

### **Next Generation Networks (NGN)**

Next Generation Networks (NGN), is decoupling of services from networks, description of open interfaces between them.

The to be developed standards are to describe

- creation, deployment and management of all kinds of services.
- Use of all kinds of media (audio, visual, audiovisual), with all kinds of encoding schemes and data services, Conversational, Unicast, Multicast and Broadcast, Messaging, simple data transfer services, Real time and Non-Real time, delay sensitive and delay tolerant services.

Architecture: Global networking requires interoperability between networks. Scenarios are being described for interworking including legacy networks.

NGN compliant architecture will allow also the provisioning of both existing and new services independently of the network and the access type used.

Both, NGN-aware terminals and non-NGN-aware will be supported.

Protocols such as SIP, H.323, MGCP or MEGACO are considered as NGN-based while Q.931 and GSM 04.08 are non-NGN legacy protocols

Quality of Service (QoS): Users and consumers must benefit from an acceptable level of end-to-end QoS, so as guaranteed by legacy services such as telephony.

The set of QoS-parameters will be completed with those necessary for multimedia services.

QoS needs as well a mechanism to control QoS between domains and networks.

Service platforms: Service platforms are a key principle for NGN to separate the networks from the service provision. The open interfaces between both are conceptual interfaces called Application Programming Interfaces (API).

Open Service Access standards with APIs describe the mechanisms to support provision of services across multiple networks covering both service roaming and interconnectivity of services. User control of service customisation and profiles will be supported.

Network management: The emergence of various forms of combined fixed, mobile, IP, access, etc. networks creates increasing complexities and challenges related to the management of such networks. This also applies to the management of existing and new services across different network types.

Basic network management services and interfaces to suit NGN requirements will be described for fault, performance, customer administration, charging/accounting, traffic and routing management.

Lawful Interception (LI): LI is a legal requirement to provide interfaces between the network and the law enforcement agencies. Such LI specifications had been developed for legacy networks (rather closed set of protocols).

NGN will bring a more complex environment of inter networking. As NGN will embrace many different protocols and many new services, and older services delivered in a new form, LI needs to be completed according to the new demand. This will include transparency, accountability, traceability; and uniqueness.

Security: Users/Consumers trust and confidence in ICT is based on security. With the changes in the ICT environment with more network operators and more service providers involved, networks cannot be conceived as monolithic blocs with clear interfaces.

#### Standardization needs for NGN

With this in mind, standardization needs to:

- capture security requirements for compound next generation networks including those security requirements that stem from next generation applications and from next generation services;
- review and evaluate other SDOs security work and figure out how those pieces relate to NGNs;
- build complete integrated security architectures; aim at sound and uniform security within NGNs;
- define security interaction between network/transport security and service level security, consider security APIs and address how security components (e.g., firewalls, smart-cards) are placed within the NGN architecture;
- ascertain that security concepts and security features fit together and interwork;
- describe the required NGN security infrastructure and key-management, and how it is deployed for NGNs;
- issue guidelines for secure operation of NGNs and enable secure NGN management;
- define NGN specific security profiles;
- develop those security parts that are identified missing for NGNs.

ETSI and its partners: Although the NGN-initiative started in ETSI, the objectives can only be achieved in close co-operation with all partner organizations (i.e. CENELEC for the SMH) which share NGN principles.

The protocols supporting NGN-principles are usually ITU-T-specified protocols or specifications which come from the IETF.

The Open Service Access is being worked on in collaboration with PARLEY.

There are also European RTD projects in this field which provide testing platforms and involve the ETSI PLUGTESTS.