Mission

TC NTECH will:

- Be the ETSI competence centre on network technologies, including interconnection to other networks.
- Provide detailed technical specifications for network solutions fitting the overall architecture defined by EP E2NA.
- Be the ETSI competence centre on ‘Future Networks’ technologies.

Responsibility

Consistent with the mission TC NTECH will

- Provide detailed architecture and protocol (profile) specifications for use in networks addressing the control, data and management planes in both the service and transport layers of these networks, including security.
- Provide protocol profile specifications for service interconnection and network interconnection,
- Identify and monitor relevant work on Future Networks technologies performed outside ETSI and provide guidelines on their applicability to ETSI compliant networks.
Main aims of TC NTECH

- Development of assured security capabilities for future networks
  - Also ensuring that deployed networks remain and improve security and privacy
- Development of the Design for Assurance paradigm
- Deployment of the Design for Assurance paradigm
- Development of methods to support privacy by design
- Deployment of privacy by design in ETSI’s standards for networks
Stakeholders in network Security

- **Society**
  - Networks underpin almost all societal interactions and provide benefit to all of society

- **Industry**
  - Billions of phones, billions of internet connected devices, billions of people able to move and interact through networks

- **Government**
  - Need to manage networks and telecommunications as a societal benefit and ensure it fits to the other government managed societal benefits
  - Need to ensure global cooperation for network availability
CURRENT WORK PROGRAMME

Aims of TC NTECH in the security area
Finalising the NGN

Work carried over from TISPAN’s NGN

- Closure of NGN Security Requirements (*RTS/NTECH-00008-SEC-REQ (TS 187 001) TISPAN NGN Security (SEC); Requirements - Release 3*)
Defining in detail “Design for Assurance”

- How to apply evaluation logic in the design process to define standards able to give high levels of security assurance
- Develop new ETSI report (TR or EG) on the definition and practice of design for assurance
- Update existing DfA document suite to explicitly identify they are DfA documents

Defining what privacy by design means in standardisation

- Building the foundation for systems that have privacy protection in depth irrespective of the specific technology
- Develop new ETSI report (TR or EG) on the definition and practice of privacy by design
Defining security for future networks

Security architecture for future networks

• An abstract architecture that can then be mapped on actual architectures.

• It is unlikely that there will be a single functional architecture for future networks so, such abstract security architecture would certainly be appropriate.

To include support for ...

• Cloud security

• Software defined networks
Ensuring networks can deliver risk managed services

- Where networks support multiple conflicting capabilities
- Where networks have to support law enforcement and regulatory requirement

Further development of core standards taking account of work from ISGs and other TBs and SDOs

- Including ISG ISI, ISG ANF, M2M, ITS ...