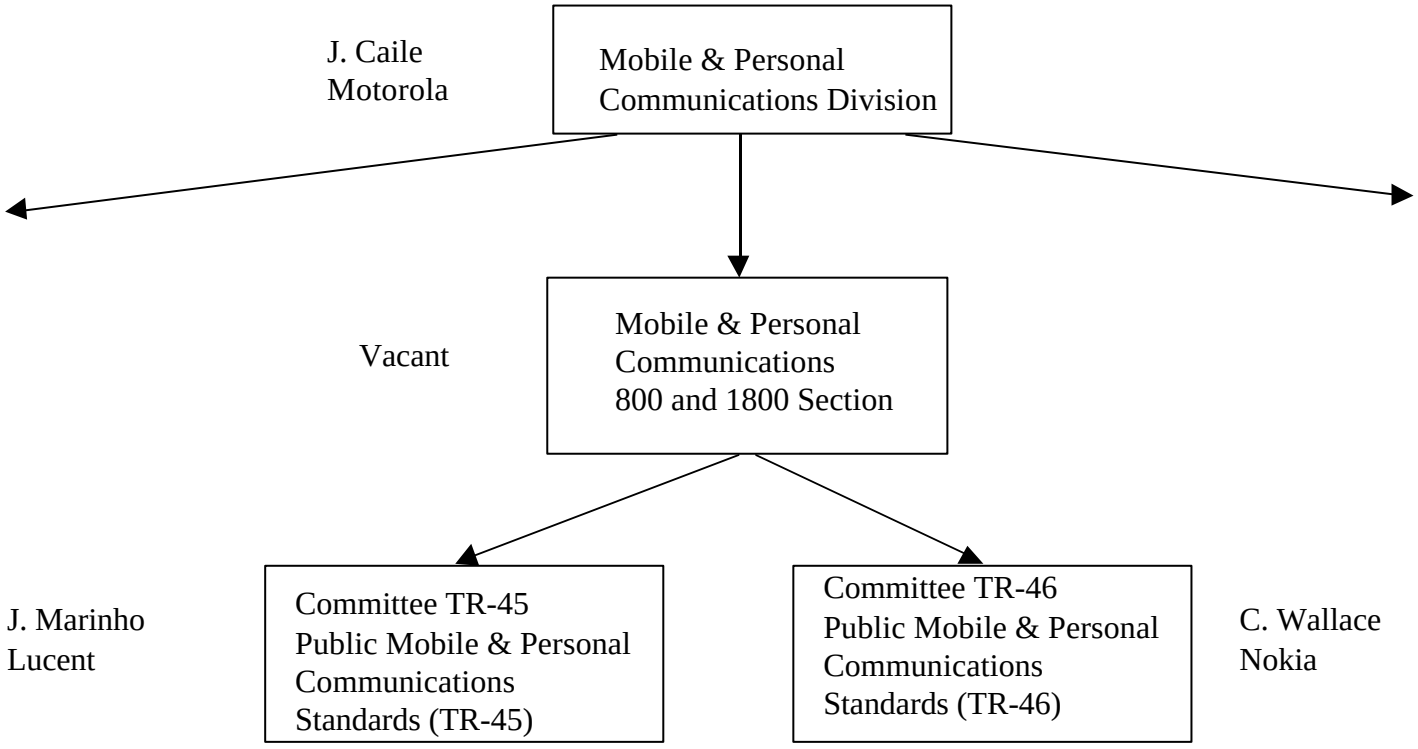
Outline

- **Telecommunications Industry Association**
- **TIA Hierarchy**
- **TR-45 Standards**
- **3GPP2**
- **Engineering Committee TR-45**
- **Adhoc Authentication Group (AHAG)**
- **AHAG Scope and Charter**
- **Next-Generation Security**

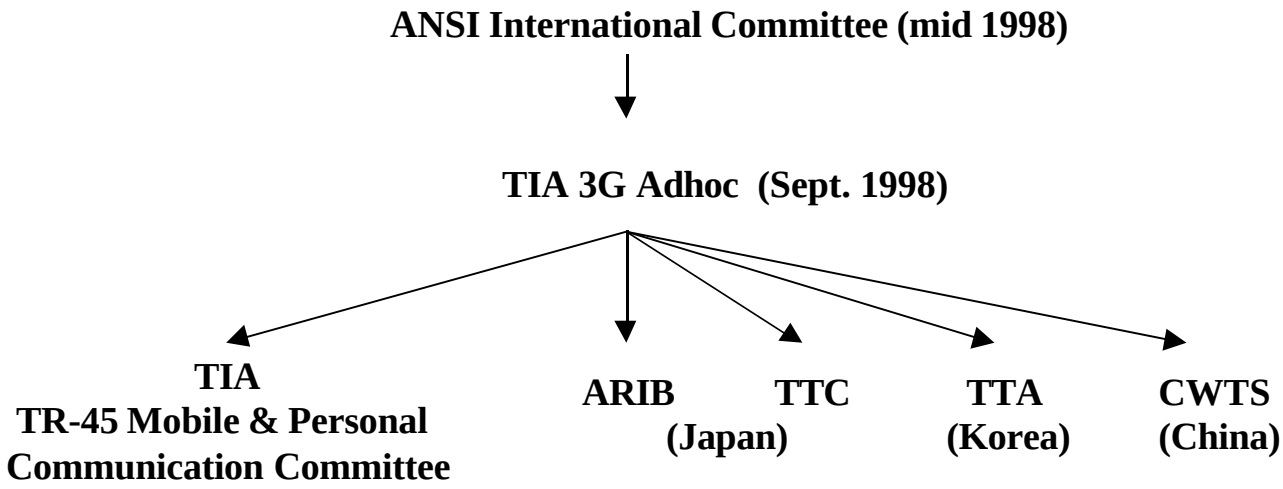
Telecommunications Industry Association

- **ANSI Accredited Standards Setting**
- **Activity since 1920's (EIA)**
- **Telecommunications sector**
  - **Fiber Optics**
  - **Network Equipment**
  - **User Premises**
  - **Satellite**
  - **Mobile & Personal Communications**

Mobile & Personal Communications Division



3GPP2 History



3GPP2 – Steve Dennett

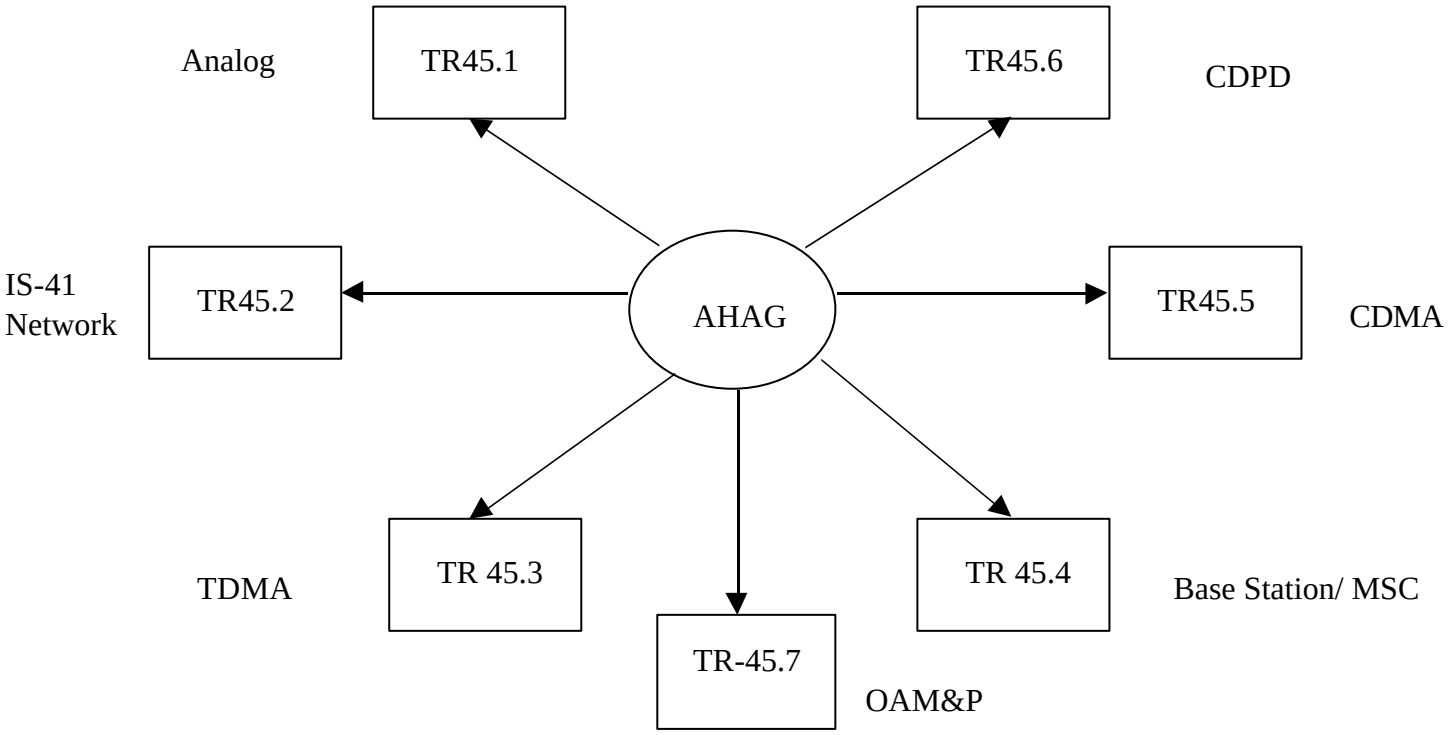
TR-45 Standards

- **Air Interface**
  - **Analog: TIA/EIA-553**
  - **TDMA: TIA/EIA-136**
  - **CDMA: TIA/EIA-95**
  - **Cellular & PCS**
- **Network**
  - **WIN**
  - **ANSI-41**
- **A-Interface (BS-MSC)**
  - **IS-634**
- **Cellular Digital Packet Data (CDPD)**
  - **IS-732**

3GPP2/TR-45

TR-45		3GPP2	
TR-45.1	Analog Air Interface		
TR-45.2		ANSI-41	TSG-N
TR-45.3	3G TDMA Wireless		
TR-45.4		A-Interface	TSG-A
TR-45.5		cdma 2000 Air Interface	TSG-C
TR-45.6		Wireless IP	TSG-P
TR-45.7	Wireless OAM&P		TSG-S
TR-45		Requirement, Workplan	TSG-S

TR-45 AHAG - Full-time security consultation



AHAG Scope & Charter

- **Security consultant to TR-45**
- **Authentication**
- **Encryption**
- **Key management / distribution**
- **Security procedures and algorithms**
- **Export liaison with U.S. government**

TR-45.2 Enhanced Security Focus Group

- ANSI-41/SS7 protocols and procedures
- 3GPP AKA protocol efficiency
- Security impacts
  - Network loading
  - Network delay
- Backwards compatibility
- Operational requirements

Next-Generation Security

- **Enhanced Authentication**
- **Enhanced Privacy**
- **Utilize public crypto community**
- **Public review process**
- **Ensure security evolvability**
- **New key distribution techniques**
- **Explore new security services (public key certificates, ECC, key escrow, smart cards, etc...)**

Goals

- **Incorporate best crypto algorithms and security procedures into standards**
- **Ensure system is evolution capable**
- **Maintain backwards compatibility**

Public Development Process

- **Originally closed crypto development**
- **Vulnerabilities identified in TR-45 encryption**
- **AHAG recognized need for stronger review process**
- **New public crypto policy adopted January 1998**

Five Step Crypto Development Process

1) Develop Security Requirements.

2) Accept contributions on proposed security designs and models.

3) Conduct internal review of security proposals.

4) Conduct external review of security proposals.

5) Select proposal(s) for standardization.